Scientific Research Publishing

Open Journal of Political Science, 2025, 15(4), 749-769
https://www.scirp.org/journal/ojps
ISSN Online: 2164-0513
ISSN Print: 2164-0505

Empowering Cybercrime Prevention through Digital Innovation Policy in Kenya: Opportunities and Implications

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). Empowering Cybercrime Prevention through Digital Innovation Policy in Kenya: Opportunities and Implications. *Open Journal of Political Science, 15,* 749-769.
https://doi.org/10.4236/ojps.2025.154041

Received: July 18, 2025
Accepted: August 18, 2025
Published: August 21, 2025

Abstract

The article assessed Kenya's ICT policy initiative focused on digital innovation empowerment, emphasizing its influence on cybercrime prevention and the unintended challenges that emerged during implementation. It utilized a cross-sectional research design combined with a concurrent mixed-methods approach. Primary data was collected from personnel within cybercrime prevention agencies, including mobile network operators like Airtel and Safaricom. To achieve the study's aims, a simple linear regression model was applied for analysis. The article revealed that digital innovation empowerment significantly enhanced cybercrime prevention by equipping officers with advanced tools and strategies. Institutions directly involved in cyber operations showed stronger innovation adoption due to better infrastructure, leadership, and resource commitment. Conversely, regulatory bodies faced challenges like limited funding and weak integration. Overall, structural issues such as poor coordination, cultural resistance, and slow procurement hindered progress. The article concluded that digital innovation empowerment enhances cybercrime prevention, especially in operational institutions, but challenges like weak leadership, poor infrastructure, and bureaucratic hurdles limited broader institutional effectiveness. The article recommended a coordinated digital innovation framework, streamlined procurement, public-private partnerships, targeted capacity building, and strong monitoring systems to enhance cybercrime prevention and sustain impactful innovation efforts.

Keywords

Digital Innovation Empowerment Policy, Cybercrime Prevention, Opportunities, Implications

1. Introduction

As digital technologies continue to advance globally, the threat landscape in cyberspace has expanded rapidly, positioning cybersecurity as a critical concern for governments, businesses, and individuals alike (Basak, 2024). Kenya, undergoing a fast-paced digital transformation, has found itself increasingly vulnerable to cybercrime due to its heavy reliance on online services such as mobile money platforms, e-governance, and digital commerce (Okuku, Renaud, & Valeriano, 2015). Despite ongoing governmental interventions, the nation recorded a marked escalation in cyber-related incidents between 2011 and 2019, with web-based intrusions and internal system compromises consistently dominating official reports (KNBS Economic Survey, 2020). The situation worsened year-on-year, with cyber threats rising from 22.1 million incidents in 2012-2013 to 51.9 million in 2013-2014. Notably, by the last quarter of 2019, reported attacks had grown by 47.3% compared to the previous quarter. The financial repercussions were equally severe, with estimated losses reaching Sh18 billion by 2016 (Gitari, 2020). In response, the Kenyan government embedded multi-agency information sharing within its ICT policy framework as a key strategic measure to combat cyber threats. Section 15.1 of the National ICT Policy emphasizes the vital role of inter-agency cooperation in detecting, preventing, and mitigating cyber risks (Government of Kenya, 2016). This policy commitment underscored the government's recognition of the increasing complexity of cyber threats fueled by internet proliferation, widespread smart device usage, and sophisticated cybercriminal tactics. Promoting collaborative capacity-building approaches such as inter-agency data exchange was seen as central to strengthening Kenya's cyber resilience and creating a trustworthy digital space that supports economic and social growth (The National KE-CIRT/CC, 2024).

Kenya's cybersecurity crisis has evolved into a national concern, threatening public safety, financial institutions, and citizens' personal data. Criminal practices like data theft, online fraud, phishing, ransomware, and identity scams have surged, targeting a wide spectrum of organizations (Ndeda & Odoyo, 2019). Agencies such as the Communications Authority (CA) and KE-CIRT/CC have continually reported a high volume of attempted breaches annually. Without a robust framework that allows stakeholders to exchange cybersecurity intelligence, Kenya remains exposed to costly data compromises and reputational damage (The National KE-CIRT/CC, 2023). To counter this, the government's National Cybersecurity Strategy (2022-2027) was formulated in harmony with the Computer Misuse and Cyber Crimes Act to guide national response efforts. The strategy outlines a unified, cross-sectoral approach to addressing cybercrime through collective prevention, detection, and mitigation mechanisms (Government of Kenya, 2022). Additionally, Government of Kenya (2019) highlights cybersecurity as an indispensable pillar in Kenya's digital advancement. It advocates for skills development and institutional capacity strengthening, aiming to foster seamless information-sharing protocols across cybersecurity actors to more effectively address emerging

digital threats (Government of Kenya, 2019).

While digital innovation was anticipated to play a significant role in mitigating cyber threats, it became increasingly important to evaluate the actual outcomes of this intervention on cybercrime prevention, especially given the limited availability of in-depth studies focusing on its impact within the Kenyan context. Measuring its effectiveness required concrete indicators such as declines in reported cyber incidents, faster response capabilities, and increased rates of successful legal action against offenders. Although policy documents and academic literature acknowledged the conceptual relevance of digital innovation empowerment in enhancing cybersecurity, there remained a noticeable lack of empirical analysis assessing how these innovations were performing on the ground. Recent Kenyan studies have emphasized similar concerns. For instance, Kiarie (2024) examined the impact of digital infrastructure readiness on public sector cybersecurity, revealing significant gaps in implementation. Likewise, Chiro & Kyalo (2024) highlighted how low inter-agency trust constrained effective use of shared cyber intelligence platforms. These studies provide a local evidence base reinforcing the need to evaluate how digital innovation is operationalized in Kenya's cybersecurity ecosystem. The degree to which such empowerment initiatives had influenced Kenya's ability to prevent cybercrime had not been sufficiently investigated. This shortfall highlighted the need for a comprehensive study aimed at evaluating the real-world outcomes of digital innovation empowerment, uncovering any implementation bottlenecks, and offering actionable recommendations for enhancing its effectiveness.

Addressing this research gap is important because, despite theoretical recognition of digital innovation's role in cybersecurity, there was limited empirical evidence on its actual impact in Kenya. Without such analysis, it remained unclear whether these initiatives were effectively reducing cyber threats or simply existing in policy. A thorough investigation was necessary to assess real-world outcomes, identify implementation barriers, and generate practical recommendations to strengthen Kenya's cybersecurity through informed, evidence-based interventions.

In conclusion, while Kenya had made significant strides in digital innovation empowerment in cybersecurity, the practical impact of these initiatives on cybercrime prevention remained inadequately explored. The objective of this article was to therefore establish the impact of digital innovation empowerment on cybercrime prevention in Kenya. The corresponding research question sought to determine the extent to which such digital innovations had affected cybercrime prevention efforts. The article also hypothesized that digital innovation empowerment of officers by the government has contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures. The article finally sought to offer recommendations grounded in evidence to bolster the nation's cybersecurity capacity-building initiative of digital innovation by analyzing the initiative's strengths, weaknesses, implications and potential areas for enhancement.

2. Theoretical Framework

Rational Choice Theory (RCT), originally formulated by Adam Smith in 1776, provided a valuable lens for analyzing how digital innovation empowerment contributed to cybercrime prevention efforts in Kenya. Rational Choice Theory, served as a useful analytical tool for examining how institutions and individuals make strategic decisions based on expected outcomes. At its core, the theory posits that actors, whether individuals or organizations act rationally by evaluating various courses of action and selecting the one that promises the greatest net benefit. In this view, decisions are not arbitrary but grounded in a logical assessment of the anticipated rewards versus the costs involved (Stalans & Donner, 2018). The assumption is that decision-makers have relatively stable preferences, adequate information, and a clear understanding of the consequences of their choices, which ultimately guides them toward utility-maximizing behavior.

This theoretical lens has proven particularly valuable in the realm of crime prevention and public policy. In various settings, RCT has helped explain both cooperative behaviors among law enforcement agencies and the calculated actions of offenders (Paternoster et al., 2015). For instance, prior studies have shown that the fear of detection or punishment often deters potential criminals, while the expectation of shared benefits such as efficiency or effectiveness encourages institutions to collaborate (Zhao et al., 2021). Rational Choice Theory, therefore, helps us understand both the incentives that shape institutional policy adoption and the deterrents that influence criminal decision-making in cyberspace (Whitmire, 2020).

Applying Rational Choice Theory to the relationship between digital innovation empowerment and cybercrime prevention in Kenya reveals meaningful insights. The study's findings suggest that government and institutional actors invest in digital innovation through tools, infrastructure, partnerships, and skilled personnel because they perceive these efforts to yield substantial security gains. Empowering cybercrime prevention officers with advanced technology and capacity-building initiatives is a rational policy choice, grounded in the expectation that these innovations will reduce threats, improve responsiveness, and enhance national resilience. Manifestations of RCT in current policy interventions are evident in the prioritization of digital infrastructure, strategic collaborations with tech partners, and emphasis on real-time system upgrades all reflecting deliberate decisions aimed at maximizing societal security outcomes. Thus, the theory not only supports the rationale behind such empowerment strategies but also reinforces the notion that sustainable cybercrime prevention hinges on consistently favoring options with the greatest public benefit.

3. Research Design and Methodology

The study employed a descriptive research design. To effectively fulfill the research objective, a concurrent mixed-methods approach was utilized, combining both quantitative and qualitative data collection strategies. This approach was essential in capturing statistical evidence through structured questionnaires while

also eliciting rich, contextual insights via Key Informant Interviews (KIIs). Quantitative data were primarily obtained from seventy-two (72) officers working within cybercrime prevention institutions and telecommunications firms across Kenya. Simultaneously, qualitative data were gathered using open-ended questions and in-depth interviews with eleven (11) key informants. These informants included departmental heads from critical organizations such as the Cyber Crime Unit–Investigation (CCU-I), Digital Forensic Laboratory of Kenya (DFLK), Ministry of ICT, Anti-Counterfeit Authority (ACA), Communications Authority of Kenya (CAK), Central Bank of Kenya's Cybercrime Prevention Unit (CBK-CPU), National Intelligence Service's Cyber Security Unit (NIS-CSU), Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), National Cyber Command Centre (NC3), as well as officials from Safaricom and Airtel. Table 1 presents a breakdown of the number of officers sampled from each institution.

Table 1. Respondent's working institution.

Institution	Frequency	Percent
CCU-I	14	19.4
DFLK	4	5.6
ACU	6	8.3
CAK	5	6.9
NIS-CSU	4	5.6
KE-CIRT/CC	11	15.3
NC3	13	18.1
Ministry of ICT	5	6.9
CBK	4	5.6
Safaricom	4	5.6
Airtel	2	2.8
Total	**72**	**100.0**

This section provides a comprehensive analysis of how digital innovation empowerment influences cybercrime prevention efforts within selected institutions in Kenya. The study engaged participants drawn from key organizations directly involved in combating cybercrime in the country. These participants included officers and cybersecurity experts from government agencies, regulatory authorities, law enforcement, intelligence services, and the telecommunications sector. The institutions represented in the study comprised the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), National Cyber Command Centre (NC3), Communications Authority of Kenya (CAK), Central Bank of Kenya's Cybercrime Prevention Unit (CBK-CPU), National Intelligence Service's Cyber Security Unit (NIS-CSU), Cyber Crime Unit–Investigation (CCU-I), Digital Forensic Laboratory of Kenya (DFLK), Anti-Counterfeit Unit (ACU), the Ministry of ICT, as well as major telecom providers Safaricom and Airtel. These organiza-

tions were purposefully selected due to their pivotal roles in the detection, investigation, prosecution, and adjudication of cybercrime within Kenya. Snowball sampling was used to identify the 72 officers across cybersecurity institutions and telecom firms. This approach was suitable given the specialized nature of cybercrime prevention roles, which often operate within tight professional networks. Starting from a few initial contacts, referrals enabled access to additional officers actively engaged in cybercrime detection, response, and enforcement. This method ensured participation from individuals with direct, practical involvement in national cybersecurity efforts, thereby enhancing the relevance and credibility of the findings. In parallel, purposive sampling was employed to select the 11 institutional heads for interviews. These individuals were chosen based on their strategic roles in shaping, implementing, or overseeing digital innovation in their respective organizations. Together, the sample composition provided a comprehensive representation of Kenya's cybercrime prevention landscape, combining operational and policy-level perspectives.

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, "*Digital innovation empowerment of officers by the government has contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures*", 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.

To analyze the qualitative data derived from key informant interviews, the study employed thematic analysis. The process began with an initial familiarization phase, during which the researcher thoroughly reviewed the transcripts multiple times to gain a comprehensive understanding and took preliminary notes. This was followed by a systematic coding phase, where significant segments of the data were identified and labeled based on their relevance to the study's objective. Related codes were then clustered into broader themes that captured recurring patterns across the responses. These emerging themes were carefully examined to ensure they accurately reflected both the coded extracts and the overall data context. Once refined, each theme was distinctly defined and named to encapsulate its central meaning. The final stage involved constructing a detailed narrative that wove together the identified themes, supported by representative quotes, and clearly linked the findings back to the study's objective.

4. Data Analysis

Data analysis was based on testing the hypothesis that "*Digital innovation empowerment of officers by the government has contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures*". This analysis sought to determine the impact of digital innova-

tion empowerment on cybercrime prevention in Kenya, focusing on the extent to which digital innovation empowerment had contributed to *providing officers with state-of-the art tools for implementing advanced security measures*. A simple linear regression model was employed to test the significance of the relationship between digital innovation empowerment 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 digital innovation empowerment 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 *Digital innovation empowerment of officers by the government has contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures*, respondents were asked to indicate their level of agreement with a set of statements reflecting key aspects of digital innovation empowerment. These included whether the agency used advanced digital technologies (e.g., AI, blockchain) to detect and prevent cybercrime effectively; whether the agency consistently invested in upgrading digital infrastructure to support cybercrime prevention initiatives; whether agency promoted a culture that encourages innovation in developing cybersecurity solutions; weather the agency integrated digital tools into our daily operations to improve responsiveness to cyber threats; whether the agency staff were digitally skilled and encouraged to apply innovative approaches in cybersecurity tasks and lastly, whether the agency partnered with external innovators (e.g., tech firms, researchers) to co-create digital tools for fighting cybercrime. These questions formed the basis for analyzing the impact of digital innovation empowerment on cybercrime prevention.

To explore the relationship between digital innovation empowerment 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 digital innovation empowerment 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): Digital innovation empowerment of officers by the government has not contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures.

4.1. The Model Summary Table

Table 2 presents a summary of the regression model used to assess the influence

of digital innovation empowerment (die) on cybercrime prevention (cp). The correlation coefficient (R) was 0.695, indicating a strong positive linear relationship between the two variables. This suggests that as digital innovation empowerment increases, so does the effectiveness of cybercrime prevention efforts. The R Square value stood at 0.483, meaning that digital innovation empowerment accounted for 48.3% of the variability in cybercrime prevention. The Adjusted R Square, which corrects for the number of predictors and provides a more accurate measure, was slightly lower at 0.476, further confirming the strength of the model. The low standard error of the estimate indicated that the model closely fit the observed data. Additionally, the significance of the F statistic (Sig. F Change = 0.000) confirmed that including digital innovation empowerment significantly enhanced the model's ability to predict cybercrime prevention outcomes. These findings demonstrate that digital innovation empowerment is a statistically significant and influential predictor of cybercrime prevention. Overall, the regression analysis suggests that empowering institutions and individuals through digital innovation plays a critical role in curbing cybercrime. The results not only validate the theoretical linkage between innovation and security but also underscore the importance of technological advancement in strengthening national cybersecurity frameworks.

Table 2. 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	0.695[a]	0.483	0.476	1.07211	0.483	65.477	1	70	0.000

a. Predictors: (Constant), die; b. Dependent Variable: cp.

4.2. The ANOVA Table

Table 3, which presents the ANOVA results, assessed the overall statistical significance of the regression model used to predict the dependent variable, *cybercrime prevention* (cp), using *digital innovation empowerment* (die) as the independent variable. The regression row in the table reflected how well the model explained the variation in cybercrime prevention. Specifically, the Sum of Squares for Regression (75.260) indicated the portion of the total variability in cybercrime prevention that could be attributed to digital innovation empowerment. In contrast, the Sum of Squares for Residuals (80.459) captured the amount of variance in cybercrime prevention that remained unexplained by the model. The associated p-value (Sig.) for the F statistic was 0.000, which is well below the standard significance threshold of 0.05. This result confirmed that the regression model was statistically significant, implying that digital innovation empowerment made a meaningful contribution to predicting levels of cybercrime prevention. In essence, the ANOVA findings validated the effectiveness of the regression model and established that the inclusion of digital innovation empowerment as a predictor signif-

icantly enhanced the model's ability to explain changes in cybercrime prevention. Therefore, ***the Null Hypothesis (H_0) stating that digital innovation empowerment of officers by the government has not contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures was rejected. This therefore meant that that digital innovation empowerment of officers by the government has contributed to cybercrime prevention by providing them with state-of-the art tools for implementing advanced security measures.***

Table 3. ANOVA table.

ANOVA[a]						
	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	75.260	1	75.260	65.477	0.000[b]
	Residual	80.459	70	1.149		
	Total	155.719	71			

a. Dependent Variable: cp; b. Predictors: (Constant), die.

4.3. The Coefficients Table

Table 4 presented the coefficients for the regression model, highlighting the relationship between digital innovation empowerment (die) and cybercrime prevention (cp). The coefficient for digital innovation empowerment was statistically significant ($p < 0.05$), with a standardized Beta value of 0.695, indicating a strong positive influence on cybercrime prevention. Specifically, a one-unit increase in digital innovation empowerment was associated with an estimated 1.802-unit increase in cybercrime prevention. The low p-value and significant t-value further confirmed the strength of this relationship. These findings emphasize the critical role of enhancing institutional capacity through advanced digital tools and infrastructure to effectively address and reduce cybercrime threats in Kenya.

Table 4. Coefficients table.

ANOVA[a]						
	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	75.260	1	75.260	65.477	0.000[b]
	Residual	80.459	70	1.149		
	Total	155.719	71			

a. Dependent Variable: cp; b. Predictors: (Constant), die.

The findings indicated that digital innovation empowerment has contributed positively to strengthening cybercrime prevention efforts. Security officers provided with modern technologies and cutting-edge tools demonstrated greater capacity to implement sophisticated security strategies, resulting in improved deterrence of cybercrime activities.

Building upon the tested hypothesis, the study explored the specific elements of digital innovation empowerment that influenced the effectiveness of cybercrime prevention. Instead of relying solely on quantitative outcomes, the research examined how various public and security institutions operationalized digital innovation empowerment and identified the distinguishing factors behind more successful implementations. This section provided a comparative analysis of institutional performance through aggregated mean scores, evaluating the scope and quality of empowerment initiatives. Key areas of focus included the adoption of emerging technologies, investment in digital infrastructure, promotion of innovation culture, integration of digital tools in daily operations, enhancement of staff digital skills, and strategic innovation partnerships.

Table 5. Comparative institutional scores on key dimensions of digital innovation empowerment.

Respondent's working institution		Minimum	Maximum	Mean	Std. Deviation
CCU-I	die	2.83	5.00	3.9643	0.59978
	Valid N (listwise)				
NIS-CSU	die	3.33	5.00	4.0833	0.70053
	Valid N (listwise)				
CBK-CPU	die	2.83	4.50	4.0556	0.62063
	Valid N (listwise)				
CAK	die	2.83	4.00	3.6000	0.48016
	Valid N (listwise)				
NC3	die	3.33	4.17	3.8333	0.36004
	Valid N (listwise)				
DFLK	die	2.83	5.00	4.0455	0.57296
	Valid N (listwise)				
KE-CIRT/CC	die	2.83	5.00	3.9231	0.64412
	Valid N (listwise)				
ACU	die	2.83	4.00	3.6000	0.48016
	Valid N (listwise)				
Safaricom	die	2.83	4.33	3.8750	0.71200
	Valid N (listwise)				
Ministry of ICT	die	2.83	4.00	3.5833	0.51819
	Valid N (listwise)				
Airtel	die	3.33	4.17	3.7500	0.58926
	Valid N (listwise)				

Qualitative data from institutional leaders offered deeper insights into practical challenges, organizational dynamics, and enabling conditions that shaped the im-

plementation of digital innovation. These perspectives enriched the analysis by highlighting institutional strengths and revealing how supportive policy environments, robust infrastructure, and strong leadership contributed to achieving empowerment goals. This, in turn, informed evidence-based recommendations for enhancing cybercrime prevention efforts. Institutions across different sectors, government, regulatory, law enforcement, intelligence, and telecommunications were evaluated using mean scores to identify both achievements and gaps. Participants rated their agreement with statements aligned to the six empowerment dimensions, and the results, as illustrated in Table 5, provided a comparative snapshot of institutional performance in applying digital innovation to counter cyber threats.

Table 5 offered a side-by-side comparison of how different institutions viewed the presence and impact of digital innovation empowerment (DIE), using statistical measures such as minimum, maximum, mean, and standard deviation. The results highlighted clear differences in how digital innovation was perceived across the various organizations involved in cybercrime prevention.

The highest average score came from respondents at NIS-CSU (mean = 4.0833), indicating a strong belief that their institution effectively utilized modern digital tools and practices in support of cybercrime prevention. Similar positive perceptions were observed in CBK-CPU (mean = 4.0556), DFLK (mean = 4.0455), and CCU-I (mean = 3.9643), where respondents also reported considerable digital innovation activity within their institutions.

KE-CIRT/CC and Safaricom followed closely, with mean scores of 3.9231 and 3.8750 respectively, reflecting favorable impressions of innovation initiatives. On the other hand, slightly lower ratings were reported by NC3 (mean = 3.8333) and Airtel (mean = 3.7500), suggesting moderate levels of empowerment in terms of digital innovation. At the lower end, CAK, ACU, and the Ministry of ICT had mean scores of 3.6000 or below, implying that staff in these institutions perceived limited digital innovation, potentially due to underinvestment in digital tools, training, or infrastructure.

Differences in standard deviation also reflected the spread of views within each institution. Safaricom, with the highest standard deviation (SD = 0.71200), showed a wide range of opinions among its staff, while NC3 had the most consistent responses (SD = 0.36004), indicating a shared view among its personnel.

Overall, the analysis revealed that institutions more actively engaged in technical and operational cybercrime response tended to report stronger perceptions of digital innovation empowerment. This likely reflects targeted investments and a hands-on approach to innovation. Conversely, organizations with more administrative or regulatory functions exhibited lower ratings, possibly linked to structural or resource limitations. The varying standard deviation values also suggest internal differences in access to innovation across some institutions.

Given the notable differences in how digital innovation empowerment was experienced, the study sought to understand what accounted for these variations. This prompted a central question: *Why did perceptions of digital innovation em-*

powerment differ across institutions involved in cybercrime prevention in Kenya?

To explore this, descriptive statistics particularly mean scores were used to analyze perceptions of digital innovation across five thematic areas: the clarity and relevance of each institution's operational mandate, the availability and accessibility of technological infrastructure, the extent of internal investment dedicated to innovation initiatives, the level of awareness and capacity-building efforts around innovation among staff, and the strength of leadership vision coupled with commitment to driving transformative change. These factors were identified as critical to understanding how institutions implement and benefit from digital innovation.

To deepen this analysis, interviews were conducted with senior officials from the eleven participating organizations. Their input helped clarify the reasons behind the differences observed in the quantitative data and validated the patterns identified. A detailed account of this combined analysis is presented in Table 6.

Table 6. Differences in digital innovation empowerment among cybercrime prevention agencies.

Institution	the clarity and relevance of each institution's operational mandate	Availability and accessibility of technological infrastructure	Extent of internal investment dedicated to innovation initiatives	Level of awareness and capacity-building efforts around innovation	Leadership vision coupled with commitment to driving transformative change
DFLK	3.80	3.70	3.60	3.55	3.65
NIS-CSU	4.10	4.20	4.00	4.05	4.10
CBK-CPU	3.85	3.90	3.75	3.80	3.95
CAK	3.60	3.50	3.45	3.40	3.55
NC3	4.25	4.40	4.35	4.30	4.25
KE-CIRT/CC	4.30	4.50	4.45	4.40	4.35
CCU-I	3.75	3.80	3.65	3.70	3.85
Ministry of ICT	3.90	3.60	3.55	3.75	3.80
Airtel	3.70	3.85	3.60	3.65	3.75
ACU	3.50	3.45	3.30	3.35	3.40
Safaricom	4.00	4.25	4.10	4.15	4.20

The results presented in Table 6 revealed notable differences among institutions in how they perceived the integration of digital innovation empowerment into their cybercrime prevention strategies. The assessment focused on five thematic areas: institutional role and mandate, access to digital infrastructure, investment in innovation, awareness and capacity-building, and leadership vision. Together, these dimensions provided a broad understanding of how institutions were applying digital innovation to improve their cyber defense mechanisms.

Institutions like KE-CIRT/CC and NC3 achieved consistently high mean scores across most themes, with KE-CIRT/CC posting a 4.30 on its role and mandate and 4.50 for access to technological infrastructure. NC3 followed closely, scoring 4.25 and 4.40 in the same areas, respectively. These high scores reflected a strong cor-

relation between their core responsibilities and their readiness to adopt digital innovations. A statement from the Head of KE-CIRT/CC affirmed this, noting that the institution actively aligns operational requirements with strategic technology investments to keep up with emerging cyber threats.

Leadership emerged as a pivotal factor in advancing digital innovation. High scores in this area were recorded by NIS-CSU (4.10), KE-CIRT/CC (4.35), and Safaricom (4.20), pointing to the influence of senior leadership in fostering innovation. The Head of NIS-CSU emphasized that without leadership that embraces digital transformation, innovation becomes inconsistent and ineffective, a sentiment highlighting the strategic role leadership plays in shaping innovation culture.

There were also noticeable disparities in technological infrastructure. KE-CIRT/CC (4.50), NC3 (4.40), and Safaricom (4.25) stood out, most likely due to stronger technical mandates and greater financial resources. In contrast, ACU (3.45) and CAK (3.50) lagged behind, suggesting infrastructural gaps that limited their effectiveness in dealing with digital threats. As the Head of ACU remarked, their teams often lacked real-time access to the tools needed for timely cybercrime detection, leading to reliance on external support and delayed response.

Regarding institutional investment in innovation, KE-CIRT/CC (4.45) and NC3 (4.35) again led, indicating not only access to resources but a proactive approach to funding innovation. By contrast, institutions like ACU (3.30), CAK (3.45), and the Ministry of ICT (3.55) showed weaker financial commitment. The Head of the Ministry of ICT noted that despite their policymaking authority, limited budgets hindered internal innovation efforts, underscoring a contradiction where key policy bodies lack the capacity to implement what they advocate.

In the area of innovation awareness and capacity development, KE-CIRT/CC, NC3, and Safaricom scored between 4.15 and 4.40, reflecting strong support for training and continuous learning. On the other hand, ACU (3.35) and CAK (3.40) recorded lower scores, indicating less emphasis on developing digital competencies. The Head of CAK admitted that although their officers were well-versed in regulatory matters, many lacked training in the advanced digital tools used by cybercriminals highlighting a crucial skill gap in enforcement.

Finally, institutions with roles directly linked to cybersecurity operations such as KE-CIRT/CC, NC3, and NIS-CSU displayed consistently higher confidence in digital innovation empowerment. Their proximity to real-time cyber threats appeared to drive a greater sense of urgency and commitment to innovation. The Head of NC3 captured this sentiment aptly, noting that working on the frontlines demanded constant evolution in both systems and personnel to stay ahead of ever-changing threats.

The results highlighted significant differences in how various institutions applied digital innovation to combat cybercrime. Agencies with a direct operational focus showed stronger alignment between their mandates and digital investments, benefiting from better infrastructure, dynamic leadership, and a clear commitment to innovation and staff development. These organizations were more pro-

active in allocating resources toward technological advancement and enhancing internal capabilities. On the other hand, institutions with policy or regulatory functions displayed weaker integration of digital innovation, often hindered by inadequate infrastructure, limited funding for innovation, and fewer training opportunities. Overall, the analysis emphasized that being closely engaged in cyber operations, coupled with forward-looking leadership, played a crucial role in driving digital innovation. In contrast, institutions removed from frontline responsibilities tended to exhibit lower innovation capacity and struggled to keep pace with rapidly evolving cyber threats.

Recognizing the variation in digital innovation empowerment among institutions involved in cybercrime prevention, the study sought to understand the specific obstacles limiting its effectiveness as a capacity-building strategy. This led to a focused inquiry into the challenges faced by both high-performing and low-performing agencies in implementing digital innovation. Gaining clarity on these barriers was critical not only for explaining the inconsistent outcomes observed but also for uncovering deeper systemic issues that need to be addressed to support stronger, more uniform national efforts in combating cybercrime.

Table 7. Identified challenges hindering digital innovation empowerment within cybercrime prevention agencies.

Institution	Weak Organizational Support for Innovation	Delays in Acquiring Technological Solutions	Limited Collaboration with Technology Sector	Overlapping and Unclear Innovation Responsibilities	Challenges in Incorporating New Digital Tools	Resistance to Adoption by End Users	Lack of Systems to Track and Assess Innovation Outcomes
DFLK	4.10	4.20	4.05	4.15	4.00	3.85	4.25
NIS-CSU	4.00	4.30	4.10	3.95	3.90	3.80	4.20
CBK-CPU	3.85	4.00	3.90	4.10	3.95	3.70	4.00
CAK	3.75	3.90	3.85	3.80	3.75	3.65	3.95
NC3	4.25	4.35	4.30	4.20	4.10	4.00	4.35
KE-CIRT/CC	4.15	4.10	4.20	4.00	4.05	3.90	4.25
CCU-I	4.05	4.25	4.15	4.10	4.00	3.95	4.30
Ministry of ICT	4.20	4.00	4.25	3.85	4.10	3.85	4.10
Airtel	3.70	3.85	3.95	3.75	3.60	3.55	3.90
ACU	3.80	3.95	3.80	3.90	3.85	3.60	3.95
Safaricom	3.65	3.90	3.75	3.70	3.60	3.55	3.85

To unpack the factors contributing to institutional disparities, participants were asked to highlight the major challenges impacting the rollout of digital innovation initiatives. Their responses were analyzed using descriptive statistics, particularly mean scores, to gauge the severity of each challenge across the institutions. The

data, drawn from staff across eleven agencies engaged in cybercrime prevention, was measured on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). The analysis focused on seven key areas of concern: weak organizational support for innovation, delays in acquiring technological solutions, limited collaboration with technology sector, overlapping and unclear innovation responsibilities, challenges in incorporating new digital tools, resistance to adoption by end users and lack of systems to track and assess innovation outcomes. These quantitative findings were further enriched by qualitative insights from interviews with 11 department heads, as detailed in Table 7.

Insights drawn from Table 7 uncovered a range of institutional and structural challenges that hindered the advancement and uptake of digital innovation across Kenya's cybercrime prevention agencies. The seven identified challenge areas spanning organizational culture, procurement systems, partnerships, and technology adoption revealed both internal and inter-agency factors constraining innovation-driven capacity building.

A consistent concern across many agencies was the *lack of an innovation-supportive culture*. Government institutions such as the Ministry of ICT (4.20), NC3 (4.25), and KE-CIRT/CC (4.15) scored highest, suggesting that even agencies at the center of national digital policy and operations face resistance to innovation. The Ministry of ICT's leadership acknowledged that rigid legacy systems and bureaucratic mindsets often undermine new ideas and discourage experimentation. Interestingly, private firms like Safaricom (3.65) and Airtel (3.70) also reported challenges, suggesting that even agile, market-driven organizations struggle to cultivate innovation in cybersecurity contexts.

Another major barrier was *delayed procurement procedures*, with the highest average ratings overall. Institutions such as NIS-CSU (4.30), NC3 (4.35), and CCU-I (4.25) pointed to inefficient procurement systems as a core limitation. Respondents noted that by the time new tools are cleared for use, they are often obsolete. Such delays stifle responsiveness and make it harder for agencies to keep up with fast-evolving cyber threats.

Weak partnerships with the technology industry also emerged as a recurring issue. Agencies including NC3 (4.30), KE-CIRT/CC (4.20), and the Ministry of ICT (4.25) acknowledged the absence of formalized collaboration with tech firms, resulting in limited knowledge sharing and underutilization of existing digital solutions. Leadership from KE-CIRT/CC observed that leveraging external expertise could reduce redundancy and accelerate deployment of more refined tools.

Overlapping mandates across institutions further diluted innovation efforts. DFLK (4.15), CBK-CPU (4.10), and CCU-I (4.10) highlighted the inefficiencies caused by siloed operations and a lack of coordinated planning. With multiple agencies working independently on similar initiatives, resources are often wasted, and promising innovations rarely progress beyond the pilot stage. CBK-CPU's leadership emphasized the urgency of a unified national framework to guide innovation efforts.

While not rated as highly as other issues, *technology integration challenges* still posed concerns for some. NC3 (4.10), KE-CIRT/CC (4.05), and the Ministry of ICT (4.10) highlighted the incompatibility between legacy infrastructure and new digital tools. The Ministry's representative noted that successful integration requires alignment of not just systems, but institutional vision and strategy an area where gaps still exist.

The challenge of *user acceptance and adoption* was particularly relevant to service providers like Airtel and Safaricom, both scoring 3.55. Their leadership noted that innovations must be intuitive and practically relevant to gain traction among staff. Without adequate training and workflow alignment, even the best tools face limited uptake.

Lastly, the lack of monitoring and evaluation (M&E) mechanisms ranked among the top concerns. Institutions such as DFLK (4.25), NC3 (4.35), and CCU-I (4.30) admitted to rolling out initiatives with no structured systems for tracking their effectiveness or outcomes. As one department head observed, innovation efforts often proceed without clear metrics, leaving agencies unsure whether their solutions are delivering intended results.

Altogether, these findings underscore systemic bottlenecks impeding innovation in cybercrime prevention. Cultural resistance, sluggish procurement, insufficient collaboration with industry, unclear mandates, and weak follow-through mechanisms collectively erode institutional readiness. Addressing these challenges calls for coordinated reforms clear policy direction, streamlined processes, structured partnerships, and effective monitoring to build a resilient and innovation-driven cyber defense landscape.

5. Discussion of Results

The study's findings demonstrate that digital innovation empowerment through the adoption of modern technologies, infrastructure upgrades, tool integration, and staff capacity enhancement significantly improved cybercrime prevention mirror and extend various scholarly perspectives. For instance, Manoharan and Sarker (2023) suggest that artificial intelligence (AI) and big data analytics enhance anomaly detection and responsiveness. Aminu et al. (2024) emphasize innovation's role in improving agility and real-time threat detection. Similarly, VMWare (2020) argues that trained and digitally empowered personnel are central to effective cyber defense, while Herpig and Schuetze (2021) point to Germany's consistent tech investment as a success factor in responding to cyber threats.

Other researchers, such as Walumoli (2021) and Tahiru (2018), advocate for technological advancement but caution that uneven resource distribution limits impact, particularly in regions like Kenya and Nigeria. Schmitt (2023) also highlights the importance of AI-enabled systems in strengthening digital defenses and recommends integrating machine learning classifiers to enhance detection accuracy. Elluri et al. (2023) similarly find that machine learning significantly boosts anomaly detection and proactive response capabilities, an argument that supports this

study's finding that innovation tools and skilled personnel jointly influence cyber resilience.

However, some scholars advise a more cautious approach. Salem, Azzam, and Emam (2024) critique AI tools for their lack of transparency and explainability, suggesting that trust among users can be undermined, thereby limiting practical adoption. Their viewpoint highlights the need for digital innovation to be both effective and interpretable something not fully covered in the current study. Similarly, Chinedu et al. (2021) note that despite the increasing use of AI-driven security models, cybercrime-related financial losses continue to escalate. Their findings reinforce the current study's observation that innovation, while vital, must be supported by systemic strategies to have a lasting impact. While much of the literature affirms the importance of digital innovation in enhancing cybersecurity, voices like Salem et al. and Chinedu et al. stress the need for a more holistic, integrated approach that prioritizes coordination, transparency, and contextual relevance.

The study also identified key institutional barriers to innovation adoption. These included rigid cultures, lengthy procurement cycles, weak strategic partnerships, fragmented mandates, outdated systems, limited user acceptance, and a lack of evaluation frameworks. Prior research aligns with several of these findings. For example, Tucker (2022) and Motaung and Sifolo (2023) found that traditional procurement procedures, low digital literacy among procurement officers, and inefficient processes hinder digital transformation efforts similar to the delays reported in this study. Gholami et al. (2017) discuss how legacy systems are resistant to change due to technical debt and organizational inertia, reinforcing this study's conclusion that such systems obstruct effective tech integration. Similar patterns have been observed in other Sub-Saharan countries. For instance, in Nigeria, Ogene (2024) found that limited access to innovation funding and overlapping agency roles impeded cyber policy implementation, while in Uganda, Ukwuoma et al. (2022) reported that weak leadership vision and fragmented inter-agency collaboration hindered cybersecurity innovation adoption. These parallels affirm the regional relevance of Kenya's experience and underscore the shared institutional challenges facing digital innovation empowerment in African cybercrime prevention contexts.

User resistance has also been explained using the theory of status quo bias, where individuals are inclined to maintain current practices despite available innovations (Nugawela & Sedera, 2022). This insight complements this study's emphasis on building internal awareness and digital literacy. Notably, the present study diverges by placing strong emphasis on fragmented mandates and absent evaluation systems issues that, while acknowledged in literature, are rarely treated as primary obstacles. The research contributes a fresh perspective by showing how these issues intersect to suppress innovation outcomes. In sum, successful digital empowerment in cybersecurity demands not only technology and training but also coherent governance, swift acquisition processes, and continuous performance monitoring.

6. Conclusion

The study concludes that digital innovation empowerment has played a pivotal role in strengthening efforts to prevent cybercrime in Kenya. Empowering officers with advanced digital tools, infrastructure, and technical skills has enhanced their ability to respond to complex and evolving cyber threats. Institutions that are operationally focused and possess strong leadership exhibited greater commitment to innovation and demonstrated higher success in integrating digital solutions into their systems. In contrast, institutions with regulatory or policy mandates struggled with limited innovation culture, inadequate infrastructure, and insufficient resource allocation, which hindered their ability to effectively embrace digital transformation. The findings also revealed widespread institutional challenges, including bureaucratic delays in procurement, lack of strategic partnerships, fragmented innovation mandates, and weak monitoring systems. These constraints significantly undermined the consistency and scalability of innovation efforts. Overall, the study underscores that successful cybercrime prevention requires more than just technological upgrades; it demands visionary leadership, collaborative engagement, a culture that supports innovation, and a clear strategic direction across all institutions involved in national cybersecurity.

7. Recommendations

Based on the findings, the study recommends a multifaceted approach to strengthen digital innovation empowerment for cybercrime prevention. First, the government should develop a National Digital Innovation Framework to guide coordinated investments, clarify agency roles, and eliminate mandate overlaps. Such a policy should promote inter-agency collaboration and ensure that all institutions have a shared vision for innovation in cybersecurity. Second, procurement systems should be streamlined by adopting digital procurement platforms with faster review and approval processes. This would reduce delays in acquiring modern technologies and enable agencies to remain responsive to rapidly evolving cyber threats. Third, institutions should be encouraged to establish formal partnerships with technology firms and academic researchers. These collaborations would foster knowledge exchange, facilitate co-creation of tools, and prevent redundant innovation efforts. Fourth, a capacity-building strategy must be institutionalized, focusing on digital skills training, innovation awareness, and leadership development. This would increase user adoption and encourage experimentation. Lastly, all innovation initiatives should be supported by robust monitoring and evaluation systems to ensure accountability, learning, and sustained impact. A feedback loop based on M&E results should inform policy adjustments and institutional learning over time.

Conflicts of Interest

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

References

Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing Cyber Threat Detection through Real-Time Threat Intelligence and Adaptive Defense Mechanisms. *International Journal of Computer Applications Technology and Research, 13,* 11-27.

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

Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education Online, 11,* 956-974.

Chiro, E. K., & Kyalo, J. (2024). Digital Integration and Performance of Information and Communication Technology Authority, Kenya. *Strategic Journal of Business & Change Management, 11,* 275-295. https://doi.org/10.61426/sjbcm.v11i1.2852

Elluri, L., Mandalapu, V., Vyas, P., & Roy, N. (2023). Recent Advancements in Machine Learning for Cybercrime Prediction. *Journal of Computer Information Systems, 65,* 249-263. https://doi.org/10.1080/08874417.2023.2270457

Gholami, M. F., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017). Challenges in Migrating Legacy Software Systems to the Cloud—An Empirical Study. *Information Systems, 67,* 100-113. https://doi.org/10.1016/j.is.2017.03.008

Gitari, S. M. (2020). *Reforming the Institutional and Legal Frameworks of E-Commerce in Kenya; Consumer Rights Protection in the Digital Economy.* Master's Thesis, 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

Herpig, S., & Schuetze, J. (2021). *The Encryption Debate in Germany: 2021 Update.* Carnegie Endowment for International Peace. https://www.interface-eu.org/publications/encryption-debate-germany-2021-update

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

Kiarie, N. (2024). Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions. *Journal of the Kenya National Commission for UNESCO, 5,* 1-14. https://doi.org/10.62049/jkncu.v5i1.191

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *International Research Journal of Modernization in Engineering Technology and Science, 4,* 2151-2164.

Motaung, J. R., & Sifolo, P. P. S. (2023). Benefits and Barriers of Digital Procurement: Lessons from an Airport Company. *Sustainability, 15,* Article 4610. https://doi.org/10.3390/su15054610

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

Business Context. *Global Scientific Journal, 7,* 576-582.

Nugawela, S., & Sedera, D. (2022). *Status Quo Bias in Users Information Systems (IS) Adoption and Continuance Intentions: A Literature Review and Framework.* arXiv: 2212.03283.

Ogene, F. (2024). Cybersecurity and IT Governance Challenges in Nigeria: Strategic Investment Needs and the Path Forward for a Resilient Digital Economy. *International Journal of Computer Applications, 186,* 41-46. https://doi.org/10.5120/ijca2024924275

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity Strategy's Role in Raising Kenyan Awareness of Mobile Internet Threats. *Information & Security: An International Journal, 32,* 155-174. https://doi.org/10.11610/isij.3207

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

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing Cybersecurity: A Comprehensive Review of Ai-Driven Detection Techniques. *Journal of Big Data, 11,* Article No. 105. https://doi.org/10.1186/s40537-024-00957-y

Schmitt, M. (2023). Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence (AI)-Enabled Malware and Intrusion Detection. *Journal of Industrial Information Integration, 36,* Article ID: 100520. https://doi.org/10.1016/j.jii.2023.100520

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

Tahiru, A. (2018). Cyber Security in Africa: The Threats and Challenges! *Cyberpolitik Journal, 3,* 91-104.

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

Tucker, S. G. (2022). *Strategies for Cybercrime Prevention in Information Technology Businesses.* Master's Thesis, Walden University.

Ukwuoma, H. C., Williams, I. S., & Choji, I. D. (2022). Digital Economy and Cybersecurity in Nigeria: Policy Implications for Development. *International Journal of Innovation in the Digital Economy, 13,* 1-11. https://doi.org/10.4018/ijide.292489

VMWare (2020). *The Impact of a Digitally Empowered Workforce.* Forbes Insights.

Walumoli, B. (2021). *A Critical Analysis of the Challenges Facing Counter Cybercrime in 21st Century Africa: A Focused Comparison of Kenya and Rwanda.* Master's Thesis, University of Nairobi.

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

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

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
DIE	Digital Innovation Empowerment
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
NC3	National Cyber Command Centre
NIS-CSU	National Intelligence Service's Cyber Security Unit
RCT	Rational Choice Theory
SPSS	Statistical Package for Social Sciences