The Implications of Emerging Technologies on Civil Military Relations: A Case of Kenya's National Security Since 2010

Odhiambo Barnabas Owuor

095147

A dissertation submitted in partial fulfilment of the requirements for the Degree of Master of Arts in Diplomacy, Intelligence and Security at Strathmore University

School of Humanities and Social Sciences

Strathmore University

Nairobi, Kenya

June, 2025

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Name: Odhiambo Barnabas Owuor

Signature: 

Date: 21st May 2025

Approval

The dissertation of **Owuor Barnabas Odhiambo** was reviewed and approved for by the following:

Dr. James Nyawo,
Lecturer, School of Humanities and Social Sciences
Strathmore University

Dr. Magdalene Dimba,
Dean, School of Humanities and Social Sciences
Strathmore University

Prof. Bernard Shibwabo,
Director of Graduate Studies,
Strathmore University

Abstract

Emerging technologies have disrupted the operations of civil-military relations, which have in turn impacted the national security of states in a rapid technological evolution. Despite efforts to adapt to these developments, there remains a substantial gap in comprehensive understanding how new technologies affect civil-military interactions, particularly in the context of national security. This research investigates the impact of emerging technologies on civil-military relations, with a specific focus on the historical evolution of these relations since 2010. The study had three objectives; first, to analyze the nature of civil-military relations in Kenya, since 2010; second, to investigate the extent to which emerging technologies have impacted these relations since the adoption of the 2010 Constitution; and third, to assess how the effects of emerging technologies on these relations have affected Kenya's national security. Using agency theory and critical theory of technology, this research adopted exploratory research design. The sampling population consisted of military personnel, technology practitioners in national security, and policy experts. Data collection involved both primary and secondary sources within Nairobi area, with primary data gathered through in-depth interviews and structured questionnaires, while secondary data was sourced from reports, academic journals, books, and other relevant publications. Seventeen (17) respondents with five key informants were engaged in this research. Lastly, the research applied thematic analysis to analyze the information and data collected. The study reveals that emerging technologies have introduced both opportunities and tensions, including concerns around transparency, accountability, and militarization of civilian space. Findings indicate that while technology has enabled better and efficient response to threats and national security, it has also blurred the traditional roles between civil and military actors. By examining these issues, this research provides valuable insights into the interplay between emerging technologies and civil-military relations in Kenya, ultimately informing policy recommendations that enhance national security in an increasingly complex technological environment. Ultimately, the study contributes to knowledge by shedding light on pertinent matters mentioned above, while recommending the need to increase research and innovation, ethical regulatory frameworks and collaboration in use of emerging technologies. The study suggests potential areas of further research gaps including a need to study the foreign influence in national digital sovereignty in the advent of emerging technologies and future research including a comparative analysis with another state.

Table of Contents

List of Tables

List of Figures

Definition of Terms

Emerging Technologies: Emerging technology is a term generally used to describe a new technology, but it may also refer to the continuing development of an existing technology. This definition applies to technologies that are creating significant social or economic effects (Mohiddin et al., 2021). From artificial intelligence and machine learning to block-chain and the Internet of Things, autonomous systems and fifth generation (5G) internet, these technologies are reshaping industries, military and socio-economic relations across the globe. They are characterized by their disruptive nature and the transformative impact they can bring (Rotolo et al., 2015).

National Security: Chapter 14, Article 238 (1) of the Constitution of Kenya 2010 defines national security as, "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests" (Kenya Law Reform Commission, 2024). The military can be deployed to deal with any event that manifests itself to the extent of threatening the national security as described by the Kenyan Constitution 2010. In achieving national security, civilian leaders want militaries that are more than just compliant; they want them to be effective in carrying out their tasks as assigned (Pion-Berlin et al., 2024). Essentially, the civilian side expects military expertise, while the military side needs financial resources and some degree of operational independence to forestall any crises or tensions that may be a threat to national security (Gaub, 2016).

Military: The military (sometimes known as the armed forces) is the only state agency with a near-complete monopoly on coercion and is responsible for maintaining a nation's territorial integrity and sovereignty (Pion-Berlin et al., 2024). The military is a professional organization made up of commanders and enlisted soldiers with unique institutional characteristics, culture, and values. It has a direct relationship with, but is distinct from government and society.

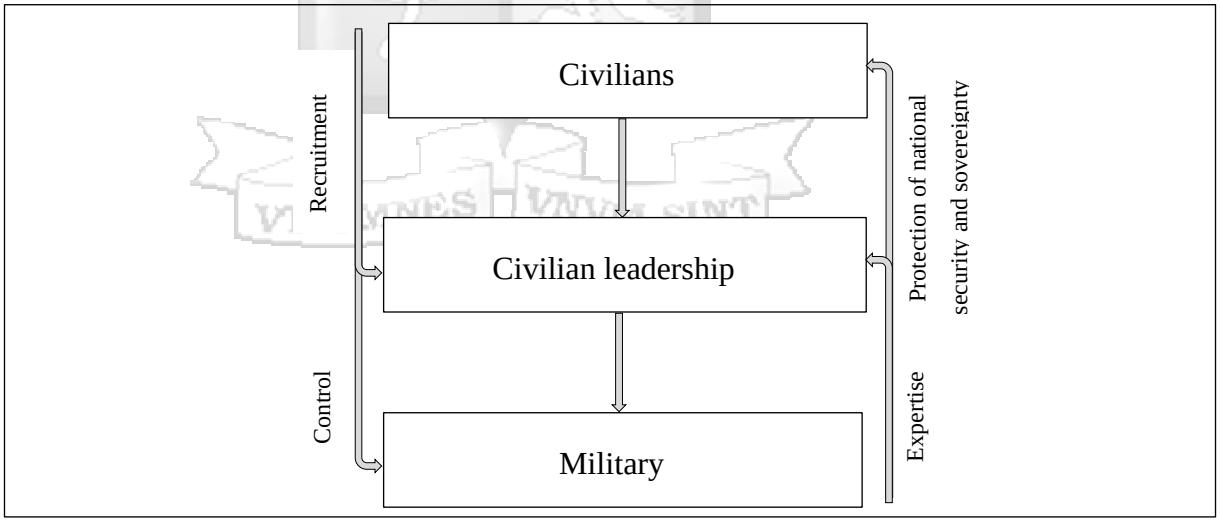
Civilians: Simply put, civilians are persons who are not members of the armed forces. The civilian population comprises of all persons who are civilians (*Customary IHL - IHL Databases - ICRC*, 2024). Civilians are also non-uniformed individuals in government positions, non-uniformed societal elites with organizational affiliations,

whose opinions and votes impact civil-military relations, and who in totality are known as civilian authority or leadership (Pion-Berlin et al., 2024).

Civil-Military Relations: Civil-military relations are a specific, extreme case of democratic theory, in which designated political agents control military agents. Democratic theory is summarized as the people may choose political agents or experts, such as the military, to act on their behalf, but this does not imply that they have given up their political rights (P. D. Feaver, 1999). Civilian leaders are the principals in the relationship, while the military is the agent. Civilians establish the military for their own needs, allocate finances and staff, and provide strategic direction. In practice, the asymmetry of the relationship is complicated by the armed forces' possession of weapons and control over collective violence (Gaub, 2016).

As show in figure 1 below, the relationship between the military, civilian leadership and civilians point to providing security expertise, ensuring control of military activities and general recruitment of the practitioners from the civilian circles with a goal to enhance national security.

Figure 1: Relations Between Civilians and the Military



This study will focus on the emerging technologies, civil-military relations and the national security of Kenya. Thus, military control is about a division of authority between political leaders and officers, which allows the former to create and adjust policies without being hindered by military threats or vetoes (Pion-Berlin et al., 2024).

Acknowledgement

I thank God for good health, clarity of mind and consolation during this study. I extend my appreciation to my supervisor, Dr. James Nyawo, for his invaluable support and guidance throughout the research. Additionally, I owe much gratitude for the support I received from the faculty at Strathmore University who enriched my academic experience and research. I am especially grateful to my loved ones, family and dear friends whose constant encouragement, understanding, and presence provided the emotional strength I needed to complete this journey. Lastly, I would like to express my gratitude to the respondents who participated in this research and provided open and thoughtful contributions to the enrichment of this research.

Chapter One: Introduction

1.1 Background to the Study

This Chapter introduces the background to the research explaining the area of study and its context, the statement of the problem, research questions and research objectives. The first section – the Background – provides a detailed foundation of the dynamics between national security and emerging technologies effect with a global lens. In addition, it provides a look into civil-military relations in the face of emerging technologies. The chapter outlines the research objectives, as well as the research questions, which are formulated to further guide this research. Lastly, the justification and the scope of the study to guide a comprehensive coverage of the objectives.

1.2 National Security around the World

When discussing the concept of security, David Baldwin (1997) raises crucial arguments that aim at expanding the traditional view of security that places the state as the main subject with the military as the only actor who can deal with national security threats. Firstly, the approach to security needs to be broadened to include political, economic and environmental security since policies created to enhance security in one sector may inadvertently affect a different sector. He contends that security is relative, dependent on context, and not absolute, and argues that improving security in one area could compromise it in another (Baldwin, 1997).

After the end of Cold War in the 1990's, number scholarly articles that sought to redefine the concept of national security gained traction. Anton Grizold (1994) in his article argues that, changes in global trends and the rise of new, non-traditional dangers have led to substantial evolution in national security. Grizold (1994) underlines that in today's world, national security must address a wide variety of challenges, including economic, environmental, and international crimes, as well as other developing risks capable of collapsing state security. He believes that the transition away from traditional approaches has made national security a more complicated and diverse concept that necessitates collaboration across several sectors, to security that prioritizes the state and institutions, both domestically and globally (Grizold, 1994).

Barry Buzan (1983), through his approaches that align with the Copenhagen School of thought brings forward similar thoughts on broadening of national security. He contends that national security goes beyond the traditional military strategy to encompass political, economic, sociological, and environmental considerations. Buzan (1983) criticizes the narrow, state-centric concept of security that dominates international relations, while encouraging for a more comprehensive approach that takes into account both individual and state security. This redefining of security reflects the complex interdependence of modern international systems, in which non-military elements play an important role in shaping the security environment (Buzan, 1983).

According to Barry Buzan's (1998) securitization theory, any public issue can be classified as non-politicized where the state does not deal with it as it is not a priority-issue that warrants public debate and policy decision. However, a politicized issue makes it part of public policy, requiring government decision through priority action of allocating resources, among other decisions or securitized (Buzan et al., 1998). This concept feature in this research where technological products which are viewed as commercially viable are as well be perceived as security threats by the government. Similarly, same products can be used by the military to enhance the national security of a state.

Baldwin (1997) hence presents the importance of clarity in understanding what security implies, as it involves several elements. Seeing security as intrinsically relational, he posits that security is determined by what referent object is being considered, what risks are being faced, and how they will be addressed. Baldwin's (1997) approach and Barry Buzan (1998) concept of security align with the Kenyan definition of national security, with its expansive dimensions of the concept's meaning and the threats to it altogether. Chapter 14, Article 238 (1) of the Constitution of Kenya 2010 defines national security as, "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests" (Kenya Law Reform Commission, 2024).

Globally in democratic states, emerging technologies have challenged traditional, narrowly defined ideas of national security. However, there is yet to be a concerted

political discussion about how the concept might grow to meet the difficult challenges of the twenty-first century. For example, the first comprehensive regulation on artificial intelligence (AI), issued by a major authority worldwide was done in 2024 by the European Union (*EU AI Act*, 2023). Jude Blanchette (2020) when analyzing a speech by Xi Jinping, the president of China in 2020 on the national security outlook posits that, China's approach in comparison to the USA government covers that the overall national security outlook of those states seek to combine the broadened aspects of national security. Understanding that economics, culture, technology, governance, and other factors are not only critical inputs but also necessary results in a modernized approach to national security (Blanchette, 2020).

Simon Ramo (1989), argues that military strategies focused at addressing national security issues are now yielding more technology benefits for consumer markets than ever before. At the same time, the line between military and civilian research and development is becoming blurred with the distinction between simply consumer technology and those with military purpose fading (Ramo, 1989). Advanced electronics and robotic technologies have already demonstrated the ability to increase the effectiveness of a defensive army, allowing it to surpass a bigger, offensively focused force using traditional military techniques. Smart robotic weapons can accurately identify and neutralize enemy tanks, aircraft, and infantry. Furthermore, strong electronic warfare capabilities allow a state to disrupt the enemy's communications while protecting its own from interference, demonstrating the critical significance of technology in contemporary military strategy (Ramo, 1989). These critical discourse by Ramo raised in 1989 are realities that states are living in, and a cornerstone to approaching national security of various states.

Barry Buzan (1998), emphasizes that in advanced democracies, defense of the state is becoming one of the many functions of the armed forces unlike before where it was the de facto role. Their militaries may be trained to support emerging world challenges like peacekeeping or humanitarian intervention, which are not considered existential threats to their states or emergency actions that require suspension of normal rules (Buzan et al., 1998).

States have resorted to various approaches to ensure their national security is achieved or maintained. They formulate strategies that align and correspond to the emerging

threats to national security including emerging technologies. States have reverted to formation of alliances, investments in modern technologies, diplomatic approaches, and increasing their capabilities in fields like intelligence gathering and economic engagements to ensure success in their national security strategies. For example, the U.S. National Security Strategy (NSS) released in October 2022 by President Biden's administration addresses the shifting global security landscape. The approach revolves around the need to strike a balance between competition and cooperation. The United States perceives two major strategic challenges: the rebirth of superpower competition and an array of transnational issues such as climate change, global health, and financial stability. The NSS advocates for forming a strong coalition of democracies to shape international laws and deal with other common issues (House, 2022).

Kenya has also implemented a range of ways to combat national security challenges. During the Uhuru Kenyatta administration (between 2013 and 2022), the government strengthened its multi-agency framework for better coordination and collaboration among security agencies. Furthermore, technological improvements played an important role, with enhanced surveillance on digital platforms to tackle cyber threats and terrorism. Disarmament programs were also carried out to curb the spread of illegal firearms, and Kenya participated in both bilateral and international security cooperation (Parliament of Kenya, 2020). Furthermore, the administration placed a high priority on citizen participation in national security activities. These approaches are efforts by Kenya to adapt to changing security environment, especially in the face of modern threats like terrorism, cybercrime, and cross border conflicts.

These events in Kenya have shown how technology may both facilitate enhanced security cooperation, while creating new spheres of vulnerabilities. The Kenya's National Cybersecurity Strategy 2014, that was revised in 2022, places a strong emphasis on cyber resilience, threat intelligence sharing, and multi-stakeholder cooperation as part of a plan to combat new cyberthreats (*National Cybersecurity Strategy 2022 – 2027 | NC4*, 2022). The Strategy describes a multiagency approach for the detection, prohibition, prevention, response, investigation, and prosecution of cybercrime. It follows the Computer Misuse and Cybercrimes Act (CMCA) of 2018 (*The Computer Misuse and Cybercrimes Act 2018 | NC4*, 2024) that stablished governance structures, robust policies, and regulatory frameworks. One significant

milestone is the creation of Nairobi's Integrated Command and Control Centre (IC3), which has improved real-time surveillance, traffic control, and coordinated emergency response (*National Police Service Annual Report 2022*.). However, technological improvements bring additional threats, such as surveillance overreach, data privacy issues, and a blurring of the lines between military, intelligence, and civilian functions. As such, Kenya offers a compelling case study to investigate how emerging technologies intersect with national security and civil-military relations.

In dealing with both traditional and emerging threats to the state, the military can be deployed to deal with any event that manifests itself as a national security issue. In achieving national security, civilian leaders want militaries that are more than just compliant; they want them to be effective in carrying out their tasks as assigned (Pion-Berlin et al., 2024). Essentially, the civilian sector expects input from military experts, while the military institutions need financial resources from civilian allocation and some degree of operational independence to forestall any crises or tensions that may be a threat to national security (Gaub, 2016). Bridging collaboration between the civilian operators and military sector is highly important for states to secure their national security in times when emerging technologies are blurring the gap between the two actors.

1.3 Emerging Technologies as Enablers to National Security

Emerging technology is a term used to describe a new technology, and also refer to the continuing development of an existing technology in the market or military use. This definition is applies to technologies that are creating, or may create, significant social, legal and economic effects (Rotolo et al., 2015). From artificial intelligence and machine learning to block-chain and the Internet of Things, autonomous systems and fifth generation (5G) internet, these technologies are reshaping industries, military and socio-economic relations across the globe. They are characterized by their disruptive nature and the transformative impact they can bring

The vast amounts of data presently available have created new opportunities to monitor and analyze publicly available information such as web search queries, social media posts, internet traffic, and financial markets. These capabilities are open to both civilian and government institutions in conducting their daily activities. This

information can be used to forecast and anticipate a variety of national security concerns, including political upheaval, resource scarcity, and economic downturns (Mordini, 2014). The incorporation of these technologies into national security frameworks indicates the growing interaction between technology, military intelligence, and civilian control.

Technology has a broad impact on national security, affecting everything from economic competitiveness to the future of democracy, as well as the military and national security intelligence operations. Specifically, the complex intersection between economic and security concerns brought about by new technology has also brought about challenging trade-offs that national security organs have never planned to make in the structure of their strategies. In addition to military operations being made easier by technological advancements, such as improvements in weaponry or changes in the geopolitical power structure, many of the problems we confront today also pose new risks in and of themselves, such as information operations, cyberattacks, or biological threats with genetic engineering (McCord & Weinberg, 2020). Technology has enabled improvement in societal relations by empowering democratic participation in issues like national security maintenance.

Technology has been playing different roles within the public and the security apparatus sphere. Different scenarios have shown these roles. In disaster management, technology may play a role in early detection and resource for response equipment. However, as put by Alexander (2014) in reference to the 2012 earthquake in Italy, social media played a crucial role that was likened to the loud chorus in the ancient Greek theatres. Social media interactions commented and provided a collective voice about the earthquake, hence bringing together the country in times of disasters that threaten its survival (Alexander, 2014). Alexander points out that trust, and representation in communication, are essential to crisis and disaster management that touch both the military and civilian population.

1.3 Emerging Technologies as Threats to National Security

As Dorothy Denning (2015) posits, technology has opened the military operational domain to a further possibility, different from the existing traditional domains of sea, land, air and space (Denning, 2015). This new addition did not only bring prosperity

in terms of the existing opportunities, but it brought with it threats that affect not only the civil sector, but the military sphere as well. These new threats and security exposure that result from advances in the civil and military technologies challenge traditional notions of security. Consequently, boundaries between the military and the civilians especially in instances where the technology is rendered for dual use is blurred.

Loren Thompson (2020) in his analysis of the United States of America national security in the face of increased technological advancements and the need for increased robust innovation observes how emerging technologies have changed how national security is viewed (Thompson, 2020). For example, long range weapons like continental ballistic missiles have significantly reduced the essence of distance with guarantees to attacks i.e. from the Eurasian and North America's Land separated by huge oceans. This same argument is strengthened by the observation that technological innovations are spearheaded by many states across the world, unlike before when technological innovations were largely headed by the United States. The capabilities reached by different states have widened threats to national security as attribution of potential attacks have increased immensely.

When making a congressional testimony, Gregory Allen (2023) observed that technological capabilities have become less expensive and complicated, radically changing the face of national security. Activities that previously required the resources and skill of huge governments or military groups are now available to private enterprises and even individuals (Allen, 2023). This democratization of technology has numerous benefits, including increased innovation and efficiency in private and government operations, but it also poses enormous challenges to national security. Previously, the high cost and complexity served as deterrents to harmful activities, but these barriers to access of technological capabilities are disappearing. For example, the widespread availability of commercial drones has allowed non-state entities such as terrorist organizations and rebel groups to carry out military activities that were previously limited to well-funded military forces (Allen, 2023).

This transformation has had a significant impact on the battlefield. During the 2016 Battle of Mosul for example, the Islamic State which is a terrorist group in Iraq, launched over 300 drone missions in a single month, with around 100 of them used to

transport explosives. Similarly, in Ukraine-Russian war that started in February 2022, low-cost commercial drones are used to dump grenades on Russian tanks and vise versa, demonstrating how inexpensive technology (around USD 1600 Dollars in total) may eventually eliminate high-value military weapons valued at millions (Allen, 2023). Russian forces on the other hand, have also used kamikaze drones with autonomous navigation capabilities to wage attacks. These instances demonstrate how technological improvements, while increasing access, have blurred the distinctions between civilian and military applications, providing substantial issues for countries like the United States, which must adapt to rising threats to national security from dual-use technologies.

The recent Covid-19 pandemic was not only a national but a global security threat. In that it required modern technological and medical approaches to ensure its eradication. A publication by Institute of Electrical and Electronics Engineers (IEEE) on the attached technological threats puts the following scenario: a patient may regard a technology that indicates if they are infected by Covid-19 as harmless. However, that same patient may be wary of a human who has the capacity to override the technology system to alter the patient's status to "infectious/quarantined" and thus prevent them from doing certain activities like exercising their civil rights. Technological systems can both erroneously or intentionally prevent people from accessing specific services, as well as lock them into undesirable conditions (Bonaci et al., 2022). With the ability of emerging technologies to be malleable to specific user demands, attacks are imminent in ways that can misinform, and hence corrupt the national security approaches of states.

The digital era has defined cyber warfare as the strategic use of cyber-attacks to threaten and attack another country's national security (Slonopas, 2024). States, as well as non-state actors such as terrorist organizations and private businesses, generally initiate cyber assaults against other countries in order to destroy key infrastructure, steal sensitive information, or achieve political and military objectives. The rise of cyber warfare has resulted in a variety of attacks, including espionage, sabotage, and denial-of-service strikes (Gervais, 2021).

Cyber warfare poses a substantial threat to national security by targeting critical infrastructure such as electrical grids, banking systems, and communication networks.

Espionage allows opponents to steal vital government or corporate data, whereas sabotage directly targets physical systems such as power grids and other national essential infrastructures. Denial-of service attacks can take down online platforms and impair critical government and commercial services. The economic ramifications of cyber warfare are particularly severe, as attacks on financial markets can result in large losses and security disruption. These various forms of cyber warfare demonstrate the wide range of damage that both state and non-state actors can cause in the digital era (Slonopas, 2024).

While the above description of emerging technologies is central in relation to national security and civil military relations, they are by no means exhaustive. Additional technologies and dynamics will be explored later this study to provide a more comprehensive analysis. Different technologies have different effects to national security and civil-military relations, whereas different governments have initiated specific response mechanisms depending on the laws of the day and perception of national security.

1.4 Emerging Technologies and Civil-Military Relations

Emerging technologies are transforming the landscape of civil-military relations and national security. According to theories of participatory democracy, citizen participation can support democratic governance. This strategy opines that civic engagement outside of the scheduled elections can help address significant issues with democratic governance. States that already have an established institutionalized practice of citizen participation can adopt and implement digital participatory tools to enhance democratic practice (Hovik & Giannoumis, 2022). In extension, the practice of accountability, evidence and information gathering, decision making processes which need civilian input and that would need civilian at the center of consideration in military operations, have involved the use of emerging technologies. Militaries can use these technologies to identify potential hotspots of conflict before they escalate, as witnessed with social media surveillance during the Arab Spring upheavals (Blas, 2018).

Emerging technologies in the hardware aspects like smartphones are readily available to populations worldwide with their related or corresponding services which affect or help both the civil-military sectors (Thompson, 2020). The same gadgets, like memory

and processor chips are easily applicable for use in military weapons and communication installations.

Machine learning for commercial products and algorithms are used to guide unmanned aerial vehicles and autonomous systems. In equal applicability, internet of things used for home appliances and normal business operations in civil sectors can be used to link military weapons and capabilities in times of war and just normal logistical operations.

Nearly all technology has applications in both the military and the civilian worlds, in the dual-use principle. The dual use nature of technology matters because it creates a dilemma for cooperation civil-military relations and globally. A good example is the space exploration, where countries are vying for military platforms particularly anti-satellite weapons. States are reluctant or facing a dilemma in instituting international agreements to govern them as it could limit their reach in competition over dangerous weapons. At the same time, the value of such explorations to the civilian sector cannot be dismissed hence the commercial sector is also racing to field orbital systems for peaceful purposes (Vaynman & Volpe, 2023). States have controlled a wide range of military technologies with civilian counterparts through the use of international institutions.

Some technological innovations are commercially led, through government partnerships or sanctions, giving much emphasis on the role played by the civilian sectors in enhancing technological innovations that impact national security. For example, the Chief Digital and Artificial Intelligence Office (CDAO) was founded by the US Department of Defense (DoD) in January 2022 with the goal of increasing their capacity for innovation by closely integrating advancements in data analytics, artificial intelligence (AI), and other digital technologies throughout the DoD. The ultimate purpose of the CDAO was to create value-added approaches by mainstreaming the innovative industry experience of large corporate technology operators into the Department of Defense operations (Csernatoni & Martins, 2024).

1.5 Statement of the Problem

Utilizing emerging technologies, such as artificial intelligence, autonomous systems, global positioning system, big data analytics, social media among others, complicates civil-military relations by creating new opportunities and challenges in maintaining

national security of states. Emerging technologies have disrupted civil-military relations, altering the decision-making processes, accountability mechanisms and national security operations as described above. States have made efforts to adapt and take the lead in adopting and regulating these developments (Csernatoni & Martins, 2024).

Various challenges arise between civil and military institutions as they navigate the new environment created by the emerging technological capacities availed to them. They include balancing decision making and technological autonomy, accountability and oversight mechanisms, and restriction for access on civilian use among others. These technologies continue to affect civil-military relations in the increasingly complex world, with significant implications for democratic governance, especially in contexts where civil-military relations have historically been complex. Similarly, emerging technologies have introduced additional layers of threats to national security.

Patterns of civil-military relations in the world and across Africa are characterized by tensions between military institutions and civilians. In Kenya, civil-military relations have experienced continuous evolution since independence, marked by periods of tension and contestation. The 2010 Constitution, which is deemed progressive, introduced reforms aimed at strengthening democratic governance, and civilian oversight. However, Kenya is still grappling with challenges of balancing military autonomy, transparency, civilian oversight and control, which has been compounded by the integration of emerging technologies into national security functions.

Despite the increasing utilization of emerging technologies, there remains a gap in understanding how their adoption has affected the military operations, oversight mechanisms, and the nature of civil-military engagement in Kenya. While global scholarship has acknowledged the disruptive potential of technology in security governance, empirical evidence specific to Kenya is limited. This research address this gap by examining the impact of emerging technologies on civil-military relations in Kenya since the 2010 Constitution. It focuses on the historical trajectory of these relations, adoption of emerging technologies, and the resulting implications for Kenya's national security.

The study is guided by the following questions: 1. What is the history of civil-military relations in Kenya, since 2010 Constitution? 2. How has emerging technologies influenced civil-military relations in Kenya since 2010? and 3. What are the national security implications to Kenya because of evolving civil-military relations due to emerging technologies?

1.6 Research Objectives

General Objective

The primary objective of this research was to examine the impact of emerging technologies on civil-military relations and their influence on national security.

The specific objectives were:

1. To analyze the nature of civil-military relations in Kenya, since 2010.
2. To investigate the extent to which emerging technologies have impacted civil-military relations since the adoption of 2010 constitution.
3. To assess how the effects of emerging technologies on civil-military relations has affected Kenya's national security.

1.7 Research Questions

The research was guided by the following questions:

1. What is the nature of civil-military relations in Kenya, since 2010?
2. How have emerging technologies influenced civil-military relations in Kenya since the adoption of 2010 constitution?
3. What are the national security implications to Kenya because of evolving civil-military relations due to emerging technologies?

1.8 Justification of the Study

The rapid development of emerging technologies has created new challenges within civil military relations, particularly in Kenya. Despite efforts to adapt to these

developments, there is still a lack of comprehensive knowledge of how new technologies affect civil-military interactions in the context of national security, given the complicated issues they can cause. Even after the referendum that introduced the 2010 Constitution which was progressive in the democratic system, the problems of reconciling military authority with civilian control remain, highlighting the necessity for more investigation into these concerns. This research is critical for understanding the historical evolution of civil-military interactions in Kenya with the additional influence of technological developments since 2010. Examining these connections gives useful insights for policy makers, military commanders, and researchers. This research may create an understanding on how best to integrate technology within civil-military frameworks to safeguard national security.

1.9 Scope of the Study

This study conducted an in-depth analysis of how emerging technologies are affecting the civil-military relations in Kenya, and the wider implications for national security. The research also assessed the historical development of civil-military relations in Kenya, after the new Constitution of Kenya 2010. Additionally, the study analyzed the general development and adoption of key technologies since 2010, and their impact on civil-military relations and national security.

The study reviewed the development and deployment of important disruptive technologies since 2010, including social media, 5G, artificial intelligence, autonomous systems, algorithms and global positioning system, to determine their influence on both civilian and military sectors. The research focused on how these technologies affect decision making, communication and organizational changes among other impacts emerging technologies have brought to civil-military relations and national security.

Using the parameters of national security specified by the 2010 Constitution as a benchmark, which reads according to Chapter 14, Article 238 (1) of the Constitution of Kenya 2010 "defines national security as the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests," this research conducted thorough examination of how these technologies are redefining

civil-military dynamics and influencing national security in Kenya. By focusing on these areas, the study answers important concerns regarding the impact of emerging technologies on civil-military relations and national security in Kenya.

Chapter Two: Literature Review

2.1 Introduction

This chapter reviews existing literature on the topic of the study. The review focuses on two major aspects the history of civil-military relations in Kenya since independence to the period after 2010. It will highlight major events that showed interaction in the aspect of civil-military relations. Secondly, this chapter analyzes the impact of emerging technologies on the civil-military relations of Kenya with examples. Lastly, this chapter ropes in the national security implication to highlight the impact to national security by the interaction between civilians and the military in the face of emerging technologies.

2.2 The History of Civil-Military Relations in Kenya

In his book, *The Soldier and the State*, Samuel Huntington (1957) (the pioneer academic on civil-military in a modern democratic society) explores different issues in military policies that spark debates across multiple dimensions of military management, both within the military ranks and civilian oversight. These issues include a wide range of subjects. For example, within the quantitative spectrum, disputes center on the size of the military personnel, the hiring procedures, and the percentage of national resources budgeted for military purposes. On the qualitative spectrum, discussions about the composition and organization of the military, the types and numbers of weaponry, the alliance structures, and important strategic locations fall under the qualitative spectrum. Lastly, there are debates around distinct operational and strategic domains, which influence the dynamic features of military operations and the direct use of military forces in diverse contexts (Huntington, 1957).

Military policy is crucial for a state to balance. It must consider its national security (which mainly involves the military security and national interests), with the least amount of sacrifice to the social values of a state and its community. To achieve the entire objective, a delicate and a complex balance of power and attitudes of civilians and military groups must be established (Huntington, 1957). For states that establish a strong pattern of civil-military, relations have a great advantage in search and establishment of security. The opposite includes squander of resources and uncalculated risks for states that fail to establish balanced civil-military relations. This

is because, as Feaver (1999) argues, the very institution created to protect the people and sovereignty of the state is given sufficient power to become a threat to the people and the state itself (Feaver, 1999)

In line with the democratic theory, it is encapsulated in the principle that those who are governed should also govern. While individuals can elect political representatives to act on their behalf, this delegation of authority does not mean they have given up their political rights. Much of democratic theory focuses on developing methods to ensure that the people maintain power even as government professionals handle day-to-day operations. Civil-military interactions are a unique and intense application of democratic ideology, in which designated political agents supervise and control designated military agents (Feaver, 1999)

The Second World War (1939–1945) broke out simultaneously putting Kenya into the international system, and being an ally of Britain, became a crucial British military base for successful operations against Italy in Ethiopia and the Somali region. After the conflict, the Kenya African Rifles (KAR) soldiers returned and joined the independence movement that had been sparked by several factions, including the Mau Mau. Africans who rose to leadership positions after their countries gained independence are credited with perfecting the politicization of the military, militarization of politics, which was a practice mostly inherited from the legacy of colonialism (Odhiambo, 2021). According to Frazer (1995), post-colonial civil military relations were heavily influenced by the means that Great Britain had taken to quell the Mau Mau revolt and other uprisings during the pre-independence talks and Kenyan war (Frazer, 1995).

Kenya is one of the few states in Africa that has never experienced military control. But as Boubacar D'ndiaye (2002) contends in his research published in the early 2000s, there is still uncertainty about growing civilian power and the state's continued desire for long-term stability. Instead of establishing institutionalized coup prevention measures, the majority of states, including Kenya, took action to prevent coups when they historically swept the continent of Africa (N'Diaye, 2002). The was timely research as Kenya was entering a multiparty electoral system that ushered in a long-standing democratic system of elections. This practice came with institutionalized forms of governance that was the basis of this research.

As Decalo (1989) observes while writing about the phenomenon, “at any given time, military administrators rule over more than half of Africa's nations and up to 65% of its population. In several countries, civil rule is but a memory from the past.” (Decalo, 1989). This informed the need by many leaders and heads of state in Africa to formulate modalities that subordinated military to civilian power, and ensure their regime survival. For a long time, the founding head of state in Kenya, President Jomo Kenyatta (Founding President of Kenya) and his predecessor President Daniel Arap Moi conducted civilian control of the military in similar approaches. Most of these approaches were not based on established institutionalism, but a short-term coup prevention measures (N’Diaye, 2002).

Shortly after independence, there emerged transitional challenges from Kenyatta’s administration. There was the prospect of secession from Somalia among other internal and external threats that were crucial to Kenya's survival. For instance, in the North-Eastern Part of Kenya, as commonly referred to as the Northern Frontier District the community wanted to reunite with Somalia, Kenya’s neighbor. This led to war known as the Shifta War. Kenyatta's military actions in the Shifta war took three years to protect the region against secession (Meredith, 2013). This was the first instance where the military was used to not only deal with external enemies (Those supporting the Shifta secessionists), but dealing with civilians in Kenya’s territory.

The second challenge came up in January 1964, when African military personnel from Kenya staged a mutiny in protest of their unfulfilled aspirations for independence since the control of the armed forces was still ran by British officers. Kenyatta used the help same British officers to put an end to the rebellion, upgraded the barracks and living quarters, and promoted additional African personnel to important roles. More significantly, the January 1964 military mutiny in Lanet raised attention to the issue of civil-military relations by exposing the divide in Kenya's army and weakness of the leadership in the immediate post-independence period (Odhiambo, 2021)

The coup or mutiny was an important wakeup call to the Kenyatta's government that in order to secure national priorities and national security, there needed to be paramount civilian control of the military with enhanced civil-military relations (N’Diaye, 2002). There emerged several instances where the state started to make efforts in professionalizing some aspects of the military. As Professor Nying’uro

(1999) acknowledges, that as part of advanced military training, majority of the Kenyan military personnel commissioned after independence attended Sand Hurst military academy in Britain (Nyinguro, 1999)

The government of Kenyatta and Moi as indicated with the response to the fist mutiny in 1964 resorted to certain approaches to ensure avoidance of a coup or an uprising among the military. Some included buying off the loyalty of the military or providing largesse like land to individual officers, which encouraged the need to acquire more wealth, usually in illegal and unethical means (Decalo, 1989). Second approach was promotion of officer corps from their respective tribes to sensitive positions in the military. Lastly was the setting up the General Service Units (GSU), a paramilitary to act as a countermeasure to the military excesses especially in the application of violence (Decalo, 1989). The extensive training of the military, assisted by foreign powers especially Britain, was not an indication to professionalize the military, but to ensure the suppression of the Shifta and any other uprising (N'Diaye, 2002).

One notable illustration of the tribal-card strategy is the fact that the Kamba constituted a majority in Kenya's army upon its independence. Kenyatta made it a top priority to address this ethnic disparity when the soldiers mutinied in 1964. Naturally, it was impossible to build an army composed primarily of Kikuyu people in a nation where Kikuyu people made up only 21% of the population and where Kamba, Kalenjin, and other ethnic groups had traditionally chosen to join the military. However, it was undoubtedly possible to heavily infiltrate the officer corps and staff important control units with Kikuyu, particularly in an increasing army when it was evident that recruitment from all groups was also advancing (N'Diaye, 2002).

Additional measures that constituted civilian control through quantitative and strategic measures were brought forth by Kenyatta regime. There was implementation of operational and logistical safeguards to make it more difficult for the military to stage coups. For example, smaller numbers of personnel were admitted to the army. Additionally, different infantry units were dispersed to remote flank locations throughout the nation, away from the city which represented the center of power. This was justified through the five-year development plan of 1970-1974, which argued that it was not regarded necessary to build up vast and unbearably large Armed Forces, which are costly, and a wasteful drain on the country's finite economic resources. The

ideal is the maintenance of a small force that has been properly trained how to use of modern weapons, equipment, and tactics (*National Development Plan for the Period 1970-1974*, 1970).

Furthermore, when it came to promoting leadership, Kenyatta gave preference to Kikuyus over seniority in promotions, and frequent disregard the promotion board in charge of recommending promotions. The administration goals in extending material privileges to military leadership were served by the use of state-controlled enterprises and resources (Decalo, 1989). Rapid army deployments were to be dependent on the air force hence fragmentation of a unitary act in the case of a coup

When President Moi succeeded President Kenyatta in 1978, the bulk of African armies had experienced substantial improvements in the caliber of their workforce after their independence. Officer corps and cadets were from more modern strata and had higher levels of education in various countries; also, urban staff-training institutes had grown even more rigorous in emphasizing the importance of the political order with civilian authority and control taking lead. However, coups and military conspiracies continued to occur in Africa, like the 1982 coup attempt led by military personnel from the air force. The fact that the legitimate center of power of the military, which its members were raised to revere and obey, with a welleducated, highly skilled, and contemporary Kenyan Air Force attempted a coup in 1982 is remarkable (Decalo, 1989).

In the same veil, President Moi followed similar playbook to Kenyatta in instituting civilian control of the military. He used tribal cards, i.e. Promotion of the Kalenjin to the ranks of the military to replace the Kikuyu that had largely been promoted by the regime of President Kenyatta. Land grants were issued to the leadership and extended to mid-level officers especially after the development across the continent where a coup was initiated in Ghana by junior officers in 1981. Some retired commanders were put in charge of key state agencies or parastatals as witnessed with appointment of Arap Sawe to the Kenya Industrial Estates in 1990 (Decalo, 1989).

As N'diaye (2002) argues, Kenyatta and Moi's strategies blatantly demonstrated the military professionalism, independence, and political neutrality were sacrificed in enhancing civilmilitary relations. Professionalism and autonomy are the first to go when promotion boards are disregarded, command assignments are given, and

recruitment decisions are based only on ethnicity. The professional ethics, subject-matter expertise, objectivity, and other values associated with the military are gone. Thus, in military circles, the social tensions in Kenya are manufactured and politicized, exacerbating the grave decline in military professionalism. The coup of 1982 demonstrated the breakdown of civil-military relations and erosion of objective civilian control of the military (N'Diaye, 2002).

Boubacar notes that the absence of coups in a civilian controlled state should not be an indication that successful strategies were put forth by the existing regimes to manage civil military relations. He points out that the Kenyan strategies were an indication of this notion since they increased the probability of a coup in the long run. The first coup of 1964 was mainly triggered by the post-independence policies of the Kenyatta Government. Even with the indication that the coup was not against the whole government, the entire military establishment drew a sharp and keen interest from the civilian government with focus to control their power (N'Diaye, 2002).

There were a total of four attempted coups or conspiracies on record in the era of President Kenyatta and Moi. The attempted coups took place in 1964, 1971, 1978 and 1982. All these were a manifestation of serious limitations and weaknesses by the government institutionalizing civilian control of the military. With 1982 being the most hardened challenge to the ultimate civilian authority, and control of the military. There was a close link with the consequences of the Moi regime's failing legitimacy as they could not attend to the needs of the general populous and those of the wider military as there was increased dominance by one ethnic group (Maren, 1987)

Cynthia Enloe surmises that it is not only a question of an ethnically biased military makeup; it also has to do with how the public views the military as a result. The idea that a military can be recruited from one or two ethnic communities instead of a representation of the national population undermines the legitimacy of the government, since the military is the institution most intimately associated with the state as a symbol of the nation-state. Despite the widespread theoretical argument that technology-driven professionalism and primal bonds are mutually exclusive, they coexist peacefully in many situations. This argument captures the very core of Huntington's (1957) objective control of the military that ensures proper civilian control, stronger democratic institutions and limited politicization of the military. With

tensions that have been created, which undermines the legitimacy of the state may in the end lead to national security implications, both in the short and long term.

On December 27, 2002, Kenyans voted to elect Mwai Kibaki as the country's third president, marking Kenya's first electoral change of administration since independence. The election marked the end of Daniel Arap Moi's twenty four-year rule. The 2002 event marked the dawn of a new century with a beginning of continuous electoral processes in Kenya, a practiced that has been witnessed for twenty years now (Barkan, 2004). The elections marked the process by which a democratic system are formed with checks and balances that would hence work better and enhance civil-military relations.

The election of Kibaki was met by an increased push by the United States of America (USA) for states to adopt the global war on terror. This was after the bombing that happened in the USA on 9/11 and an earlier attack to the USA Embassy in Nairobi in 1998 by terrorists. Over the years up to 2013 when the new Constitution 2010 was coming into effect, Kenya had deployed military to deal with internal matters like terror activities in Lamu or Cattle rustling in the rift valley region.

Kenya has experienced an increased terror activity within its borders, ranging from grenade attacks to massive assaults including the Westgate attack (September 2013), Dusit D2 (January 2019) and Garissa University (April 2015) attack that contributed to massive loss of life. Between 2011 and 2012, the country experienced more than 70 similar incidents (Gitau, 2016).

In response to Al Shabaab's intensifying terror assaults, the Kenyan government deployed the Kenya Defense Forces (KDF) to Somalia with the goal of stabilizing the neighboring country and mitigating future threats to national security. Despite the military deployment to Somalia, Kenya still faced increased terror attacks, resulting in severe loss of life and widespread destruction of livelihood. The continuous violence caused popular outrage, with increasing calls for the KDF to withdraw from Somalia—a civil response that had a direct impact on military operations (Shahow, 2022). Additionally, there emerged instances where the military activities were conducted at the home soil to intervene in hotspots and protect critical infrastructure. This approach

has led to unprecedented debate and interaction between the military and the civilian on the consequences and costs of foreign military deployments (Gitau, 2016).

The largest terrorist attacks in the coast province were organized in Lamu County which hosts Boni Forest, an ideal hideout and training base for fresh Al Shabaab recruits. Some major attacks have taken place in Mpeketoni, resulting in the deaths of many Kenyans. This development prompted Kenyan government to launch a multi-agency operation, codenamed 'Operation Linda Boni' in 2015 with the goal of freeing Lamu County from Al-Shabaab (Muthee & Mulu, 2022). The Kenyan military was at the center of this operation, leading to increased civil-military interaction at the ground or basic level.

In 2008, the Kenyan military launched an operation against the Sabaot Land Defence Force (SLDF), a group known for committing serious human rights violations in the Mount Elgon region. The SLDF had exacerbated conflict over property ownership and rival claims to land titles in the region (OMCT, 2008). However, the deaths, injuries, and displacement caused by the military involvement exacerbated tensions, adding a new layer of complexity to Kenya's civil-military relations. From the start of the joint army-police operation in March 2008, the conflict in Mt. Elgon evolved to the status of an intrastate armed conflict under international humanitarian law. As Human Rights Watch reported, the degree of human rights crimes committed by Kenyan security forces throughout their operations against the SLDF was concerning (Human Rights Watch, 2008).

The Kenyan Constitution of 2010 establishes accountability and supervision measures for the security sector in its fourteenth chapter on national security, as well as appropriate subsidiary legislation. In theory, civilian oversight of the National Police Service (NPS), Kenya Defense Forces (KDF), and National Intelligence Service (NIS) is anchored in the Constitution of Kenya 2010 that gives mandate to the National Assembly, the Executive and in some cases, formation of oversight authorities and commissions. With specific regard to the KDF, the Constitution, The National Assembly strictly regulates civil-military interactions (Gitau, 2016).

Since the inauguration of Uhuru Kenyatta’s government - (2013-2022), the 2010 Constitution has been the bedrock of reference on civil-military issues,

2.3 Impact of Emerging Technologies to Civil-Military Relations Since the Adoption of the 2010 Constitution.

The skills and capabilities of a military officer and the responsibilities accorded to them by the state distinguish them from other societal social roles. The ultimate test of a military officer's professional capabilities is the application of their technical role in the human context. The behavior and conduct of the military hence be guided by a complex number of laws, regulations, customs and traditions approved by the society through a political agent of the state (Huntington, 1957).

With the rising challenges to the national security of states, the role of the military in maintaining national security is also challenged and evolving. The military (sometimes known as the armed forces) is the only state agency with a near-complete monopoly on coercion and is responsible for maintaining a nation's territorial integrity and sovereignty (Pion-Berlin et al., 2024). The military is a professional organization made up of commanders and enlisted soldiers with unique institutional characteristics, culture, and values.

In a huge part of the 20th century, the defense sector took the lead in technological innovation, with technology developed in military defense labs eventually trickled into the civilian sectors. Moreover, World Wars I and II propelled innovation pushing states to invest in large research and development initiatives to obtain technological superiority in the conduct of war. However, this development reduced in the 1990s due to a dramatic decrease in defense budgets, most of it fueled by reduction in interstate conflicts and the diversion of funds to commercial sectors, the flow and uptake of innovation-reversed direction. Kenya, which has been dependent on weapons imports historically, established and opened a small arms manufacturing operation under the Kenya Ordnance Factories Corporation (KOFC) (Military Africa, 2020). The firm, which sources 60% of its inputs domestically, intends to increase its security self-reliance by focusing on domestic equipment and technology manufacturing (Huaxia, 2021).

In an increasingly multi-polar world, a fierce global competition is emerging between NATO, China, and Russia among other global military and security players. The

theatre of competition touch on matters data, artificial intelligence, autonomous decision systems (ADS), and autonomous weapons systems (AWS) among other technological inventions (Linney & Xiaomin, 2024). Lionel Beehner (2021) raises several areas that emerging technologies have on the civilian military technology. Firstly, the impact is felt on organizational implications due to technological change and innovation for military institutions and civilian actors (Beehner & Maurer, 2021). The government of Kenya through the National Defense University of Kenya held 3rd Multi-Sectoral Conference on Science, Technology and Innovation (MS-COSTI 3) to chart an innovation and technology driven agenda on national security (National Defense University - Kenya, 2024). Second is the various opportunities and challenges emerging technologies pose for civilian efforts in oversight of the military. Thirdly, the introduction of technology in policy making at a strategic level may bring tensions in strategic assessment where military advice is expected, while technological data is available. Lastly the evolving character of the profession of arms and the diminution or limitation of the military's exclusive domain of expertise in the use of technology and weapons relative to civilian actors who are gaining more foothold in the same (Reuven, 2023). These areas were covered in the National AI Strategy of Kenya that discussed among other issues, ethical development, human rights and national security goals (Gichohi, 2024)

The weaponing and use of emerging technologies in military fields raises challenging legal issues with respect to the law of armed conflict. The development of law is generally reactive; facts and circumstances typically drive the desire for legal rules (Alcala & Jensen, 2019). These legal issues are sometimes created to prevent excessive civilian involvement in matters security in instances where the use of technology in advisory processes can affect the provision of military advice and blur the lines. As a reactionary measure, the Kenya Civil Aviation passed the Unmanned Aircraft System legislation in March 2020, long after drones were introduced in the civil-military world, to ensure maximum regulation of the field (Kenya Civil Aviation Authority, 2020).

As military and intelligence technological systems are being transferred to the civilian spheres, the implications on civilian privacy and the ultimate balance between national security and civilian rights are substantial. In the same breadth, vice versa would have

destabilizing effects within the military culture and organization. The theatre of wars in the recent pasts have outgrown geographical boundaries due to the efficient way of technology. Cyberwarfare and unmanned vehicles or drones are directed from a different continent to cause harm, not only to combatants but sometimes to civilians. These are raising concerns about the ability of existing and developing laws to cover such theatres of wars. For example, Kenya experienced its most catastrophic cyberattack in almost two decades of digital advancement in July 2023, crippling major government internet services such as Huduma Center and raising concerns about the attack's origin (Kamau, 2024).

While technological advancements offer opportunities for enhancing defense capabilities, they also pose challenges and raise ethical, legal, and strategic concerns which are increasingly being blurred through civil-military relations. For instance, drones with the ability to independently identify and engage targets can lead to unintended consequences and potential violations of international humanitarian law. In Kenya, modern counterterrorism policies emphasize the need of surveillance in public safety initiatives, as indicated by the Security Laws Amendment Act of 2014 (IDRC - International Development Research Centre, 2017). However, the use of advanced surveillance technologies for national security purposes can infringe on individual privacy rights. Mass surveillance, facial recognition, and data mining raise concerns about the balance between security and citizens' civil liberties and in the same way, bring the concept of dual use of technologies that benefit the military and civilians in equal but differentiated ways (Allenby, 2013)

Emerging technologies in the modern era have upended longstanding relationships between military and civilian spaces. Aerial reconnaissance and automated assistants have democratized access to military maneuvers so easily than before, with drones hovering overhead and gathering and storage of big data, non-combatants can now monitor motions and movements that were once largely mysterious to the public. The threat on national security arises when surveillance the equipment, capabilities and resources that were only secluded for military use find themselves in the hands of civilians. Nairobi became the first African city to install Huawei's Safe City system, a surveillance network designed to improve public safety. However, in 2017, Privacy International expressed alarm about the potential risks of gathering and storing

massive amounts of data without clear policies governing how the information is managed or safeguarded (Wangari, 2023).

Emerging technologies continually shift who wields power and control. The advancements in AI, robots, and cyber technologies have transformed the very nature of warfare itself and disrupting the existing status quo on who holds power on national security matters. The increasing use of unmanned aerial vehicles understandably arouses concerns about transparency and accountability when decisions with enormous consequences get made especially where human lives are put in line (Ward, 2021). It also obscures the boundaries between combatants and non-combatants on virtual battlefields where conflict occurs mostly in an asymmetrical environment as explained by Mary Kaldor 2012 in ‘New wars’. Because of their low cost and accessibility, terrorist organizations like as Al Shabaab can simply obtain several drones, considerably increasing their operational capabilities (Kaldor, 2012). In 2020, Al Shabaab allegedly utilized drones to organize an attack on a US military base in Manda, Kenya. This incident raises concerns that Al Shabaab may increasingly rely on drones for broader monitoring and reconnaissance, raising the group's threat in Kenya's national security (Aguilera, 2023).

With strides in AI, drones, and sensors, social media, GPS systems, civilians can now track troop movements with more precision than ever seen before from the comfort of their homes. Terms like "digitizing the battleground" and "military internet" showing this change have become common talk (Heickerö, 2010). This is enhanced with an increased merging of research and development in new technologies that cut access to civil and military spaces. As technology keeps bursting ahead, civilians and military must learn to adapt quickly and find a meeting point amid this fresh balance that would require collaboration, either by design or forced.

Laksmana outlines two distinct conditions that can make a state increase its military innovation in anticipation for attacks or in light of existing threats. One of them is a cohesive civil-military relationship that allows centralized decision-making procedures on defense policy to "trickle down" from top to bottom, beginning with civilian policymakers and ending with military implementation. Additionally, technological advancement may improve the integration, responsiveness, skill, and quality of the military which may intern enhance the civil-military relations of a state

(Laksmana, 2017). The utilization of developing technologies, such as cybersecurity tools, autonomous systems, and improved surveillance, is regarded as critical in combating future security threats (Laksmana, 2017). The use of emerging technologies in Singapore presents both benefits and challenges in civil-military relations. On one hand, technological advancement improves the military's operational capability. However, it raises concerns about the long-term viability of such advances particularly in terms of preserving civilian control and avoiding overreliance on military competence in technologies and associated costs (Laksmana, 2017).

A unified civil-military connection is evident when civilians have undisputed power with the ability to make strategic and operational defense decisions based on their legitimate social and political standing or when political and military officials work together (Feaver, 2021). In contrast, a strained civil-military relationship makes agreement on strategic policies more difficult. When civilian leaders dislike their military, they tend to use harsh measures to impose control, which may inhibit learning among the officer corps and further limit the potential to innovate or adopt new technologies (Laksmana, 2017).

Over time, a process of adoption and adaptation that favors some emerging technologies, while rejecting others, sometimes due to budget constraints, alters an army. While technological progress can give military benefits, Gray (2006) warns that over-reliance on technology can also be dangerous. Militaries that place too much emphasis on technology may overlook other important parts of defense, such as strategic planning or human rights concerns (Gray, 2006). This could result in a gap between civilian-military relations in terms of broader national objectives, as well as a prioritizing of technological capabilities. With few exceptions throughout history, technology has been and continues to be a driver of defense transformation. However, this does not imply that it has always been the driving force behind such extreme change (Gray, 2006). Gray underlines that effective defense transformation, fueled by rising technology, necessitates strong cooperation between civilian and military officials.

Not only do technologies like autonomous weapons and cyber lessen risk to both soldiers and civilians by enhancing detection among other capabilities, but they also broaden the field for a range of non-state actors who might pursue policy goals through

military methods. As a result, the development of technology may increase the likelihood of using force while lowering individual risk. Furthermore, changing how troops fight alters who they are, which has far-reaching consequences not only for military recruiting and training, but also for the military's relationship with the society it defends (Pfaff, 2020). Because these technologies carry danger at the very least, there is a tension between limiting their creation and application or use and fully exploiting their capabilities. For state actors who are bound by the social contract allowing such vulnerabilities and disadvantages implies a form of moral failing to ensure their citizens' security and well-being which is detrimental to civil-military relations (Pfaff, 2020).

Even when designed with the best intentions, emerging technologies run the risk of being introduced or used in an unjust manner. Given the intimate relationship between ends and methods, acquiring these technologies risk falling short of one's moral obligations as well as compromising the cause for which one fights, which is primarily a society value held in civil-military relations (Pfaff, 2020). Pfaff (2020) posits that military technologies are not developed in isolation, and their distinct characteristics will eventually find a civilian application, allowing them to enter civilian sectors and vice versa. It is vital to oversee the transfer of technology to society. This includes examining how technological attributes will be used in civilian sectors and ensuring that military research does not exclude technology that is better suited for civilian usage (Pfaff, 2020).

Risa Brooks (2018) creates a scenario, where she argues that today, a field commander may direct a system to assault a target or assist with logistics coordination. As autonomous systems evolve, the inputs may become more expansive and issued by leaders at higher levels in the chain of command (Brooks, 2018). This development requires civilian engagement to guarantee that existing checks and balances, particularly those derived from the constitution, are not breached. The obstacles to admission into the defense establishment will grow as civilian political appointees may struggle to challenge and evaluate military behavior, as well as test military leaders' arguments based on artificial intelligence. This puts additional strain on the already trusting civilian-military relationships. The civilian leadership may have reason to be

concerned that the military is obfuscating, hiding behind technology, or otherwise attempting to exploit it to favor a chosen strategy or policy outcome (Brooks, 2018).

Maintaining solid civil-military links has enabled regimes to deploy contemporary conventional weapons and technologies efficiently. In regimes such as Iraq, the fear of military political violence offers significant incentives for civilian engagement in order to reduce the military's access and utilization of advanced technology. The civilian interventions include rotation of commanders; suppression of horizontal communications within the military hierarchy and command; divided lines of command; isolation from foreign training and capacity building; using ethnic divisions in recruitment or combat unit organization; surveillance and promotion based on political loyalty rather than professional capabilities; or execution of suspected dissidents. In the process, the dictatorship or civilian leaders can make military conspiracies very difficult (Biddle & Zirkle, 1996).

2.4 The National Security Implications of Evolving Civil-Military Relations in Kenya Due to Emerging Technologies?

The Constitution of Kenya 2010, defines National security in Article 238, Chapter 14 (1) as the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests (Kenya Law Reform Commission, 2024). The people of Kenya are expected to initiate means that ensures there is maximum protection of these ideals. In certain instances, the government of Kenya through a representative democratic process would appoint or allocate resources to specialized entities, including the military to achieve the national security goals. It is hence imperative that the various attributions of emerging technologies and resultant impacts on civil-military relations are analyzed in the lenses of national security.

Globally, different cases of threats to national security of emerging technologies play, as well as their negative impact on individuals and states have been recorded. For example, AI powered tools have been used to persecute, monitor, and target specific groups during misinformation operations during elections, as well as in regular police (Razakamaharavo, 2021). Razakamaharavo contends that little is understood about the

implications of emerging technologies for peace, conflict, and security dynamics, especially in the global South, particularly Africa (Razakamaharavo, 2021).

The world today is facing myriads of national security challenges, not only from the economic, social, military, technological and more sources, but still need approaches that broaden security to address the threats. When addressing the modern security environment after the cold war, Julian Richards contends that with the removal of the Soviet threat, it allowed for a focus on other national security threats and the allocation of resources to address them. This is similar to governments' securitizing speech act during the post-Cold War era (Richards, 2012). The securitization speech act now addresses any emerging and perceived threats to national security.

State and non-state actors have taken over the space provided by easy access to technological tools to spread disinformation and misinformation. In certain areas, deep-fake technologies use deep learning to create synthetic media, such as videos and voices to create violent narratives. This increased civilian worry and fear while reducing the general trust in the authorities. For example, during the 2017 Kenyan elections, people were victims of Cambridge Analytica's micro-targeting operation. This company targeted Kenyans based on their personal information (race, gender, religion, and age). People were exposed to dreadful messages, including the exploitation and manipulation of previous post-election violence in the country to sway the attitudes and perception towards certain candidates in the presidential elections (Razakamaharavo, 2021).

The threats and opportunities from emerging technologies have forced states to incorporate technological strategies in their national security strategies across the board. In recent times, Germany's national security strategy prioritizes integrated security, which combines military and non-military measures to counter cyber threats (Federal Foreign Office, 2023); The Israeli Defense Forces (IDF) have implemented modern technologies such as artificial intelligence (AI), drones, and cybersecurity tools to protect against threats to national security (Dolinko & Antebi, 2024); South Africa considers cybersecurity to be a critical national security issue, and has implemented a national cybersecurity policy as well as a military Cyber Command (Devanny & Buchan, 2024). This shows a widespread acknowledgement and move by

states to take lead in utilizing emerging technologies in securing their national security strategies.

The deployment of lethal autonomous weapons and systems capable of identifying, selecting, and engaging a target without substantial human supervision has been documented in many regions of the world, presenting serious ethical and legal considerations. There were reports that the US strike against Iranian scientist Mohsen Fakhrizadeh used an AI-powered weapon, adding to the debate about the usage of such technologies in warfare. Israel recently revealed that artificial intelligence (AI) played a critical part in its military operations against Hamas in the Gaza Strip during the most recent conflict, employing machine learning algorithms to evaluate massive amounts of data and improve decision making (Razakamaharavo, 2021). These advancements show a rising dependence on AI in modern combat, which may redefine global military dynamics and heighten arguments over the responsibility of autonomous systems in conflict zones.

In 2014, Kenya saw an increase in cyber-attacks against both the corporate and state sectors. The rising reliance on ICT has exacerbated these vulnerabilities while also posing a substantial threat to Kenya's national security. Recognizing the importance of national security, Kenya has developed a cyber-strategy to protect the country's critical infrastructure and sensitive information (*National Cybersecurity Strategy 2022 – 2027 | NC4*, 2022). Despite these efforts, the number and sophistication of cyber-attacks continues to increase. According to the Communications Authority of Kenya (CAK) (*2023-24-Q3-Cyber-Security-Report.Pdf*), current cybersecurity safeguards are primarily passive. Additionally, they do not cover the entire scope of operations, leaving important national security assets vulnerable to possible threats.

Stephen Biddle and Robert Zirkle (1996), when discussing the consequences of emerging technology on national security, emphasize the significance of proper organization for national security success. They point out that the use of new technology does not always translate into increased military effectiveness. The incorporation of new technologies frequently necessitates significant institutional and organizational changes, which are influenced by the state of civil-military relations. This is despite emerging technologies' propensity to serve as key force multipliers for

underdeveloped countries in terms of achieving national security objectives (Biddle & Zirkle, 1996).

2.5 Theoretical Framework

A theory is a generalized statement of abstractions or ideas that explains or anticipates within the parameters of crucial limiting assumptions the links or connections between or among phenomena (Abend, 2008). Glanz (2008) support this definition by adding that the generalized concepts bring definitions and propositions that are interrelated together, to clarify relations among variables. This can also be used to explain or predict events (Glanz et al., 2008). A theory is hence a collection of connected definitions, hypotheses, and constructions that together give a systematic explanation and prediction of a phenomenon by defining relationships between various variables (Kivunja, 2018). Following on these definitions, a theory should have certain characteristics that make it qualify to be a theory. It must be coherent; should be logical and be applicable to a given domain or field; must be able to describe and connect various variables and their relationship. Among other characteristics, a theory should be able to clearly predict the future with the use of empirical data. This research used the critical theory of technology and agency theory to explain phenomena in emerging technologies and civil-military relations that may in turn affect the national security of Kenya.

2.5.1 Critical Theory of Technology

Critical theory of Technology originated in the 1930s at the Institute for Social Research in Frankfurt and is recognized for research that integrates philosophy and social science in an interdisciplinary and practical goal of advancing emancipation (Celikates & Flynn, 2023). The first generation of the Frankfurt School were inspired by an earlier generation of critical theorists. They reformed and updated Marxism by combining it with the works of Sigmund Freud, Max Weber, and Friedrich Nietzsche, while also constructing a model of radical critique that is fundamentally rooted in social reality. They used this model to analyze a wide range of issues, from a political formation of authoritarianism to the effects of capitalism on psychological, social, cultural, and political formations, as well as on knowledge production itself (Celikates & Flynn, 2023). Critical theory seeks to develop insights into the forces of domination at in society to inspire practical action and stimulate change, rather than just describing social reality. This research applied the use of Critical Theory of

Technology, borrowed from the Frankfurt School on Critical Theory to describe and explain the various variables.

According to Andrew Feeberg (2016), Critical Theory of Technology is concerned with the threat posed by modern societies' dominant technocratic structure. In science and technology studies, he develops an explicit philosophy of democratic technological interventions. Critical theory of technology remains distinct from most contributions to science and security studies by emphasizing key Frankfurt School topics, particularly the critique of rationality in modern civilization. As a result, it broadens the scope of science and technology studies to include more philosophical and social views of modernity (Felt et al., 2016).

Prior to the establishment of science and technology studies as a scholarly area, most studies of technology were related with Marxism, pragmatism, Heideggerian phenomenology, and other theories. These broad and often speculative theories investigated the relationship between technology and society, drawing on sociological studies to better comprehend their specific impact on modernity. The theories focused on scientific and technological breakthroughs and attempted to base social study to explain the numerous problems of modernity, particularly the lack of human agency in a technologized society. Feenberg (2016) posits that technology itself gets lost within these huge problems of the society (Felt et al., 2016). Science and Technology Studies concerns grew as major debates about medical care, the Internet, and the environment directly included technology in so many facets of current political life.

The critical theory of technology builds on Science and Technology Studies while situating the challenges within the Frankfurt School's critique of modernity. German Marxists developed Critical Theory during the 1920s and 1930s. Its most well known members were Max Horkheimer, Theodor Adorno, Herbert Marcuse, and Walter Benjamin. The theory agrees with Science and Technology Studies that technology is neither value neutral nor universal, and it proposes an explicit framework of democratic interventions in technology to ensure that the values and ideologies of people using it are considered (Felt et al., 2016). Feenberg (2016) posits that rather than view technology as an autonomous force, an emphasis on the cultural and social settings outlook, which reflect the power dynamics of the cultures that make and employ it should be of value to researchers.

In this regard, the notion that the development and application of technology like drones, surveillance and autonomous systems, artificial intelligence, and other cyber capabilities is not neutral or universal (Felt et al., 2016). Civilians influence their use based on political, strategic, and social objectives, frequently enhancing their authority and control over the military or reinforcing the military's dominance in society. The implementation of these technologies is determined by civilian and military officials' perceptions of the implications for national security. Military officials may frequently prioritize national security over civil liberties or democratic accountability, jeopardizing civil-military relations (Pantev, 2005). The military's technology capabilities may become disproportionate to civilian oversight, tipping the power balance in favor of the military and making civilian oversight difficult. Similarly, technologies can be utilized to conduct surveillance not only against external foes but also domestically under the pretense of national security, blurring the distinction between civilian and military sectors. The employment of proxies in cyberattacks, disinformation, and propaganda blurs the border between civil-military ties, even on a global scale, with significant implications for security (Kaspersen, 2016).

Whereas the Frankfurt School provided a very general critique to the practice of instrumental rationality, critical theory of technology seeks a more precise critique of the bias of social structures and technologies. Feenberg introduced the instrumental approach, which was originally intended as a foundation for comprehending technology. However, the method is applicable to other systems of social reason as well, particularly in situations where specialized institutions function in the civil domain. The instrumental approach regards military technology as a neutral tool for attaining national security objectives (Felt et al., 2016).

The instrumental approach is used to analyze technology two levels: primary instrumentalization, which explains how functions are separated from everyday life and subjects positioned to relate to them, and secondary instrumentalization, which emphasizes the social, cultural, and political factors that shape design decisions as these functions are implemented in systems and devices (Grimes & Feenberg, 2009). The second approach is important under the critical theory to understand how emerging technologies have and are shaping the civil-military relations in Kenya. For example, emerging technologies, such as AI powered drones, may lessen the

importance of human decision-making in conflict, complicating civil-military oversight and accountability. Brianna Rosen raises similar sentiments that While humans may continue to approve of lethal force, AI will play a more widespread role in shaping underlying decisions of who lives and dies and what gets destroyed. As AI reduces human participation in actions like killing, drone warfare will most likely become less explainable and transparent than it currently is (Rosen, 2023).

The critical theory of technology aligns with the constructivist approach, which emphasizes the role of interpretation in the development of technologies, an alternative to technological determinism. Feenberg rejects technological determinism, which holds that technology unavoidably shapes outcomes, and instead emphasizes the role of human agency in shaping technologies (Felt et al., 2016). This eliminates the unilateral acts of the military that may determine the direction of national security strategy and introduces civilian oversight that eliminates the possibility of over militarization. Moreover, Feenberg's critical theory of technology is concerned with the threat to human agency posed by the technocratic system that governs modern societies. He argues that human agency should not be prioritized over the agency of things (Felt et al., 2016).

In critical theory of technology, citizens' actions in technological conflicts are referred to as "democratic interventions." Democratic intervention promotes more societal involvement in technology decisions. For years, the victims of development were too weak, uninformed, or marginalized to organize meaningful protests. However, situations gradually changed, particularly during World War II. The adverse effects of more powerful technologies became apparent, prompting a public response. Unions and social movements advocated for industry regulation. As technologies become more harmful, regulation from the government blurs the barrier between the state and the private sector, leading to tensions between the civilian and military sectors (Felt et al., 2016).

In critical technology theory, the "democratic interventions" frequently "posteriori," which means they take place after technologies have already been released into the public domain. Recent instances include debates over environmental pollution or medical treatments, which may result in public hearings, litigation, or boycotts. These debates frequently result in regulatory changes and new practices. A second type of

intervention is the creative appropriation of technology, in which people modify or "hack" equipment to meet unexpected requirements. Abbate (1999) notes that this method was crucial in the emergence of the internet (Abbate, 1999). A third way of involvement is "a priori," which entails taking action before technology is released to the general public. This proactive method often includes public engagement in "citizen juries" or "hybrid forums" to evaluate suggested innovations, as well as collaboration during the design process. In these circumstances, authorities actively ask people to participate, eliminating the necessity for conflict-driven, a posteriori response. Sebastian support this notion, that open government and open democracy initiatives seek to make policymaking more responsive and transparent. Policies can be better suited to the requirements of citizens by allowing them to actively engage with governmental authorities (Berg & Hofmann, 2021).

The choice of the Critical Theory of Technology developed by Andrew Feenberg (2016) challenges the assumption that technology is neutral and instead argues that technologies are socially constructed and politically contested. The theory interrogates how power, control, and ideology influence the design and deployment of technologies with critical impacts to societies. In the context of Kenya, emerging technologies such as surveillance systems, artificial intelligence, integrated command centers, and cybersecurity strategies are shape and reshape power relations between civilians, the military, and the policy makers. The theory has been applied by several scholars such as Graeme Kirkpatrick (2004) have used critical theory to explore how digital systems reinforce dominant ideologies in governance (Kirkpatrick, 2004). In the African context, Gagliardone (2016) have examined how surveillance and digital authoritarianism are embedded in broader political agendas (Gagliardone, 2016). This makes Critical Theory of Technology a fitting lens for examining how technological integration in Kenya's security and civil-military relations landscape reflects deeper questions of democratic governance, control, and human rights.

2.5.2 Agency Theory

The Agency Theory was first proposed by Barry M. Mitnick in 1975 with a centrality to look at political and social sciences, likening the study of politics to a broader sense, the study of agency relations (Mitnick, 1975). Mitnick (1975) posits that the principal's difficulty of motivating his agent to act in his favor is equivalent to a

constituency's problem of regulating the behavior of its representative in a representative democracy, hence the authority relation with its policing concerns is a sort of agency relationship. "Acting for" shares many characteristics with traditional governance, which brings the idea of civilian control of the military (Mitnick, 1975).

Mitnick (1975) defines agency as a relationship in which one party, the "agent," acts on behalf of another, the "principal." Taking "acting for" in a broad sense, but with the assumption that the agent's actions are explicitly intended to "benefit" the principle. He defines an "act" simply as a "partitioning of behavior" (Mitnick, 1975). Agency behavior involves performing acts that benefit the principal's goal, representing the principal in matters that are important to them. They include acting as a trustee, administering something valuable in the principal's interest, acting as an employee, taking orders from the principal. This is geared towards enabling the principal to complete tasks he could not perform alone, and acting as an adviser or expert helper to the principal (Mitnick, 1975). The key assumption in this theory implies the principal consents, which align with this research with focus on a representative system of democracy.

Mitnick (1975) defines the principal-agent connection as both behavioral, in which agents act on behalf of principals, and institutional, in which systems that control conduct assume the agents' mandate under the dual agency perspective. This is a significant consideration because the theory addresses institutional democratic control of both civil and military affairs. In the same breadth, he applies agency theory to political or institutional settings where he explains how agents, like government officials or military leaders, are held accountable to the public or other authorities (Mitnick, 1975).

On the other hand, Jensen and Mackling (1976) define agency theory as agency relationship as a contract under which one or more persons who are the principals engage another person who are the agents to perform some service or task on their behalf. This involves delegating some decision-making authority or autonomy to the agent (Jensen & Meckling, 1976). Jensen and Meckling (1976) go further to note that when both parties in that relationship prioritize utility, the agent is unlikely to constantly behave in the principal's best interests. The principal can mitigate these

conflicts by providing appropriate incentives to the agent and incurring monitoring fees to minimize the agent's departure from planned conduct.

Furthermore, in certain cases, the agent may choose to undertake bonding costs in order to satisfy the principal that no damaging activities will be performed or to ensure reimbursement if they do occur. However, neither party can guarantee that the agent will always make judgments that are in the best interests of the principal. In most agency arrangements, both the principal and the agent will incur positive monitoring and bonding expenses in monitoring the behavior and activities of the other to thwart or minimize excesses (Jensen & Meckling, 1976). Moreover, there will almost always be some difference between the agent's judgments and those that maximize the principal's welfare which may bring a significant cost to the agency relationship, both in monetary or non-monetary.

Contrasting the relationship between stockholders and a corporation's manager meets the criteria of an agency relationship. The challenges originating from the "separation of ownership and control" in modern businesses are linked to the larger problem of agency according to (Jensen & Meckling, 1976). The issue of persuading an agent to operate in a manner that enhances the principal's welfare is universal. This issue arises in all organizations, at all levels of management for example businesses, universities, cooperatives, government agencies, bureaus, unions, and other settings with agency connections. Jensen and Meckling (1976) recommend the developing of ideas to explain these many circumstances which will help to build a more complete explanation of organizations, economics, and the social sciences in general. This strengthened the ability of the agency theory to be applicable in the social sciences, more so, the civil-military relations in a democratic system.

The use of emerging technologies such as autonomous drones, AI systems, and cyber defenses may increase agency expenses, which may put a strain to the civilians. Civilian authorities may need to invest in monitoring and incentive structures to prevent the military from misusing these technologies (Mitnick, 1975). Mitnick's (1975) framework implies that civil-military ties in the age of technological advancement may necessitate institutional modifications. These reforms could include updating defense policies and legal frameworks, as well as establishing new oversight institutions to deal with the increasing complexity of military technologies.

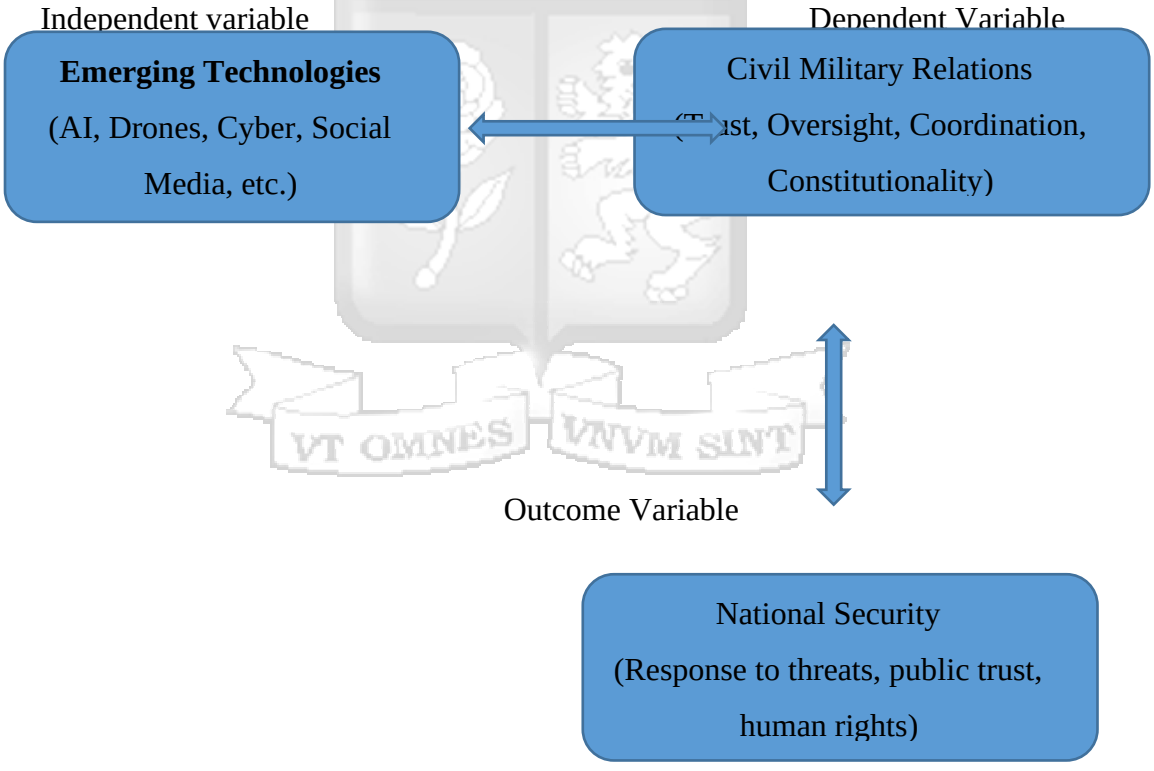
This research used Agency Theory spearheaded by its two main proponents to investigate the relationship in the civil-military sphere in the time where emerging technologies are creating more challenges to national security of states. For example, Kathleen Eisenhardt (1989) when analyzing the agency theory, emphasizes the issue of information asymmetry, in which the agent (military) frequently has more specialized expertise than the principal (civilian authorities). This asymmetry can lead to oversight issues as military officers may pursue policies or actions that are not entirely transparent to civilian authorities. This is especially important in high technological and cyber fields, where military knowledge may outweigh civilian authority (Eisenhardt, 1989).

Agency Theory has been widely applied to issues of institutional accountability and oversight in security governance. Scholars such as Peter Feaver (2009) has used the theory to examine fluctuations in civilian control in response to threat perceptions, delegation in private military contracting, and the challenges of monitoring autonomous security actors (P. Feaver, 2009). In cybersecurity and AI governance, Buchanan (2020) adapted Agency Theory to explore the evolving relationship between the state and tech companies in national security ("The AI Triad and What It Means for National Security Strategy," 2020). This makes the theory relevant for examining how Kenya's national security institutions are empowered or constrained by legal and institutional mechanisms, and how emerging technologies may exacerbate accountability gaps and weaken civilian oversight under complex securitization pressures.

2.6 Conceptual Framework

According to figure 2 below, the independent variable is emerging technologies, which bring new capabilities like artificial intelligence (AI), drones, surveillance tools, social media and cybersecurity systems that are drastically changing the security environment. These technologies have a direct impact on civil-military relations, which is the dependent variable, impacting balance of power, reshaping institutional roles, and generating opportunities and tensions in cooperation, oversight, and accountability. Lastly, national security, which serves as a more general outcome variable, is impacted by changes in civil-military dynamics which determine how best to respond to security scenarios.

Figure 2.1: Conceptual Framework



Chapter Three: Research Methodology

3.1 Introduction

This section present the methods used in the research including the research design, the target population, data collection and analysis techniques as well as sampling procedures. This research focused on Kenya with targets ranging from military officers, national security operators, and technology experts or scholars.

3.2 The Research Design

This research applied the use of exploratory research designs. This research design is particularly timely for this research as it is leaning towards qualitative methods. Exploratory research is highly effective in qualitative research due to its flexibility, allowing researchers to adapt their focus as new insights emerge without rigid constraints (Dudovskiy, 2024). This design is particularly valuable when analyzing phenomena that are not well documented or where knowledge is fragmented, as is often the case with emerging technologies in Kenya and across Africa (Research, 2022). Furthermore, qualitative methods, such as unstructured interviews, capture rich, nuanced human experiences and social interactions—essential for understanding complex issues like civil-military relations and national security. As Barry Buzan suggests, these areas often involve perceptions shaped by securitization, making it crucial to explore underlying dynamics (Buzan et al., 1998). By employing an exploratory research design, this study aims to navigate the uncharted territory of emerging technologies, civil-military relations, and national security in modern Kenya.

Exploratory research design is a research method used when an issue is not well defined or when there is little knowledge about the phenomenon under investigation. This design is very adaptable, open-ended, and often qualitative, but it can contain quantitative features as needed. It seeks to gather as much information as possible to gain a deeper understanding of the subject and lay the groundwork for further research. Exploratory research is ideal for investigating new or undiscovered themes, clarifying issues, and developing hypotheses for future research.

3.3 Location of the Study

Nairobi, Kenya was selected as the research site due to its strategic significance as the administrative and institutional hub. It hosts key national institutions such as major military agencies, policy making bodies like the parliament and technology related organizations that are involved in shaping civil-military relations. As a centralized location with well-developed infrastructure, it made it easier and cost effective to access the respondents for this study. The proximity to relevant data and resources, including critical actors in the study area enhanced efficiency and depth of the study.

3.4 Target Population

The target population for this research comprised scholars, military personnel, policy makers and analysts, technological analysists with specialized knowledge in national security and civil-military relations. National security experts who have either published research or practiced in the fields of security and emerging technologies were the target. These experts helped contextualize the broader implications of emerging technologies on national security and civil-military relations.

As the research was guided by thematic analysis, it was paramount that the target population be a certain number. Braun and Clarke (2013) provide guidelines for thematic analysis, suggesting sample sizes based on the type of data collection and project scale. For smaller studies, they recommend 6–10 participants for interviews, 2–4 for focus groups, 10–50 for participant-generated text, and 10–100 for secondary sources, while larger projects may involve 400 or more participants (Braun & Clarke, 2013). The goal is to strike a balance by ensuring there is sufficient data to identify meaningful patterns without becoming overwhelming to analyze to achieve the research objectives (Andrew & Henry, 2015).

The choice to employ the range of 10-20 in this study is supported by research showing that thematic saturation in qualitative investigations can frequently be reached with 10 to 20 interviews. For example, Guest, Bunce, and Johnson discovered that key elements for meta themes were present as early as six interviews, and that saturation happened during the first twelve interviews (Guest et al., 2006). Francis et al. (2010) also offered recommendations for figuring out saturation, recommending a sample for analysis at first, then more interviews until no new themes surfaced (Francis et al.,

2009). These results are consistent with the sample size of seventeen (17) that was selected, which guaranteed a thorough examination of the topic and objectives of research.

The study engaged seventeen (17) participants, with five in-depth interviews and twelve (12) through questionnaires. Emphasis was placed on engaging national security experts who have either conducted research or practiced in the domains of emerging technologies and security policy. The participants were based in Nairobi, Kenya, although with an understanding of the national level of policymaking and impact of emerging technologies on civil-military relations and national security. In addition to primary data, the study explored and analyzed relevant literature and case studies to critically analyze emerging technologies, their implications for national security, and the dynamics of civil-military relations.

3.4.1 Population Groups

Table 3.1 below is made up of the seventeen (17) respondents chosen for this study, who came from a variety of organizations involved in Kenya's civil-military and national security affairs. The Ministry of Defense was the most represented with (4), followed by the Ministry of Interior with (3). One respondent from Ernst & Young's Cybersecurity Advisory (1), the National Computer and Cybercrimes Coordination Committee (1), and the National Counter Terrorism Center (2), a classified security respondent (1), and media intelligence from BBC Monitoring (1), a private security consultant, and academic experts from Strathmore University and United States International University were also included in the sample. The wide and diverse respondent pool provided an all-rounded perspective on the intersection of emerging technology, civil-military relations and National security.

Table 3.1: Population Groups

Population Category	**Sample size**
Ministry of Defence	4

National counter terrorism center	2
SF Group, Information and Research	1
Ministry of Interior	3
Ernst & Young, Cyber Security Advisory	1
National Computer and Cybercrimes Coordination Committee (NC4)	1
Strathmore University – School of Computing	1
British Broadcasting Company Monitoring	1
United States International University – History and International Relations	1
Information Security Consultant	1
Classified Respondent in Security	1
Total	**17**

3.5 Exclusion and Inclusion Criteria

By defining the military as distinct from government and society, the research draws attention to its unique position as an organization separate from civilian institutions. The police, by contrast, are often viewed as an extension of civilian authority and governance, which positions them outside the specific civil-military paradigm under study. Including the police would introduce additional layers of complexity, as their interactions with civilians often revolve around law enforcement and community engagement rather than the strategic, sovereignty-related concerns addressed by the

military. Exclusion of the police ensures that the research maintains a clear and focused scope, allowing for a more in-depth exploration of the implications of emerging technologies on the military's role in national security.

The military typically addresses external and strategic threats, while the national police focus on internal security and civilian interactions. The military is characterized as the national institution specifically tasked with safeguarding territorial integrity and sovereignty. This is distinct from the police, whose primary role is to maintain internal order, enforce laws, and address civil issues. The research centers on the military's unique institutional culture, values, and its strategic relationship with government and society, aspects that are not directly applicable to police functions.

The study of civil-military relations traditionally focuses on the relationship between the military, as a specialized coercive institution, and civilian authority, which encompass non-military governmental actors and the broader society. The police operate under different organizational norms, cultures, and societal interactions that do not align with the defined framework of civil-military relations used in the research.

3.6 Sampling Technique

This research adopted both purposive and snowballing sampling techniques. Purposive sampling as defined by Patton (2002) is a technique widely used in qualitative research for the identification and selection of information-rich to make the most use available resources that are scarce (Patton, 2002). Purposive sampling in this research aims to identify people with specific qualities, operational expertise, and abilities who can provide timely information on a particular topic (Stewart, 2024).

This strategy entails discovering and selecting individuals or groups of individuals who are particularly educated or skilled with a field of interest (J. W. Creswell & Clark, 2007). Purposive sampling enabled the research to come up with a sample size of seventeen respondents based on the following inclusion criteria that was relevant to the study: individuals with direct experience or expertise in civil-military relations, national security, and the application or governance of emerging technologies in Kenya. Applying these criteria enabled the research to reach a detailed understanding rather than a generalized result of the study. The respondents from academia, military,

security, technological and intelligence reflected the understanding of research topic and objectives more richly and in depth.

Some types of purposive sampling include extreme case sampling, intensity sampling, homogenous sampling, stratified purposive sampling, critical case sampling, snowball sampling, convenience sampling, cluster sampling and heterogeneous sampling among others (Jackson et al., 2018).

To ensure efficient reach, this research also employed snowball sampling. Snowball sampling is defined as a non-probability sampling technique in which the samples have rare traits. This sampling method uses referrals from current participants to find the samples needed for a study (Bhat, 2018). Due to the sensitivity and exclusivity of the target population this research relied on one respondent referring a friend or an expert in the field (Mahin Naderifar, et al., 2017). Given that the research focus is on national security issues, traditional sampling methods would have been ineffective in reaching these groups. Many of these individuals operate within hard-to-reach networks, making direct recruitment challenging. By leveraging these social connections, snowball sampling facilitated access to these populations, ensuring a more representative and insightful dataset while maintaining the necessary level of confidentiality and trust.

3.7 Data Collection Methods

This study used both primary and secondary data. Primary data were collected through interviews and structured interviews. Seventeen (17) participants were reached, with five (5) key informant interviews and twelve (12) structured questionnaires. The interviews and structured questionnaires were in line with the study objectives.

The interviews with five key informants were carried out through a face to face discussions, mobile, and virtual calls. The range for these interviews was between forty (40) minutes to one (1) hour. The interviews generated information by asking detailed questions that yield qualitative data. Moreover, structured questionnaires complemented the rich data that the research collected.

Secondary data were obtained from the library through the study of other scholars' books, journals, news, and the internet. For example, Kenya Civil Aviation Authority.

(2020, March), Kenya Law Reform Commission, (KLRC), National Cybersecurity Strategy 2022 – 2027 | NC4. (2022, September 29), and Parliament of Kenya. (2020, March) report on Administration and Internal Security, among others. Similarly, important secondary data were collected from reports and publications around the world.

The research applied data collection by focusing on the following sources, as explained by Robert Yin (1993). Archival records with organizational records, maps, service records, with a full awareness of the time, target audience and context to ensure an accurate capture of events. Interviews with open-ended questions, focused interviews with a keen effort to corroborate the information for objectivity. Lastly, analyzing physical artefacts like technological weapons or equipment (Yin, 1993).

3.8 Data analysis

Miles and Huberman's framework of thematic analysis guided the analysis of the captured data. The four crucial steps for deriving meanings from participant data collected are "data reduction, data display, drawing conclusion and verification of findings." These steps equate to the researcher becoming "familiar with data, resulting in initial codes, capturing themes, evaluating emerging issues, and compiling a research report (Bakhtawar, 2020)."

3.8.1 Data analysis

The qualitative data collected from the field research was thematically analyzed. Thematic analysis is a technique that, in addition to minimally organizing and describing your data set in detail and it interprets various parts of the study issue, is used to detect, analyze, and report patterns in data (Boyatzis, 1998). This study conducted data analysis with consideration to the research objectives which guided the coding of thematic areas.

Some of the themes captured includes; the nature of civil-military relations in Kenya, the role of emerging technologies in national security, changes in emerging technologies, the role of emerging technologies in military operations and ethical and regulatory issues in civil-military relations when using emerging technologies, among others.

Braun and Clarke 2006 argue that thematic analysis should be a foundational method for qualitative analysis due to its flexibility (Braun & Clarke, 2012). A theme represents a recurrent pattern of meaning within the data set and highlights an important component of the data in relation to the research objectives (Braun & Clarke, 2012). The goal of this research was to check whether the set themes capture something important in relation to the overall research objectives rather than leaning towards quantifiable measures.

The process of doing a thematic analysis entailed repeatedly switching between the coded data extracts, the whole data set, and the analysis that was produced. An in-depth analysis of the data was made possible by a repetitive technique, which guaranteed a careful investigation of themes and patterns (Braun & Clarke, 2012). This process ensured that the analysis stays rooted in the data while attempting to catch nuanced topics by improving codes and themes several times.

Braun and Clarke suggest that thematic analysis offers theoretical flexibility, allowing for the identification, description, and in-depth interpretation of patterns (themes) within a dataset (Braun & and Clarke, 2006). The research used an aspect of inductive analysis where key themes from the informants were collected to shape the themes of the research findings. Moreover, the paper was keen to analyze some findings and codes in relations to the objectives and theoretical interests of the research.

As Saraswati Dawadi posits, a deductive approach can serve as the starting point, enabling the analysis of data based on themes identified from the literature review or the study's research questions. However, any interesting or relevant themes that emerge from the data can also be incorporated. Even unexpected themes may be considered, providing a more comprehensive understanding of the phenomenon under investigation (Dawadi, 2020). These unexpected themes include recent phenomenon that were mentioned by the respondents, including the Gen-Z protests in Kenya (Barnabas, 2024) to show the interaction between the military and the civilians with technology (social media) as a medium.

The process of coding to extract themes and meaning of the data took several steps guided by the research questions and objectives in the following respective ways: familiarization of data to pick up the initial points of interest; Generating codes with

single words or sentence; Searching for themes b relating the codes and data collected with the main purpose to find out the patterns and relationships between and across the entire data set (Braun & and Clarke, 2006). Several instances where issues identified in the literature review were also identified to inform the themes further; Consequently, the research reviewed the themes to bring together main themes and sub-themes, to present them in a more systematic manner and enhance consistency and coherency. This process merged, renamed and discarded some subthemes to ensure there was no overlap in what the paper is trying to achieve with the objectives.

The final stage of the analysis involved documenting the findings. According to Braun and Clarke, a thematic analysis report should persuasively convey the validity and significance of the analysis to readers. Therefore, great effort was taken to present a concise, coherent, and logically structured narrative that accurately reflected the data across themes. This was achieved by incorporating sufficient evidence, specific examples, and relevant extracts to effectively illustrate key points (Braun & and Clarke, 2006).

3.9 Ethical Considerations

As part of the ethical considerations addressed in this study, measures were made to guarantee that the rights of respondents to informed consent were fully respected. Prior to conducting the interviews, each participant's consent was obtained. Participants were given a consent form with important research information. They were given a full explanation of the consent form and advised that their participation in the process was completely voluntary. Given the sensitive nature of the study and the roles some participants occupy in national security and governance, strict confidentiality and complete anonymity were upheld throughout the research process.

To ethically conduct the study, the researcher obtained formal approval from the Strathmore University Ethical Review Board and secured research clearance from the National Commission for Science, Technology and Innovation (NACOSTI), in compliance with Kenya’s legal and institutional research requirements. These approvals ensured that the study met the necessary ethical standards and legal protocols for working with human subjects in sensitive sectors.

3.10 Methodological Contribution

The first phase of this project involved conducting a comprehensive literature analysis to uncover theoretical gaps at the intersection of emerging technologies and civil-military relations in Kenya. This influenced the use of Critical Theory of Technology and Agency Theory as analytical frameworks. The study used a qualitative case study design, which allowed for a thorough examination of scholarly work, institutional practices and governance systems.

Key informant interviews were performed with security experts, technology experts, intelligence officers, policymakers, and academics. During data collection, difficulties such as access to expert respondents and bureaucratic gatekeeping necessitated flexible scheduling, hybrid interviews, confidentiality assurance, and ethical declaration to ensure quality response. The study also used document analysis, including national policies, legislative texts, and annual reports, to help triangulate findings and compensate for interview limitations.

As research progressed, themes such as the blurred roles of civilian and military actors and the militarization of civilian space became more prominent than expected. However, the interview questions and questionnaires remained unchanged, maintaining consistency across respondents and data comparability at the end, which ensured methodological consistency and analytical flexibility.

Chapter Four: Research Findings and Discussion

4.1 Introduction

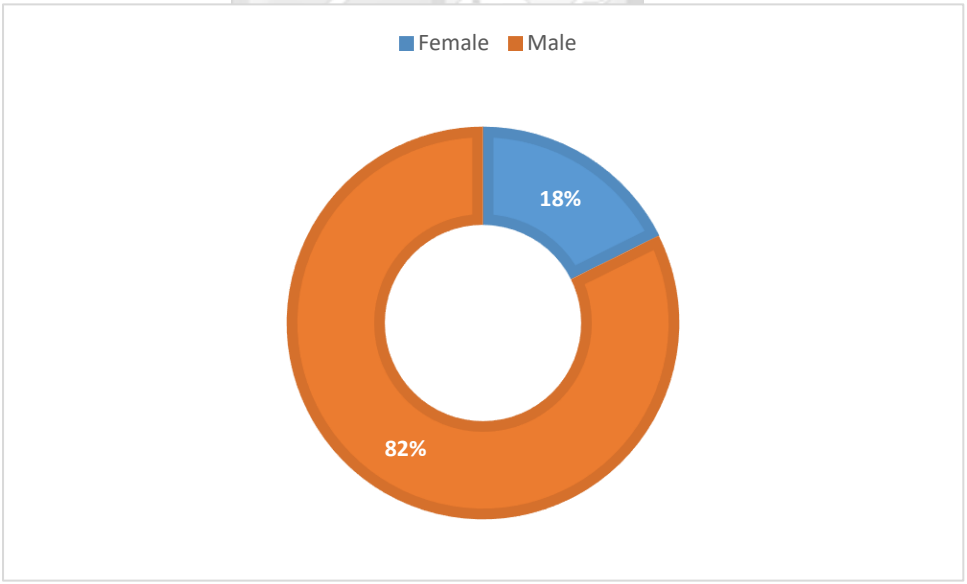
This chapter presents the research findings. The findings are presented in accordance to each of the set objectives namely: analysis of the nature of civil-military relations in Kenya, since 2010; investigation of the extent to which emerging technologies have impacted these relations since the adoption of the 2010 Constitution; and to assessing how the effects of emerging technologies on these relations have affected Kenya's national security.

4.2. Bio Data

4.2.1. Gender of Respondents

Figure 4.1 below illustrates the gender distribution of the respondents. Out of seventeen participants, fourteen were male (82%), while three were female (18%), reflecting a gender imbalance among individuals engaged in national security and civil-military affairs within the study sample.

Figure 4.1: Gender of Respondents

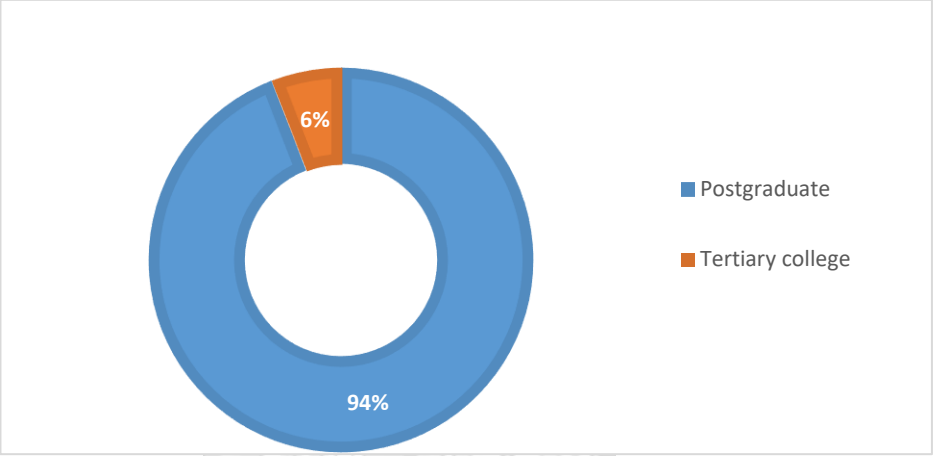


4.2.2. Level of Education of Respondents

Figure 4.2 below represents the level of education of participants. Out of the seventeen respondents, one had earned a tertiary college degree, and sixteen had finished

postgraduate studies. One important determinant of the respondents' ability to handle intricate policy matters pertaining to civil-military relations and national security was their high degree of education. Additionally, their wealth of experience offered both historical and modern viewpoints, which improved the study's depth and applicability of the insights discovered.

Figure 4.2: Level of Education of Respondents



4.3. Response Rate and Classification of Questions

The interview questions were split into three sections to ensure a nuanced response was captured from all participants. While still maintaining the objectives of the research, the three sections were labeled as Understanding Emerging Technologies in National Security; Role of Technology in Civil-Military Relations; and the Impact of Emerging Technologies on Kenya's National Security where the interplay of civil-military relations were captured.

Seventeen respondents for this research were reached through purposive sampling and snowballing in some instances were from different backgrounds with 100% response rate. Some were military personnel and security professionals who consisted of Kenya Defense Forces (KDF), National Counter Terrorism Center (NCTC), and compliance and enforcement agencies. Others were intelligence and strategic affairs experts from private intelligence firms and government research units who give expert opinion on national security policy issues. Additional respondents were technology and policy analysts from academia, and technology think tanks. A good number were experienced in civil society and public sector advocates where they are concerned with

public trust, regulatory frameworks, and civil-military cooperation based on their responses.

4.4 Findings

4.4.1: The Nature of Civil-Military Relations in Kenya, Since 2010

Under objective 1, the main findings indicated that Kenya's civil-military relations have become more dynamic and visible since 2010 constitution was adopted. This is reflecting both growing tension and increased collaboration. In addition to improving coordination and operational effectiveness, the military's growing involvement in civilian domains like internal security, infrastructure, and crisis response has also sparked worries about overreach and blurred institutional boundaries. The public opinion of the of the military use of emerging technologies is divided. Although many see their benefits in enhancing response and national security, others worry about potential abuse, privacy concerns and surveillance. The public still strongly supports democratic governance and rejects military rule, even in the face of the military's increasing involvement in civilian affairs.

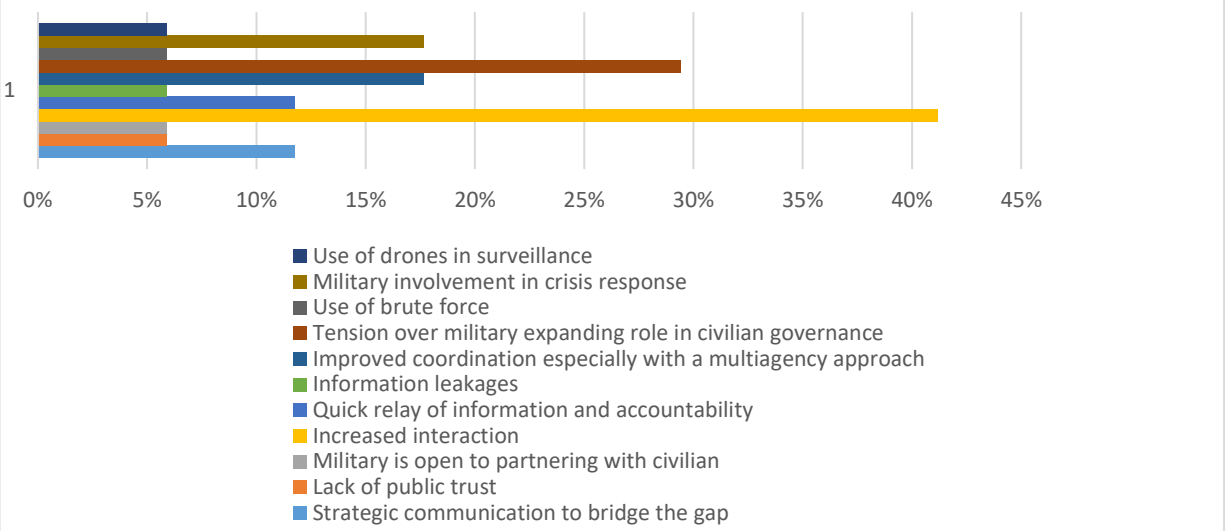
Changes in Civil-Military Relations

Figure 4.3 below illustrates key changes observed in civil-military relations in Kenya since 2010. The most commonly mentioned change by the respondents are "Increased Interaction" between the military and civilians, according to seven respondents (41.1%), suggesting a move toward more visible and cooperative interactions. Closely behind this is "Tension over Military Expanding Role in Civilian Governance," which was mentioned by five respondents (29.4%). This suggests that although cooperation has increased, there are now concerns about the military's role in areas that have historically been civilian. Three respondents (17.6%) each cited "Military Involvement in Crisis Response" and "Improved Coordination, especially with a Multiagency Approach," emphasizing the rising involvement of the military in interagency efforts, like in disaster relief.

Other trends that were noted include "Quick Relay of Information and Accountability" and "Strategic Communication to Bridge the Gap," both of which were mentioned by two respondents (11.7%), and they both represent small attempts to improve openness

and build public confidence. However, only one respondent (5.8%) mentioned topics like "Use of Brute Force," "Use of Drones in Surveillance," "Information Leakages," "Military Openness to Partnering with Civilians," and "Lack of Public Trust,".

Figure 4.3: Changes Observed in Civil-Military Relations Over the Past Decade



Based on the understanding of the emerging technologies, respondents observed great changes and developments in the civil-military relations in Kenya since 2010. A huge observation was made especially with increased interaction between the military and civilians standing at 40%. Observadly, this is due to an increased military involvement in civilian sectors in different capacities inluding crisis response, and civilian governance standing at close to 30% of respondents input.

However, while interaction has improved and increased collaboration especially coordination of security responses, tensions persist due to underlying issues such as blurring of roles between armed civilians and military personnel, and the military's growing footprint in civilian spaces. Cases like the military's involvement in the Nairobi Metropolitan Services (NMS), infrastructure projects, and internal security operations, including responses to protests, such as Gen Z protests have raised eyebrows among the respondents. There is growing concern that the military's increasing role in economic and administrative functions risks politicizing the institution and undermining democratic principles. These dynamics reveal a delicate balance between partnership and control between the military and civilians.

To reach the above findings, Respondent 12 from BBC monitoring in the African region gave feedback on the following question: "8. What changes have you observed in civil-military relations over the past decade?"

> *"Over the past decade, civil-military relations in Kenya have become more visible, especially during times of crisis like elections or natural disasters. The military is now more involved in helping with things like infrastructure and emergency response. However, some people are concerned that the military is being given too many roles that should be handled by civilians, which can raise questions about transparency and accountability,"* (**Respondent 12, 4/8/2025-Nairobi)**

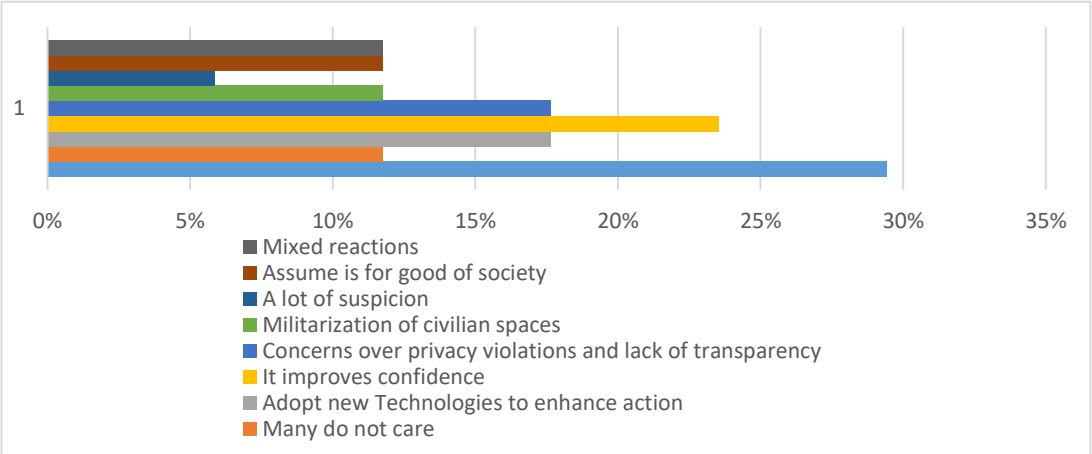
Respondent 16 from the Ministry of Defence shares similar sentiment as follows:

> *"There has been increased KDF involvement in internal security operations North Rift, Gen Z protests and terror attacks response. Political Dynamics and Civilian Oversight where there has been increased calls for accountability. Increased involvement in unrelated security projects – stadium constructions and aid support,"* ***(Respondent 16, 3/25/2025-Nairobi.)***

Perception by Civilians on Military's Use of Emerging Technologies

Figure 4.4 below shows how the public views Kenya's military use of emerging technologies. According to the majority of respondents, seven out of seventeen (41.2%), they improve operational efficiency and national security. Five (29.4%) respondents voiced concerns, mainly about potential abuse of power, privacy violations, and surveillance. Three (17.6%) respondents expressed a neutral or unsure position, indicating either a lack of awareness or a wait-and-see attitude. However, two (11.8%) respondents expressed strong disapproval and were critical, citing concerns about civil liberties violations and the militarization of public space.

Figure 4.4: Perception of Civilians on the Military's Use of Advanced Technologies in Kenya



According to the data, most civilians have a positive opinion of military technological advancement and are aware of its security advantages. Nearly half of the respondents also voiced caution, highlighting the value of transparent policies, civilian oversight, and ethical concerns when deploying emerging technologies. In Kenya's evolving civil-military environment, this mixture of support and concern reflects the public's desire for a balance between security effectiveness and the defense of democratic rights and liberties.

Respondent 12, from BBC Monitoring, captured the sentiments as follows:

"Most civilians see the military's use of advanced technology as helpful for security, but some worry about misuse or lack of oversight." (Respondent 12, 4/8/2025 – Nairobi)

Respondent 14 who is in academia shows the reason for support or mixed reaction if technologies are not deployed in civilian spaces:

> *"They know that the military have advanced technologies and assume is for the good of society. The use and deployment of these equipment have not been against the civilians so far especially during the Gen Z protests. They are called to assist with some tasks that involve civilians like demolition of a building in Mombasa."* **(Respondent 14, 4/9/2025 – Nairobi)**

A practitioner at the Ministry of Defence cyber security and technology department summarizes the views as follows:

> *"Due to the limited exposure to civilians by the military, the citizens have mixed perception of the militarys use of advanced technologies. This perception is shaped by various factors, including security concerns, ethical considerations, and the impact of technology on civil liberties and freedoms."* **(Respondent 16, 3/25/2025 – Nairobi)**

These findings are aligning with existing literature that captures the perception and the realities of civil-military relations in Kenya since 2010, after the promulgation of a new constitution that gave civilian supremacy in controlling the military, while maintaining military autonomy in operational matters.

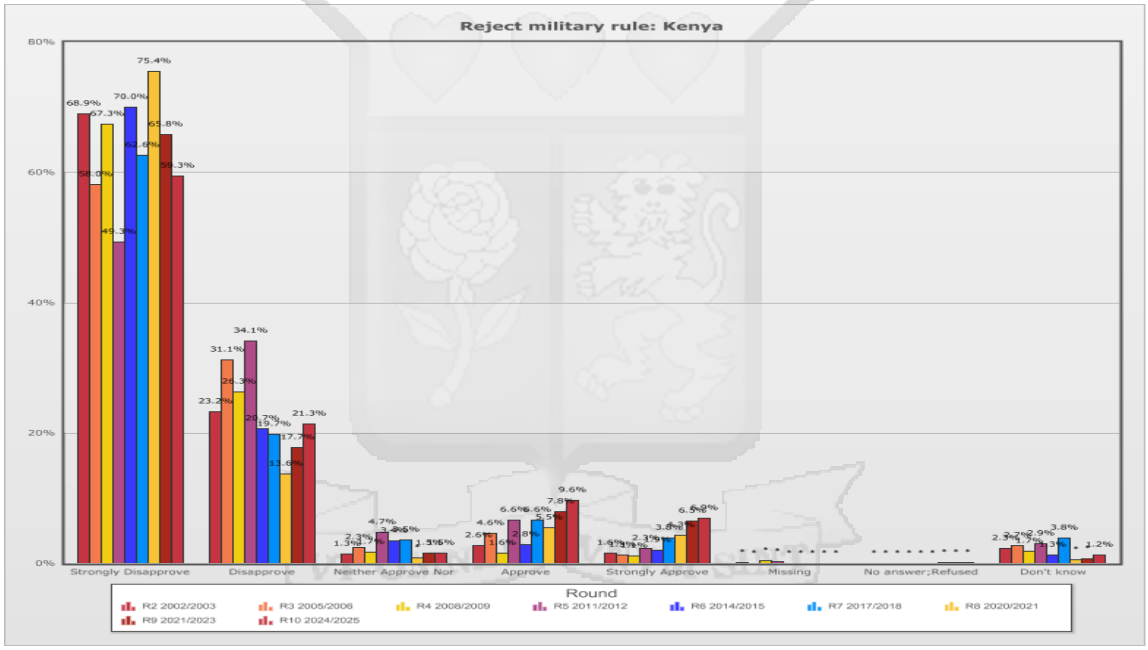
The research also captured the overall country perception on military rule using data from Afro Barometer as follows, where rounds are years the study was conducted (R4 – 2008/2009) (R5-2011/2012) (R6-2014/2015) (R7-2017/2018) (R8 – 2020/2021) (R9 – 2021/2023) (R10 – 2024-2025) (Afrobarometer, 2025)

According to Afrobarometer data on figure 4.5 and 4.6 below, from rounds 4 (2008/2009) through 10 (2024/2025), a sizable majority of Kenyans consistently oppose military rule as a system of government. Over 70% of respondents "disapproved" or "strongly disapproved" of the idea in each round; Round 8 (2020/2021) saw the highest opposition, with 75.4% strongly disapproving. Throughout, approval was consistently very low, never exceeding 16.5%, and there were very few neutral or unsure answers. The data sample ranging from approximately 1,680 to 1,800 respondents out of each sample of 2,400 was used.

Figure 4.5: Approval or Disapproval of Military Rule in Kenya - Afrobarometer

	R4	R5	R6	R7	R8	R9	R10
Country - Kenya							
Strongly Disapprove	67.3%	49.3%	70.0%	62.6%	75.4%	65.8%	59.3%
Disapprove	26.3%	34.1%	20.7%	19.7%	13.6%	17.7%	21.3%
Neither Approve Nor Disapprove	1.7%	4.7%	3.4%	3.5%	0.7%	1.5%	1.5%
Approve	1.6%	6.6%	2.8%	6.6%	5.5%	7.8%	9.6%
Strongly Approve	1.1%	2.3%	1.9%	3.8%	4.3%	6.5%	6.9%
Missing	0.3%	0.2%	-	-	-	-	-
No answer;Refused	-	-	-	-	0.0%	0.0%	0.1%
Don't know	1.7%	2.9%	1.3%	3.8%	0.5%	0.6%	1.2%
(N)	1,104 (100%)	2,399 (100%)	2,397 (100%)	1,599 (100%)	2,400 (100%)	2,400 (100%)	2,400 (100%)

Figure 4.6: Rejection of Military Rule - Afrobarometer



Despite the military's increasing involvement in civilian tasks, this trend demonstrates the public's persistent and evident preference for democratic civilian governance and widespread mistrust of military leadership. It implies that although Kenyans might be open to military participation in crisis management and national security, they are adamantly against the idea of the army assuming political power.

4.4.2: Conclusion - Nature of Civil-Military Relations In Kenya, Since 2010

The results under objective 1 show that since the 2010, Kenya's civil-military relations have grown more vibrant and noticeable. Although cooperation has increased

significantly, particularly in areas like infrastructure development, crisis response, and multi-agency coordination, these increased responsibilities have also raised worries about the blurring of the lines separating military and civilian spaces. The biggest shift was found to be an increase in military-civilian interaction, but this comes at a time when civilians are becoming increasingly concerned about the military's growing presence in formerly civilian areas. This dual reality reflects a contested and adaptive civil-military environment where civilian oversight and liberties must be carefully balanced with operational effectiveness.

This complexity is further reinforced by public perception. Many civilians are still wary, voicing worries about surveillance, power abuse, and the militarization of public areas, even though many recognize the military's increased effectiveness as a result of emerging technologies and see their contribution to national security as generally positive. The Kenyan public consistently opposes military rule and strongly supports democratic civilian governance, according to Afrobarometer data, despite the military's increased prominence and duties. These observations imply that although new technologies have changed the civil-military relationship in Kenya, transparency, accountability, and the upholding of democratic values remain essential for the legitimacy of military engagement.

4.4.3. The Extent to which Emerging Technologies have Impacted Civil-Military Relations

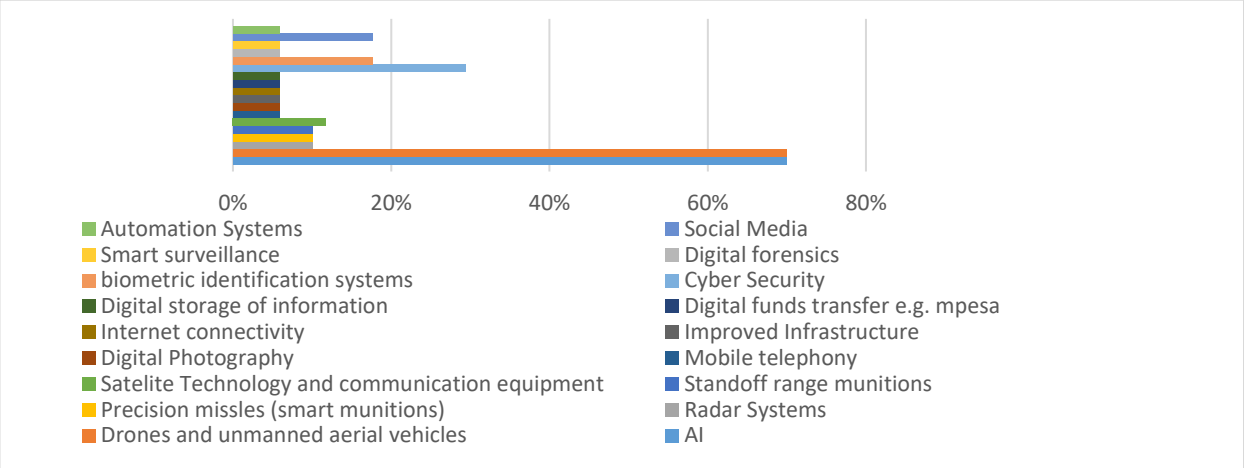
The main findings under objective 2 indicate that emerging technologies have progressively influenced the dynamics of civil-military relations since the adoption of Kenya's 2010 Constitution, exposing both new areas of tension and cooperative advancements to a moderate extent. According to the data gathered, respondents are clearly aware of the dual-use nature of technologies like social media, drones, mobile phones, artificial intelligence, and satellite surveillance. The boundaries between personal liberties and national security operations are blurred due to their dual-use nature. This duality introduces a delicate balancing act in maintaining trust between the military and the civilian population.

Emerging Technologies with most Impact to National Security

Figure 4.7 below shows the technologies that respondents felt had the biggest influence on Kenya's national security. With thirteen out of seventeen respondents (roughly 76%) mentioning social media and biometric identification systems, these were the most often mentioned technologies. These results demonstrate how social media has taken center stage in intelligence operations, public perception management, and information distribution, while biometric systems are essential for access control, identity verification, and surveillance in national security organizations. Following closely behind, cybersecurity was mentioned by seven respondents (41%), indicating a growing concern for digital vulnerabilities, cyber threats, and the need for improved protective infrastructure.

Four respondents (24%) mentioned digital forensics, satellite technology, and communication equipment as additional technologies with moderate visibility. In both military and civilian operations, these tools facilitate remote communication and investigative capabilities. In the meantime, two to three respondents (12–18%) each mentioned technologies like Internet connectivity, digital photography, mobile telephony, digital storage, indicating their supporting but less direct role in security strategy. Automation systems, standoff range munitions, and smart surveillance were less frequently mentioned, which may be in the early phases of integration or have limited applications.

Figure 4.7: Showing Emerging Technologies that have had the Most Impact on National Security in Kenya



The findings from the survey above was supported by one of the key respondent who works for the Ministry of Interior and National Administration who when asked the question - What emerging technologies have had the most impact on national security in Kenya since 2010? Said:

"Since 2010, drones, artificial intelligence (AI), and cybersecurity measures have had the most impact on Kenya's national security by enhancing surveillance, intelligence gathering, and counterterrorism operations, particularly against Al-Shabaab threats along the Somalia border. Additionally, biometric identification systems, digital forensics, and smart surveillance technologies have strengthened law enforcement efforts, improved border security, and bolstered cybersecurity defenses against cybercrime and digital threats from viruses like ransom Ware." **(Respondent 7, 4/2/2025 – Nairobi)**

This was also confirmed by Respondent 1, working in the Ministry of Defence, who said:

"Technologies such AI, drones and unmanned aerial vehicles, radar systems, precision missiles (smart munitions), standoff range munitions, satellite tech and communications equipment." **(Respondent 1, 4/1/2025 – Nairobi)**

These responses are supported by NC4, Kenya's government agency that looks into emerging threats and developments in the cyber domain. The National Computer and Cybercrime Coordination Committee that advises the government on security related

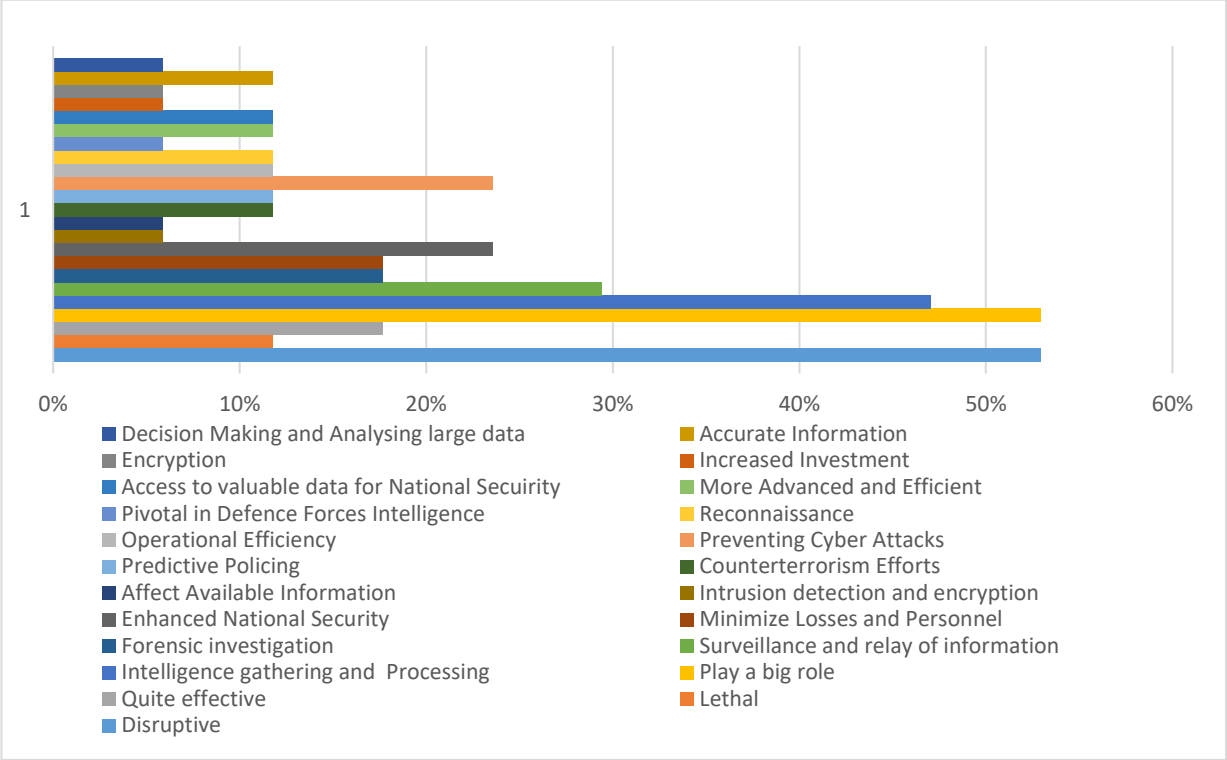
aspects touching on critical information infrastructure and New and Emerging Technologies (Block chain, 5G, AI, Internet of Things (IoT) (*NC4 - Protecting Kenya's Cyberpace*, 2016)

Role of Emerging Technologies in Military Operations

Figure 4.8 below illustrates the multifaceted roles that technologies such as artificial intelligence, drones, and cybersecurity measures play in shaping contemporary military operations in Kenya. Nine out of seventeen respondents (52.9%) cited "disruptive" technologies, while nine respondents (52.9%) marked "accurate information," which was the most prevalent perception. These results point to a broad agreement that these technologies improve the accuracy and timeliness of intelligence while also changing the battlefield environment. Eight respondents (47.0%) further supported these inputs by mentioning, "Predictive Policing" and "Play a Big Role." Six respondents (35.2%) named "Access to Valuable Data for National Security" as a major contribution, and highlighted the importance of data-led capabilities in operational planning and threat anticipation.

Additional crosscutting functions were mention, for example, five respondents (29.4%) highlighted; "Preventing Cyber Attacks," while four respondents (23.5%) highlighted; "Reconnaissance," "Minimize Losses and Personnel," and "Operational Efficiency." "Enhanced National Security," "Encryption," and "Pivotal in Defence Forces Intelligence" were covered by three responses (17.6%) each. "Lethal Effects" was mentioned less frequently, but it was still significant as it had two respondents (11.7%). Lastly "Forensic Investigation, Surveillance and Relay of Information, Intelligence Gathering and Processing, Increased Investment," and "Decision-Making using Large Data," which were each mentioned by one ot two respondents (5.8% to 11.7%).

Figure 4.8: The Role of Technologies Like Artificial Intelligence, Drones, or Cybersecurity Measures in Shaping Military Operations



These findings suggest that although some roles, particularly those pertaining to intelligence, and accuracy dominate the conversation, a broad range of operational improvements provided by emerging technologies are valued as per the respondents input. Emerging technologies enhance both the strategic and operational levels of Kenya's military and national security apparatus.

The increasing role of AI and emerging technologies is also underscored by Africa Peace and Security Council of African Union on the capabilities they bring. AI's revolutionary potential for peacebuilding was emphasized during the 1214th session in June 2024, along with its uses in early warning systems, conflict prevention, and post-conflict recovery. But most significantly, it acknowledged the dangers of its quick development in the absence of regulations (*Artificial Intelligence and Its Impact on Peace, Security and Governance – Amani Africa*, 2025)

These insights were articulated by Respondent 7, a representative from the Ministry of Interior and National Administration, in response to the question: "How would you describe the role of technologies like artificial intelligence, drones, or cybersecurity measures in shaping military operations?"

In the Kenyan context, technologies like artificial intelligence (AI), drones, and cybersecurity measures are increasingly shaping military operations by enhancing border security, counterterrorism efforts, and intelligence gathering. The Kenya Defence Forces (KDF) and security agencies utilize drones for surveillance and reconnaissance, particularly in countering threats from militant groups like Al-Shabaab along the Kenya-Somalia border, enabling real-time monitoring of insurgent movements while minimizing risks to soldiers. AI-driven data analytics assist in threat detection, intelligence processing, and predictive policing, helping security forces respond proactively to emerging threats. Meanwhile, cybersecurity measures play a crucial role in safeguarding Kenya's military communication networks, preventing cyber-attacks on critical infrastructure, and countering cyber warfare threats from hostile actors. As Kenya continues modernizing its defense capabilities, the integration of these technologies enhances operational efficiency, strengthens national security, and improves the ability to combat evolving security challenges."
(**Respondent 7, 4/2/2025 – Nairobi)**

Respondent 10 from the Ministry of Defence added to the question as follows:

"The uptake of artificial intelligence is still a little bit novel. However, drones have become pivotal in Kenya Defence Forces' intelligence. They are used for monitoring borders, conducting aerial surveillance in remote areas, and supporting anti-terrorism operations. The ability to gather real-time intelligence from hard-to-reach locations enhances operational effectiveness and situational awareness, which is crucial for national security. On Cyber security measures, KDF forms part of the NC4 and offers response mechanisms to national cyber threats through the Moran centre. Kenya has experienced an increase in cyber threats, prompting the government to invest in advanced cybersecurity measures. Technologies such as intrusion detection systems and encryption tools are being implemented by the KDF's Cyber branch to protect sensitive data and critical infrastructure from cyberattacks. The establishment of the National Cybersecurity Strategy reflects the urgency of addressing these

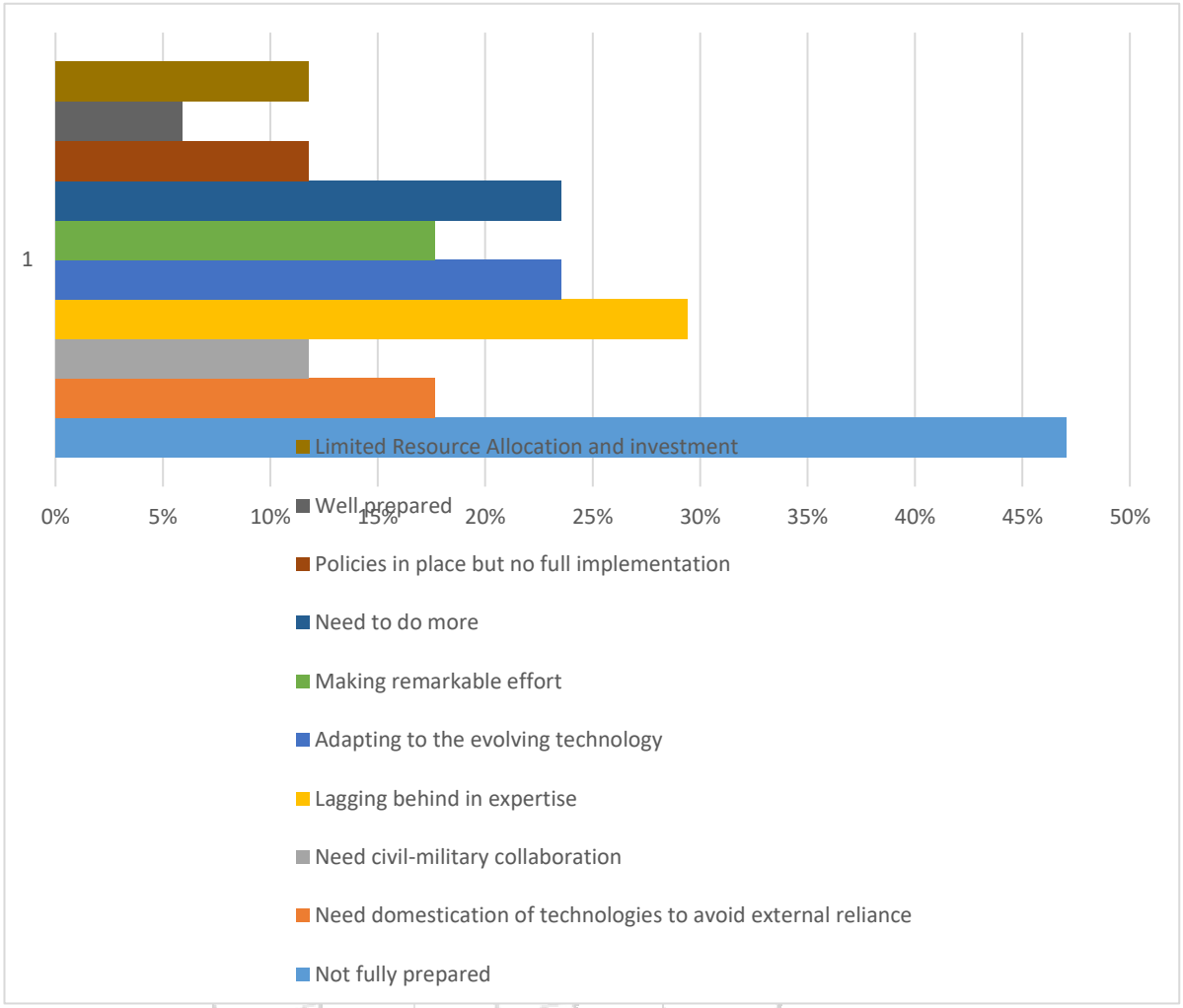
threats to safeguard national interests," **(Respondent 10, 4/4/2025-Nairobi)**

Readiness of Civil-Military Sectors with Regards to Technological Evolution.

According to Figure 4.9 below, eight respondents (47%) think Kenya's military and civil sectors are "not fully prepared" to handle the rate of technological advancement. Moreover, seven (29%) believe that the sectors are "lagging behind in expertise", while six respondents (24%) believe that they are "adapting to the evolving technology" . This suggest that although some efforts are being made, they are still insufficient. Additionally, five (19%) respondents expressed the sentiment that the sectors are "making remarkable effort," indicating some optimism amid concern.

Some respondents, however, identified structural and systemic flaws for examples, "need domestication of technologies to avoid external reliance" which four respondents (17%) of the respondents, opined. Observation on "policies in place but not fully implemented" were made by three respondents (12%). Fewer respondents thought the sectors were "well prepared" two respondents (7%), "limited resource allocation and investment" two respondents (7%), or "need civil-military collaboration" one respondent (5%).

Figure 4.9: How Well Prepared are Kenya's Civil and Military Sectors for the Rapid Evolution of Technology



A look at the take from an information security consultant who is Respondent 15 the question, "3. In your opinion, how well-prepared are Kenya's civil and military sectors for the rapid evolution of technology?" goes as follows:

> *"Not very well prepared. They appear to be working hard, but they have resource constraints. Not enough competent personell and finances to be advanced. Nowhere near the advanced states. Not enough policies,"* **(Respondent 15 4/9/2025-Nairobi.)**

Additionally. Respondent 1 from the Ministry of Defence responds as follows:

> *"Somewhat but not fully prepared. Need for indigenization or domestication of technologies to avoid overlying on original producers that are often external. Need for the civil sector to get involved (both with*

military) to identify areas of collaboration," **(Respondent 1, 4/1/2025 – Nairobi**.)

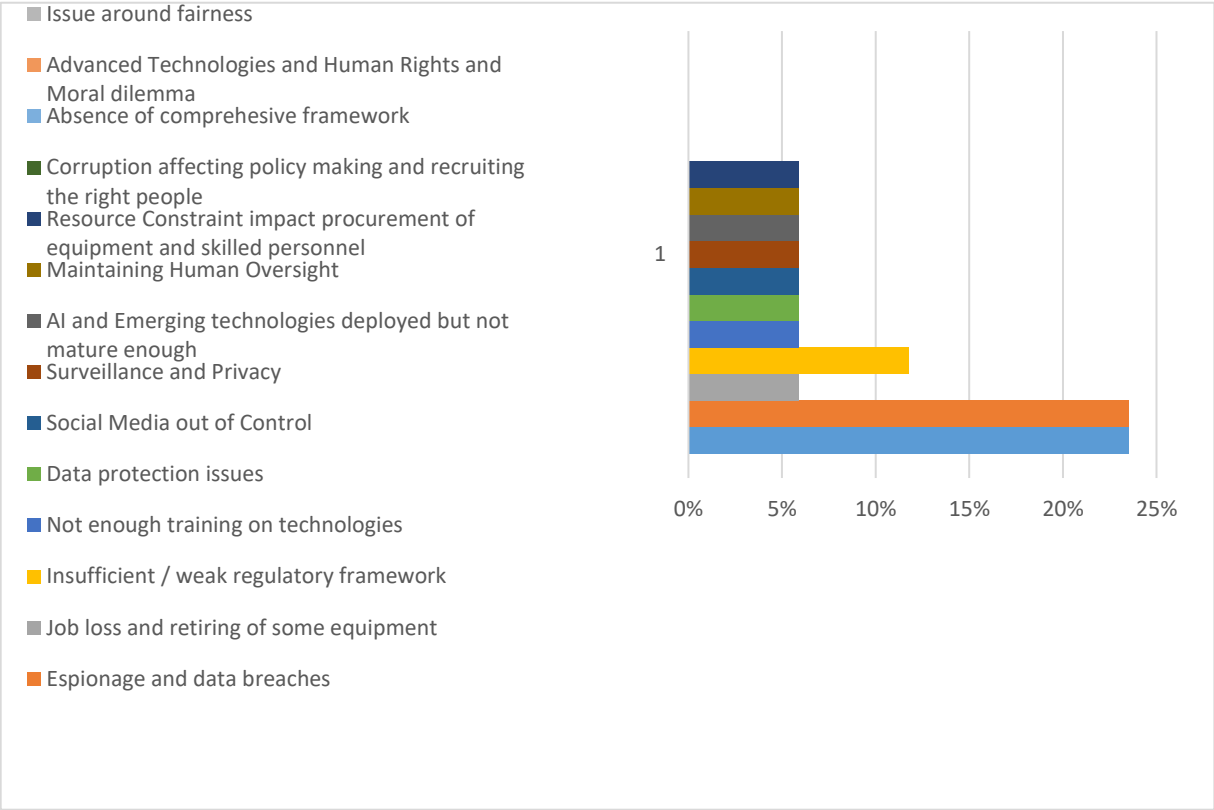
According to these observations, although the technological imperative is becoming more widely recognized, Kenya's readiness is hindered by its limited technical and resource capacity, inconsistent policy implementation, and requirement for greater institutional alignment and investment. Additionally, concerns such as external technological dependence, incomplete policy implementation, and limited resource investment are notable. It is also important to acknowledge the steps Kenya is making to ensure adapting to the technological environment. A recent case of National AI Strategy that was launched is a positive sign, however slow, towards the right direction (*Kenya AI Strategy 2025-2030 | Ministry of ICT and the Digital Economy*, 2025)

Ethical and Regulatory Challenges in Integrating Emerging Technologies

Figure 4.10 below illustrate the ethical and legal issues Kenya faces when incorporating new technologies into its military. Four out of seventeen respondents (23.5%) identified espionage and data breaches as the two most urgent issues, along with the belief that non-Kenyan technology is unsafe and vulnerable to backdoor access. These issues draw attention to serious worries about national cybersecurity and reliance on technology. Stronger governance structures are required to direct the adoption of safe and ethical technology, as indicated by the fact that two respondents (11.8%) cited inadequate or weak regulatory frameworks as a barrier.

One respondent (5.9%) identified each of the remaining eleven categories of challenges, providing a comprehensive picture of ethical and systemic barriers. These include the loss of jobs and retirement of equipment, privacy and surveillance, the early adoption of new technologies, the need for human oversight, data protection concerns, inadequate training, resource limitations, corruption in hiring and policymaking, the lack of a comprehensive framework, moral quandaries and human rights, and issues with justice.

Figure 4.10: Regulatory or Ethical Challenges in Integrating Emerging Technologies within its Military



These insights indicate that, despite the dominance of certain challenges, a wide range of regulatory, infrastructure, and ethical issues need to be addressed holistically. A notable mention is emerging technologies are used to infringe on civil liberties which may widen the trust gap between the military and the public. The concern on human rights is closely related to the need to formulate a comprehensive regulatory framework to ensure rule of law and civil-military relations is maintained.

Some respondents shared similar sentiments to support the findings: Respondent 1 from the Ministry of Defence

> *"A technology that Kenya does not own is insecure and open to back doors users (espionage). Integrating new technologies are disruptive and make some equipment be retired because they cannot be upgraded anymore."* **(Respondent 1, 4/1/2025-Nairobi.)**

Respondent 14 who is a scholar speaks on the vice that impedes best practices when adopting emerging technologies as follows:

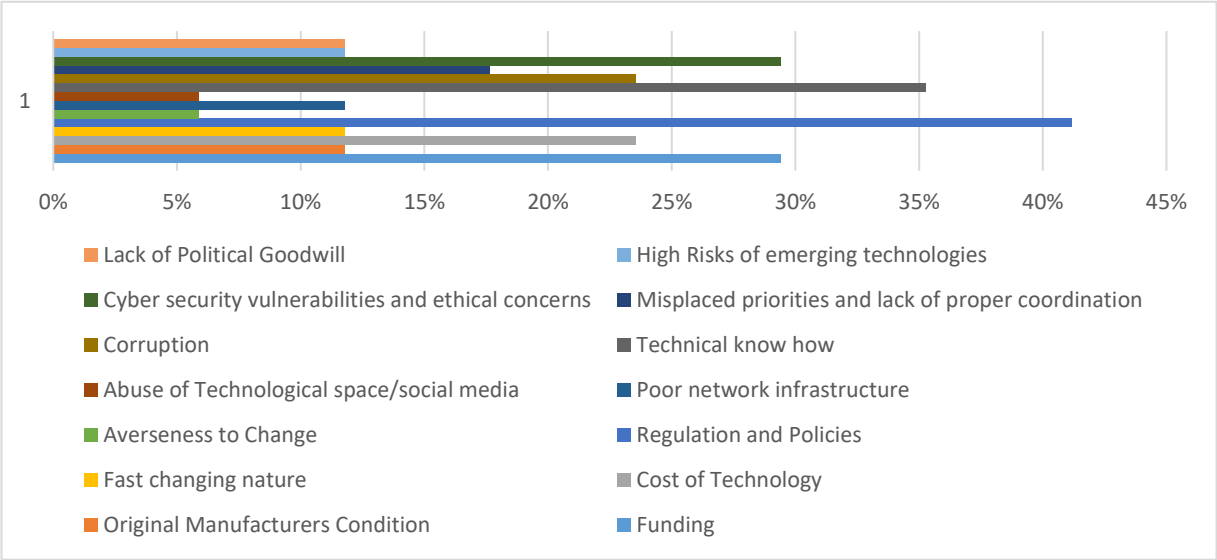
"Corruption is the main obstacle meaning the right people or policies will not go through or recruited. The national vice is a threat to national security making it hard to deal with the internal threats i.e corrupt decision makers, ignorance on what technology to adopt and who to partner or do the business with the state." **(Respondent 14, 4/9/2025-Nairobi)**

In the recent discussions, the military has acknowledged the need to develop a comprehensive framework to navigate the emerging technological world, as said by Chief of Defence Forces of Kenya, "Developing a comprehensive regulatory framework that governs the use of AI in military operations is essential. Building local capabilities to develop, deploy and regulate AI is crucial. These frameworks should address issues such as data privacy, security and ethical use. Policymakers must work closely with technologies, ethicists and military experts to create policies that balance innovation with responsibility." (*RESPONSIBLE AI IN THE MILITARY DOMAIN – Ministry of Defence – Kenya*, 2024)

Figure 4.11 below highlights the key challenges Kenya faces in adopting emerging technologies for security purposes. Seven out of seventeen respondents (41.2%) cited funding as the most important issue, while six respondents (35.3%) cited technical know-how. These results imply that the largest barriers to technology adoption in the security industry are limited technical expertise and financial constraints. Five respondents (29.4%) mentioned cybersecurity vulnerabilities, ethical issues, and corruption as additional noteworthy concerns. These issues highlight enduring structural and governance problems that impede safe and efficient tech integration.

Additional obstacles include the cost of technology and the conditions of original manufacturers, which were mentioned by four respondents (23.5%). Absence of political will, the high risks associated with emerging technologies, the misuse of social media and regulations and policies, all of which were mentioned three times (17.6%). Two respondents (11.8%) mentioned aversion to change, poor network infrastructure, misaligned priorities and lack of coordination, and the rapidly evolving nature of technology, all of which are less common but still important.

Figure 4.11: Some of the Primary Challenges Kenya Faces in Adopting Emerging Technologies for Security Purposes



These findings highlight how difficult it is to adopt technology in Kenya's security environment, where institutional, financial, ethical, and infrastructure factors interact to influence results. The respondents answered the question leading to these findings as follows; "5. What are some of the primary challenges Kenya faces in adopting emerging technologies for security purposes?"

> *"There is both increased interaction between the two sectors- civil sector report information faster while military sector take action. Information exchange and or complaint raising channel and action has improved. Quick relay of information has demanded accountability, while information leakages has led to constantly declassification of otherwise confidential information."* **(Respondent 4, 4/2/2025-Nairobi)**

> *"First, there has been increased KDF involvement in internal security operations in the North Rift areas of Kenya, Gen Z protests in 2024 and terror attacks response. Second, political dynamics and civilian oversight where there has been increased calls for accountability. Thirdly, increased involvement in unrelated security projects – stadium constructions and aid support."* **(Respondent 9, 4/4/2025-Nairobi)**

4.4.4 Conclusion – The Extent to which Emerging Technologies have Affected these Relations Since the Adoption of the 2010 Constitution

Respondents highlighted the increasing role of technology in proactive, data-driven surveillance, counterterrorism, and predictive policing initiatives, which can breed mistrust when transparency is lacking. Concerns regarding corruption in hiring and policymaking were voiced by a number of participants, as this compromises public trust and operational integrity. Furthermore, the widespread use of these platforms has increased scrutiny of the use of state power, especially in situations where civilian oversight is thought to be inadequate.

Emerging technologies have increased intelligence gathering, increased operational efficiency, strengthened border security and overall national security. However, they have also revealed regulatory framework flaws, which has prompted ethical concerns regarding data privacy, human rights, and surveillance. This means that the integration of strong technologies without strong accountability mechanisms runs the risk of upsetting the post-2010 constitutional order's goal of promoting civilian oversight and democratic control of the military.

The nature of civil-military relations according to the findings have been deeply impacted by the application and use of emerging technologies for military operations. Similarly, some of these technologies are also applicable in civilian use, making it harder to distinguish between military and civilian domains. This integration of emerging technologies is poised to reshape civil-military relations, introducing new complexities, pressures, and potential points of friction across various domains and operational contexts (*The Civil-Military Implications of Emerging Technology*, 2021).

On the role of emerging technologies on civil-military relations, the respondents noted the rise in both cooperation and tensions between military and civilian sectors. The results demonstrate how new technologies are becoming more and more important to military operations, improving surveillance, intelligence collection, predictive policing, and counterterrorism initiatives. Respondents underlined that defense mechanisms have evolved into more proactive, tech-driven strategies due to the availability of data and the capacity to analyze it instantly. Although they help the military in its operations, emerging technologies also cause discomfort in civilian

spaces, especially when there is no adequate oversight and transparency in their deployment.

Other key challenge mentioned by respondents include corruption affecting policymaking and recruitment, a crucial step in ensuring the personnel recruited in the military are competent enough to maintain national security while upholding human rights which is at the heart of civil-military relations. Additionally, concerns raised by the respondents speak to technological immaturity and fairness, which further complicate the use of emerging technologies in military operations. Collectively, these issues may contribute to strained civil-military where institutional weaknesses in terms of regulation frameworks and ethical concerns impede trust and cooperation.

4.4.5. The effects of emerging technologies on Kenya's national security.

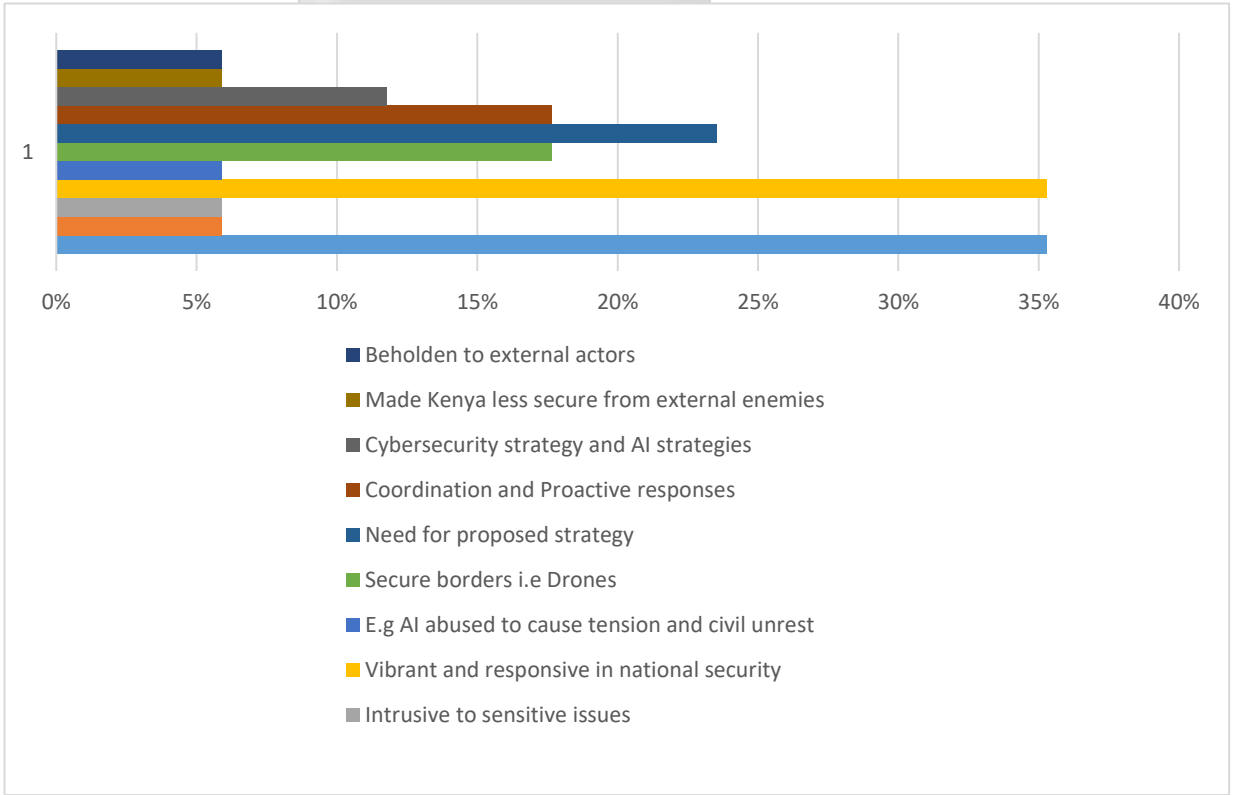
The main findings under objective 3 according to the data collected for this study, the state's capacity to monitor, identify, and react to internal and external threats has been significantly improved by emerging technologies like AI-driven surveillance, drone deployments, biometric systems, and social media platforms. Kenya's national security has been strengthened through operational precision, interagency cooperation, accelerated response times, and minimized personnel loss. Cases like the border monitoring between Kenya and Somalia where drones are used to track terrorists, for example, show how these instruments have enhanced territorial security. However an intentional effort by the the military to work with civilian institutions not only to win the public's trust, but to balance the blurring line in the dual use technologies is a necessary tool for their success.

Figure 4.12 below illustrates varied perspectives on how emerging technologies are shaping Kenya's national security strategy. The two most frequently mentioned effects, according to 6 out of 17 respondents (35.3%), were that new technologies have made national security more dynamic and responsive, but they also raise concerns over privacy and surveillance. This reveals a conflicting view of adopting emerging technologies, both for civil and military use. Four more respondents (23.5%) underlined the necessity of a well-defined national strategy to guide the development and use of emerging technologies. Furthermore, three respondents (17.6%) reported enhanced coordination and proactive responses. Same number of respondents, three,

acknowledged their role in border security, including the use of drone technology to track and combat terrorists.

Conversely, fewer people paid attention to possible hazards. Two respondents (11.8%) emphasized the significance of putting robust cybersecurity and artificial intelligence strategies into place, while two more respondents (11.8%) thought that new technologies had actually made Kenya less safe from outside threats. Concerns about foreign technological dependencies were reflected in the fact that only one respondent (5.9%) expressed concern that Kenya is becoming more dependent and beholden to external parties, especially when there is need to develop technological independence. In a similar vein, one respondent (5.9%) said that the misuse of AI would cause civil unrest.

Figure 4.12: Impact Emerging Technologies have on Kenya's Overall National Security Strategy



These findings underscore the urgency of designing a comprehensive, locally grounded national security and AI strategy that balances innovation with national interests. Respondent 1, from the Ministry of Defence support the enhancement in national security as follows: "11. What impact have emerging technologies had on Kenya's overall national security strategy?"

"Both enhanced such as reconnaissance and surveillance, navigation, enhanced ranges, ease in communications and reduced collateral damages because of improved precision." The respondent opines that critical cases have been successful in security operations due to the use of emerging technologies. *"Location of hostile agents and asymmetric agents in Boni Forest and Somalia. Surveillance and location of cattle rustlers in North Rift."(***Respondent 1, 4/1/2025- Nairobi)**

Respondent 3, an intelligence analyst add into the question as follows,

"In some areas it has strengthened like the use of drones to surveil militant territory in other cases like AI, its use has been abused and led to tensions and eruptions of civil unrest." **(Respondent 3, 4/2/2025-Nairobi)**

On the same breadth, Respondent 1 from the Ministry of Defence shares that technology has increased risks to the national security as follows:

"*However, there are threats in that some technologies have been intrusive and safeguards to sensitive issues have been challenged."* **(Respondent 1, 4/1/2025- Nairobi)**

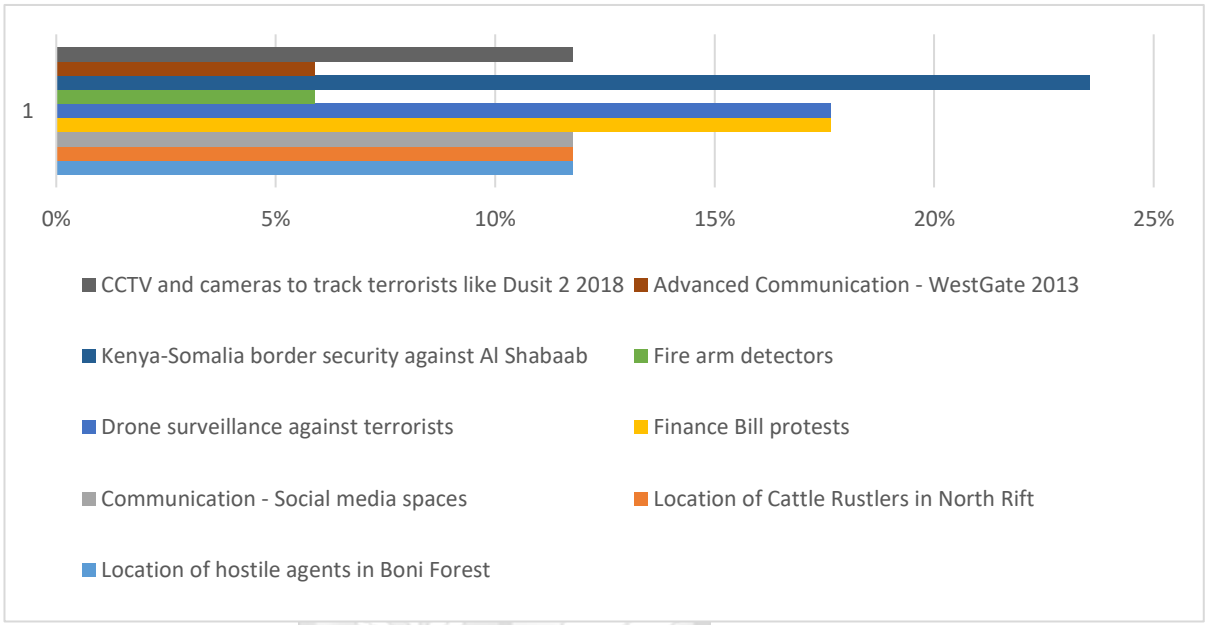
The rapid adoption of emerging technologies in the national security operations has opened new avenues of vulnerabilities to respective government ministries. As Respondent 8, a cybersecurity advisor and consultant observes,

"surveillance and privacy concerns, cybersecurity threats are among the biggest risks." (**Respondent 8, 4/3/2025-Nairobi**.)

According to Figure 4.13 below, the use of technology to improve border security between Kenya and Somalia against Al-Shabaab was the most noteworthy example, as reported by four (23.5%) of respondents. Their feedback demonstrate the strategic importance of surveillance and monitoring in reducing the threat of terrorism especially using drones and cyber space. Additionally, the growing role of technology in counterterrorism and civil unrest management is reflected in the responses of three participants each (17.6%) share of both drone surveillance against terrorists and technological support during the Finance Bill protests in 2024, another indicator of

technological application in civilian spaces. The use of cameras and CCTV during the Dusit D2 2018 attack, social media communication in security context, and advanced communication during the West Gate 2013 attack, spotting cattle rustlers in North Rift mentioned by one of the responders (5.9%) were other noteworthy mentions.

Figure 4.13: Specific Cases where Technology Played a Critical Role in a National Security Situation



Respondent 7 from the Ministry of Interior and Administration puts it as follows, when asked the question, "12. Can you identify any specific cases where technology played a critical role in a national security situation?"

> *"One specific case where technology played a critical role was during the Westgate Mall attack in 2013, where Kenya's security forces utilized advanced communication and surveillance technologies to coordinate the rescue operation and neutralize the attackers. Additionally, drones and AI-powered intelligence systems have been instrumental in Kenya's ongoing efforts to combat Al-Shabaab along the Somalia border,"* **(Respondent 7, 4/2/2025 – Nairobi)**

Respondent 1 from the Ministry of Defence shares similar sentiments as follows,

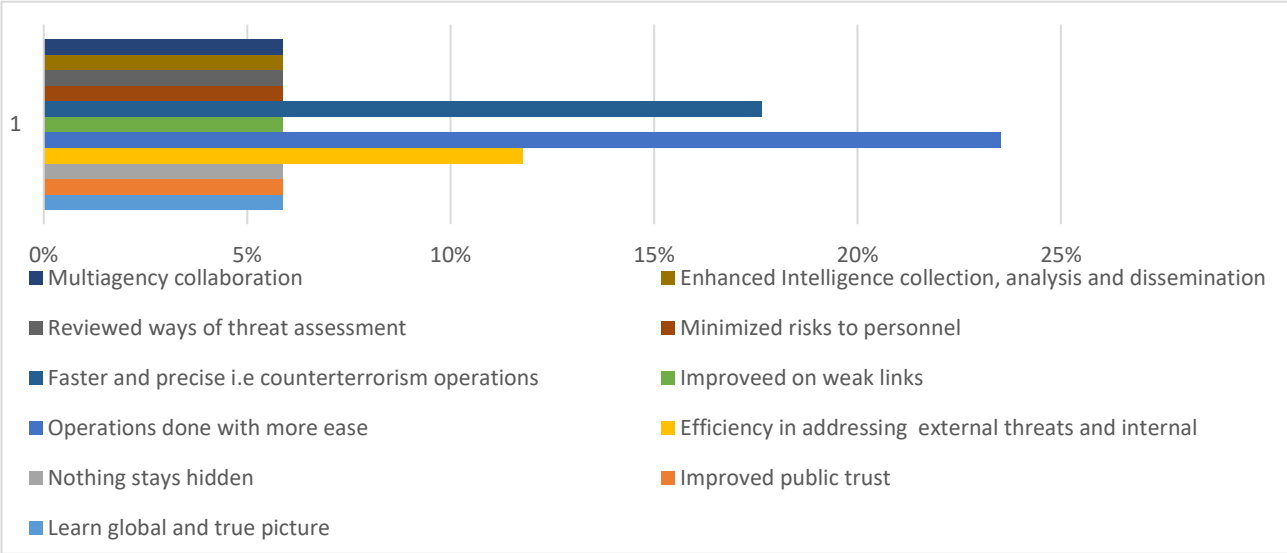
> *"Location of hostile agents and asymmetric agents in Boni Forest and Somalia. Surveillance and location of cattle rustlers in North Rift,"* **(Respondent 1, 4/1/2025 – Nairobi.)**

Conversely, respondent 9 from National Computer and Cyber Crime mentions the adverse threats emerging technologies can have to national security in the following ways,

> *"Yes. During the Gen Z protests. AI and related Social media technologies used extensively to undermine both state authority and national security,"* **(Respondent 9, 4/4/2025-Nairobi.)**

When analyzing the impact of technologies in addressing both internal and external threats, the improvement of intelligence gathering, analysis, and distribution is the most important according to four (23.5%) of respondents according to figure 4.14 below. This highlight the vital role that timely, accurate data plays in strategic decision-making especially where time is of essence. Improved speed and accuracy in counterterrorism operations with three (17.6%) respondents opining come in second, indicating that technology is simplifying tactical effectiveness, while preserving lives. Technology also promotes coordination and responsiveness among security forces, as evidenced by increased efficiency in addressing threats and multiagency collaboration as mentioned by two respondents each (11.8%). Additional noteworthy outcomes are enhanced public trust, and decreased personnel risks 5.9% each, with a better comprehension of the global security environment.

Figure 4.14: How these Technologies Affected the Way the Military Addresses Internal or External Threats



Respondent 7's from the Ministry of Defence take on this when asked the question, "13. How have these technologies affected the way the military addresses internal or external threats?"

> *"These technologies have revolutionized how the military addresses both internal and external threats by enabling more precise intelligence gathering, surveillance, and targeted strikes, especially in counterterrorism operations. Drones, AI, and cybersecurity measures allow for faster decision-making, reducing response time in high-stakes situations while minimizing risks to personnel."* **(Respondent 7, 4/2/2025 – Nairobi)**

Respondents 12 and 13 from BBC monitoring share close to similar sentiments, respectively

> *"These technologies have helped the military respond to threats faster and more accurately. Tools like drones, surveillance cameras, and phone tracking make it easier to monitor dangerous areas, gather information, and take action before things get worse."* **(Respondent 12, 4/8/2025-Nairobi)**

"*Emerging technologies offer innovative solutions with increased accuracy, reliability and efficiency in identification and managing internal and external threats. For instance, AI and drone technologies provide effective solutions to monitor the borders."***(Respondent 13, 4/9/2025-Nairobi.)**

4.4.6 Conclusion - The Effects of Emerging Technologies on National Security.

Technologies used to monitor social media or manage protests such as during the Finance Bill demonstrations in 2024, have raised concerns over human rights and the militarization of civilian governance. These tensions suggest that the benefits of technological integration are conditional on how they are perceived and governed. A militarized response or continued involvement of the military in civilian issues using emerging technologies, risks alienating the population and weakening the social contract that underpins democratic governance.

Emerging technologies are not neutral, they are shaped by how the civil-military relations evolve. The success in national security of Kenya would be achieved if these technologies are used in a collaborative, transparent and constitutional dictates as opined by the respondents. Circumventing the legal and ethical frameworks when deploying these technologies may cause distrust and exacerbate civil-military tensions, which may directly affect national security. It is therefore important to note from the findings that strength of emerging technologies lies not just in their technical capabilities, but in the strength of civil-military engagement and legitimacy that they are built on.

4.5 Triangulation

To enhance the validity of the findings, this study employed methodological triangulation by integrating qualitative interviews, structured questionnaires, and secondary document analysis. Respondents were drawn from diverse sectors of the military and intelligence personnel, civilian policy experts, and technology practitioners with postgraduate level of education, allowing for cross-validation of perspectives on how emerging technologies have influenced civil-military relations in Kenya and implications for national security. The use of in-depth interviews provided nuanced insights into themes such as blurred roles, ethical dilemmas, and

accountability challenges, while the structured questionnaires offered quantifiable data to support these observations. Additionally, secondary sources, including government reports, national security strategies and reports, academic literature were used to contextualize the primary data.

Theoretical Lenses

Agency Theory highlights the role of the civilian choosing or creating an agency to carry out specialized tasks for the state. This research highlights power shifts in decision making due to increased role of emerging technology in security operations like surveillance and intelligence gathering where AI featuring. Moreover, the military's access to sophisticated surveillance tools has increased their autonomy in security operations, which as respondents observe raises question of accountability. These instances happen in scenarios where privacy and rights of civilians are not upheld.

Critical Theory of Technology captures emerging questions of power and ethical use of technology in security operations. This follows that technology centralization in state security raises privacy, accountability, and ethical concerns. *"If misused, emerging technologies can cause social disharmony and undermine democratic governance,"* Respondent 5, from the Ministry of Defence warned.

Chapter Five: Summary, Recommendations and Policy Implications

5.1 Introduction

Emerging technologies such as artificial intelligence, surveillance systems, drones, autonomous weapons, and social media and cyber tools have fundamentally changed the dynamics of civil-military interactions, according to the study. Tensions are generating around control, oversight, and responsibility, especially on ethical use, human rights and efficiency. Moreover, these technologies have enabled civilian authorities as well as the military in varying and disruptive ways.

Although Kenya's constitutional framework gives civilian control over military institutions, in reality tensions remain high because of legal framework gaps, poor policy execution, and fast technology developments that are surpassing control. This affects operational effectiveness, and strategic decision making matters national security from local and international lenses.

While these technologies have enhanced surveillance and threat response, the study also found that they have created vulnerabilities especially in cyberspace and social media, presenting fresh ethical and legal conundrums. The dual-use technologies are blurring boundaries between civilian and military spheres, so generating tensions and operational overlaps. The use of artificial intelligence has exacerbated these impacts especially with the rapid evolution in ways that Kenya is not catching up.

5.2 Summary of the Findings

The Key findings under this study are as follows:

5.2.1 The History of Civil-Military Relations in Kenya, Since 2010

Since the 2010 Constitution was enacted, Kenya's civil-military relations have grown more dynamic and significant, according to the findings under Objective 1. Although cooperation has improved, especially in the areas of crisis response, infrastructure development, and multi-agency coordination, worries about overreach and blurred boundaries have been raised by the military's growing presence in civilian roles. This increasing presence is demonstrated by well-known instances like the military's participation in infrastructure projects, the Nairobi Metropolitan Services (NMS), and

internal security operations during occasions like the Gen Z protests. Respondents were concerned that the military's involvement in administrative and economic duties could politicize the organization and erode democratic accountability. The delicate and frequently disputed balance between maintaining civilian oversight and operational effectiveness is reflected in this changing relationship.

This complexity is further highlighted by public perception. There is still considerable concern about surveillance, the possible misuse of power, and the militarization of public life, despite the fact that many civilians see the military's use of emerging technologies as a force for better responsiveness and national security. According to the Afrobarometer data, Kenyans are adamantly opposed to military rule and strongly favor democratic civilian governance, even though they may accept the military's role in emergency response and national security.

5.2.2 How Emerging Technologies have Influenced Civil-Military Relations in Kenya Since the Adoption of 2010 Constitution

In addition to increasing military effectiveness, emerging technologies have given civilians and civilian-led institutions more influence over national security. As argued by Critical theory of technology that technological systems reflect the sociopolitical structures in which they function, concerns around privacy, human rights, and the militarization of public space were raised by respondents, in as much as they value the national security imperative. Conversely, as opined by Agency theory, the military could take decision-making authority away from elected civilian leaders as they gain insights from advanced technologies like data-driven decision-making.

According to the study, the traditional lines separating the military and civilian spheres have become less distinct due to the dual-use nature of many technologies. The findings point that civilian organizations are essential to military operations, particularly in the areas of data analytics, cybersecurity, and public surveillance. Hierarchical control, which is synonymous with the military, is made more difficult as there is increased technological interdependence.

Critical theory hence shows that if emerging technologies are not developed or regulated inclusively, they may serve to strengthen existing power structures. From the standpoint of agency theory, the principal-agent dynamics have been rebalanced

by emerging technologies where decision making capabilities by civilians may be taken away as military continues to depend on machine, enabled decision making. The dual-use of emerging technologies have blurred the line between the military and civilian sectors, especially in cases where military operations depend heavily on civilian organizations. This is evident when government ministries and technological companies, take lead in assisting particularly in the areas of cybersecurity, data analytics, and public surveillance.

5.2.3 The National Security Implications to Kenya Because of Evolving Civil-Military Relations Due to Emerging Technologies

The opportunities and risks availed by use of emerging technologies are staggering and must not be ignored especially in the face of national security. On one hand, emerging technologies have enhanced Kenya's national security, resulting in more aggressive border security and counterterrorism measures through predictive analysis and AI-powered surveillance, among others. However, the study discovered that these same tools may be used to compromise civil liberties and creating public mistrust. This may in turn compromise internal security, if there is no sufficient checks and balances leading to overall threat to national security.

Despite their necessity, military cybersecurity operations frequently lack transparency, which raise concerns about the militarization of digital infrastructure in a moment where there is increased integration of emerging technologies in civilian and government services. Additionally, the study highlights the growing use of military surveillance in public spaces like during public protests, which could exacerbate social unrest and undermine democratic systems.

Critical theory of technology cautions against this blind adoption of technology, which may strengthen coercive state power under the pretense of security. Similarly, according to agency theory, unbridled military actors' autonomy in tech domains could lead to overreach, jeopardizing the democratic balance. Moreover, Kenya’s responses are made more difficult by the democratization of technology, which has given non-state actors like Al-Shabaab more power through access to emerging technologies. With the adjustment of both civilian and military sectors in the new environment created by emerging technologies becoming a more significant factor in Kenya's

national security, the findings direct towards a human rights approach and proper regulatory frameworks to technological adoption.

5.3 Recommendations

Strengthen Capacity and Institutional Integrity

Investing in capacity building through training and equipping both military and civilian institutions to ensure effective adoption and ethical use of emerging technologies. This must consider strong anti-corruption measures to enhance professionalism, accountability, and public trust especially in acquisition of new technologies.

Promote Collaborative Research and Innovation

Enhancing partnerships between government, universities, and technology companies can support localized research and development. This will not only reduce dependency on external actors in our national security, but also ensure that we have context-specific technologies that align with the national interests.

Establish Ethical and Regulatory Frameworks

Developing clear, responsible, and enforceable regulatory frameworks is critical for guiding the development and deployment of emerging technologies. These frameworks should uphold democratic values, protect civil liberties, and define the increasingly blurring boundaries of military and civilian roles in national security.

5.4 Policy Contribution of Study

One of the few analyses of Kenya that looks at how emerging technologies like artificial intelligence, drones, surveillance systems, social media and cybersecurity tools are changing civil-military relations within the framework of a constitutional democracy. The study provides crucial contextual insight into the changing nature of that relationship. It fills a significant gap or contribute to the region's scholarly literature and policy discussions.

These findings give policymakers a solid foundation on which to build ethically sound and responsive frameworks that take into account the realities of Kenya's changing

civil-military. This is timely when digital surveillance, cyber threats, and AI-driven technological capabilities are the current concerns. Shedding light to the existing tensions between the military, security agencies and civilians is a relevant contribution to the field of study and policy.

5.5 Areas of Further Research Gaps

In relation to this study, future research study would benefit from comparative regional study that may compare Kenya's experience with emerging technologies in civil-military relations compares to that of other African states or regions, particularly those lacking robust constitutional frameworks.

Lastly, a potential gap for future research is the role of private technology companies and foreign actors in shaping Kenya's national security and general security infrastructure. With most of emerging technologies adopted and deployed in Kenya foreign based, exploring the implications on issues like digital sovereignty, and ethical implications would shed light on the geopolitical and economic influences that drive technological adoption.

References

Afrobarometer. (2025, April 16). https://www.afrobarometer.org/online-data-analysis/

Andrew, J. B. F., & Henry, W. W. P. (2015, February 10). *Supporting thinking on sample sizes for thematic analyses: A quantitative tool*. Taylor and Francis. https://www.tandfonline.com/doi/full/10.1080/13645579.2015.1005453?utm_source=chatgpt.com#d1e304

Artificial Intelligence and its impact on peace, security and governance – Amani Africa. (2025, March 19). https://amaniafrica-et.org/artificial-intelligence-and-its-impact-on-peace-security-and-governance/

Barnabas, O. (2024, August 14). *THE APPLICATION OF CYBER IN KENYAN PROTESTS: AN ANALYSIS*. LinkedIn. https://www.linkedin.com/pulse/application-cyber-kenyan-protests-analysis-barnabas-owuor-lvuue

Bhat, A. (2018, August 1). Snowball Sampling: Definition, Method, Pros & Cons. *QuestionPro*. https://www.questionpro.com/blog/snowball-sampling/

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

Braun, V., & Clarke, V. (2013). *Successful Qualitative Research A Practical Guide for Beginners. SAGE Publication, London. - References—Scientific Research Publishing*. https://www.scirp.org/reference/referencespapers?referenceid=1623262

Customary IHL - IHL Databases—ICRC. (2024, September). https://ihl-databases.icrc.org/en/customary-ihl

Dawadi, S. (2020). Thematic Analysis Approach: A Step by Step Guide for ELT Research Practitioners. *Journal of NELTA*, *25*(1–2), 62–71. https://doi.org/10.3126/nelta.v25i1-2.49731

Feaver, P. (2009). *Armed Servants: Agency, Oversight, and Civil-Military Relations*. Harvard University Press.

Feaver, P. D. (1999). *CIVIL-MILITARY RELATIONS1 | Annual Reviews*. Annual Review of Political Science Volume 2,. https://www.annualreviews.org/content/journals/10.1146/annurev.polisci.2.1.211

Francis, J. J., Johnston, M., Robertson, & Liz Glidewell. (2009, October). *What is adequate sample size? Operationalising data saturation for theory-based interview studies*. Research Gate. https://www.researchgate.net/publication/41762423_What_is_adequate_sample_size_Operationalising_data_saturation_for_theory-based_interview_studies

Gagliardone, I. (2016). *The Politics of Technology in Africa: Communication, Development, and Nation-Building in Ethiopia*. Cambridge University Press. https://doi.org/10.1017/9781316823149

Gaub, F. (2016). *Civil-military relations: The basics* (Civil-Military Relations in the MENA:, pp. 9–12). European Union Institute for Security Studies (EUISS). https://www.jstor.org/stable/resrep06944.5

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Kenya AI Strategy 2025-2030 | Ministry of ICT and the Digital Economy. (2025, March 27). https://ict.go.ke/node/641

Kenya Law Reform Commission, (KLRC). (2024). *Constitution of Kenya*. https://www.klrc.go.ke/index.php/constitution-of-kenya/

Kirkpatrick, G. (2004). *Critical Technology: A Social Theory of Personal Computing*. https://doi.org/10.4324/9781351160643

Mahin Naderifar, Hamideh Goli, & Fereshteh Ghaljaie. (2017, September). *Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research*. ResearchGate. https://www.researchgate.net/publication/324590206_Snowball_Sampling_A_Purposeful_Method_of_Sampling_in_Qualitative_Research

Mohiddin, F., Susanto, H., & Ibrahim, F. (2021). Implications of Knowledge Management Adoption Within Higher Education Institutions: Business Process Reengineering Approach. In P. Ordóñez De Pablos, M. N. Almunawar, K. T. Chui, & M. Kaliannan (Eds.), *Advances in Educational Technologies and Instructional Design* (pp. 307–351). IGI Global. https://doi.org/10.4018/978-1-7998-7184-2.ch016

National Cybersecurity Strategy 2022 – 2027 | NC4. (2022, September 29). https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/

National Police Service Annual Report 2022. (n.d.). Retrieved May 20, 2025, from https://www.nationalpolice.go.ke/sites/default/files/2024-10/ANNUAL%20REPORT%202022%20A4%20SIZE.pdf

NC4—Protecting Kenya's Cyberpace. (2016, June 23). https://nc4.go.ke/

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods*. SAGE.

Pion-Berlin, D., Croissant, A., & Kuehn, D. (2024). *Chapter 1: Introduction to the Research Handbook on Civil–Military Relations*. https://www.elgaronline.com/edcollchap/book/9781800889842/book-part-9781800889842-7.xml

RESPONSIBLE AI IN THE MILITARY DOMAIN – Ministry of Defence – Kenya. (2024, June 11). https://www.mod.go.ke/news/responsible-ai-in-the-military-domain/

Rotolo, D., Hicks, D., & Martin, B. (2015). *What Is an Emerging Technology?* (SSRN Scholarly Paper No. 2564094). Social Science Research Network. https://doi.org/10.2139/ssrn.2564094

The AI Triad and What It Means for National Security Strategy. (2020, August). *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy/

The Civil-Military Implications of Emerging Technology. (2021, February). ResearchGate. https://www.researchgate.net/publication/347056718_The_Civil-Military_Implications_of_Emerging_Technology

The Computer Misuse and Cybercrimes Act 2018 | NC4. (2024, May 24). https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/

2023-24-Q3-Cyber-Security-Report.pdf. Retrieved August 30, 2024, from https://kecirt.go.ke/wp-content/uploads/2024/04/2023-24-Q3-Cyber-Security-Report.pdf

Abbate, J. (1999, January 1). *Inventing the Internet (Inside Technology)*. Goodreads. https://www.goodreads.com/book/show/753865.Inventing_the_Internet

Abend, G. (2008). The Meaning of 'Theory'*. *Sociological Theory*, *26*, 173–199. https://doi.org/10.1111/j.1467-9558.2008.00324.x

Aguilera, A. (2023, July 5). Drone Use by Violent Extremist Organisations in Africa: The Case of Al-Shabaab. *GNET*. https://gnet-research.org/2023/07/05/drone-use-by-violentextremist-organisations-in-africa-a-case-study-of-al-shabaab/

Alcala, R. T. P., & Jensen, E. T. (Eds.). (2019). Introduction: New Technologies and Warfare. In *The Impact of Emerging Technologies on the Law of Armed Conflict* (p. 0). Oxford

University Press. https://doi.org/10.1093/oso/9780190915322.002.0008

Alexander, D. E. (2014). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, *20*(3), 717–733. https://doi.org/10.1007/s11948-0139502-z

Allen, G. C. (2023). *Advanced Technology: Examining Threats to National Security*.

https://www.csis.org/analysis/advanced-technology-examining-threats-nationalsecurity

Allenby, B. (2013). The Implications of Emerging Technologies for Just War Theory. *Public Affairs Quarterly*, *27*(1), 49–67. https://www.jstor.org/stable/43574496

Bakhtawar, B. (2020). *An Introduction to Qualitative Research (Flick, U. (2014). An introduction to qualitative research. Sage.) Book Review for Academic Consultation*.

https://doi.org/10.13140/RG.2.2.11809.22887

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, *23*, 5–26.

Barkan, J. D. (2004, February). *Kenya after Moi*. https://www.jstor.org/stable/20033831

Beehner, L., & Maurer, D. (2021). Introduction. In L. Beehner, R. Brooks, & D. Maurer (Eds.), *Reconsidering American Civil-Military Relations: The Military, Society, Politics, and*

Modern War (p. 0). Oxford University Press. https://doi.org/10.1093/oso/9780197535493.003.0001

Berg, S., & Hofmann, J. (2021). Digital democracy. *Internet Policy Review*, *10*(4). https://policyreview.info/articles/analysis/digital-democracy

Biddle, S., & Zirkle, R. (1996). Technology, civil-military relations, and warfare in the developing world. *The Journal of Strategic Studies*. https://doi.org/10.1080/01402399608437634

Blanchette, J. (2020). *Ideological Security as National Security*.
https://www.csis.org/analysis/ideological-security-national-security Blas, S. N. (2018). *Social Media and the Arab Spring*.
Bonaci, T., Michael, K., Rivas, P., Robertson, L. J., & Zimmer, M. (2022). Emerging Technologies, Evolving Threats: Next-Generation Security Challenges. *IEEE Transactions on Technology and Society*, *3*(3), 155–162. https://doi.org/10.1109/TTS.2022.3202323
Boyatzis, R. E. (1998, April). *Transforming Qualitative Information*. SAGE Publications Inc.
https://us.sagepub.com/en-us/nam/transforming-qualitative-information/book7714 Braun, V., & Clarke, V. (2012). *Thematic analysis.* (pp. 57–71).
Brooks, R. (2018, November 26). *Technology and Future War Will Test U.S. Civil-Military Relations*. War on the Rocks. https://warontherocks.com/2018/11/technology-andfuture-war-will-test-u-s-civil-military-relations/
Buzan, B. (1983). *People, States, and Fear: The National Security Problem in International Relations*. University of North Carolina Press.
Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.
Celikates, R., & Flynn, J. (2023). Critical Theory (Frankfurt School). In E. N. Zalta & U.
Nodelman (Eds.), *The Stanford Encyclopedia of Philosophy* (Winter 2023). Metaphysics Research Lab, Stanford University.
https://plato.stanford.edu/archives/win2023/entries/critical-theory/
Csernatoni, R., & Martins, B. O. (2024). Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics*, *29*(3), 849–872. https://doi.org/10.1080/14650045.2023.2224235
Decalo, S. (1989). Modalities of Civil—Military Stability in Africa. *The Journal of Modern*
African Studies, *27*(4), 547–578.
https://www.jstor.org.ezproxy.library.strathmore.edu/stable/161109
Denning. (2015). *Joint-Force-Quarterly-Rethinking Cyber Deterrence*. https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewe

r.html?
file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fd
ocume nts%2F4367805%2FDorothy-Denning-Joint-Force-Quarterly-
Rethinking.pdf

Devanny, J., & Buchan, R. (2024, January 12). *South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/01/south-africas-cyber-strategyunder-ramaphosa-limited-progress-low-priority?lang=en

Dolinko, I., & Antebi, L. (2024). Embracing the Organized Mess: Defense AI in Israel. In H. Borchert, T. Schütz, & J. Verbovszky (Eds.), *The Very Long Game: 25 Case Studies on the Global State of Defense AI* (pp. 397–420). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-58649-1_18

Dudovskiy, J. (2024). *Exploratory Research*. Research-Methodology. https://researchmethodology.net/research-methodology/research-design/exploratory-research/

Eisenhardt, K. M. (1989, January). *Agency Theory: An Assessment and Review on JSTOR*. https://www.jstor.org/stable/258191

EU AI Act: First regulation on artificial intelligence. (2023, August 6). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/euai-act-first-regulation-on-artificial-intelligence

Feaver, P. D. (1999). *CIVIL-MILITARY RELATIONS1 | Annual Reviews*. Annual Review of

Political Science Volume 2,.

https://www.annualreviews.org/content/journals/10.1146/annurev.polisci.2.1.211

Feaver, P. D. (2021). *Civil--Military Relations in the United States: What Senior Leaders Need to Know (and Usually Don't)*.

Federal Foreign Office. (2023, June). *National Security Strategy adopted by the German Federal Cabinet*. German Federal Foreign Office. https://www.auswaertigesamt.de/en/aussenpolitik/themen/-/2601730

Felt, U., Fouche, R., Miller, C. A., & Smith-Doerr, L. (Eds.). (2016). *The Handbook of Science and Technology Studies, fourth edition* (4th edition). The MIT Press.

Frazer, J. (1995). Conceptualizing Civil-Military Relations during Democratic Transition.

Africa Today, *42*(1/2), 39–48. https://www.jstor.org.ezproxy.library.strathmore.edu/stable/4187029

Gaub, F. (2016). *Civil-military relations: The basics* (Civil-Military Relations in the MENA:, pp. 9–12). European Union Institute for Security Studies (EUISS). https://www.jstor.org/stable/resrep06944.5

Gervais, V. (2021). *Emerging technologies and the future of warfare*. Trends Research & advisory.

Gichohi, L. (2024, May 6). *Kenya Unveils National Emerging Technologies and AI Strategy Framework | KICTANet Think Tank*. https://www.kictanet.or.ke/kenya-unveilsnational-emerging-technologies-and-ai-strategy-framework/

Gitau, J. (2016). *Civil-military relations in an era of violent extremism: Policy options for the Kenya Defence Forces*. CHRIPS, Centre for Human Rights and Policy Studies.

Glanz, K., K. Rimer, B., & K. Viswanath. (2008, August 28). *Health Behavior and Health Education: Theory, Research, and Practice—Google Books*. https://books.google.co.ke/books/about/Health_Behavior_and_Health_Education.html?id=1xuGErZCfbsC&redir_esc=y

Gray, C. S. (2006). Technology as a Dynamic of Defence Transformation. *Defence Studies*, *6*(1), 26–51. https://doi.org/10.1080/14702430600838461

Grimes, S., & Feenberg, A. (2009). Rationalizing Play: A Critical Theory of Digital Gaming. *Inf. Soc.*, *25*, 105–118. https://doi.org/10.1080/01972240802701643

Grizold, A. (1994). The Concept of National Security in the Contemporary World. *International Journal on World Peace*, *11*(3), 37–53. https://www.jstor.org/stable/20751984

Heickerö, R. (2010). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. FOI, Swedish Defence Research Agency, Division of Defence Analysis.

House, T. W. (2022, October 12). *FACT SHEET: The Biden-Harris Administration's National Security Strategy*. The White House. https://www.whitehouse.gov/briefingroom/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrationsnational-security-strategy/

Hovik, S., & Giannoumis, G. A. (2022). Linkages Between Citizen Participation, Digital Technology, and Urban Development. In S. Hovik, G. A. Giannoumis, K. ReichbornKjennerud, J. M. Ruano, I. McShane, & S. Legard (Eds.), *Citizen Participation in the Information Society: Comparing Participatory Channels in Urban Development* (pp. 1–23). Springer International Publishing. https://doi.org/10.1007/978-3-030-999407_1

Huaxia. (2021, April 8). *Kenya unveils new weaponry factory—Xinhua | English.news.cn*. http://www.xinhuanet.com/english/africa/2021-04/08/c_139867631.htm

Human Rights Watch. (2008, July 28). *"All the men have gone" War crimes in Kenya's Mt. Elgon conflict—Kenya | ReliefWeb*. https://reliefweb.int/report/kenya/all-men-havegone-war-crimes-kenyas-mt-elgon-conflict

Huntington, S. P. (1957). *The Soldier and the State: The Theory and Politics of Civil–Military Relations*. Harvard University Press.

IDRC - International Development Research Centre. (2017, October 17). *Scholars from Asia and Africa exchange knowledge at CPR South Conference in Myanmar | IDRC - International Development Research Centre*. https://idrc-crdi.ca/en/research-inaction/scholars-asia-and-africa-exchange-knowledge-cpr-south-conference-myanmar

Jackson, D. J. R., McDowall, A., Mackenzie-Davey, K., & Whiting, R. (2018). *Principles of Applied Research Methods*. Sage.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

https://doi.org/10.1016/0304-405X(76)90026-X

Jörg, H., & Kalpokas, N. (2024). *Bias in Research | Types, Identifying & Avoiding*. ATLAS.Ti.

https://atlasti.com/guides/qualitative-research-guide-part-1/research-bias Kaldor, M. (2012). *New and Old Wars*. Stanford University Press.

Kamau, W. (2024, January 23). Cyber Attacks On Kenya's Critical Information Infrastructure Cause of Concern. *Talk Africa*. https://www.talkafrica.co.ke/cyber-attacks-on-kenyascritical-information-infrastructure-cause-of-concern/

Kaspersen, A. (2016, February 12). *Is technology blurring the lines between war and peace?* World Economic Forum. https://www.weforum.org/agenda/2016/02/is-technologyblurring-the-lines-between-war-and-peace/

Kenya Civil Aviation Authority. (2020, March). *Unmanned Aircraft Systems (Drones) | Kenya Civil Aviation Authority*. https://www.kcaa.or.ke/safety-security-oversight/unmannedaircraft-systems

Kenya Law Reform Commission, (KLRC). (2024). *Constitution of Kenya*.

https://www.klrc.go.ke/index.php/constitution-of-kenya/

Kivunja, C. (2018). Distinguishing between Theory, Theoretical Framework, and Conceptual Framework: A Systematic Review of Lessons from the Field. *International Journal of Higher Education*, *7*(6), 44–53. https://eric.ed.gov/?id=EJ1198682

Laksmana, E. A. (2017). Threats and civil–military relations: Explaining Singapore's "trickle down" military innovation. *Defense & Security Analysis*, *33*(4), 347–365. https://doi.org/10.1080/14751798.2017.1377369

Linney, C., & Xiaomin, T. (2024, May 15). *AI and autonomous weapons systems: The time for action is now*. Saferworld. https://www.saferworld-global.org/resources/news-andanalysis/post/1037-ai-and-autonomous-weapons-systems-the-time-for-action-is-now

Maren, M. P. (1987, May). *Kenya: The Dissolution of Democracy*.

https://www.jstor.org.ezproxy.library.strathmore.edu/stable/45315892

McCord, B., & Weinberg, Z. A. Y. (2020). *Center for International Security and Cooperation, Freeman Spogli Institute for International Studies, Stanford University*.

Meredith, M. (2013, January 1). *The State of Africa*.

https://www.perlego.com/book/778586/the-state-of-africa-a-history-of-the-continentsince-independence-pdf

Military Africa. (2020, January 23). Kenyan made weapons, the complete list. *Military Africa*. https://www.military.africa/2020/01/kenyan-made-weapons-the-complete-list/

Mitnick, B. M. (1975). *The Theory of Agency: A Framework* (SSRN Scholarly Paper 1021642). https://doi.org/10.2139/ssrn.1021642

Mordini, E. (2014, November 6). *Considering the Human Implications of New and Emerging Technologies in the Area of Human Security*. Science and Engineering Ethics. https://link.springer.com/article/10.1007/s11948-014-9555-7

Murray, W. R., & Millett, A. R. (1998). *Military Innovation in the Interwar Period*. Cambridge University Press.

Muthee, K., & 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 (IJSRP), 12*, 501.

https://doi.org/10.29322/IJSRP.12.05.2022.p12561

National Cybersecurity Strategy 2022 – 2027 | NC4. (2022, September 29).

https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/

National Defense University - Kenya. (2024, October 5). *ENHANCING NATIONAL SECURITY THROUGH INNOVATIVE INITIATIVES | National Defence University-*

Kenya. https://ndu.ac.ke/enhancing-national-security-through-innovative-initiatives

National Development Plan for the Period 1970-1974. (1970).

https://repository.kippra.or.ke/handle/123456789/1421

N'Diaye, B. (2002). How Not to Institutionalize Civilian Control: Kenya's Coup Prevention Strategies, 1964-1997. *Armed Forces & Society, 28*(4), 619–640. https://doi.org/10.1177/0095327X0202800406

Nyinguro, P. (1999). *UNITED STATES POLICY AND THE TRANSITION TO DEMOCRACY IN KENYA, 1990-1992*.

Odhiambo, E. O. S. (2021). The Origins and Evolution of Anglo-Kenyan Military Diplomatic Relations Since 1963. *Open Access Library Journal*, *8*(9), Article 9. https://doi.org/10.4236/oalib.1107801

OMCT. (2008, June 6). *Kenya: Military action against the sabaot land defence force in Mount…*. OMCT World Organisation Against Torture 2024.

https://www.omct.org/en/resources/urgent-interventions/kenya-military-actionagainst-the-sabaot-land-defence-force-in-mount-elgon-involves-serious-human-rightsviolations-against-civilians

Pantev, P. (Ed.). (2005). *Civil-military relations and democratic control of the security sector: A handbook for military officers, servicemen and servicewomen of the security and intelligence agencies and for civilian politicians and security experts*. ProCon Ltd.

Parliament of Kenya. (2020, March). *ADMINISTRATION & INTERNAL SECURITY | The Kenyan Parliament Website*. http://www.parliament.go.ke/the-nationalassembly/committees/12/administration-national-security

Pfaff, C. A. (2020, January 27). *The Ethics of Acquiring Disruptive Military Technologies*. Texas National Security Review. https://tnsr.org/2020/01/the-ethics-of-acquiringdisruptive-military-technologies/

Pion-Berlin, D., Croissant, A., & Kuehn, D. (2024). *Chapter 1: Introduction to the Research*

Handbook on Civil–Military Relations.

https://www.elgaronline.com/edcollchap/book/9781800889842/book-part9781800889842-7.xml

Ramo, S. (1989, November 1). National Security and Our Technology Edge. *Harvard Business Review*. https://hbr.org/1989/11/national-security-and-our-technology-edge

Razakamaharavo, V. T. (2021, August 24). Implications of Emerging Technologies on Peace and Security in Africa. *ACCORD*. https://www.accord.org.za/conflict-trends/implications-of-emerging-technologies-on-peace-and-security-in-africa/

Research, A. (2022, May 23). *Exploratory Research: Definition & How To Conduct This Research*. Anpar Research Ltd. https://www.anparresearchltd.com/post/exploratoryresearch

Reuven, N. (2023, July 4). The Shift in Technological Innovation from the Defense Sector to the Civilian Sector. *Begin-Sadat Center for Strategic Studies*.

https://besacenter.org/the-shift-in-technological-innovation-from-the-defense-sectorto-the-civilian-sector/

Richards, J. (2012). *A Guide to National Security: Threats, Responses and Strategies*. OUP Oxford.

Rosen, B. (2023, October 3). *AI and the Future of Drone Warfare: Risks and Recommendations*. Just Security. https://www.justsecurity.org/89033/ai-and-thefuture-of-drone-warfare-risks-and-recommendations/

Rotolo, D., Hicks, D., & Martin, B. (2015). What Is an Emerging Technology? *Research Policy, 44*, 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Shahow. (2022, April 8). *Kenya's Military Incursion into Somalia Ten Years On—The Elephant*. https://www.theelephant.info/analysis/2022/04/08/kenyas-militaryincursion-into-somalia-ten-years-on/

Slonopas, A. (2024, April 16). *What Is Cyber Warfare? Various Strategies for Preventing It.*

https://www.apu.apus.edu/area-of-study/information-technology/resources/what-iscyber-warfare/

Stewart, L. (2024). *What is Purposive Sampling? | Explanation, Uses, Pros & Cons*.

ATLAS.Ti. https://atlasti.com/research-hub/purposive-sampling

Thompson, L. B. (2020, October). *Breaking Defense*. Breaking Defense.

https://www.lexingtoninstitute.org/wp-content/uploads/2020/10/100820-WHY-U.S.-NATIONAL-SECURITY-REQUIRES-A-ROBUST-INNOVATIVETECHNOLOGY-SECTOR-002.pdf

Vaynman, J., & Volpe, T. A. (2023). Dual Use Deception: How Technology Shapes Cooperation in International Relations. *International Organization, 77*(3), 599–632. https://doi.org/10.1017/S0020818323000140

Wangari, N. (2023, November 8). In Africa's first 'safe city,' surveillance reigns. *Coda Story*. https://www.codastory.com/authoritarian-tech/africa-surveillance-china-magnum/

Ward, K. J. (2021, August 14). *Educating Senior Service College Students on Emerging and Disruptive Technologies*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2808080/educating-senior-service-college-students-on-emerging-anddisruptive

Yin, R. K. (1993). *Applications of Case Study Research*. SAGE Publications.

Appendices

Appendix I: Similarity Report

Page 1 of 118 - Cover Page

BARNABAS OWUOR

Final Dissertation.docx

Strathmore University (Main Account)

Document Details

Submission ID **trn:oid:::2945:278090468**

Submission Date

Apr 16, 2025, 7:30 PM GMT+3

Download Date

Apr 16, 2025, 7:39 PM GMT+3

File Name

Final Dissertation.docx

File Size

701.4 KB

97 Pages

28,324 Words

178,658 Characters

Page 1 of 118 - Cover Page

Page 2 of 118 - Integrity Overview

17% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

3 Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 5%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

1 % Internet sources
8% Publications
1 % Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Page 2 of 118 - Integrity Overview

Page 3 of 118 - Integrity Overview

Match Groups

3 Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 5%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

1 % Internet sources
8% Publications
1 % Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Interne	
vdoc.pub		< %
2	Interne	
ir-library.ku.ac.ke		< %
3	Interne	
hdl.handle.net		< %
4	Interne	
su-plus.strathmore.edu		< %
5	Interne	
www.coursehero.com		< %
6	Interne	
tnsr.org		< %
7	Submitted works	
Strathmore University on 2014-04-03		< %
8	Publication	
Florina Cristiana Matei, Carolyn Halladay, Thomas C. Bruneau. "The Routledge Ha...		< %
9	Interne	
link.springer.com		< %
1	Interne	
warontherocks.com		< %

Page 3 of 118 - Integrity Overview

Appendix II: Questions for Key Informants

Personal Background

Personal Background *(For Classification Purposes)*

Gender: □ Male □ Female

Educational level: □ Secondary □ Tertiary college □ Undergraduate □ Postgraduate □ Other (specify)

Organization and department: _____

Can you briefly describe your role and how it relates to national security and/or technology
policy?……
……

Understanding Emerging Technologies

1. What emerging technologies have had the most impact on national security in Kenya since 2010?
……
……

2. How would you describe the role of technologies like artificial intelligence, drones, or cybersecurity measures in shaping military operations?
……
……

3. In your opinion, how well-prepared are Kenya's civil and military sectors for the rapid evolution of technology?
……
……

4. What regulatory or ethical challenges does Kenya face in integrating emerging technologies within its military?

……

……

5. What are some of the primary challenges Kenya faces in adopting emerging technologies for security purposes?

……

……

6. Have there been any unintended consequences or risks associated with the adoption of these technologies?

……

……

Role of Technology in Civil-Military Relations

7. How has your organization been involved in integrating emerging technologies into national security operations?

   ……

   ……

8. What changes have you observed in civil-military relations over the past decade?

   ……

   ……

9. Are there specific technologies that have led to greater collaboration or tension between military and civilian institutions?

   ……

   ……

10. How do civilians perceive the military's use of advanced technologies in Kenya?

    ……

    ……

Impact of Emerging Technologies on National Security

11. What impact have emerging technologies had on Kenya's overall national security strategy?

    ……

12. Can you identify any specific cases where technology played a critical role in a national security situation?

    ……

13. How have these technologies affected the way the military addresses internal or external threats?

    ……
    ……

Recommendations & Additional Insights

14. What recommendations would you offer for improving the integration of technology within Kenya's national security framework?

    ……

15. Is there anything we haven't discussed that you think is important to understanding the role of emerging technologies in civil-military relations?

    ……

Appendix III: Consent Form for Key Informants

Date.....

Border Management and National Security Survey Form

The purpose of this form is to ask for your consent as a practitioner/policy maker/expert/author in the field of emerging technologies, civil-military relations and national security. The research aims to pursue the implications if emerging technologies on civil-military relations, and national security of Kenya. The information obtained will be confidential and we shall not divulge any personal information. No monetary compensation will be given for responses provided. The study does not foresee any major risks in providing the information and we are not going to ask for any personal information which can easily be traced back to the respondent. Feel free to respond or not to respond to information requested. The information will be destroyed once the specific data have been aggregated.

Respondent's Consent;

I ....., hereby □agree/ □don't agree (tick the appropriate box) that I am giving the feedback freely.

Full name.....

Contact Information .....

Signature.....

(In case you have further enquiries, you can reach out to the contact person below, who can provide more information about the Student-parental Engagement Survey.)

Researcher's Full Name: Barnabas Owuor

Contact: 0705486898

Appendix IV: NACOSTI Ethical Clearance

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **340615**

Date of Issue: **03/February/2025**

RESEARCH LICENSE

This is to Certify that Mr.. Barnabas Odhiambo Owuor of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: The Implications of Emerging Technologies on Civil Military Relations: A Case of Kenya's National Security Since 2010 for the period ending : 03/February/2026.

License No: **NACOSTI/P/25/415491**

340615

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix V: Institutional Ethics Clearance

Strathmore UNIVERSITY

20th January 2025

Mr Odhiambo Barnabas,
barnabas.owuor@strathmore.edu

Dear Mr Odhiambo,

RE: The Implications of Emerging Technologies on Civil Military Relations: A Case of Kenya's National Security Since 2010

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU-masters** proposal. Your application reference number is **SU-ISERC2457/24.** The approval period is from **20th January 2025 to 19th January 2026.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu