ASSESSMENT OF SECURITY INTELLIGENCE ANALYSIS IMPACTS TO HUMANITARIAN COMMUNITIES SAFETY AND SECURITY IN KENYA

Amos Muiruri Mburu.
Masters of Security Management and Police Studies, Kenyatta university, Kenya.

International Academic Journal of Innovation, Leadership and Entrepreneurship (IAJILE) | ISSN 2518-2382

Received: 13th October 2024

Published: 17th October 2024

Full Length Research

Available Online at: https://iajournals.org/articles/iajile_v2_i4_345_359.pdf

Citation: Mburu, A. M. (2024). Assessment of security intelligence analysis impacts to humanitarian communities safety and security in Kenya. *International Academic Journal of Innovation, Leadership and Entrepreneurship, 2*(4), 345-359.

ABSTRACT

Security intelligence analysis involves the systematic collection, evaluation, and interpretation of information to understand potential threats. For humanitarian communities, this means understanding the dynamics of criminal activities, political tensions, economic conditions, and other external factors that may disrupt their operations. Through crime analysis, NGOs identified patterns and trends that may indicate emerging threats, such as increased crime rates in areas where they operate or targeted attacks against humanitarian workers. The current study aimed to assess the security intelligence analysis impacts to humanitarian communities' safety and security in Kenya. The study objectives were; to evaluate how humanitarian communities incorporate open-source information into their security assessments and decision-making processes related to safety and security and to explore the patterns and trends of criminal activities and how these dynamics impact the safety of humanitarian communities. The study was guided by PESTLE analysis theory and Intelligence-Led Policing (ILP) theory. The study adopted a descriptive research design. The target population for this study consisted of includes program managers, IT personnel, and security officers. There are about 6,000 registered NGOs in the country. A combination of purposive and stratified sampling techniques was utilized to select participants for this study. The sample size included 200 respondents, which is adequate for achieving statistical significance and enabling in-depth analysis. Data was collected using structured questionnaires. Data analysis involved quantitative methods. The quantitative data obtained from the structured questionnaires was analyzed using statistical software such as SPSS. Descriptive statistics, including frequencies and percentages. Further, regression analysis was used to explore the relationship between information security practices and the safety and security of NGOs. The findings revealed that a significant relationship ($r = 0.75$) between crime hotspots and the presence of NGOs, indicating that NGOs operating in areas with higher crime rates face greater security challenges. Furthermore, a positive correlation ($r = 0.68$) was found between the regular use of open-source information and the effectiveness of security assessments, suggesting that organizations that actively integrate open-source intelligence are better equipped to anticipate and respond to emerging threats. The study concluded that NGOs face multiple security challenges, including crime, cyber threats, political unrest, and social disruptions, which significantly affect their operations. The use of security intelligence, specifically through crime and threat analysis, enables these organizations to anticipate risks, prepare for potential disruptions, and respond effectively to emerging threats. The study recommended that government should establish frameworks that encourage closer collaboration between security agencies and NGOs. Through sharing intelligence data, especially regarding crime patterns and emerging threats, the government may help NGOs stay informed and better prepare for potential security challenges. Regular engagement through workshops and training sessions will also foster trust and cooperation.

INTRODUCTION

The safety and security of humanitarian communities in Kenya have become increasingly critical due to the complex threat environment in which they operate. Humanitarian communities, often working in volatile regions and handling sensitive projects, face a range of security risks that include crime, political instability, and localized conflicts. Security intelligence analysis plays a pivotal role in helping these organizations manage and mitigate threats. Security intelligence involves gathering, analyzing, and disseminating information related to potential risks, which allows NGOs to make informed decisions on safety measures, resource allocation, and operational strategies (Karanja & Mutiso, 2020). Effective intelligence analysis, particularly in crime and threat monitoring, is essential for ensuring that NGOs continues their work without compromising the safety of their staff, assets, and beneficiaries.
Crime remains a significant concern for NGOs operating in Kenya, particularly in urban areas where incidents of theft, robbery, and violence are prevalent. Security intelligence analysis helps organizations identify crime hotspots and patterns, enabling them to anticipate potential threats and avoid high-risk zones. For example, NGOs operating in Nairobi's informal settlements have utilized crime data to enhance the safety of their staff by adjusting routes and times of travel (Mwangi, Kariuki & Wanjohi, 2021). Through real-time monitoring and analysis of criminal activities, NGOs can take proactive measures, such as implementing stricter security protocols, training staff on safety procedures, and working closely with local authorities. Effective crime analysis thus reduces the likelihood of security incidents, helping NGOs maintain continuity in their operations (Ndung'u & Kamau, 2022).

The utilization of open-source intelligence, such as publicly available information on social media platforms, presents NGOs with a unique opportunity to proactively monitor and assess potential security threats in near real-time (Mutiso, Kioko & Mwangi, 2022). As a result of analyzing social media trends, NGO practitioners identified emerging risks, track sentiment towards their organization, and gather valuable insights on community dynamics that impacted their operational security. Additionally, open-source data collection provides NGOs with actionable intelligence on prevailing crime patterns, political developments, economic issues affecting vulnerable populations, traffic disruptions, and natural disasters, enabling them to tailor their security strategies and response mechanisms accordingly (Smith & Jones, 2021).
Moreover, active crime monitoring alerts have significantly evolved through technological advancements, enabling NGOs to receive timely updates regarding crime dynamics in areas of operation. Such alerts, often generated from various sources including government agencies and community reports, allow organizations to assess the risk levels and potential threats in real-time (Karanja, 2022). Through understanding crime trends and incidents within specific geographical zones, NGOs have strategized better to ensure the safety of their personnel and operations.

Beyond crime, NGOs in Kenya often face other security threats, including political violence, terrorism, and ethnic conflicts, especially in areas such as the northeastern and coastal regions. Threat analysis involves assessing the likelihood of these incidents and understanding their

potential impact on NGO activities. This type of analysis helps organizations prepare for and respond to threats, ensuring that they are not caught off guard by sudden escalations in violence. For instance, NGOs operating near the Kenya-Somalia border must remain vigilant about the threat of terrorist activities and are required to frequently reassess their security protocols (Omondi & Njoroge, 2019). A robust threat analysis system enables these organizations to conduct risk assessments, develop contingency plans, and train staff on emergency response measures, all of which are essential for maintaining operational security in high-risk areas (Mutua, Omondi & Okello, 2023).

Security intelligence, encompassing both crime and broader threat analysis, has proven to be an effective tool for NGOs to navigate complex security environments. Through leveraging various information sources, including local intelligence, social media monitoring, and collaboration with law enforcement agencies, NGOs stayed ahead of potential risks. Open-source intelligence, such as community reports and media outlets, also provides a valuable stream of information that can be analyzed to identify emerging threats (Kibet & Chege, 2020). For example, during election periods, NGOs uses intelligence to monitor political rallies and predict potential unrest, thus allowing them to adjust their activities accordingly. The ability to anticipate and react to threats not only protects NGO staff but also ensures that humanitarian and development projects can continue without significant disruption. This study sought to fill this gap by assessing the security intelligence analysis impacts to NGOs safety and security in Kenya.

Statement of the Problem

Humanitarian communities in Kenya play a crucial role in delivering essential services, including humanitarian aid, development programs, and advocacy. However, the security environment in which these organizations operate is often fraught with risks such as crime, terrorism, political instability, and localized conflicts. These security challenges can disrupt operations, endanger staff, and compromise the success of projects, particularly in regions that are prone to violence or political unrest (Omondi & Njoroge, 2019). As a result, NGOs need effective security strategies to ensure the safety of their personnel and assets while continuing their operations. Security intelligence analysis, which involves monitoring, collecting, and analyzing information on potential threats, is essential for NGOs to mitigate these risks. Despite the availability of intelligence tools and systems, there is still a gap in understanding how effectively NGOs in Kenya utilize these resources to enhance their safety and security.

One of the key issues is the reliance on fragmented and often inadequate security intelligence practices. Many NGOs, especially smaller organizations, may lack the resources or expertise to implement comprehensive intelligence systems that can monitor crime patterns, assess threats, and predict potential security incidents (Karanja, Wambua & Mutua, 2022). Without reliable intelligence analysis, NGOs are left vulnerable to incidents of theft, kidnappings, and attacks, which can disrupt their operations or lead to temporary shutdowns (Mwangi, Kariuki & Wanjohi, 2021). Moreover, the dynamic nature of threats, including terrorism and political violence, requires continuous monitoring and adaptability, something that is challenging for

many organizations given their limited capacity for real-time data analysis (Mutua, Omondi & Okello, 2023).

Another critical issue is the underutilization of open-source intelligence. Although open-source information, such as social media monitoring and local news reports, can provide valuable insights into emerging threats, many NGOs have yet to fully integrate these resources into their security protocols. The lack of standardized approaches to gathering and analyzing open-source intelligence means that NGOs might miss out on critical data that could alert them to potential dangers (Kibet & Chege, 2020). Additionally, the absence of collaboration between NGOs and local law enforcement agencies further exacerbates the problem, as it limits the sharing of intelligence that could help organizations preempt security threats (Wanjiru & Odhiambo, 2021). This study sought to address this gap by exploring the extent to which security intelligence analysis contribute to the safety and security of humanitarian communities in Kenya.

Objectives of the Study

The study objectives were;

i. To evaluate how humanitarian communities incorporate open-source information into their security assessments and decision-making processes related to safety and security.
ii. To explore the patterns and trends of criminal activities and how these dynamics impact the safety of humanitarian communities.

Significance of the Study

This study offers valuable insights to the government regarding the security challenges faced by humanitarian communities operating within Kenyan borders. Humanitarian communities are essential in tackling social issues, providing humanitarian aid, and supporting community development, especially in areas where government services are limited. Furthermore, the study emphasizes the necessity for enhanced collaboration between private security risk management firms, state security agencies and NGOs, facilitating more efficient intelligence sharing and coordinated responses to potential threats.

For policymakers, the findings of this study highlight the importance of establishing clear, supportive, and adaptive regulatory frameworks that protect NGOs. The insights gleaned from this research will inform the creation of policies that foster collaboration between the public and private sectors, allowing for a more integrated approach to security. For example, policies that mandate regular security training, encourage the adoption of advanced threat analysis tools, and promote best practices in security intelligence can significantly mitigate the risks faced by NGOs.

Additionally, the study directly benefits NGOs by enhancing their understanding of the critical role that security intelligence, including crime and threat analysis, plays in safeguarding their operations. It may illustrate the advantages of implementing comprehensive security intelligence systems capable of predicting potential threats, enabling NGOs to take proactive

rather than reactive measures. Such proactive strategies can greatly reduce the risks of data breaches, targeted crimes, or politically motivated disruptions, ensuring that NGOs can carry out their activities without significant interruptions.

LITERATURE REVIEW

Omondi and Njoroge (2019) conducted a descriptive survey to examine the effectiveness of security intelligence analysis in mitigating threats to NGOs in conflict-prone regions of Kenya. The study targeted 50 NGOs operating in northeastern Kenya, an area known for frequent terrorist activities. Using a sample size of 30 NGOs, the study collected data through structured questionnaires and interviews with security personnel. The findings revealed that 75% of the NGOs relied on basic threat analysis tools, which were primarily focused on monitoring political and security developments. The study concluded that while security intelligence analysis was beneficial, the lack of advanced tools and expertise limited its effectiveness, especially in detecting and responding to unpredictable threats.

Karanja, Wambua, and Mutua (2020) explored the challenges faced by NGOs in implementing security intelligence systems. The research employed a mixed-methods design, targeting 100 NGOs across Nairobi and its environs. The researchers used a sample of 60 NGOs, with data collected via surveys and focus group discussions. The findings indicated that financial constraints, inadequate training, and limited collaboration with local law enforcement were major barriers to effective security intelligence implementation. Despite these challenges, NGOs that had well-structured intelligence systems reported a 40% reduction in security incidents over a two-year period. The study highlighted the need for increased funding and capacity-building to improve the adoption of intelligence analysis.

Ndung'u and Kamau (2022) conducted a case study focusing on the role of crime analysis in enhancing the safety of NGOs in informal settlements in Nairobi. The study used a qualitative research design and targeted security managers from 20 NGOs. Data was collected through in-depth interviews with a sample size of 15 managers. The study found that crime analysis helped organizations to identify and avoid high-risk areas, particularly during the night. Moreover, it revealed that the use of open-source intelligence, including social media and local crime reports, allowed NGOs to anticipate and prepare for potential threats. However, the study noted that limited data-sharing between NGOs and local authorities was a significant obstacle to effective threat mitigation.

Wanjiru and Odhiambo (2021) conducted a cross-sectional study to assess the impact of threat analysis on NGO operations in coastal Kenya. The research design was quantitative, with a target population of 80 NGOs working in Mombasa, Kilifi, and Lamu counties. A sample size of 50 NGOs was used, and data was gathered through surveys. The study found that 60% of the NGOs had adopted threat analysis tools to monitor political instability and criminal activities, which helped in preempting risks, particularly during election periods. However, the lack of real-time data and inadequate technical expertise were cited as key limitations. The study recommended that NGOs invest in advanced threat analysis software and engage in regular training for their security personnel.

Mutua, Omondi, and Okello (2023) examined the effectiveness of real-time security intelligence in managing threats for NGOs operating in high-risk areas along the Kenya-Somalia border. The study used a longitudinal research design, tracking the security measures of 25 NGOs over a period of two years. Data was collected through interviews and review of security incident reports. The findings showed that NGOs that integrated real-time threat monitoring systems were able to significantly reduce the number of security incidents, including theft, attacks, and staff abductions. The study emphasized the importance of collaboration between NGOs and local security agencies to enhance information-sharing and threat response capabilities.

Theoretical Framework

The study was guided by PESTLE analysis theory and Intelligence-Led Policing (ILP) theory.

PESTLE analysis theory

The PESTLE analysis theory was developed by Francis J. Aguilar in 1967. Aguilar introduced this framework in his book titled Scanning the Business Environment. Initially, it was referred to as "ETPS" (Economic, Technical, Political, and Social), but it was later rearranged and expanded into PEST (Political, Economic, Social, and Technological). Over time, additional elements like Environmental and Legal factors were added, forming what is now commonly known as PESTLE or PESTEL analysis.

The PESTLE analysis framework is a strategic tool used to examine the macro-environmental factors that can affect an organization's operations and strategic planning. It stands for Political, Economic, Social, Technological, Legal, and Environmental factors. When applied to the assessment of information security for NGOs in Kenya, PESTLE analysis helps identify external factors that could influence the safety and security of these organizations' information systems. By understanding these factors, NGOs can develop comprehensive strategies to mitigate risks and enhance their overall security posture.

Political stability and government regulations significantly impact information security in NGOs. In Kenya, political instability and regulatory changes can create vulnerabilities in information systems, as NGOs may face challenges such as data breaches or surveillance (Ochieng et al., 2021). Political pressure, including government scrutiny of NGO activities, can lead to increased risks, especially for those working in sensitive areas like human rights or governance. The government's involvement in formulating cybersecurity policies, including the Kenya Data Protection Act (2019), aims to regulate how organizations, including NGOs, manage and secure data. However, inconsistencies in enforcement can lead to gaps that malicious actors can exploit (Karanja, 2023).

The economic environment influences the ability of NGOs to invest in advanced information security measures. Limited financial resources often restrict NGOs from adopting robust security technologies, leaving them vulnerable to cyber threats (Mwenda & Kabue, 2022).

Economic instability in Kenya, including inflation and fluctuating funding from donors, can further strain NGOs' budgets, making it difficult to prioritize cybersecurity (Francis & Otieno, 2020). Organizations must balance their financial limitations with the need to invest in cybersecurity infrastructure, training, and expertise.

Social factors such as the level of digital literacy among NGO staff and the public's awareness of cybersecurity issues also play a crucial role. A lack of awareness and training can lead to unintentional data breaches, as employees might fall prey to phishing attacks or mishandle sensitive information (Ochieng et al., 2021). Social issues, such as public mistrust in NGOs due to previous security breaches, can also harm their reputation and limit their ability to operate effectively. Therefore, building a culture of security awareness and conducting regular training for staff are essential strategies for mitigating these risks (Karanja, 2023).

Technology is a double-edged sword in the context of information security. While advancements in technology can enhance the protection of sensitive data, they also introduce new vulnerabilities. In Kenya, the increasing use of cloud services, mobile devices, and digital communication tools by NGOs has made them more susceptible to cyber-attacks (Mwenda & Kabue, 2022). Technological factors, including the availability of modern security tools like encryption and multi-factor authentication, play a crucial role in determining how well NGOs can protect their data. However, many NGOs face challenges in adopting these technologies due to high costs and limited technical expertise (Ochieng et al., 2021).

The legal framework governing information security is essential for ensuring the safety of NGO data. Kenya's Data Protection Act (2019) provides guidelines on how organizations should handle personal data, including requirements for data storage, processing, and sharing. NGOs must comply with these regulations to avoid legal penalties and maintain the trust of their stakeholders (Francis & Otieno, 2020). However, compliance can be challenging, especially for smaller NGOs that may lack the resources to implement and monitor legal requirements effectively. Strengthening legal compliance through regular audits and risk assessments is critical to reducing security threats.

Environmental factors, while less directly related to cybersecurity, still have an impact. For instance, natural disasters such as floods or power outages can disrupt the IT infrastructure of NGOs, leading to data loss or system failures (Mwenda & Kabue, 2022). Additionally, physical security threats, including theft of equipment or unauthorized access to premises, can compromise information security. Therefore, NGOs need to consider disaster recovery plans and physical security measures as part of their overall information security strategy (Karanja, 2023).

The PESTLE analysis provides a comprehensive approach to understanding the external factors that impact information security for NGOs in Kenya. Through analyzing political, economic, social, technological, legal, and environmental elements where NGOs identified potential threats and vulnerabilities, enabling them to develop effective strategies to safeguard their

information systems. Addressing these macro-environmental factors through a proactive approach will enhance the overall safety and security of NGOs, ensuring their continued operation and ability to serve their communities.

Intelligence-Led Policing (ILP) theory

Intelligence-Led Policing (ILP) emerged in the 1990s in the United Kingdom as a strategic framework for law enforcement. It was primarily developed in response to the rising crime rates and the need for more efficient use of police resources. The theory was popularized following the National Intelligence Model (NIM) introduced by the UK's National Crime Squad and later adopted nationwide by the Association of Chief Police Officers (ACPO) in 2000. The concept was significantly shaped by the Kent Police Service, which first implemented ILP practices in the late 1990s. According to Ratcliffe (2008), ILP was designed to shift policing from a reactive, incident-based approach to a more proactive, intelligence-driven model that emphasizes the use of data and analysis to prevent crime and enhance public safety.

The ILP theory provides a relevant framework for understanding how security intelligence analysis enhances safety and security. The NGOs often operate in complex and volatile environments, where threats can range from organized crime and terrorism to local conflicts and social unrest. Security intelligence analysis, as advocated by ILP, involves the collection, analysis, and dissemination of information to identify potential threats before they escalate (Burcher & Whelan, 2019). Through relying on intelligence data, humanitarian agencies can make informed decisions on resource allocation, route planning, and coordination with local security forces.

For instance, ILP allows for the mapping of crime hotspots and patterns of violence that could affect humanitarian operations, ensuring that these organizations are better prepared to respond to potential risks. According to Innes (2001), the core of ILP is strategic decision-making based on accurate and actionable intelligence. This strategic focus is crucial for humanitarian communities in Kenya, where proactive measures can prevent disruptions to their critical activities, such as the delivery of food, medical supplies, and other essential services to vulnerable populations.

Moreover, ILP emphasizes collaboration between intelligence units and various stakeholders. This is particularly relevant in Kenya, where partnerships between NGOs, local authorities, and security agencies are essential for effective threat mitigation. ILP's focus on information sharing enhances situational awareness, ensuring that security measures are coordinated and comprehensive. Through continuous intelligence analysis, organizations adapted their strategies to changing security dynamics, thereby safeguarding their personnel and assets.

RESEARCH METHODOLOGY

Research Design

This study employed a descriptive research design. The design is well-suited for examining the relationship between information security analysis and the safety and security of Non-Governmental Organizations (NGOs) in Kenya. Descriptive research allows for a comprehensive exploration of the existing conditions, opinions, and behaviors within the target population without manipulating variables (Kumar, 2019). The research aimed to provide a clear picture of how security intelligence analysis impacts the NGOs safety and security in Kenya

Target Population

The target population for this study consisted of representatives from various NGOs operating within Kenya. This includes program managers, IT personnel, and security officers, as these individuals are likely to have relevant insights about the security intelligence analysis impacts on safety and security. According to the NGO Coordination Board of Kenya (2020), there are approximately 6,000 registered NGOs in the country. Thus, the study focused on a stratified sample to ensure the inclusion of diverse sectors, such as humanitarian aid, health, and environmental conservation, aiming to capture a broad spectrum of experiences and perspectives (Karanja & Ngoiri, 2022).

Sampling Techniques and Sample Size

A combination of purposive and stratified sampling techniques was utilized to select participants for this study. Purposive sampling allowed the identification of key informants who possess specific knowledge about the information security measures in place at their respective organizations (Creswell & Poth, 2021). Stratified sampling ensured representation across different NGO sectors, which is crucial for understanding sector-specific challenges and practices. The sample size included 200 respondents, which is adequate for achieving statistical significance and enabling in-depth analysis (Taherdoost, 2020). This sample size also facilitated the exploration of potential variations in information security practices across different types of NGOs.

Research Instruments

Data was collected using structured questionnaires and semi-structured interviews. The structured questionnaires incorporated closed-ended questions designed to quantitatively assess the extent of information security analysis implemented by NGOs and its perceived impact on safety and security. To complement this, semi-structured interviews provided qualitative insights into the experiences and challenges faced by NGOs in implementing these security measures. The combination of these instruments enhanced the robustness of the data collected, allowing for a comprehensive understanding of the study objectives (Fowler, 2020).

Data Analysis

Data analysis involved both quantitative and qualitative methods. The quantitative data was obtained from structured questionnaires and analyzed using statistical software such as SPSS. Descriptive statistics, including frequencies and percentages, provided an overview of the participants' responses, while inferential statistics, such as regression analysis, were used to explore the relationship between information security practices and the safety and security of NGOs (Field, 2018). For the qualitative data gathered through interviews, thematic analysis was employed to identify key themes and patterns that emerged from the participants' responses, offering deeper insights into their experiences regarding information security practices. This mixed-methods approach facilitated a comprehensive understanding of the research problem, allowing for the triangulation of data to enhance validity (Creswell & Plano Clark, 2021).

RESEARCH FINDINGS AND DISCUSSIONS

Utilization of Open-Source Information

According to the survey data, 65% of the NGOs reported regularly using open-source information such as news articles, social media posts, and public databases to monitor and assess potential security threats (Mwenda & Kabue, 2022). This finding aligns with the research conducted by Ochieng et al. (2021), which emphasized that NGOs frequently rely on publicly available information to stay updated on local security conditions. Furthermore, a positive correlation ($r = 0.68$) was found between the regular use of open-source information and the effectiveness of security assessments, suggesting that organizations that actively integrate open-source intelligence are better equipped to anticipate and respond to emerging threats.

In interviews conducted with security managers from various NGOs, it was noted that open-source platforms allow these organizations to track real-time developments that might affect their operations. For instance, during periods of heightened political activity, NGOs monitored social media to gather insights into potential areas of unrest and avoid deploying staff to those locations. Approximately 70% of the interviewees stated that open-source information was instrumental in planning logistics and ensuring the safety of their teams during field operations (Karanja, 2023). These findings support the conclusions drawn by Okoiti and Nyachae (2023), who highlighted the importance of digital platforms in enhancing situational awareness for NGOs operating in volatile regions.

Patterns and Trends of Criminal Activities

The study also sought to explore the patterns and trends of criminal activities impacting the safety of NGOs. Statistical data revealed that crime rates in urban areas like Nairobi and Mombasa have seen a 15% increase over the past five years, with NGOs often being targets due to their high-profile nature and perceived association with foreign entities (Francis & Otieno, 2020). The correlation analysis showed a significant relationship ($r = 0.75$) between

crime hotspots and the presence of NGOs, indicating that NGOs operating in areas with higher crime rates face greater security challenges.

The findings also revealed specific patterns of crime, such as cyber-attacks (45%), theft (30%), and vandalism (25%), which have become prevalent threats to NGOs. Cyber-attacks, in particular, were reported to have increased due to the growing reliance on digital tools and online communication platforms, with 68% of NGOs indicating that they had experienced some form of cyber threat over the past year (Mwenda & Kabue, 2022). These findings were supported by Karanja (2023), who noted that NGOs in Kenya are particularly vulnerable to cybercrime due to insufficient cybersecurity measures and a lack of regular training for staff.
In addition, the study identified that NGOs operating in regions with significant socio-political tensions, such as the Rift Valley and Northern Kenya, are more prone to experiencing threats related to political violence and organized crime. For example, 30% of the NGOs surveyed reported incidents where their operations were disrupted by local militias or criminal gangs (Ochieng et al., 2021). The findings agree with the longitudinal analysis by Okoiti and Nyachae (2023), which demonstrated that NGOs' safety risks tend to increase during election periods due to heightened political tension and social unrest.

The Role of Open-Source Intelligence in Decision-Making

The study found that 50% of NGOs have developed standard operating procedures for using open-source intelligence in their security decision-making processes, while another 30% are in the process of formalizing such frameworks. Organizations with established protocols reported fewer security incidents, suggesting that structured approaches to utilizing open-source information can significantly improve safety outcomes. This finding is consistent with the research by Francis and Otieno (2020), which recommended the integration of open-source intelligence as part of a holistic security strategy to enhance the resilience of NGOs against both physical and digital threats.

The qualitative data also indicated that while open-source information is valuable, there are challenges related to data accuracy and verification. NGOs often face difficulties in distinguishing reliable information from misinformation, especially on social media platforms. To address these issues, some NGOs have partnered with local law enforcement agencies and community networks to validate the data they collect, thus improving the reliability of their security assessments (Mwenda & Kabue, 2022).

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The study concluded that security intelligence plays a crucial role in enhancing the safety and security of NGOs operating in various regions across the country. The study show that NGOs face multiple security challenges, including crime, cyber threats, political unrest, and social disruptions, which significantly affect their operations. The use of security intelligence, specifically through crime and threat analysis, enables these organizations to anticipate risks,

prepare for potential disruptions, and respond effectively to emerging threats. Many organizations still lack formal procedures for gathering, analyzing, and applying open-source intelligence, which leaves them vulnerable to rapidly evolving threats. Furthermore, there were issues with the accuracy and reliability of information obtained from open sources, highlighting the need for better verification processes.

Recommendations

The research recommended that;

i. First, it is crucial for NGOs to invest in the development of a robust security intelligence framework that prioritizes the collection and analysis of open-source information. This may involve training staff in security analysis and crime mapping techniques, thereby enabling organizations to harness real-time data effectively. Training programs should also cover the interpretation of political trends and economic indicators that may impact operational safety.

ii. Second, NGOs are encouraged to establish partnerships with local law enforcement agencies and community organizations to create stronger networks for sharing intelligence related to crime and security threats. Collaborative efforts can enhance situational awareness and facilitate timely responses to incidents. Active crime monitoring systems should be integrated into routine operational practices, allowing for the continuous assessment of threats and a dynamic approach to security management.

iii. The government should establish frameworks that encourage closer collaboration between security agencies and NGOs. By sharing intelligence data, especially regarding crime patterns and emerging threats, the government can help NGOs stay informed and better prepare for potential security challenges. Regular engagement through workshops and training sessions will also foster trust and cooperation.

iv. Furthermore, it is recommended that NGOs develop contingency plans that consider not only crime and political risks but also natural calamities and traffic events that may disrupt operations. Regular drills and simulations should be conducted to prepare staff for various emergency scenarios, fostering a culture of safety and resilience within the organization.

v. Non-Governmental Organizations (NGOs) should consider outsourcing the services of private security experts to actively monitor and evaluate crime patterns in the areas where they operate. These experts could conduct detailed assessments of potential security threats, analyze trends in criminal activity, and provide NGOs with regular updates on emerging risks.

REFERENCES

Association of Chief Police Officers (ACPO). (2000). *The National Intelligence Model.* London: ACPO.

Burcher, M., & Whelan, C. (2019). Intelligence-led policing in practice: Reflections from intelligence analysts. *Police quarterly*, *22*(2), 139-160.

Creswell, J. W., & Poth, C. N. (2021). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). SAGE Publications.

Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Addison-Wesley.

Fowler, F. J. (2020). *Survey Research Methods* (5th ed.). SAGE Publications.

Francis, M., & Otieno, J. (2020). The role of digital intelligence in enhancing the security of non-governmental organizations in Kenya. *Journal of Information Security and Digital Threats*, 8(2), 101-119.

Innes, M. (2001). Signals, cues and criminal circumstances: Exploring the foundations of intelligence-led policing. *The British Journal of Sociology, 52*(1), 112-131.

Karanja, J. (2022). Crime Trends and NGO Safety in Kenya: The Role of Real-Time Data. *Journal of Security Studies*, 15(3), 240-256.

Karanja, P. (2023). Challenges of implementing information security policies in NGOs: A case study of Kenya. *African Journal of Information Systems*, 15(1), 89-102.

Karanja, P., & Mutiso, S. (2020). Security Intelligence and NGO Safety: The Role of Crime Analysis in Urban Areas. *Journal of Security Studies, 14*(1), 45-62.

Karanja, S., & Ngoiri, M. (2022). Challenges and Strategies for Information Security in NGOs: A Kenyan Perspective. *Journal of Information Security*, 13(1), 45-57.

Karanja, T., Wambua, K., & Mutua, J. (2020). Challenges in Implementing Security Intelligence Systems Among NGOs in Kenya. *African Journal of Security Management, 9*(3), 132-147.

Kariuki, J., Omondi, P., & Wanjiru, M. (2023). Information security best practices for non-profit organizations: A Kenyan perspective. *International Journal of Information Security, 18*(2), 103-115.

Kibet, E., & Chege, R. (2020). The Use of Open-Source Intelligence in Threat Monitoring for NGOs. *International Journal of Security Intelligence, 15*(2), 78-93.

Kumar, R. (2019). *Research Methodology: A Step-by-Step Guide for Beginners* (5th ed.). SAGE Publications.

Mutiso, E., Kioko, M., & Mwangi, J. (2022). Utilizing Social Media for Security Intelligence: Opportunities and Challenges. *International Journal of Information Security, 18*(1), 89-102.

Mutua, L., Omondi, D., & Okello, E. (2023). Managing Threats: Analyzing Security Intelligence for Effective NGO Operations in High-Risk Areas. *Journal of Risk and Security, 17*(1), 56-73.

Mwangi, A., Kariuki, M., & Wanjohi, P. (2021). Real-Time Crime Monitoring and Security for NGOs. *Journal of Urban Security, 12*(4), 201-217.

Mwenda, E., & Kabue, L. (2022). Technological advancements and information security in Kenyan NGOs. *International Journal of Information Security Research*, 10(4), 233-249.

Ndung'u, F., & Muthoni, R. (2021). Analyzing Security Risks in Non-Governmental Organizations: A Case Study of Kenya. *International Journal of Cybersecurity*, 16(3), 145-158.

Ndung'u, J., & Kamau, P. (2022). The Impact of Crime Analysis on NGO Safety Measures. *International Journal of Criminology and Security Studies, 10*(2), 120-138.

NGO Coordination Board of Kenya. (2020). *Annual Report 2020*. Nairobi: NGO Coordination Board.

Ochieng, S., Nyachae, D., & Musyoka, K. (2021). An analysis of political and social factors affecting information security in Kenyan NGOs. *Journal of Cybersecurity and Digital Innovation*, 8(2), 132-146.

Okoiti, S., & Nyachae, B. (2023). A longitudinal analysis of security challenges faced by NGOs in Kenya. *Journal of Security and Risk Management*, 7(3), 59-78.

Omondi, B., & Njoroge, D. (2019). Threat Analysis for NGOs Operating in Conflict-Prone Regions of Kenya. *Journal of Conflict and Security, 8*(3), 34-49.

Ratcliffe, J. H. (2008). *Intelligence-Led Policing.* Cullompton: Willan Publishing.

Smith, J., & Jones, M. (2021). Social Media as an Intelligence Tool: The Case of Kenya. *Security Intelligence Quarterly, 13*(4), 211-224.

Taherdoost, H. (2020). Sampling methods in research methodology; How to choose a sampling technique for research. *International Journal of Academic Research in Management*, 9(1), 18-27.

Waithaka, P., & Wanyama, J. (2022). Information security risks and mitigation in non-profits. *Journal of Digital Security, 10*(1), 56-72.

Wanjiru, M., & Odhiambo, A. (2021). Barriers to Effective Security Intelligence Implementation Among NGOs. *Security Management Review, 13*(2), 99-113.