Humanities and Social Sciences
2024, Vol. 12, No. 4, pp. 80-90
https://doi.org/10.11648/j.hss.20241204.12

Research Article

Critical Analysis of Status of Counter-Terrorism Strategies in Manda, Lamu County, Kenya: A Multifaceted Examination of HUMINT and SIGINT

Kennedy Obumba Ogutu[1, *], **Fredrick Okeyo Nyagwara**[2]

[1]Department of Political Science and Public Administration, University of Nairobi, Nairobi, Kenya
[2]School of Security, Diplomacy and Peace Studies, Kenyatta University, Nairobi, Kenya

Abstract

This paper presents a critical analysis of counter-terrorism strategies in Kenya, with a specific focus on the multifaceted examination of Human Intelligence (HUMINT) and Signals Intelligence (SIGINT). The study employed a sequential explanatory mixed-methods research design integrates both qualitative and quantitative approaches to provide a thorough understanding of Kenya's efforts to combat terrorism. The target population of this study encompassed participants involved in counter-terrorism activities in Kenya. This included officers in security agencies such as the National Intelligence Service and the Kenya Defense Forces which formed our target population. A total of 93 officers participated. The respondents were drawn through purposive sampling. By addressing multiple levels of involvement, the paper provides a holistic view of counter-terrorism strategies and their impact. Quantitative data was collected through surveys administered to a representative sample of security personnel in the NIS and KDF. Qualitative data on the other hand was collected through interviews. Semi-structured interviews were done with key informants, such as heads of the National Intelligence Service and Kenya Defense Forces helped capture the nuanced perspectives on HUMINT and SIGINT. STATA and Statistical Package for Social Scences (SPSS) Software were used to analyze quantitative data from the survey. The statistical significance between the average expectations and average perceptions in both security agencies was analyzed using two-sample t-tests. Additionally, the significance of the gaps between the agencies was assessed with Hotelling's T-squared test at a 5% significance level. Pearson's correlation coefficients were also used to determine the strength and direction of the relationship between the independent variable (s) and the dependent variable. The study generally found that the indicators of the HUMINT strategy were effective in countering terrorism except for source penetration. Further, the study determined that all indicators of SIGINT strategy were ineffective in countering terrorism except for interception of communication and timely warnings.

Keywords

Counterterrorism, Human Intelligence (HUMINT), Signals Intelligence (SIGINT)

[*]Corresponding author: kenobumba@gmail.com (Kennedy Obumba Ogutu)

Received: 10 June 2024; **Accepted:** 3 July 2024; **Published:** 23 July 2024

1. Introduction

HUMINT includes collecting information from human sources, such as informants, diplomats and spies while SIGINT, on the other hand, is the collection and analysis of electronic communications, including radio signals, phone conversations, and internet traffic [3].

According to [1] HUMINT often referred to as the "oldest" form of intelligence collection, has a rich history in the United States that predates the nation's formal founding. Even before the United States became an independent nation, espionage played a crucial role in the American Revolution. Figures like Nathan Hale and Benjamin Tallmadge worked as early American spies, gathering information on British troop movements and activities [9]. The United States formally established its first centralized intelligence agency during World War II, known as the Office of Strategic Services (OSS). The OSS collected HUMINT on Axis powers and supported resistance movements in Europe and Asia. After World War II, the OSS was disbanded, and its functions were split between the Department of State and the Department of War (now the Department of Defense). The Central Intelligence Agency (CIA) was created in 1947 and played a significant role in developing HUMINT capabilities during the Cold War. The Cold War era saw intense competition between the United States and the Soviet Union. HUMINT was pivotal in collecting information about the Soviet Union's military capabilities, intentions, and espionage activities [3].

The U.S. intelligence community has had its share of successes and failures in HUMINT. Notable cases include the recruitment of Oleg Gordievsky, a high-ranking KGB officer turned double agent, and the Aldrich Ames espionage case, where a CIA officer was revealed as a Soviet mole [8]. In the post-Cold War era, HUMINT has evolved to meet new challenges, including counterterrorism, counterproliferation, and the monitoring of transnational criminal organizations. The United States has expanded its network of intelligence agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) and the Defense Intelligence Agency (DIA) to support HUMINT efforts [7].

The United States' involvement in World War I marked the birth of organized SIGINT efforts. The Army's Signal Intelligence Service (SIS) was established to intercept and decipher German communications. SIGINT played a critical role in World War II, with the United States and its allies intercepting and decrypting Axis communications. After the war, the National Security Agency (NSA) was created in 1952 to coordinate and consolidate SIGINT efforts. During the Cold War, SIGINT was a key tool in monitoring Soviet military activities and tracking the global spread of communism [16]. The United States and its Five Eyes partners (Australia, Canada, New Zealand, and the United Kingdom) cooperated extensively in SIGINT sharing and analysis. Advances in technology, particularly in the field of telecommunications, have transformed SIGINT. The NSA has been at the forefront of these developments, engaging in electronic eavesdropping and monitoring digital communications worldwide. The revelations by Edward Snowden in 2013 exposed the extent of NSA surveillance and raised significant privacy concerns. In recent years, there has been a growing debate about the balance between national security and individual privacy. Legal and policy frameworks have been established to govern SIGINT activities and ensure that they are conducted within the boundaries of the law and the Constitution [4].

Before Nigeria's independence in 1960, British colonial authorities employed HUMINT to gather information on various political, social, and economic aspects of the region [12]. This intelligence was used to maintain colonial control and address potential threats. After gaining independence, Nigeria established its intelligence agencies namely; the National Intelligence Agency (NIA) and the State Security Service (SSS) to conduct HUMINT operations [11]. These agencies focused on gathering information on domestic and international security issues. During periods of military rule in Nigeria, HUMINT was often used to monitor political dissidents, opposition groups, and potential threats to the government. These agencies were known for their role in suppressing dissent. In recent years, Nigeria has intensified its HUMINT efforts in the fight against terrorism, particularly against the Boko Haram insurgency in the northeastern part of the country. HUMINT sources have been crucial in identifying and tracking terrorist elements [12].

Nigeria began developing its SIGINT capabilities in the mid-20th century. The Nigerian Armed Forces and intelligence agencies, including the DIA, have been responsible for signals intelligence collection. Nigeria has engaged in regional cooperation with neighboring countries on SIGINT matters, especially in addressing cross-border security threats. Shared SIGINT intelligence has been vital in addressing issues like transnational crime and terrorism [6]. Like many other countries, Nigeria's SIGINT capabilities have evolved with advancements in technology. The Nigerian government has invested in modernizing its electronic surveillance and interception capabilities to monitor communications networks. As cybersecurity threats have grown, Nigeria has expanded its focus on electronic intelligence, including monitoring cyber threats and protecting critical information infrastructure [12].

During Kenya's colonial period under British rule, HUMINT was employed to gather information about local communities and political movements [2]. The colonial authorities relied on human sources to maintain control and manage potential challenges to their rule [13]. After gaining independence in 1963, Kenya established the Kenya Police Special Branch, responsible for domestic intelligence in 1969. In 1999, the Kenyan government restructured and rebranded its intelligence agencies. The National Security Intelligence Service (NSIS) was established as the primary domestic and

external intelligence agency responsible for safeguarding national security. Kenya adopted a new constitution in 2010, which brought significant changes to the intelligence landscape. The NSIS was reconstituted as the NIS, and its mandate was clearly defined in the Constitution of Kenya. This agency has focused on conducting HUMINT operations to gather information on various domestic and international security matters. Throughout Kenya's post-independence history, HUMINT has been used to monitor political dissent, opposition groups, and potential threats to the government. Intelligence agencies have been involved in addressing various domestic security challenges [14]. In recent years, Kenya has increased its HUMINT efforts in the fight against terrorism, particularly against Al-Shabaab and other extremist groups operating in the region [5]. Gathering intelligence from human sources has been crucial in identifying and countering terrorist elements.

Kenya began developing its SIGINT capabilities in the post-independence era. The country's intelligence and military agencies have been responsible for signals intelligence collection. Kenya has engaged in regional cooperation with neighboring countries on SIGINT matters to address cross-border security threats. Shared SIGINT intelligence has played a vital role in addressing issues like transnational crime and terrorism [15]. As technology has advanced, Kenya has invested in modernizing its electronic surveillance and interception capabilities. This includes monitoring communications networks, particularly in the context of addressing cybersecurity threats. The Kenyan government has expanded its focus on electronic intelligence, especially in the realm of cybersecurity. This involves monitoring and countering cyber threats while safeguarding critical information infrastructure [10].

2. Purpose and Objectives of the Study

The study aimed to do a critical analysis of the status of counter-terrorism strategies in Manda, Lamu County, Kenya focusing on a multifaceted examination of HUMINT and SIGINT. The study was guided by the following objectives:

1) To determine the officers' perceptions of the effectiveness of Human Intelligence (HUMINT) in Counter-Terrorism in Manda, Lamu County, Kenya.
2) To determine the officers' perceptions of the effectiveness of Signals Intelligence (SIGINT) in Counter-Terrorism in Manda, Lamu County, Kenya.

3. Research Hypotheses

1) H01: Human Intelligence (HUMINT) has no statistically significant effect on Counter-Terrorism in Manda, Lamu County, Kenya.
2) H02: Signals Intelligence (SIGINT) has no statistically significant effect on Counter-Terrorism in Manda, Lamu County, Kenya.

4. Methodology

The sequential explanatory mix methods research design was employed in this study. The study was conducted in Manda, Lamu County, Kenya. The target population was the officers in the NIS and KDF. The number of officers who participated was 93. The sample was selected through purposive sampling. The questionnaire used was researcher-administered. A structured questionnaire was used to obtain information from the officers while interview schedule guides were used to obtain information from the heads of NIS and KDF. The questionnaire was administered to 93 officers. Quantitative and qualitative techniques were used to analyze data. STATA and SPSS software were used to analyze quantitative data from the survey. The expectations and perceptions of counter-terrorism strategies were analyzed. This was achieved by identifying the gaps by getting the difference between expectations and perceptions. Statistical significance between the average perceptions and average expectations in both security agencies was examined using two-sample t-tests. Additionally, the significance of the gaps within the security agencies was assessed through Hotelling's T-squared test at a 5% significance level. Pearson's correlation coefficients were also used to determine the strength and direction of the relationship between the independent variable (s) and the dependent variable.

5. Results

The following questions and hypotheses were answered and tested respectively:

Status of Counter-Terrorism Strategies

Respondents were asked to fill out the questionnaires and indicate the expectations they have on particular counter-terrorism strategies and then indicate what they had experienced with them. HUMINT questions gauged different aspects relating to actionable intelligence, source penetration, source reliability, accuracy & validation, and operational impact while SIGINT questions gauged different aspects relating to intercepted communications/ Signal interception patterns, timely warnings, identification & location, terrorist network mapping and anomaly detection. All the respondents had experienced and/or utilized the two strategies and they all had certain expectations of the level of effectiveness.

To determine the officers' perceptions of the effectiveness of Human Intelligence (HUMINT) in Counter-Terrorism in Manda, Lamu County, Kenya

Actionable intelligence gauges the extent to which HUMINT provides information that leads to practical, successful actions or outcomes in counter-terrorism efforts. Among NIS officers, the average expectation score was 2.141, while the average perception score was 5.483 on a scale of 1 to 7 for actionable intelligence. KDF officers reported an average expectation score of 2.508 and an average perception score of 5.965. This indicates that both agencies

largely agree that actionable intelligence meets their expectations. The gap between expectations and perceptions was 3.342 for NIS and 3.457 for KDF regarding actionable intelligence. A T-test conducted in the security agencies revealed significant differences between expectations and perceptions, with NIS showing a T-test value of 29.920 and a p-value of 0.000, indicating a statistically significant difference between the means. Similarly, KDF had a T-test value of 21.204 with a p-value of 0.000, confirming the statistical significance of the difference between mean expectations and perceptions. Furthermore, a Hotelling's T-squared test was performed to compare the differences between expectations and perceptions across the two security agencies. The test yielded a T score of 2.728 with a p-value of 0.509, indicating no statistically significant difference between the agencies. This suggests that officers from both NIS and KDF similarly rate this aspect of HUMINT, believing that actionable intelligence has exceeded their expectations.

Source penetration looks at the number of successful human sources recruited and maintained, indicating the agency's ability to infiltrate or engage with target groups or individuals. Regarding source penetration, NIS officers had an average expectation score of 5.114 and an average perception score of 1.763 on a scale of 1 to 7, indicating a significant discrepancy. Similarly, KDF officers reported a mean expectation score of 5.173 and a mean perception score of 2.602, also showing a notable disagreement. The gap between how source penetration meets expectations was -3.351 for NIS officers and -2.571 for KDF officers. T-tests conducted in both security agencies revealed significant differences between expectations and perceptions. NIS recorded a T-test value of 36.481 with a p-value of 0.000, indicating a statistically significant difference between the means. KDF showed a T-test value of 11.025 with a p-value of 0.000, also confirming the statistical significance of the difference between mean expectations and perceptions. Additionally, a Hotelling's T-squared test was performed to determine if the difference between expectations and perceptions varied significantly between the two security agencies. The test yielded a T score of 13.878 with a p-value of 0.061, indicating that the differences were not statistically significant. This suggests that officers from both NIS and KDF rated source penetration similarly, although NIS officers expressed more negative perceptions.

Source reliability assesses the credibility and trustworthiness of human sources providing intelligence information. On source reliability, NIS respondents had an average expectation score of 2.949 and an average perception score of 5.996 on a scale of 1 to 7, while KDF officers reported a mean expectation score of 2.785 and a mean perception score of 5.714. These ratings are quite high for both agencies. The gap between expectations and perceptions regarding source reliability was 3.047 for NIS and 2.929 for KDF. T-tests conducted in both security agencies revealed significant differences between expectations and perceptions. NIS showed a T-test value of 35.330 with a p-value of 0.000, indicating a statistically significant difference between the means. Similarly, KDF had a T-test value of 20.411 with a p-value of 0.000, confirming the statistical significance of the difference between mean expectations and perceptions. Additionally, a Hotelling's T-squared test was performed to compare the differences between expectations and perceptions across the two security agencies. The test yielded a T score of 28.307 with a p-value of 0.087, indicating that the differences were not statistically significant. This suggests that officers from both NIS and KDF similarly rate source reliability, despite the differences in their mean scores. This shows that officers from both agencies had the same ratings on the source reliability with NIS showing more positive perceptions that the credibility and trustworthiness of human sources providing intelligence information was on point.

Accuracy and validation gauge the degree to which HUMINT reports are validated and corroborated by other sources, reducing the risk of misinformation. NIS respondents reported an average expectation score of 2.036 and an average perception score of 5.613 for accuracy and validation on a scale of 1 to 7. KDF officers had a mean expectation score of 2.651 and a mean perception score of 5.564. These scores indicate strong agreement that officers' expectations are being met. The gap between expectations and perceptions was 3.577 for NIS and 2.913 for KDF. T-tests conducted in both agencies revealed significant differences between expectations and perceptions. NIS showed a T-test value of 28.258 with a p-value of 0.000, indicating a statistically significant difference. Similarly, KDF had a T-test value of 26.442 with a p-value of 0.000, confirming the statistical significance of the difference between mean expectations and perceptions. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 2.054 with a p-value of 0.056, indicating that the differences were not statistically significant. This suggests that officers from both NIS and KDF rated accuracy and validation similarly i.e., the information provided by the intelligence sources could be validated and corroborated by other sources hence ameliorating the risk of misinformation.

Operational impact assesses the demonstrable impact of HUMINT on disrupting terrorist activities, arresting suspects, or dismantling networks. NIS respondents gave an average expectation score of 1.918 and an average perception score of 5.055 for operational impact on a scale of 1 to 7, indicating strong agreement. KDF officers reported a mean expectation score of 2.507 and a mean perception score of 5.974, also showing high approval. The gap between expectations and perceptions was 3.137 for NIS and 3.467 for KDF. T-tests conducted in both security agencies showed significant differences between expectations and perceptions. NIS had a T-test value of 32.493 with a p-value of 0.000, indicating a statistically significant difference, while KDF showed a T-test

value of 12.720 with a p-value of 0.000, also confirming the significance of the difference. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 11.987 with a p-value of 0.074, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated the operational impact similarly, with KDF respondents having slightly more positive perceptions.

Thus, the overall status of the counter-terrorism strategy of HUMINT indicates that NIS respondents had an average expectation score of 2.193 and an average perception score of 5.183 on a scale of 1 to 7. This demonstrates a strong agreement that officers' expectations have been met, reflecting high approval. KDF officers reported a mean expectation score of 2.549 and a mean perception score of 5.005, also indicating significant approval. The overall gap was 2.990 for NIS and 2.456 for KDF regarding how HUMINT meets their expectations. These similarities highlight the importance of HUMINT as a counter-terrorism strategy.

A T-test was conducted in both security agencies to determine if the general expectations and perceptions were significantly different. In NIS, a T-test value of 53.196 with a p-value of 0.000 indicated that the difference between the mean expectations and perceptions was statistically significant. Similarly, in KDF, a T-test value of 40.452 with a p-value of 0.000 also showed a significant difference. Additionally, a Hotelling's T-squared test was performed to see if the difference between expectations and perceptions was statistically different between the two agencies. The test yielded a T score of 10.693 with a p-value of 0.083, indicating that the differences were not statistically significant. This suggests that officers from both NIS and KDF rated the HUMINT strategy similarly, showing strong approval of its effectiveness in counter-terrorism efforts. They generally said that the strategy was aiding in countering terrorism as expected. The details are as presented in Table 1 below.

Table 1. *Participants Perceptions of Expectations, Gap scores, Corresponding T-test values, and Hotelling's T-square values of service quality in both security agencies.*

Security Agency	**National Intelligence Service (NIS)**				**Kenya Defense Forces (KDF)**				
Mean Measures	**Perception**	**Expectation**	**Gap(B) (P-E)**	**T-test (P & E)**	**Perception**	**Expectation**	**Gap(A) (P-E)**	**T-test (P&E)**	**Hoteling T sq. (B&A)**
Actionable Intelligence	5.483	2.142	3.542	29.920 0.000	5.965	2.508	3.457	21.204 0.000	2.728 P=0.509
Source Penetration	1.763	5.114	-3.351	36.487 0.000	2.602	5.173	-2.571	11.025 0.000	13.878 0.061
Source Reliability	5.996	2.949	3.047	35.330 0.000	5.714	2.785	2.929	20.411 0.000	28.307 0.000
Accuracy and Validation	5.613	2.036	3.577	28.258 0.000	5.564	2.651	2.913	26.442 0.000	2.054 0.056
Operational Impact	5.055	1.918	3.137	32.493 0.000	5.974	2.507	3.467	12.720 0.000	11.987 0.074
Overall Mean	5.183	2.193	2.990		5.005	2.549	2.456		Largely significant

Pearson's correlation coefficient was also done to corroborate the findings on whether HUMINT was effective in countering terrorism. Table 2 below gives the information.

Table 2. *Correlation of HUMINT Indicators and Countering Terrorism*

Indicators	**HUMINT**	**Countering terrorism**	**Pearson Correlation Coefficient Values**	**Sig. (2-tailed)**
Actionable intelligence			.846*	.000

Indicators	HUMINT	Countering terrorism	Pearson Correlation Coefficient Values	Sig. (2-tailed)
Source penetration			.084	.087
Source reliability			.653*	.021
Accuracy and validation			.889*	.002
Operational impact			.764*	.000

* - Means significant at 5% level

Table 2 indicates a statistically significant impact of all HUMINT indicators except source penetration on countering terrorism. This conclusion is supported by Pearson correlation coefficients of 0.846, 0.653, 0.889, and 0.764, all indicating strong positive correlations with P-values less than 0.05. These coefficients suggest that an increase in HUMINT indicators significantly enhances efforts in countering terrorism. Therefore, the null hypothesis (H_o), 'Human Intelligence (HUMINT) has no statistically significant effect in Counter-Terrorism in Manda, Lamu County, Kenya was therefore rejected.

In source penetration, however, the Pearson's correlation coefficient (r) of the two variables i.e., source penetration (SP) and countering terrorism was not significant at 5% level.

To determine the officers' perceptions of the effectiveness of Signals Intelligence (SIGINT) in Counter-Terrorism in Manda, Lamu County, Kenya

Intercepted communications/ Signal interception patterns, gauge the volume and relevance of intercepted electronic communications, indicating the extent of the agency's coverage and ability to monitor potential threats. NIS officers reported an average expectation score of 2.712 and an average perception score of 5.111 on a scale of 1 to 7 for intercepted communications. KDF officers had a mean expectation score of 2.172 and a mean perception score of 5.830. This indicates significant agreement within both agencies that their expectations regarding intercepted communications have been met. The difference between expectations and perceptions was 2.399 for NIS and 3.658 for KDF in relation to intercepted communications. T-tests conducted in both security agencies revealed significant differences between expectations and perceptions. NIS recorded a T-test value of 27.451 with a p-value of 0.000, showing a statistically significant difference. Similarly, KDF had a T-test value of 19.117 with a p-value of 0.000, confirming the statistical significance of the difference. Additionally, a Hotelling's T-squared test was performed to compare the differences between expectations and perceptions across the two security agencies for intercepted communications. The test yielded a T score of 3.106 with a p-value of 0.654, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated this dimension of SIGINT similarly; believing that intercepted communications exceeded their expectations.

Timely warnings look at the ability of SIGINT to provide timely warnings of impending terrorist activities, allowing for preventive actions. In terms of timely warnings, NIS officers had an average expectation score of 4.276 and an average perception score of 2.691 on a scale of 1 to 7, indicating significant agreement. Similarly, KDF officers reported a mean expectation score of 5.713 and a mean perception score of 3.200, also showing strong agreement. The gap was 1.585 for NIS and 2.513 for KDF regarding how timely warnings met officers' expectations. T-tests conducted in both security agencies revealed significant differences between expectations and perceptions. NIS recorded a T-test value of 30.341 with a p-value of 0.000, demonstrating a statistically significant difference. In KDF, a T-test value of 17.213 with a p-value of 0.000 was recorded, confirming the statistical significance of the difference. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 14.156 with a p-value of 0.092, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated timely warnings similarly, although KDF officers had more positive perceptions overall.

In terms of identification and location through SIGINT data, NIS respondents had an average expectation score of 5.312 and an average perception score of 2.675 on a scale of 1 to 7. KDF officers reported a mean expectation score of 5.791 and a mean perception score of 2.123. These ratings were notably low in both agencies. The difference between expectations and perceptions was -2.637 for NIS and -3.668 for KDF regarding how identification and location met officers' expectations. T-tests conducted in both security agencies showed significant differences between expectations and perceptions. NIS recorded a T-test value of 34.129 with a p-value of 0.000, indicating a statistically significant difference. Similarly, KDF had a T-test value of 18.223 with a p-value of 0.000, confirming the statistical significance of the difference. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 27.209 with a p-value of 0.053, indicating no statistically significant difference. This shows that officers from both agencies had the

same ratings on the identification & location with KDF showing more negative perceptions that the frequency of successfully identifying and locating high-value targets or key terrorist operatives through SIGINT data was not met.

Terrorist network mapping gauges the extent to which SIGINT contributes to mapping and understanding the structure and dynamics of terrorist networks, aiding in the development of strategies to disrupt them. For terrorist network mapping, NIS respondents had an average expectation score of 5.285 and an average perception score of 2.316 on a scale of 1 to 7. KDF officers reported a mean expectation score of 5.615 and a mean perception score of 2.018. These scores indicate significant disagreement regarding officers' expectations being met. The gap was -2.969 for NIS and -3.597 for KDF regarding how terrorist network mapping met officers' expectations. T-tests conducted in both agencies revealed significant differences between expectations and perceptions. NIS recorded a T-test value of 31.245 with a p-value of 0.000, indicating a statistically significant difference. Similarly, KDF had a T-test value of 27.242 with a p-value of 0.000, confirming the statistical significance of the difference. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 2.762 with a p-value of 0.064, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated terrorist network mapping similarly, despite the differences in their mean scores. Put simply, the extent to which SIGINT contributes to mapping and understanding the structure and dynamics of terrorist networks, aiding in the development of strategies to disrupt them was not being met.

Anomaly detection identifies irregular or unexpected signal patterns that may signify hidden activities or changes in the target's behavior. NIS respondents rated operational impact with an average expectation score of 5.869 and an average perception score of 2.918 on a scale of 1 to 7, indicating substantial disagreement. KDF officers reported a mean expectation score of 5.543 and a mean perception score of 2.142. The difference was -2.951 for NIS and -3.401 for KDF in terms of how operational impact met officers' expectations. T-tests conducted in both security agencies showed significant differences between expectations and perceptions. NIS had a T-test value of 35.876 with a p-value of 0.000, indicating a statistically significant difference. Similarly, KDF had a T-test value of 20.561 with a p-value of 0.000, confirming the statistical significance of the difference. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test yielded a T score of 17.984 with a p-value of 0.082, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated anomaly detection similarly, despite KDF respondents having more negative perceptions overall.

Therefore, the overall assessment of the counter-terrorism strategy of SIGINT indicates that among NIS respondents, there was an average expectation score of 5.319 and an average perception score of 2.450 on a scale of 1 to 7. This significant difference reflects a disagreement among officers that their expectations have been met, indicating low approval. Similarly, KDF officers reported a mean expectation score of 5.218 and a mean perception score of 2.682, also suggesting low approval. The overall difference was -2.869 for NIS and -2.536 for KDF in terms of how SIGINT met officers' expectations. These substantial differences highlight weaknesses in using SIGINT as a strategy for counter-terrorism efforts.

A T-test was conducted in both security agencies to assess whether the general expectations and perceptions differed significantly. In NIS, a T-test value of 40.961 with a p-value of 0.000 indicated a statistically significant difference between the mean of all expectations and perceptions. Similarly, in KDF, a T-test value of 45.817 with a p-value of 0.000 showed a significant difference between the mean expectations and perceptions. Additionally, a Hotelling's T-squared test was performed to determine if the differences between expectations and perceptions were statistically different between the two security agencies. The test resulted in a T score of 13.095 with a p-value of 0.062, indicating no statistically significant difference. This suggests that officers from both NIS and KDF rated SIGINT similarly, indicating that they did not approve of SIGINT as an effective counter-terrorism strategy. They generally said that the strategy was not aiding in countering terrorism as expected. The details are as presented in Table 3 below;

Table 3. *Participants' Perceptions of Expectations, Gap scores, Corresponding T-test values, and Hotelling's T-square values of service quality in both sub-counties.*

Security Agency	**National Intelligence Service (NIS)**				**Kenya Defense Forces (KDF)**				
Mean Measures	**Perce-Ption**	**Expect-Ation**	**Gap(B) (P-E)**	**T-test (P & E)**	**Perce-ption**	**Expect-Ation**	**Gap(A) (P-E)**	**T-test (P&E)**	**Hoteling T sq. (B&A)**
Intercepted communications	5.111	2.712	2.172	27.451 0.000	5.830	2.399	3.658	19.117 0.000	3.106 P=0.654

Security Agency	National Intelligence Service (NIS)				Kenya Defense Forces (KDF)				
Mean Measures	**Perce-Ption**	**Expect-Ation**	**Gap(B) (P-E)**	**T-test (P & E)**	**Perce-ption**	**Expect-Ation**	**Gap(A) (P-E)**	**T-test (P&E)**	**Hoteling T sq. (B&A)**
Timely warnings	4.276	2.691	1.585	30.341 0.000	5.713	3.200	2.513	17.213 0.000	14.156 0.092
Identification & location	2.675	5.312	-2.637	34.129 0.000	2.123	5.791	-3.668	18.223 0.000	27.209 0.053
Terrorist network mapping	2.316	5.285	-2.969	31.245 0.000	2.018	5.615	-3.597	27.242 0.000	2.762 0.064
Anomaly detec-tion	2.918	-2.951	5.869	35.876 0.000	2.142	-3.401	5.543	20.561 0.000	17.984 0.082
Overall Mean	2.450	-2.869	5.319		2.682	-2.536	5.218		Largely signif-icant

Pearson's correlation coefficient was also done to corroborate the findings on whether SIGINT was effective in countering terrorism. Table 4 below gives the information.

Table 4. *Correlation of HUMINT Indicators and Countering Terrorism.*

Indicators	SIGINT	Countering terrorism	Pearson Correlation Coefficient Values	Sig. (2-tailed)
Intercepted communications			.673*	.000
Timely warnings			.584*	.034
Identification & location			.153	.053
Terrorist network mapping			.457	.062
Anomaly detection			.618	.091

* - Means significant at 5% level

Table 4 indicates a statistically significant impact of two SIGINT indicators, intercepted communications and timely warnings, on countering terrorism. This conclusion is supported by Pearson correlation coefficients of 0.673 (indicating a strong positive correlation) and 0.584 (indicating a moderate positive correlation), both with P-values less than 0.05. These coefficients suggest that an increase in HUMINT indicators such as intercepted communications and timely warnings significantly enhances efforts in countering terrorism.

However, for more than half of the SIGINT indicators-specifically identification and location, terrorist network mapping, and anomaly detection-the Pearson correlation coefficients (r) with countering terrorism were not significant at the 5% level.

VIEWS ON WHY CERTAIN INDICATORS DID NOT MEET EXPECTATIONS

To better understand the views concerning reasons why certain counter-terrorism strategies' indicators specifically, source penetration (HUMINT); identification and location, terrorist network mapping, and anomaly detection (SIGINT) did not meet expectations, interviews were done with the heads of security agencies. The following were direct statements that supported this understanding.

Views on why source penetration did not meet expectation

Source penetration remains a formidable challenge because terrorist organizations have become increasingly sophisticated in their efforts to infiltrate our ranks. They use a variety of tactics, such as double agents and moles, to compromise our sources from within, making it difficult to protect their identities and information [NIS_Male_August, 2023_KII].

One of the primary reasons source penetrations are a persistent concern is that terrorists have adapted to our col-

lection methods. They exploit our reliance on electronic communication and encryption, making it harder to protect the anonymity of our sources. As technology advances, so do the methods terrorists use to compromise our intelligence assets [KDF_Male_August, 2023_KII].

Views on why Identification and Location did not meet expectation

The challenge with identification and location in SIGINT stems from the fact that terrorists have become adept at concealing their identities and locations. They employ encryption technologies, frequently change SIM cards, and use anonymizing tools, making it extremely difficult to track their movements or pinpoint their exact whereabouts [NIS_Male_August, 2023_KII].

Terrorist groups operate in the shadows, and they have learned to exploit our reliance on electronic communication for intelligence purposes. They utilize VPNs, Tor networks, and other methods to mask their online activities, making it a daunting task to trace their digital footprints and establish their identities or locations [KDF_Male_August, 2023_KII].

Views on why terrorist network mapping did not meet expectation

Mapping terrorist networks is an intricate challenge because these organizations are highly fluid and adapt quickly. They frequently change affiliations, communication methods, and even their organizational structures. This constant evolution makes it challenging to create a stable and accurate network map [KDF_Male_August, 2023_KII].

Terrorist networks deliberately employ compartmentalization, and they use a 'need-to-know' approach, limiting the information available to individual members. This secrecy makes it difficult for us to map out the entire network comprehensively, as we often lack the full picture due to their compartmentalized structure [NIS_Male_August, 2023_KII].

Views on why anomaly detection did not meet expectation

Anomaly detection is a challenging task in the context of countering terrorism because terrorists intentionally mix their routine, non-threatening communications with covert ones. This deliberate 'noise' makes it harder to identify unusual patterns effectively, as the line between normal and suspicious activities becomes blurred [NIS_Male_August, 2023_KII].

Terrorist groups have become increasingly adept at disguising their communications and activities to evade detection. They frequently modify their patterns of behavior to avoid triggering alerts and alarms, which complicates our efforts to detect anomalies within the vast sea of communications data [KDF_Male_August, 2023_KII].

6. Conclusions

HUMINT STRATEGY

1) The role of Human Intelligence (HUMINT) in the counter-terrorism efforts led by the National Intelligence Services (NIS) and the Kenya Defense Forces (KDF) has yielded exceptional results, with all key performance indicators surpassing expectations, with one notable exception - source penetration. HUMINT has consistently provided actionable intelligence of the highest caliber. The information gathered through human sources has been timely, pertinent, and actionable, facilitating well-informed decision-making and enabling pre-emptive measures against potential terrorist threats.
2) The reliability and accuracy of HUMINT sources have consistently impressed NIS and KDF officers. The intelligence received has been rigorously vetted, corroborated by multiple sources, and demonstrated a remarkable level of accuracy. The confidence in the quality of HUMINT data has grown substantially, reflecting the dedication and professionalism of those involved in gathering and reporting the information.
3) The operational impact of HUMINT cannot be overstated. The intelligence derived from HUMINT has led to the successful disruption of terrorist networks, the thwarting of planned attacks, and the apprehension of key figures involved in terrorist activities. Counterterrorism operations have been conducted with precision and efficiency, safeguarding both civilian lives and national security.
4) Despite these notable successes, it is essential to acknowledge the persistent challenge of source penetration. The failure to recruit and maintain successful human sources in the fight against terrorism is a multifaceted challenge characterized by a culture of fear, advanced counterintelligence tactics, and the demanding task of safeguarding the security and confidentiality of sources.

SIGINT STRATEGY

1) Intercepted communications within the realm of SIGINT have exceeded expectations, providing invaluable insights into the intentions and activities of terrorist groups. The quality and quantity of intercepted communications have significantly contributed to intelligence analysis, enabling preemptive actions and enhancing overall national security.
2) Furthermore, SIGINT has consistently delivered timely warnings that have aided in the prevention of terrorist attacks. The ability to quickly identify and communicate threats has been a crucial component of successful counterterrorism efforts, saving lives and reducing potential harm to civilians and security forces.
3) However, the effectiveness of SIGINT in terms of identification & location, terrorist network mapping, and anomaly detection has faced some notable challenges. There are several reasons for these areas not meeting expectations as established by the research:
4) Identification & location: Terrorist groups often em-

ploy sophisticated encryption techniques and communication methods to hide their identities and locations. This has made it increasingly difficult for SIGINT to accurately pinpoint the exact identities and locations of key operatives.

5) Terrorist network mapping: The fluid and decentralized nature of modern terrorist networks can make mapping and understanding their structures and connections a complex and dynamic task. Often, terrorists frequently change affiliations and communication methods to avoid detection.
6) Anomaly detection: Detecting anomalies within the vast sea of communications data can be challenging, especially when terrorists intentionally mix routine, non-threatening communications with covert ones. This 'noise' makes it harder to identify unusual patterns effectively.

7. Recommendations

HUMINT STRATEGY

1) Enhance source protection and security measures through 1. Strengthening source protection protocols to ensure the safety and security of individuals providing crucial information. This includes implementing robust measures to shield the identity and location of sources 2. Training intelligence personnel and sources in the best practices for maintaining source security and personal safety. 3. Fostering a culture of source protection awareness and responsibility within the intelligence community to minimize the risk of inadvertent breaches.
2) Enhance continuous counterintelligence efforts through 1. Developing and implementing proactive counterintelligence strategies to identify and mitigate potential threats to source security. 2. Monitoring for signs of source compromise and take immediate action in response to any suspected breaches. 3. Engaging in counterespionage activities to identify and neutralize attempts by adversaries to penetrate and compromise intelligence sources. 4. Regularly review and update counterintelligence procedures in response to emerging threats and tactics used by hostile entities.

SIGINT STRATEGY

1) Enhance technical capabilities through investing in advanced signal analysis and decryption technologies to counter the sophisticated encryption techniques employed by terrorist groups. Also, develop and deploy advanced geolocation technologies that can improve the accuracy of pinpointing the locations of key operatives.
2) Improve data integration through establishing better integration between different SIGINT sources, such as communication interception and geospatial data, to enhance the ability to identify and locate terrorist operatives. Further, employ data fusion techniques to combine various intelligence sources for a more comprehensive understanding of terrorist networks.
3) Conduct continual training and skill development through investing in ongoing training for SIGINT analysts and operators to keep them updated on the latest encryption and communication technologies employed by terrorists. Similarly, develop expertise in behavioral analysis to better identify patterns and anomalies in terrorist communications.

Abbreviations

CIA	Central Intelligence Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
FBI	Federal Bureau of Investigation
HUMINT	Human Intelligence
KDF	Kenya Defense Forces
NIA	National Intelligence Agency
NIS	National Intelligence Service
NSA	National Security Agency
NSIS	National Security Intelligence Service
OSS	Office of Strategic Services
SIGINT	Signals Intelligence
SIS	Signal Intelligence Service
SPSS	Statistical Package for Social Sciences
SSS	State Security Service

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Ahlmann, M. A., & Garrett, J. (2015). Human intelligence: the discipline the intelligence community must struggle to rediscover. American Military University.

[2] Aid, M. M. (2003). All glory is fleeting: Sigint and the fight against international terrorism. Intelligence and National Security, 18(4), 72-120.

[3] Badiru, A. B., & Maloney, A. E. (2016). A conceptual framework for the application of systems approach to intelligence operations: Using HUMINT to augment SIGINT. American Intelligence Journal, 33(2), 41-46.

[4] Ball, D., & Tanter, R. (2015). US signal intelligence (SIGINT) activities in Japan 1945-2015: A Visual Guide. Nautilus Institute NAPS Net Special Report, December, 22.

[5] Bwana, R. (2023). Inside the National Intelligence Service: A Closer Look at Kenya's Security Apparatus. Available at SSRN 4454565.

[6] Falode, A. J., & Faseke, B. O. (2023). The Art of the Impossible: Intelligence and Nigeria's Boko Haram War, 2010–2021. International Journal of Intelligence and Counterintelligence, 36(4), 1319-1336.

[7] Johnson, L. (2010). Evaluating "Humint": The role of foreign agents in US security. Comparative Strategy, 29(4), 308-332.

[8] Kamiński, M. A. (2019). Intelligence Sources in the Process of Collection of Information by the US Intelligence Community. Security Dimensions. International and National Studies, (32), 82-105.

[9] Margolis, G. (2013). The lack of HUMINT: A recurring intelligence problem. Global Security Studies, 4(2), 43-60.

[10] Mwangi, S. W., & Wasonga, J. (2020). Assessing The Effectiveness Of Intelligence Gathering And Sharing (IGS) In Countering Violent Extremism (CVE) In Kenya. International Journal of Innovative Research and Advanced Studies (IJIRAS), 7(1), 149-156.

[11] Nwagboso, C. I., & Nwagboso, N. S. (2021). The Challenges of Intelligence Gathering in the Third World-A Critique of the Nexus between Poverty and Public Policy Process. International Journal of Public Administration and Management Research, 6(2), 55-71.

[12] Oche, O. (2014). Information, Intelligence and Security: Overview of the Current Security Situation in Nigeria. African Journal of International Affairs & Development, 17(2), 7.

[13] Rosenau, W. (2005). Al Qaida recruitment trends in Kenya and Tanzania. Studies in Conflict & Terrorism, 28(1), 1-10.

[14] Stottlemyre, S. A. (2015). HUMINT, OSINT, or something new? Defining crowdsourced intelligence. International Journal of Intelligence and Counter-Intelligence, 28(3), 578-589.

[15] Tobia, S. (2014). Interrogation, interviewing and questioning in the twentieth century. Interrogation in War and Conflict: A Comparative and Interdisciplinary Analysis, 268.

[16] Weinbaum, C., Berner, S., & McClintock, B. (2017). SIGINT for Anyone. The Growing Availability of Signals Intelligence in the Public Domain, RAND Corp., Santa Monica.

Biography

Kennedy Obumba Ogutu is an enigmatic figure in intelligence, investigations, and security. With a career shrouded in secrecy, he has made substantial contributions through his training programs and academic pursuits. His blend of practical experience and academic excellence makes him a formidable authority in security policies, investigative research, and cybercrime prevention. Working in a clandestine government department, Ogutu has played a pivotal role in disseminating knowledge on investigations and intelligence gathering. As a trainer, he has shaped the skills of individuals dedicated to national security, imparting the arts of investigations, intelligence gathering, and security protocols. Beyond his clandestine activities, Ogutu is a revered educator, having taught security and investigative research courses at institutions like the Kenya Institute of Security and Criminal Justice, Egerton University, Kisii University, and Tom Mboya University. An accomplished scholar, his research has provided critical insights into security policies and cybercrime prevention.

Fredrick Okeyo Nyagwara is a distinguished scholar and dedicated law enforcement officer with over 15 years of exemplary service in the Kenya Police Service. His extensive experience and academic prowess have made him a respected authority in criminology, security management, and police studies. Rising through the ranks, Nyagwara currently holds the position of Chief Inspector. His career is marked by commitment, dedication, and a relentless pursuit of justice and security. Nyagwara is also a prolific writer, contributing insightful articles to academic journals and law enforcement publications on topics such as human rights, counter-terrorism strategies, and law enforcement training advancements. His unique blend of practical experience and academic excellence has significantly advanced the capabilities of the Kenya Police Service and improved regional safety and security. As a chief inspector and scholar, he continues to inspire the next generation of law enforcement professionals.