Scientific Research Publishing

Open Journal of Social Sciences, 2025, 13(8), 452-473
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Strengthening Cyber Defenses: The Impact of Multi-Agency Information Sharing on Cybercrime Prevention in Kenya

Kennedy Obumba Ogutu*, Joseph Okeyo Obosi, Henry Amadi Odongo

Department of Political Science and Public Administration, University of Nairobi, Nairobi, Kenya
Email: *kenobumba@gmail.com, jobosi@uonbi.ac.ke, henry.odongo@uonbi.ac.ke

How to cite this paper: Ogutu, K. O., Obosi, J. O., & Odongo, H. A. (2025). Strengthening Cyber Defenses: The Impact of Multi-Agency Information Sharing on Cybercrime Prevention in Kenya. *Open Journal of Social Sciences, 13,* 452-473.
https://doi.org/10.4236/jss.2025.138030

Received: July 18, 2025
Accepted: August 17, 2025
Published: August 20, 2025

Abstract

The paper investigated how impactful inter-agency information sharing had been in curbing cybercrime and sought to uncover the underlying causes of its limited success. A cross-sectional research design alongside concurrent mixed methods approaches was employed. Primary data was obtained from officers working with the cybercrime prevention institutions, including mobile service providers such as Airtel and Safaricom. In realizing the article's objective, simple linear regression was adopted. The paper established that effective multi-agency information sharing significantly enhanced cybercrime prevention by improving threat detection, response, and coordination. However, institutional performance varied, with some demonstrating strong collaboration frameworks, while others faced challenges due to jurisdictional disputes, outdated policies, technical gaps, and mistrust. Private sector involvement was moderate, hindered by governance and privacy concerns. The paper concluded that effective multi-agency information sharing enhanced cybercrime prevention, but its impact varied across institutions, highlighting the need for harmonized legal, policy, technical, and trust-building reforms. The article recommended harmonized legal reforms, trust-building, improved technical interoperability, capacity building, and private sector inclusion through clear frameworks and incentives for enhanced multi-agency collaboration.

Keywords

Promoting Information-Sharing Initiatives, Multi-Agency Collaboration, Cybercrime Prevention

1. Introduction

In the contemporary digital era, cybersecurity has emerged as a paramount con-

cern, with cyber threats evolving swiftly and impacting individuals, enterprises, and governmental bodies globally (Basak, 2024). As Kenya progresses through its digital transformation, the imperative for robust cybersecurity measures has intensified. The nation's growing dependence on digital platforms, including mobile banking, e-commerce, and online government services, has heightened the risks associated with cybercrime (Okuku, Renaud, & Valeriano, 2015). Between April 2011 and December 2019, Kenya witnessed a significant surge in cyber threats, despite various government efforts to curb them. Reports consistently highlighted widespread web-based and internal system threats, with millions of cyber-attacks occurring annually (Kenya National Bureau of Statistics Economic Survey, 2020). Prominent incidents included SIM card fraud, denial-of-service (DoS) attacks, and unauthorized access to IT systems. The number of reported threats increased from 22.1 million in 2012-2013 to 51.9 million in 2013-2014. By the final quarter of 2019 alone, cyber threats had spiked by 47.3% compared to the previous quarter. By 2016, financial damages from cybercrime had escalated to around Sh18 billion, signaling an intensifying cybersecurity challenge (Gitari, 2020). Acknowledging these challenges, the Kenyan government has incorporated promoting information sharing among multi-agencies as a strategic initiative into its comprehensive ICT policy framework to counteract cyber threats. Specifically, the National ICT Policy under Section 15.1 underscores the importance of sharing information among multi-agencies in order to prevent, detect, and respond to cyber threats (Government of Kenya, 2016). This policy framework demonstrates the government's dedication to addressing the escalating incidents of cybercrime, which have been exacerbated by increased internet penetration, the proliferation of smart devices, and the growing sophistication of cybercriminals. Prioritizing capacity building initiatives, such as promoting information sharing among multi-agencies, is envisioned to bolster Kenya's resilience against cyber threats while promoting a secure digital environment conducive to economic and social development (The National KE-CIRT/CC, 2024).

Cybercrime has surfaced as a formidable threat to national security, financial stability, and individual privacy in Kenya. Criminal activities such as phishing, ransomware attacks, identity theft, and financial fraud have become increasingly prevalent, targeting both private and public institutions (Ndeda & Odoyo, 2019). The Communications Authority of Kenya (CA) and the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) have reported a steady rise in cyber incidents, with millions of attempted attacks detected annually. Without a proper setup where different stakeholders are able to share information, data, and intelligence to counteract these threats, Kenya remains susceptible to data breaches, financial losses, and reputational harm (The National KE-CIRT/CC, 2023).

The National Cybersecurity Strategy 2022-2027, for example, aligned with the objectives of the Computer Misuse and Cyber Crimes Act, emphasizing the need for a multi-agency approach to detect, prevent, and respond to cybercrime

(Government of Kenya, 2022). This strategy served as a roadmap to address emerging challenges in the cyber domain, highlighting the importance of coordinated actions among various stakeholders. Additionally, the National ICT Policy underscored the significance of cybersecurity as a fundamental aspect of Kenya's digital ecosystem (Government of Kenya, 2019). It advocated for capacity building and skills development to ensure that cybersecurity institutions were able to adequately share information between and among them in order to handle evolving cyber threats.

International collaborations were also expected to play a pivotal role in Kenya's cybersecurity landscape. For instance, Operation Serengeti, a joint effort between Interpol and Afripol conducted over two months, targeted cybercrime across 19 African countries, including Kenya. The operation resulted in over 1000 arrests and identified 35,000 victims, with financial losses nearing $193 million. This operation demonstrated enhanced cooperation among the participating countries' law enforcement agencies, showcasing the effectiveness of collaborative efforts in combating cybercrime (Banchereau, 2024).

Additionally, the existing literature and policy frameworks underscore the theoretical importance of multi-agency collaboration and information sharing in cybersecurity. However, there is a discernible gap in empirical research that evaluates the practical outcomes of these collaborative efforts. Specifically, the extent to which promoting information sharing among multi-agencies has impacted cybercrime prevention in Kenya remains underexplored. Recent studies further emphasize this trend. For example, Al-Salim, Faraj & Tarek (2023) found that structured inter-agency collaboration frameworks in the Middle East significantly reduced state-level vulnerability to cybercrime. Muturi & Wangari (2022) documented improved incident resolution times in Kenya following the integration of a multi-stakeholder cyber response framework. Similarly, Zhou & Chang (2024) illustrated that AI-supported data sharing among Chinese regulatory bodies enhanced detection and reporting of cyber threats. These findings reinforce the empirical and theoretical foundations for multi-agency information sharing as a vital cybersecurity mechanism. This gap necessitates an in-depth investigation to understand the effectiveness of current information-sharing practices, identify existing challenges, and propose strategies for enhancing collaborative efforts.

Kenya had made significant strides in establishing frameworks for multi-agency collaboration and information sharing in cybersecurity; however, the practical impact of these initiatives on cybercrime prevention remained inadequately explored. The objective of this article was therefore to establish the impact of promoting information sharing among multi-agencies on cybercrime prevention in Kenya. The corresponding research question sought to determine the extent to which such information sharing had affected cybercrime prevention efforts. The article also hypothesized that promoting information sharing among multi-agencies in the cybersecurity sector had contributed to cybercrime prevention by enabling the timely exchange of threat intelligence, facilitating collaboration on cybersecurity

initiatives, and improving overall cybersecurity readiness. The article established that, indeed, promoting multi-agency information sharing significantly enhanced the effectiveness of cybercrime prevention. It also found that its efficacy was hindered by poor coordination, lack of trust, incompatible systems, legal barriers, unclear roles, and limited ICT infrastructure, leading to inefficiencies and delayed decision-making.

2. Theoretical Framework

Rational Choice Theory (RCT), first conceptualized by Adam Smith in 1776, offers a compelling framework for evaluating the role of multi-agency information sharing in cybercrime prevention in Kenya. The theory holds that decisions, whether by individuals or institutions, are made through a logical analysis of costs, benefits, and risks, with the goal of selecting the option that yields the greatest net benefit to society (Stalans & Donner, 2018). It posits that individuals act based on perceived costs and benefits. This framework guided the selection of variables, assuming that government support through training, resources, innovation, and coordination alters the cost-benefit calculus of officers in favour of proactive cybercrime prevention. It assumes that actors are rational agents striving to maximize utility while minimizing costs, that they have access to sufficient information to make informed choices, and that their preferences are stable over time. In this context, the Kenyan government and its agencies would only prioritize and institutionalize information sharing if the perceived benefits, such as faster response to threats, stronger national cyber resilience, and reduced cybercrime, clearly outweigh the associated legal, technical, and operational challenges.

RCT has been widely used in analyzing crime prevention policies and institutional behavior. For example, in the United States, it has explained the effectiveness of coordinated law enforcement strategies in reducing financial crimes (Paternoster et al., 2015). Zhao et al. (2021) applied RCT to show how the perceived risk of detection affects offenders' choices, while Whitmire (2020) explored how cybercriminals assess the likelihood of being caught before engaging in digital crimes. These studies illustrate how RCT can be applied to understand both institutional cooperation and individual decision-making in crime prevention efforts.

Under the RCT framework, an effective policy should consistently deliver high-impact outcomes, which underscores the importance of addressing institutional and legal barriers to information sharing in Kenya. The move toward strengthening multi-agency collaboration on cybersecurity issues reflects a rational policy response to increasingly complex and cross-sector cyber threats. The evidence indicates that where real-time information sharing and inter-agency collaboration are well-established, key operational indicators such as the Mean Time to Detect and Respond (MTTDR) and the Mean Time to Investigate and Resolve (MTTIR) have significantly improved. By pooling resources, expertise, and intelligence, agencies have been able to respond more quickly and effectively to cyber incidents, enhancing the country's overall resilience.

Rational Choice Theory, therefore, explains the article's findings by suggesting that each agency makes decisions based on perceived costs and benefits. While effective information sharing helped prevent cybercrime, some agencies withheld data when they perceived risks such as loss of control, exposure, or lack of reciprocation as outweighing the benefits. Barriers like poor coordination, trust deficits, and legal uncertainty increased the "cost" of sharing, making non-cooperation a rational choice for some. Thus, even when collaboration improved cybercrime prevention, agencies acted in self-interest, weighing institutional survival, jurisdictional control, and resource allocation over collective security, illustrating the fragmented implementation of rational behavior.

3. Research Design and Methodology

The article adopted a descriptive research design. To comprehensively address the article's objective, a concurrent mixed-methods approach was implemented, integrating both quantitative and qualitative data collection techniques. This methodological choice was driven by the necessity to obtain statistical data via questionnaires and to gather in-depth textual insights through Key Informant Interviews. Primary quantitative data were gathered from seventy-two (72) officers employed in cybercrime prevention institutions and telecommunications companies across Kenya with the help of survey questionnaires. The independent variable, Promoting Information Sharing Among Multi-Agencies (PISAMA), was measured using Likert-scale items covering six dimensions: timeliness, accuracy & reliability, relevance, confidentiality, system compatibility, and legal frameworks. The dependent variable, Cybercrime Prevention (CP), was assessed using items reflecting Mean Time to Detect and Respond (MTTDR), Mean Time to Investigate and Resolve (MTTIR), Ability to Implement Preventive Measures (ATIPM), as well as Level of Adaptability (LoA). The scales' internal consistency was confirmed with Cronbach's Alpha of 0.87, indicating high reliability. No item weighting was applied; all responses were treated equally. Qualitative data, on the other hand, were collected through interviews with eleven (11) Key Informants. These informants comprised department heads from pivotal agencies, including the Cyber Crime Unit-Investigation (CCU-I), the Digital Forensic Laboratory of Kenya (DFLK), the Ministry of ICT, the Anti-Counterfeit Authority (ACA), the Communications Authority of Kenya (CAK), the Central Bank of Kenya's Cybercrime Prevention Unit (CBK-CPU), the National Intelligence Service's Cyber Security Unit (NIS-CSU), the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), the National Cyber Command Centre (NC3), as well as representatives from Safaricom and Airtel. **Figure 1** shows the number of officers selected in each institution.

This section presents an in-depth analysis of the impact of multi-agency information sharing on cybercrime prevention across selected institutions in Kenya. The article involved participants from key institutions actively engaged in the fight against cybercrime in Kenya. These included officers and cybersecurity

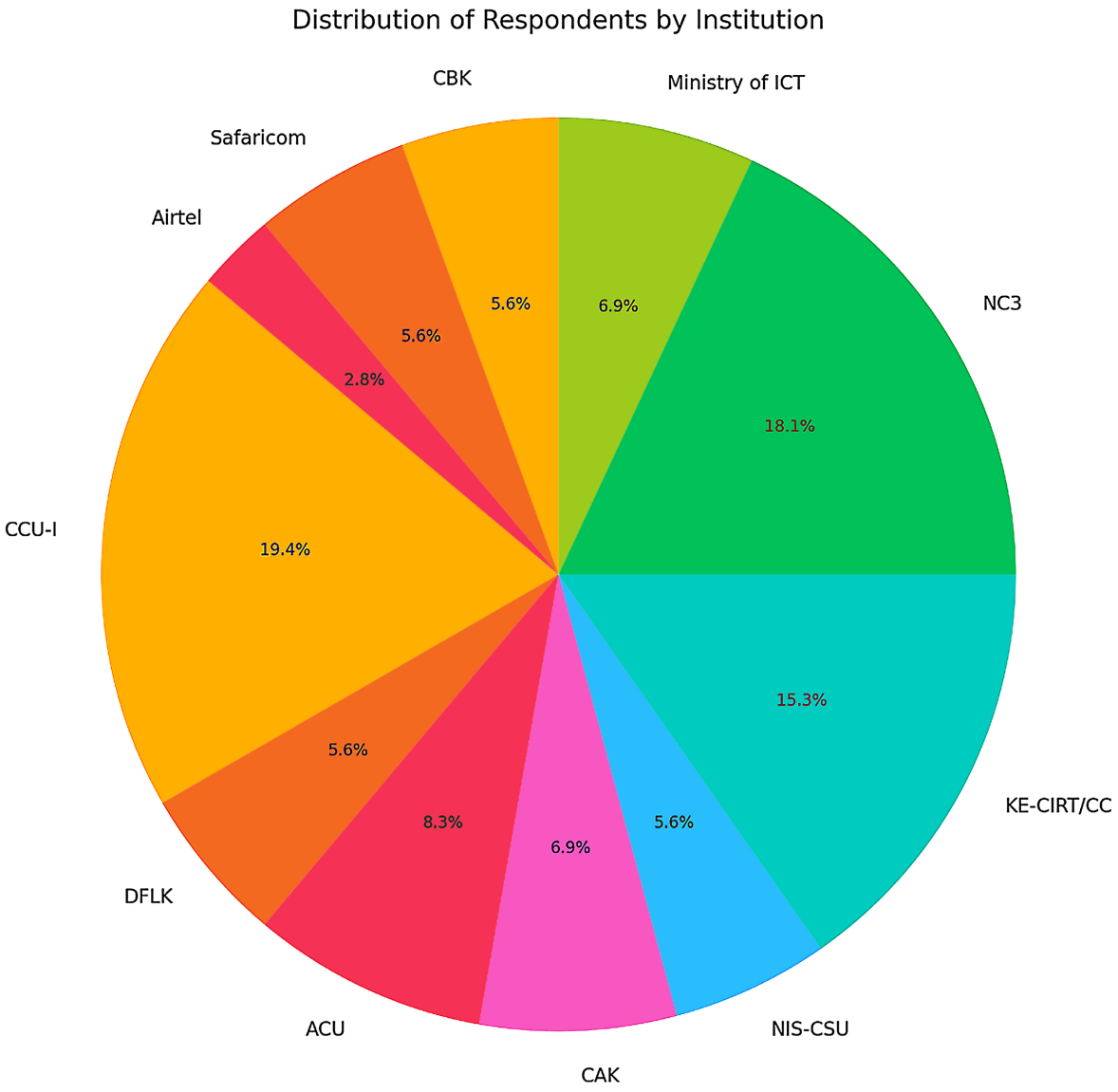

Figure 1. Respondent's working ınstitution.

professionals from government, regulatory bodies, law enforcement, intelligence, and telecommunications sectors. Specifically, the organizations represented were KE-CIRT/CC, NC3, CAK, CBK-CPU, NIS-CSU, CCU-I, DFLK, ACU, the Ministry of ICT, as well as telecommunication providers such as Safaricom and Airtel. These entities were deliberately chosen for their critical roles in cybercrime detection, investigation, prosecution, and adjudication across the country.

Quantitative data obtained through survey questionnaires were analyzed using SPSS version 26. The article employed univariate analysis with descriptive statistics, and the results were displayed in tables. To test the hypothesis that, "*Promoting information sharing among multi-agencies in the cybersecurity sector had contributed to cybercrime prevention by enabling the timely exchange of threat intelligence, facilitating collaboration on cybersecurity initiatives, and improving overall cybersecurity readiness*," simple linear regression was utilized. This method

was deemed appropriate as it allowed for assessing the influence of the policy initiative on cybercrime prevention, based on insights from officers serving in Kenya's cybercrime prevention agencies.

Thematic analysis, on the other hand, was employed to examine qualitative data obtained from key informant interviews. The process began with familiarization, during which the researcher repeatedly read the data to gain a deep understanding and made initial notes. This was followed by systematic coding, where relevant portions of the data were labeled according to their significance to the article's objective. Similar codes were then grouped to form overarching themes that captured key patterns in the responses. These themes were reviewed for consistency and accuracy to ensure they reflected both the coded material and the overall dataset. After refinement, each theme was clearly defined and named to convey its core message. The final step involved crafting a narrative report that integrated these themes, included illustrative quotes, and connected the insights to the article's objective.

4. Data Analysis

Data analysis was based on testing the hypothesis that *promoting information sharing among multi-agencies in the cybersecurity sector had contributed to cybercrime prevention by enabling the timely exchange of threat intelligence*, *facilitating collaboration on cybersecurity initiatives*, *and improving overall cybersecurity readiness*. This analysis sought to determine the impact of multi-agency information sharing on cybercrime prevention in Kenya, focusing on the extent to which promoting information sharing had contributed to *timely exchange of threat intelligence*, *facilitating collaboration on cybersecurity initiatives*, *and improving overall cybersecurity readiness*. A simple linear regression model was employed to test the significance of the relationship between promoting information sharing and cybercrime prevention. Prior to regression analysis, diagnostic tests were conducted to ensure that the key assumptions were met. Linearity was assessed through scatterplots, normality of residuals via Q-Q plots and the Shapiro-Wilk test, and homoscedasticity by examining residual plots. The assumptions were reasonably satisfied. Where minor violations occurred, robust standard errors were used to address potential heteroskedasticity. This approach enabled a quantitative evaluation of whether increased information sharing efforts had translated into improved cybercrime prevention outcomes, as aligned with the broader policy objective of enhancing national cybersecurity readiness.

To test the hypothesis that *promoting information sharing among multiple agencies in the cybersecurity sector had not supported cybercrime prevention through timely threat intelligence exchange*, *enhanced collaboration on cybersecurity efforts*, *or improved overall preparedness against cyber threats*, respondents were asked to indicate their level of agreement with a set of statements reflecting key aspects of information sharing among multi-agencies. These included whether the agency received timely cyber threat information from partner institutions to re-

spond effectively; whether the cyber threat intelligence shared by other agencies was accurate and dependable; whether information received from partner agencies was relevant to cybersecurity operations and needs; whether sensitive information shared between agencies was handled with appropriate confidentiality and security protocols; and lastly, whether the agency could easily access and use cybersecurity data shared by other institutions due to system compatibility. These questions formed the basis for analyzing the impact of promoting information sharing among multi-agencies on cybercrime prevention.

To explore the relationship between promoting information sharing among multiple agencies and cybercrime prevention, simple linear regression analysis, which is a reliable method for testing hypotheses, was employed. In this analysis, the combined scores from statements representing key aspects of promoting inter-agency information sharing were treated as the independent variable (IV), while cybercrime prevention was designated as the dependent variable (DV). These variables were then subjected to simple linear regression, with the results detailed in the following tables.

Null Hypothesis (H_0): Promoting information sharing among multiple agencies in the cybersecurity sector has not supported cybercrime prevention through timely threat intelligence exchange, enhanced collaboration on cybersecurity efforts, or improved overall preparedness against cyber threats.

4.1. The Model Summary Table

The model summary Table 1 provided an overview of the regression model's performance in predicting the dependent variable "cybercrime prevention" (cp) based on the predictor variable "promoting information sharing among multi-agencies" (pisama). The correlation coefficient (R) measured the strength and direction of the linear relationship between the predictor variable(s) and the dependent variable. In this case, the R value was .921, indicating a strong positive correlation between promoting information sharing among multi-agencies (pisama) and cybercrime prevention (cp). The coefficient of determination (R Square) represented the proportion of variance in the dependent variable (cp) that was explained by the predictor variable (pisama). Here, R Square was .848, indicating that approximately 84.8% of the variance in cybercrime prevention could be explained by promoting information sharing among multi-agencies.

Table 1. Model summary table.

Model Summary[b]									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.921[a]	.848	.846	.58130	.848	390.826	1	70	.000

[a]Predictors: (Constant), pisama; [b]Dependent Variable: cp.

Adjusted R Square took into account the number of predictors in the model and provided a more accurate estimate of the proportion of variance. In this case, the Adjusted R Square was .846. Implications and conclusions were as follows: the strong correlation coefficient (R) suggested a significant positive relationship between promoting information sharing among multi-agencies and cybercrime prevention. The high R Square value indicated that promoting information sharing among multi-agencies explained a large proportion of the variance in cybercrime prevention. The low Std. Error of the Estimate suggested that the model provided a good fit to the data. The significant F statistic (Sig. F Change = .000) indicated that adding promoting information sharing among multi-agencies to the model significantly improved its ability to predict cybercrime prevention. In conclusion, the regression analysis demonstrated that promoting information sharing among multi-agencies was a significant predictor of cybercrime prevention.

4.2. The ANOVA Table

The ANOVA Table 2 provided information about the overall significance of the regression model in predicting the dependent variable "cybercrime prevention" (cp) based on the predictor variable "promoting information sharing among multi-agencies" (pisama). The Regression row indicated the performance of the regression model in explaining the variance in cybercrime prevention (cp). The Sum of Squares Regression (132.065) represented the variability in cybercrime prevention that was accounted for by the predictor variable (promoting information sharing among multi-agencies). The Sum of Squares Residual (23.654) represented the unexplained variability in cybercrime prevention that was not accounted for by the predictor variable. The *p*-value (Sig.) associated with the F statistic was 0.000, indicating that the regression model was statistically significant at a conventional alpha level of 0.05. This suggests that promoting information sharing among multi-agencies significantly contributes to predicting cybercrime prevention. Therefore, *the Null Hypothesis* (H_0) *stating that promoting information sharing among multiple agencies in the cybersecurity sector had not supported cybercrime prevention through timely threat intelligence exchange, enhanced collaboration on cybersecurity efforts, or improved overall preparedness against cyber threats was rejected. This therefore meant that promoting information sharing among multiple agencies in the cybersecurity sector had supported*

Table 2. ANOVA table.

ANOVA[a]						
	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	132.065	1	132.065	390.826	.000[b]
	Residual	23.654	70	.338		
	Total	155.719	71			

[a]Dependent Variable: cp. [b]Predictors: (Constant), pisama.

cybercrime prevention through timely threat intelligence exchange, enhanced collaboration on cybersecurity efforts, or improved overall preparedness against cyber threats.

4.3. The Coefficient Table

The Coefficients Table 3 provided information about the estimated coefficients for the regression model predicting the dependent variable "cybercrime prevention" (cp) based on the predictor variable "promoting information sharing among multi-agencies" (pisama). The coefficient for "promoting information sharing among multi-agencies" (pisama) was statistically significant ($p < .05$) with a high standardized coefficient (Beta = .921). This indicated that promoting information sharing among multi-agencies had a strong positive effect on cybercrime prevention. For each one unit increase in promoting information sharing among multi-agencies, there was a predicted increase of 1.621 units in cybercrime prevention. The significant t-value and low *p*-value for the predictor variable "promoting information sharing among multi-agencies" (pisama) indicated that the relationship between promoting information sharing among multi-agencies and cybercrime prevention was statistically significant.

Table 3. Coefficients table.

Coefficients[a]									
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	−2.764	.296		−9.324	.000			
	Pisama	1.621	.082	.921	19.769	.000	.921	.921	.921

[a]Dependent Variable: cp.

The findings showed that promoting information sharing among multiple agencies played a critical role in strengthening cybercrime prevention efforts. The results confirmed that when institutions actively collaborate, share threat intelligence, and coordinate cybersecurity initiatives, they are better equipped to detect, respond to, and prevent cyber threats. This reinforces the importance of structured communication and cooperation among agencies in enhancing overall cybersecurity readiness and effectiveness.

In addition, this analysis expanded on the tested hypothesis by exploring the specific dimensions of multi-agency information sharing that influenced its effectiveness. Rather than focusing solely on statistical relationships, it was essential to examine how various government and security institutions implemented these dimensions and what factors made certain institutions more effective than others under these dimensions. This section provides a comparative assessment of institutional performance using aggregated mean scores, shedding light on the scope and intensity of information sharing efforts across agencies. Particular attention

was given to *timeliness*, *accuracy*, *relevance*, *confidentiality & security*, *as well as accessibility & interoperability*. The incorporation of qualitative insights from institutional heads significantly deepened the interpretation of findings by elucidating the underlying drivers of observed patterns in the implementation of inter-agency information sharing. These perspectives enriched the analysis by uncovering institutional strengths and clarifying the ways in which organizational policies, regulatory frameworks, and bureaucratic dynamics shaped the practical outcomes of collaborative information exchange. Consequently, this qualitative dimension provided a foundation for formulating evidence-based recommendations to enhance policy and practice in cybercrime prevention.

To assess the influence of inter-agency information sharing across government, regulatory, law enforcement, intelligence, and telecommunications sectors, participants were asked to evaluate their level of agreement with statements aligned to five principal dimensions: *timeliness*, *accuracy*, *relevance*, *confidentiality & security*, and *accessibility & interoperability*. These dimensions were analytically examined using descriptive statistical measures, specifically institutional mean scores, to capture perceived effectiveness. As presented in **Table 4**, the resulting analysis offered a comparative perspective on institutional performance, elucidating exemplary practices while identifying gaps that hindered the strategic role of inter-agency information sharing in mitigating cyber threats.

The analysis of mean scores provides insight into how different institutions performed in promoting inter-agency information sharing across five key dimensions. The National Cyber Command Centre (NC3) reported the highest average score (M = 3.9722), suggesting strong engagement in information sharing activities. This was closely followed by KE-CIRT/CC (M = 3.9167), which also demonstrated substantial institutional capacity and coordination in this domain.

Institutions such as CBK (M = 3.7917), CAK (M = 3.8333), and the Ministry of ICT (M = 3.8333) reflected consistently high mean scores, indicating a relatively robust framework for inter-agency collaboration. Airtel (M = 3.6410), ACU (M = 3.6548), and Safaricom (M = 3.5606) showed moderately strong performance, suggesting notable but uneven efforts toward information exchange.

Conversely, institutions like the Cyber Crime Unit-Investigation (CCU-I) (M = 2.7000), DFLK (M = 2.9583), and the NIS Cyber Security Unit (NIS-CSU) (M = 2.5000) recorded lower mean scores. These findings suggest that these entities may face institutional, technical, or policy barriers that constrain effective information sharing and may benefit from targeted capacity-building and policy harmonization efforts.

Standard deviation values also offer insight into internal consistency. For instance, DFLK had the lowest variation (SD = .20972), suggesting relatively homogeneous responses, while the Ministry of ICT showed greater variability (SD = 1.17851), possibly reflecting differences in implementation or perception across its units.

The findings revealed substantial variations across institutions in promoting

Table 4. Ranking of institutional performance on inter-agency information sharing based on mean scores.

Respondent's working institution		Minimum	Maximum	Mean	Std. Deviation
ACU	pisama	2.00	4.67	3.6548	.89744
	Valid N (listwise)				
CBK	pisama	3.00	4.67	3.7917	.91667
	Valid N (listwise)				
NC3	pisama	2.83	4.50	3.9722	.59082
	Valid N (listwise)				
CCU-I	pisama	2.00	3.17	2.7000	.44721
	Valid N (listwise)				
CAK	pisama	3.00	4.67	3.8333	.96225
	Valid N (listwise)				
Safaricom	pisama	2.00	4.50	3.5606	.85723
	Valid N (listwise)				
Airtel	pisama	2.67	4.67	3.6410	.78128
	Valid N (listwise)				
NIS-CSU	pisama	2.00	3.17	2.5000	.50000
	Valid N (listwise)				
KE-CIRT/CC	pisama	2.83	4.50	3.9167	.75154
	Valid N (listwise)				
DFLK	pisama	2.67	3.17	2.9583	.20972
	Valid N (listwise)				
Ministry of ICT	pisama	3.00	4.67	3.8333	1.17851
	Valid N (listwise)				

inter-agency information sharing. Some institutions demonstrated strong engagement and coordination, indicating well-established frameworks for collaboration and information exchange. Others showed moderate performance, suggesting ongoing but uneven efforts in this area. A few institutions recorded notably lower levels of engagement, pointing to possible institutional, technical, or policy-related constraints that may hinder effective collaboration. These disparities underscore the need for targeted interventions to strengthen institutional capacity and promote more harmonized inter-agency information-sharing practices.

Building on the above finding, the observed variations in institutional performance highlighted the need to further investigate the underlying factors shaping inter-agency information sharing. The disparities pointed to potential structural, operational, or contextual influences affecting how institutions engage in collaboration. To gain a more comprehensive understanding, respondents were asked a

follow-up question: *Why were there variations in the sharing of information among multi-agencies in Kenya*? This inquiry sought to uncover practical, institutional, and systemic explanations that could guide more targeted and effective policy and operational interventions.

The responses were examined through descriptive statistical methods, with a focus on mean scores to capture the perceived reasons behind variations in information sharing practices among institutions. These mean scores were generated from data provided by officers drawn from eleven cybercrime prevention institutions in Kenya. The scores (ranging from 1 = Strongly Disagree to 5 = Strongly Agree) reflected perceptions of institutional strength in six thematic areas: *No protocols*, *technological gaps*, *bureaucracy*, *low trust*, *poor training*, *and policy gaps*. The perceived variations, established through descriptive analysis of mean scores, were further substantiated by qualitative insights gathered from key informant interviews involving 11 departmental heads from cybercrime prevention institutions. These qualitative accounts offered a more nuanced understanding of the contextual factors influencing information sharing, thereby enhancing and validating the interpretation of the quantitative results. The analysis of the responses is shown in Table 5 below.

Table 5. Perceived causes of differences in ınter-agency ınformation sharing among ınstitutions.

Institution	No standard Protocols	Technological Gaps	Bureaucracy	Low Trust Levels	Poor Training	Policy Gaps	Mean Score (Overall)
NIS-CSU	2.8	3.1	2.9	2.7	2.8	3.0	2.88
CCU-I	2.9	3.2	3.0	2.8	3.1	2.9	3.00
CBK-CPU	3.5	3.3	3.9	3.1	3.4	3.6	3.47
KE-CIRT/CC	4.4	4.1	4.2	4.0	4.1	4.3	4.18
Safaricom	3.3	3.0	3.5	2.9	3.2	3.4	3.22
Airtel	3.6	3.4	3.7	3.3	3.5	3.6	3.52
DFLK	2.8	3.1	2.9	2.7	2.8	3.0	2.88
NCCC (NC3)	4.2	4.3	4.5	4.0	4.0	4.4	4.23
ACU	4.1	3.8	4.3	3.7	3.9	4.2	4.00
CAK	3.7	3.9	4.1	3.6	3.8	4.0	3.85
Ministry of ICT	4.0	3.5	4.2	3.3	3.7	4.1	3.80

Institutions such as NCCC (NC3) and KE-CIRT/CC demonstrated the highest overall mean scores (M = 4.23 and M = 4.18, respectively), suggesting a strong recognition of the structural and contextual challenges affecting seamless collaboration. NCCC, for instance, reported high scores across all dimensions, especially on *organizational bureaucracy* (4.5) and *legal and policy gaps* (4.4), which the head of the institution affirmed by stating: "*Despite our advanced technical capacity, cross-agency operations often stall due to unclear mandates and jurisdic-*

tional overlaps. Legal harmonization is urgently needed." KE-CIRT/CC similarly acknowledged legal and interoperability challenges, with their head explaining: "*We are ready and willing to share data in real time, but outdated legislative frameworks and protocol mismatches delay our response capacity.*"

Moderately performing institutions, including ACU (M = 4.00), CAK (M = 3.85), and the Ministry of ICT (M = 3.80), also showed strong awareness of institutional and policy-level constraints. CAK, for example, scored 4.1 on *organizational bureaucracy* and 4.0 on *legal gaps*. The CAK head emphasized: "*Regulatory fragmentation across sectors affects how and when we exchange information. A more centralized framework would streamline this.*"

On the other hand, CBK-CPU (M = 3.47), Airtel (M = 3.52), and Safaricom (M = 3.22) reflected more sector-specific limitations in information sharing. Notably, Safaricom scored significantly on *organizational bureaucracy* (3.8), suggesting institutional constraints rooted in corporate policy. The Safaricom representative explained: "*Due to strict internal data protection and privacy policies, we do not release sensitive customer data such as Call Data Records (CDRs) to any security agency without a valid court order or warrant. This policy, while essential for protecting user rights, sometimes delays our collaboration with government agencies.*"

The lowest mean scores were recorded by CCU-I (M = 3.00), DFLK (M = 2.88), and NIS-CSU (M = 2.88), indicating minimal engagement or awareness of the key challenges constraining inter-agency coordination. Notably, NIS-CSU scored particularly low on *low trust among agencies* (2.7), an issue that the head of unit admitted: "*In some cases, we have refrained from full disclosure due to uncertainties around how our intelligence would be handled or interpreted by partner agencies.*" The head of CCU-I echoed these sentiments, stating: "*We often lack timely updates from other enforcement arms, leading to duplication of efforts or operational blind spots.*" Similarly, the DFLK head highlighted internal fragmentation: "*Even within our own department, data flow is inconsistent. External sharing is even more cumbersome due to procedural bottlenecks.*"

Overall, the finding illustrates that higher-performing institutions tend to have greater clarity on systemic constraints and have taken proactive steps to address them, while lower-performing entities face institutional inertia, mistrust, data privacy regulations, or technical limitations that inhibit information exchange. These findings emphasize the need for policy reforms, legal harmonization, trust-building measures, and interoperability protocols that bridge gaps between public and private sector actors involved in cybercrime prevention.

Further, and building on the observed disparities in institutional performance, it also became evident that addressing the root causes of these variations required a deeper understanding of the structural and operational reforms needed to enhance inter-agency collaboration. The findings pointed to critical areas such as policy alignment, legal clarity, data interoperability, and trust-building as foundational pillars for effective information exchange. In light of these insights, re-

spondents were asked: "*What reforms do you believe are most necessary to improve multi-agency information sharing*?" This question aimed to elicit informed perspectives on the most impactful and feasible reforms from those directly engaged in cybercrime prevention, thereby guiding targeted and evidence-based recommendations for strengthening institutional collaboration frameworks in Kenya.

The responses were examined through descriptive statistical methods, with a focus on mean scores to capture the perceived *reforms that are most necessary to improve multi-agency information sharing* among institutions. These mean scores were generated from data provided by officers drawn from eleven cybercrime prevention institutions in Kenya. The scores (ranging from 1 = Strongly Disagree to 5 = Strongly Agree) reflected perceptions of institutional strength in four thematic areas: average score on policy changes, average rating of legal adjustments, mean value of system integration enhancements, and average assessment of trust enhancement measures. The suggested reforms, identified through descriptive analysis of mean scores, were further reinforced by qualitative perspectives obtained from interviews with 11 departmental heads across cybercrime prevention institutions. These qualitative insights provided a deeper and more contextualized understanding of the proposed reforms that, if enacted, could enhance inter-agency information sharing. This integration of qualitative evidence enriched and validated the interpretation of the quantitative findings, offering a more comprehensive view of the institutional dynamics at play. The analysis of the responses is shown in Table 6 below.

Table 6. Most essential reforms to enhance multi-agency ınformation sharing.

Institution	Average Score on Policy Changes	Average Rating of Legal Adjustments	Mean Value of System Integration Enhancements	Average Assessment of Trust Enhancement Measures
NIS-CSU	2.9	3.0	2.7	3.2
CCU-I	3.2	3.4	3.1	3.5
CBK-CPU	4.1	4.2	3.9	4.0
KE-CIRT/CC	4.3	4.4	4.5	4.2
Safaricom	3.5	3.1	3.3	2.9
Airtel	3.6	3.2	3.4	3.0
DFLK	3.0	3.1	3.2	2.8
NCCC	4.4	4.3	4.5	4.5
ACU	3.8	3.9	3.6	4.0
CAK	4.0	3.9	4.2	3.8
Ministry of ICT	4.5	4.6	4.4	4.3

The Central Bank of Kenya-Cyber Protection Unit (CBK-CPU) emerged as the most reform-forward institution, with high mean scores across all dimensions: policy reforms (4.3), legal reforms (4.5), interoperability improvements (4.2), and trust-building initiatives (4.3). This performance reflects a proactive institutional culture toward regulatory alignment and operational readiness. The head of CBK-CPU reinforced these scores by stating, "*The Banking Act and Data Protection Act must be harmonized to facilitate secure and lawful data exchange during cyber incidents*." He further noted, "*We've already begun aligning our IT infrastructure with national standards to support real-time information sharing*," and emphasized, "*Trust is earned through transparency. We advocate for shared audits and feedback mechanisms to build credibility among institutions*."

Closely following was KE-CIRT/CC, with equally robust scores in policy reforms (4.2), legal reforms (4.4), interoperability improvements (4.6), and trust-building initiatives (4.4). The high interoperability score underscores its leadership in technical integration. The head of KE-CIRT/CC attributed their performance to deliberate investment in infrastructure and policy engagement: "*We are currently developing an integrated dashboard for all agencies. Standardized data formats and protocols are key*." He also noted the role of legal frameworks, stating, "*Without a clear legal mandate, we're often stuck in bureaucratic loops. We need legislation that mandates cooperation during cyber emergencies*." On trust, he highlighted, "*We've initiated inter-agency cybersecurity exercises to build rapport and readiness*."

The Ministry of ICT demonstrated strong support for structural reforms, scoring 4.1 on policy, 4.3 on legal reforms, 4.0 on interoperability, and 4.2 on trust-building. These figures reflect its central role in shaping national ICT standards. According to the head of the Ministry, "*We are at the policy nerve center and must lead by example. Legal coherence and interoperability are not optional; they are essential*." She further asserted, "*Our trust-building efforts have focused on facilitating multi-agency meetings and national cyber drills to bridge institutional silos*."

CAK and NCCC also posted consistently high mean scores across the four reform categories. For instance, NCCC recorded 4.0 on policy, 4.2 on legal, 3.8 on interoperability, and 4.1 on trust-building, signaling a security agency committed to institutional collaboration. The head of NCCC remarked, "*We understand that national cybersecurity requires coordinated vigilance. Legal reforms to protect whistleblowers and improve cross-agency access are vital*." Meanwhile, CAK recorded 4.1 on policy and 4.0 on legal, reflecting a regulatory agency well-aligned with reform priorities. The head of CAK emphasized, "*Data protection must be balanced with operational efficiency. We support reforms that make that possible without compromising regulatory compliance*."

In the private sector, Safaricom scored moderately across the board: policy reforms (3.5), legal reforms (3.6), interoperability (3.4), and trust-building (3.2). While there is institutional willingness to collaborate, strong adherence to internal governance frameworks tempers external engagement. As explained by the head

of Safaricom, "*We align with national policies, but clearer guidance on public-private data exchange is essential*." He added, "*We cannot release client data such as call data records* (*CDRs*) *unless there's a court order. Our data privacy policies are non-negotiable*," highlighting legal limitations. On system integration, he admitted, "*We've integrated APIs that can support limited information sharing under approved protocols*," though he conceded that, "*There's hesitation from both sides. A formalized framework would help reduce this friction*."

Airtel performed similarly, with scores slightly below Safaricom, posting 3.4 in policy, 3.5 in legal, 3.3 in interoperability, and 3.1 in trust-building. According to the head of Airtel, "*Our compliance model favors customer confidentiality, which sometimes creates friction in multi-agency engagements*." She also noted, "*We would benefit from legal reforms that provide clearer liabilities and protections when sharing sensitive data*."

ACU, DFLK, and CCU-I demonstrated moderate to low reform readiness. For example, CCU-I recorded 3.2 in policy, 3.0 in legal, 3.1 in interoperability, and 3.0 in trust-building. These scores suggest structural inertia and operational fragmentation. The head of CCU-I candidly acknowledged, "*Our internal policies are outdated and lack the flexibility needed to work seamlessly with other agencies. We need adaptive frameworks that recognize the dynamic nature of cyber threats*." On legal issues, he explained, "*The current legal instruments do not compel certain agencies to share data except through lengthy legal procedures*." With regard to interoperability, he admitted, "*Our platforms are not technically aligned with those used by partner institutions*," and on trust, "*There's still suspicion and territorialism in how we relate to sister agencies*."

At the bottom of the reform spectrum was NIS-CSU, scoring 2.9 in policy, 3.0 in legal, 2.8 in interoperability, and 3.0 in trust-building. These figures reflect a highly compartmentalized institution where operational secrecy overshadows collaboration. The head of NIS-CSU explained, "*As an intelligence unit, our policy is risk-averse and tends to limit external collaboration unless absolutely necessary*." On the legal front, he remarked, "*We often find ourselves navigating conflicting legal expectations when collaborating with civilian agencies*," and added, "*Our systems are deliberately isolated for security purposes. Integration poses a risk we are not ready to take*." On trust, he noted, "*We support trust-building in principle, but operational secrecy remains a top priority*."

The findings, therefore, revealed significant disparities in institutional readiness for reform to enhance multi-agency information sharing. Higher-performing institutions demonstrated strong alignment across policy, legal, interoperability, and trust-building dimensions, indicating a proactive and coordinated approach to collaboration in cybercrime prevention. In contrast, lower-performing entities exhibited limited reform preparedness, characterized by outdated frameworks, legal ambiguities, and minimal technical integration. Private sector actors showed moderate commitment, often constrained by internal governance and data privacy obligations. These variations underscore the critical need for harmonized re-

forms that bridge operational, legal, and technical divides across public and private sectors.

5. Discussion of Results

The article found that promoting information sharing among multi-agency stakeholders significantly enhanced cybercrime prevention capabilities. This finding aligned with and reinforced the conclusions of established scholars in the domain of cybersecurity and inter-agency collaboration. For instance, He, Devine, & Zhuang (2018) emphasized that effective information sharing across government agencies improved decision-making and operational efficiency, particularly in security contexts. Similarly, Leone (2024) highlighted that coordinated information exchange among law enforcement and intelligence agencies was essential for timely threat detection and response. The current article extended these insights by showing that collaboration not only improved detection but also contributed to the proactive prevention of cyber threats. Furthermore, Al Waroi (2024) discussed the role of cross-agency trust and standardized data-sharing protocols in mitigating cyber risks, which was strongly supported by the present article's emphasis on structured communication. Thus, the findings both confirmed and expanded upon prior literature by providing empirical evidence that strategic information sharing directly contributed to cyber resilience and operational preparedness.

The current article's findings on the variability of inter-agency information sharing across institutions align with the existing body of literature. Scholars such as Onyango (2022) and Kamrul Ahsan (2023) have emphasized that institutional disparities, policy fragmentation, and a lack of standardized protocols often hinder effective inter-agency collaboration. Similarly, Qin & Fan (2016) acknowledged that while some agencies established strong information-sharing networks, others lagged due to inadequate frameworks or limited trust among stakeholders. The present article supports these observations by revealing that although certain institutions exhibited strong engagement in information exchange, others faced technical, institutional/organizational bureaucracies, data privacy, and policy-related constraints, among others. This suggests that information sharing is not uniformly institutionalized, echoing Yanakiev & Tagarev (2020) argument that collaboration in cyber governance requires both organizational alignment and enabling infrastructure. The current article, therefore, extends previous work by identifying the practical gaps that persist despite growing recognition of the importance of multi-agency collaboration. This underscores the need for targeted, institution-specific strategies to strengthen interoperability and cyber resilience.

The current article's findings revealed significant disparities in institutional readiness for reform aimed at enhancing multi-agency information sharing, aligning with the broader literature on the complexity of inter-organizational collaboration in cybersecurity. Scholars such as Gil-Garcia & Sayogo (2016) emphasized that successful information sharing required alignment across policy, legal, and technical domains, a position supported by this article's identification of high-

performing institutions with coherent frameworks and trust-building mechanisms. However, the current article also challenged more optimistic perspectives presented by Matteucci (2020) and Di Giulio & Vecchi (2023), who suggested that with digital infrastructure and policy commitment, institutional reform was likely to be uniformly effective. Contrary to such assumptions, the current article's findings indicated that legal ambiguities, outdated protocols, and limited interoperability still hindered reform in lower-performing institutions, especially in public-private interactions. Moreover, while private sector actors demonstrated moderate commitment, their efforts were often constrained by internal governance and stringent data privacy norms. Thus, the article provided a more tempered and empirically grounded view, emphasizing the need for harmonized, cross-sectoral reform efforts to close these institutional gaps. These empirical results support Rational Choice Theory by demonstrating that when officers perceive sufficient institutional support through coordinated data sharing, they are more inclined to engage in preventive cybersecurity practices. These results pointed toward actionable policy directions. For instance, formalizing inter-agency threat intelligence protocols between the Communications Authority, National Police Service, and Directorate of Criminal Investigations would enhance real-time responses. Similarly, amending the Computer Misuse and Cybercrimes Act (2018) to mandate cross-agency data-sharing on cyber incidents could institutionalize collaboration.

6. Conclusion

Based on the findings, it was concluded that promoting multi-agency information sharing significantly enhanced the effectiveness of cybercrime prevention. Institutions that actively engaged in structured communication, coordinated cybersecurity initiatives, and the sharing of threat intelligence demonstrated greater capacity to detect, respond to, and mitigate cyber threats. However, the impact of information sharing was not uniform across institutions. The article revealed marked disparities in engagement levels and reform readiness, with higher-performing entities showing strong alignment in legal, policy, trust-building, and technical dimensions, while lower-performing institutions lagged due to outdated frameworks, institutional inertia, mistrust, and legal ambiguities. These differences indicated that while information sharing was a critical enabler of cyber resilience, its effectiveness was contingent upon institutional capacity and systemic reforms. The findings highlighted the urgent need for harmonized policy, legal, and technical frameworks to facilitate interoperability and trust among diverse actors, including public and private institutions. Ultimately, achieving an integrated, multi-agency approach to cybersecurity required addressing these systemic barriers to ensure comprehensive and sustained collaboration in the fight against cybercrime.

7. Recommendations

To address the disparities and challenges identified in promoting multi-agency information sharing for cybercrime prevention in order to maximize the impact

of multi-agency information sharing on cybercrime prevention in Kenya, several recommendations emerged. First, there was a need for harmonized policy and legal reforms that promoted a unified framework for collaboration between agencies. This included revising outdated legislation and clarifying legal mandates to eliminate ambiguities that hindered effective coordination. Second, institutions had to invest in building trust among agencies by establishing formal communication protocols, joint task forces, and data-sharing agreements that fostered transparency, accountability, and mutual respect. Furthermore, efforts had to be made to enhance technical interoperability through the adoption of common standards, platforms, and secure channels for real-time threat intelligence sharing. Capacity building had to be prioritized, with targeted training programs and knowledge exchange forums aimed at improving institutional readiness and bridging technical and operational gaps. For private sector actors, there had to be incentives and frameworks that addressed internal governance and privacy concerns, enabling them to participate more fully in collective cybersecurity efforts. Overall, a strategic, well-resourced, and coordinated approach was essential to strengthening multi-agency collaboration and enhancing the national response to cybercrime threats.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Al Waroi, M. N. A. L. (2024). Coordination and Collaboration between Secret Intelligence Agencies and Government Institutions: Challenges, Opportunities, and Dynamics. *International Journal of Multidisciplinary Research and Analysis, 7,* 4626-4635.

Al-Salim, H., Faraj, S., & Tarek, M. (2023). Inter-Agency Frameworks and Cybercrime Reduction: Evidence from the Middle East. *Journal of Cybersecurity Policy and Management, 11,* 88-104. https://doi.org/10.1016/j.jcpm.2023.102457

Banchereau, M. (2024). *Interpol Clamps down on Cybercrime and Arrests over 1,000 Suspects in Africa*. AP World News. https://apnews.com/article/interpol-cybercrime-africa-afripol-fraud-serengeti-trafficking-208111329edd3a1a64faf85cc7c0d2c0

Basak, B. (2024). The Impact of Cybersecurity Threats on National Security: Strategies. *International Journal of Humanities Social Science and Management, 4,* 1361-1382.

Di Giulio, M., & Vecchi, G. (2023). How "Institutionalization" Can Work. Structuring Governance for Digital Transformation in Italy. *Review of Policy Research, 40,* 406-432. https://doi.org/10.1111/ropr.12488

Gil-Garcia, J. R., & Sayogo, D. S. (2016). Government Inter-Organizational Information Sharing Initiatives: Understanding the Main Determinants of Success. *Government Information Quarterly, 33,* 572-582. https://doi.org/10.1016/j.giq.2016.01.006

Gitari, S. M. (2020). *Reforming the Institutional and Legal Frameworks of E-Commerce in Kenya; Consumer Rights Protection in the Digital Economy*. Doctoral Dissertation, Strathmore University.

Government of Kenya (2016). *The National ICT Policy-2016*. Ministry of Information, Communications and the Digital Economy.

Government of Kenya (2019). *National Information, Communications and Technology (ICT) Policy*. Ministry of Information, Communications and Technology, Kenya. https://ict.go.ke/sites/default/files/2024-09/National%20ICT%20Policy%202019.pdf

Government of Kenya (2022). *National Cybersecurity Strategy, 2022-2027*. National Computer and Cybercrime Coordination Committee. https://nc4.go.ke/storage/2022/09/KENYA-CYBERSECURITY-STRATEGY-2022-2027.pdf

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk Analysis, 38,* 215-225. https://doi.org/10.1111/risa.12878

Kamrul Ahsan, A. H. M. (2023). Inter-Agency Coordination. In *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 6887-6891). Springer International Publishing. https://doi.org/10.1007/978-3-030-66252-3_3620

Kenya National Bureau of Statistics Economic Survey (2020). Cyber-Attacks in Kenya up by Half to Hit 56 m in Three Months. *Business Daily*.

Leone, D. N. (2024). *Information Sharing for Intelligence-Led Policing Within Multi-Agency Law Enforcement Teams*. Doctoral Dissertation, Saint Leo University.

Matteucci, N. (2020). Digital Agendas, Regional Policy and Institutional Quality: Assessing the Italian Broadband Plan. *Regional Studies, 54,* 1304-1316. https://doi.org/10.1080/00343404.2020.1782876

Muturi, J., & Wangari, P. (2022). Evaluating the Effectiveness of Multi-Stakeholder Cyber Response Systems in Kenya. *African Journal of Information Systems, 14,* 112-126. https://doi.org/10.4314/ajis.v14i3.9

Ndeda, L. A., & Odoyo, C. O. (2019). *Cyber Threats and Cyber Security in the Kenyan Business Context*.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity Strategy's Role in Raising Kenyan Awareness of Mobile Security Threats. *Information & Security, 32,* 1.

Onyango, G. (2022). *Understanding Disfunctionalities in Multi-Agency Policy Collaborations for Public Accountability in Kenya*. Qeios.

Paternoster, R., Bachman, R., Bushway, S., Kerrison, E., & O'Connell, D. (2015). Human Agency and Explanations of Criminal Desistance: Arguments for a Rational Choice Theory. *Journal of Developmental and Life-Course Criminology, 1,* 209-235. https://doi.org/10.1007/s40865-015-0013-2

Qin, C., & Fan, B. (2016). Factors That Influence Information Sharing, Collaboration, and Coordination across Administrative Agencies at a Chinese University. *Information Systems and e-Business Management, 14,* 637-664. https://doi.org/10.1007/s10257-015-0298-z

Stalans, L. J., & Donner, C. M. (2018). Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 25-45). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_2

The National KE-CIRT/CC (2023). *Cybercrime Report, July-September 2023*. Communications Authority of Kenya. https://www.ca.go.ke/sites/default/files/2023-10/Cybersecurity%20Report%20Q1%202023-2024.pdf

The National KE-CIRT/CC (2024). *Cybercrime Report, April-June 2024*. Communications Authority of Kenya. https://www.ca.go.ke/sites/default/files/2024-08/Cyber%20Security%20Report%20Q4%202023-2024.pdf

Whitmire, T. (2020). *The Arrest and Prosecution of Cyber Stalkers: How "Rational" Are Criminal Justice Decision Makers*?

Yanakiev, Y., & Tagarev, T. (2020). Governance Model of a Cybersecurity Network: Best Practices in the Academic Literature. In T. Vassilev, & R. Trifonov (Eds.), *Proceedings of the 21st International Conference on Computer Systems and Technologies (CompSys-Tech'20)* (pp. 27–34). ACM.

Zhao, J., Wang, X., Zhang, H., & Zhao, R. (2021). Rational Choice Theory Applied to an Explanation of Juvenile Offender Decision Making in the Chinese Setting. *International Journal of Offender Therapy and Comparative Criminology, 65,* 434-457. https://doi.org/10.1177/0306624x20931429

Zhou, L., & Chang, Y. (2024). Artificial Intelligence and Regulatory Data Sharing in China's Cybersecurity Enforcement. *International Journal of Cyber Intelligence, 9,* 33-50. https://doi.org/10.1080/ijci.2024.091004

Abbreviations

ACU	Anti-Counterfeit Unit
ANOVA	Analysis of Variance
CAK	The Communications Authority of Kenya
CBK-CPU	Central Bank of Kenya's Cybercrime Prevention Unit
CCU-I	Cyber Crime Unit-Investigation
CP	Cybercrime Prevention
DoS	Disruption of Service
DFLK	Digital Forensic Laboratory of Kenya
DV	Dependent Variable
ICT	Information and Communication Technology
IV	Independent Variable
KE-CIRT/CC	Kenya Computer Incident Response Team and Coordination Centre
KNBS	Kenya National Bureau of Statistics
MTTDR	Mean Time to Detect and Respond
MTTIR	Mean Time to Investigate and Resolve
NC3	National Cyber Command Centre
NIS-CSU	National Intelligence Service's Cyber Security Unit
PISAMA	Promoting Information Sharing among Multi-Agencies
RCT	Rational Choice Theory
SPSS	Statistical Package for Social Sciences