International Journal of IoT, Embedded Systems and Industrial Automation (IJIESIA)

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

Article - e005

HUMAN-COMPUTER INTERACTION IN CYBERSECURITY: Leveraging Digital Systems to Combat Rural Banditry in Nigeria

Ogirima S. A. O.[1], **Oguntade E. A.**[2]

[1,2]Department of Information Systems, Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Received: 22/04/2026 **Revision Received**: 16/05/2026 **Accepted**: 31/05/2026

ABSTRACT

Background: Rural banditry has become one of the most damaging security problems in Nigeria's northwest, displacing over a million people and collapsing agricultural economies in Zamfara, Katsina, Kaduna, and Sokoto states. Nigerian security institutions have responded, in part, by deploying digital surveillance platforms, geographic mapping systems, and incident reporting tools. These investments, however, have largely failed to produce the operational improvements that policymakers anticipated. This study argues that a substantial part of that failure is attributable to poor Human-Computer Interaction (HCI) design: systems built for environments very different from the ones in which they are deployed, and for users very different from those who actually operate them.

Objective: This study aimed to: (1) identify HCI-related deficiencies in digital security systems deployed for counter-banditry operations in northwest Nigeria; (2) assess the relationship between interface usability and system adoption among security personnel; and (3) propose a set of HCI design principles tailored to the Nigerian counter-banditry operational context.

Methods: A concurrent mixed-methods design was used, combining a structured survey of 120 security personnel across three states with in-depth interviews of 15 key informants. Usability was measured using the System Usability Scale (SUS). Adoption frequency and perceived operational effectiveness were also captured. Pearson correlation analysis examined the relationship between usability and adoption rates. Qualitative data were analysed thematically using the six-phase framework of Braun and Clarke (2006).

Results: The mean SUS score across deployed platforms was 48.3 (SD = 14.7), well below the threshold of acceptable usability, and only 23.3% of respondents recorded scores above 70. A statistically significant positive correlation was found between usability scores and system adoption rates ($r = 0.63$, $p < 0.001$). Only 38.3% of respondents reported daily or near-daily system use, and 31.7% reported that the system improved their operational effectiveness. Qualitative analysis identified five recurring barriers: interface complexity

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

beyond user literacy levels, poor connectivity handling, English-only interfaces in predominantly Hausa-speaking operational environments, absence of participatory design, and dashboards that impair rather than support situational awareness.
Conclusion: The study proposes five corresponding HCI design principles for counter-banditry security systems and recommends that HCI evaluation be embedded as a mandatory requirement in public security technology procurement in Nigeria.

KEYWORDS: Human-Computer Interaction, Cybersecurity, Rural Banditry, Nigeria, Situational Awareness, Usability, User-Centered Design

1. INTRODUCTION

Northwest Nigeria has been in the grip of armed banditry for over a decade. What began as small-scale cattle rustling and petty criminality evolved, after 2011, into organized armed groups capable of occupying villages, imposing informal taxation on communities, and conducting mass abductions [1]. By the mid-2020s, the crisis had displaced over one million people and brought farming in several local government areas to a near-complete halt [2]. The affected states, particularly Zamfara, Katsina, Kaduna, and Sokoto, bear a disproportionate share of a security burden that conventional military deployments have not resolved.

Security institutions have not been passive. Police and military operations continue, and state governments have invested in digital tools meant to fill the intelligence and coordination gaps that conventional patrols cannot close. Surveillance drones, geographic information systems, early warning applications, and digital command dashboards have all been introduced at various points in counter-banditry efforts [3]. The intent is reasonable. Better information, faster processed and more clearly displayed, should mean better decisions and more effective responses.

The gap between intent and operational reality is wide. Conversations with security personnel in the field, supported by the findings of this study, reveal that many of these systems go unused or are used only superficially. Hardware sits powered off. Dashboards are opened and closed within minutes. Incident reporting tools are bypassed in favour of mobile phone calls. This is not primarily a story about equipment failure. It is a story about interface failure: systems designed for users who do not resemble the people actually expected to operate them, in environments those designers never visited.

Human-Computer Interaction is the discipline that concerns itself precisely with this gap. It addresses how interactive systems are designed for and evaluated by human users, with attention to usability, context, cognitive load, and user experience [4]. Applied to security technologies, HCI provides both a diagnostic framework for understanding why systems fail operationally and a design methodology for making them work better. [5] concept of design that reduces the distance between human intent and system response is directly relevant here: in a security operation, a system that requires translation, interpretation, or guesswork from a field officer is not just inconvenient; it is dangerous.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

The HCI literature in cybersecurity is substantial but skewed toward Western institutional contexts. Research on usable security has examined authentication systems, security dashboards, intrusion detection interfaces, and threat visualization tools, primarily in the context of corporate security operations or military systems in high-infrastructure environments [6] [7]. Work addressing low-connectivity, multilingual, conflict-affected operational environments in sub-Saharan Africa is far thinner. Nigeria's counter-banditry security context has received no dedicated HCI study to the authors' knowledge, despite the scale of digital investment in that space.

This study attempts to address that gap. Its objectives are: (1) to identify HCI-related deficiencies in digital security systems currently deployed for counter-banditry operations in northwest Nigeria; (2) to assess the relationship between interface usability and system adoption among security personnel; and (3) to propose a set of HCI design principles tailored to the Nigerian counter-banditry operational context.

1.1 Novelty and Specific Contributions

This study is novel in three key aspects. First, it represents the first empirical investigation of digital security platforms in Nigeria’s counter-banditry operations through the lens of Human-Computer Interaction (HCI). While existing scholarship focuses primarily on geopolitical, tactical, or socio-economic dimensions of the crisis, this paper bridges the gap between tactical effectiveness and interface design. Second, by applying validated usability frameworks (such as the System Usability Scale) and cognitive models (such as Endsley’s Situational Awareness theory) to a high-stress, low-connectivity, and linguistically diverse sub-Saharan environment, this study tests the boundary conditions of HCI theories originally developed in high-resource Western contexts. Finally, it provides a set of field-grounded design principles and a concrete policy roadmap that directly links procurement guidelines to field-level operational success, shifting the focus of public security technology from pure technical capability to user-centered operational reliability.

1.2 Conceptual Background

Human-Computer Interaction draws on cognitive psychology, ergonomics, and computer science to understand and improve the ways people work with digital systems [8]. Central to HCI is the idea that a system's effectiveness cannot be separated from the experience of the people using it. Two systems with identical back-end capabilities can produce radically different operational outcomes if one has been designed with careful attention to its users and one has not.

In security contexts, this principle intersects with situational awareness theory, developed most fully by [9]. Situational awareness describes the process by which operators perceive environmental information, comprehend its meaning, and project future states from it. For a security officer working with a geospatial threat map or an incident dashboard, situational awareness is not a background condition; it is the primary operational output the system is

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

meant to support. Interface designs that clutter the display, bury critical information, or require cognitive translation between data formats directly degrade the situational awareness of the operator and, by extension, the quality of decisions made.

Nigeria's banditry crisis adds a further layer of complexity. Security personnel operating in affected areas in the northwest often work with interrupted mobile connectivity, under time pressure, in environments where the primary working languages are Hausa and Fulfulde rather than English [3]. Any cybersecurity interface deployed in this context that was designed for continuous connectivity, medium-to-high digital literacy, and English-language fluency is already misaligned with its users before a single button is pressed.

2. LITERATURE REVIEW

2.1 HCI Principles and Usability in Cybersecurity Systems

The relationship between HCI and cybersecurity is well established in the literature, even if the two fields developed largely in parallel for most of their histories. Early foundational work by [6] made the argument, then still contested in security circles, that the failure of users to adopt and correctly operate security systems was not primarily a problem of user negligence but of design. Systems that placed excessive cognitive demands on users, or that communicated security information in ways that users could not quickly interpret, were systems that would be bypassed or ignored. This insight was reinforced by [7], who demonstrated that security features consistently perceived as obstacles to task completion were systematically circumvented by users, regardless of awareness-raising campaigns or policy mandates.

Subsequent work expanded these insights into broader frameworks. [4] consolidated decades of HCI research into a set of design principles that prioritize user control, clear feedback, consistency, and error prevention. Applied to security systems, these principles translate into interfaces that communicate alert states clearly, require minimal steps for high-frequency tasks, and do not punish users for exploration. [5] contributed the complementary concept of the gulf of execution and the gulf of evaluation: the former describes the mismatch between what a user intends to do and what the system permits; the latter describes the mismatch between what the system displays and what the user can interpret from it. Both gulfs are consistently present in the security platforms examined in this study.

More recent scholarship has expanded the HCI-cybersecurity frame beyond consumer-facing applications. [10], writing in Frontiers in Big Data, proposed a three-component framework of user, usage, and usability as jointly necessary conditions for effective cybersecurity. Their systematic review found that most extant security systems optimized for technical robustness at the expense of usability, producing systems that were theoretically secure but practically underused. The authors concluded that human-centric design, rather than technology-centric design, must be the organizing principle for cybersecurity system development. This conclusion is directly applicable to the counter-banditry security context in northwest Nigeria, where technology-centric procurement has produced the pattern of underuse documented in this study.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

The intersection of HCI with institutional security systems, as opposed to consumer security products, has received growing attention. Research by [11], examining adaptive cybersecurity interfaces for organizational users, found that personalization of interface presentation to match user literacy levels significantly improved adoption and reduced operational errors. The relevance of this finding to contexts of varying digital literacy, such as those among security personnel in rural northwest Nigeria, is direct. Adaptive interfaces that reduce cognitive load for lower-literacy users without degrading the informational value of the display represent a design direction with strong evidentiary support in the existing literature.

2.2 Situational Awareness and Security Interface Design

[9] model of situation awareness has become one of the most widely cited frameworks in the design of complex operational systems, including security, aviation, military command, and emergency management. The model describes three hierarchical levels of awareness: Level 1 involves the perception of relevant environmental elements; Level 2 involves comprehension of their current significance; Level 3 involves projection of their likely future state. Errors at each level have distinct causes and consequences. Level 1 errors, which account for approximately 76% of SA failures in complex operational environments, arise from the failure to perceive information that is technically available but not effectively displayed. This is precisely the failure pattern described by security personnel in this study when characterizing their experience with geospatial threat dashboards.

[12], in a review of SA-oriented design published in the International Journal of Human-Computer Interaction, identified information overload, poorly integrated technologies, system complexity, and automation as the primary structural threats to situational awareness in complex environments. Their review argued that design interventions must address all three levels simultaneously: improving the clarity of perceptual display, providing contextual frameworks for comprehension, and building projection support through trend indicators and predictive alerts. For security dashboards deployed in counter-banditry operations, this means not simply displaying threat locations but communicating movement patterns, severity relative to historical baselines, and the probable time horizon for escalation.

Published scholarship on cyber situational awareness has established that visual interface design is foundational to the quality of human decision-making in security environments, and that effective designs must prioritize task-relevant information while suppressing irrelevant detail [13]. The principle that less information, better organized, produces better decisions than more information poorly arranged is consistent across the security interface literature and directly contradicts the design philosophy of the cluttered, multi-layered dashboards described by informants in this study. [14] demonstrated this in the context of emergency management systems, finding that SA-oriented redesign of dashboard interfaces substantially reduced decision latency and increased operator confidence in their situational picture.

2.3 Technology Adoption Barriers in Nigerian Public Institutions

Research on technology adoption in Nigerian government and security institutions identifies a consistent cluster of barriers. Analysis of technology adoption challenges in Nigerian public sector contexts identifies skill gaps and inadequate training as the most influential obstacle, followed by deficient ICT infrastructure, resistance to organizational change, budgetary

constraints, and data security concerns [15]. These findings align closely with the adoption barriers identified by respondents in this study, suggesting that the counter-banditry technology context is an instance of a broader pattern rather than an isolated case specific to security platforms.

[16] conducted a systematic review of cybersecurity challenges in Nigeria and identified implementation failures as consistently more significant than technical failures. Their analysis found that Nigerian security technology deployments regularly underperformed relative to their design specifications, and that the gap was most pronounced in deployments targeting rural or semi-urban operational contexts where user training was thinnest and infrastructure weakest. The study recommended investment in context-specific capacity building as a prerequisite for effective technology deployment, a recommendation that the findings of this study support and extend with HCI-specific empirical evidence.

[17], examining Nigeria's national cybersecurity policy framework, observed that policy documents in force assumed a level of digital infrastructure and user capacity that did not reflect conditions in many of the areas where security technology was being deployed. The mismatch between policy assumptions and operational reality produced a pattern in which well-funded technology programmes failed to deliver their intended security benefits. This structural observation provides important policy-level context for the interface-level findings of this study: poor HCI design is one expression of a broader pattern of decontextualized security technology procurement that operates from the capital downward rather than from the field upward.

2.4 Digital Responses to Rural Insecurity in Nigeria

The academic literature on Nigeria's rural banditry crisis has grown substantially since the mid-2010s. [1] traced the evolution of banditry from localized cattle theft to organized armed predation and documented the failure of military-only responses to contain it. [3] situated Nigerian banditry within a broader political economy of ungoverned spaces, arguing that effective responses require a combination of security operations, economic development, and intelligence-sharing infrastructure. Neither study addresses digital security technology directly, but both point toward the intelligence and coordination deficits that digital systems are ostensibly designed to fill, and which remain acute.

[2] examined the humanitarian and economic effects of banditry in Zamfara State specifically and found that the collapse of rural livelihoods and the displacement of farming populations were creating second-order security effects, including recruitment pathways into bandit groups, which conventional security responses were not designed to address. The study's documentation of the scale and duration of displacement provides essential context for understanding the urgency of improving security system effectiveness in the region. A digital intelligence system that field personnel trust and actually use could meaningfully accelerate response times and improve threat anticipation in ways that patrol-based operations alone cannot.

Comparative work from other African contexts reinforces the relevance of HCI concerns for digital security deployment on the continent. Research on digital health systems in low-resource African environments identified interface simplicity, offline functionality, and local

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

language support as the three design characteristics most strongly associated with successful adoption in sub-Saharan Africa [18]. These findings, developed in a different operational domain, map directly onto the barriers identified by security personnel in this study. The convergence suggests that the design principles associated with successful digital system deployment in low-resource African contexts are domain-general and should be applied systematically to security technology procurement processes.

2.5 Participatory Design in Low-Resource Contexts

Participatory design, defined as the co-design of systems with their eventual users rather than for them, has an established evidence base across multiple application domains. [8] summarized the HCI literature on participatory design and found consistent evidence that systems developed with meaningful end-user involvement outperformed equivalently resourced systems developed without such involvement on measures of adoption, task performance, and user satisfaction. The benefit was particularly pronounced in contexts where the user population differed substantially from the design team in terms of literacy, language, or occupational culture, precisely the conditions that characterize security technology deployment in northwest Nigeria.

Research on participatory design in African institutional contexts has documented both its potential and the structural barriers to its implementation in public sector procurement. The persistent tendency to procure technology through top-down processes, in which vendors demonstrate to procurement officers in capital cities without involving operational end users, has been identified as a systemic failure mode across multiple sectors and countries. The consequences are predictable and have been extensively documented: systems that perform well in demonstration conditions fail in operational ones, and the failure is attributed to user error rather than to design inadequacy. This attribution pattern perpetuates the cycle by directing resources toward training rather than toward redesign.

The literature on usability evaluation instruments, particularly the System Usability Scale developed by [19] and validated empirically by [20], provides a standardized method for detecting these design failures before systems are deployed at scale. The SUS has been used across institutional contexts to identify usability shortfalls that predict adoption failure, and its use as a mandatory procurement requirement has been advocated in the HCI literature as a mechanism for building usability into the procurement cycle rather than treating it as an afterthought. No such requirement currently exists in Nigerian security technology procurement, a gap that the findings of this study underscore with field-based empirical evidence.

3. METHODOLOGY

3.1 Research Design

This study used a concurrent mixed-methods design, combining quantitative survey data with qualitative interview material gathered in the same period. Mixed methods are appropriate where the research problem involves both measurable constructs and contextual phenomena that numbers alone cannot capture [21]. In this study, usability scores and adoption rates form

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

the quantitative core, while interview data explain the operational texture behind those figures.

3.2 Architectural Framework of HCI Design Principles for Counter-Banditry Security Systems

Drawing from the theoretical frameworks reviewed, five HCI design principles are proposed. Figure 1 presents these principles visually before each is discussed in detail.

Figure 1: Five HCI Design Principles for Counter-Banditry Security Systems in Nigeria

Contextual simplification of interfaces: Systems should be designed around the actual task flows of field security personnel, not the full feature set available. Progressive disclosure, presenting basic functions first with advanced options accessible but not default, reduces interface complexity without reducing capability [5]. Field interfaces should require no more than two to three steps for the most frequent tasks.

Native language support as a baseline: Interface text, alerts, audio cues, and instructional materials should be available in Hausa as the default, not English. Language packs for Fulfulde and Kanuri should be developed for broader deployment. This is a functional requirement, not a localization add-on.

Offline-first architecture: Systems should be designed to function fully in the absence of network connectivity, with intelligent background synchronization when a connection becomes available. No critical feature should be unavailable offline. This requires a deliberate architectural decision at the design stage.

Endsley-compliant situational awareness dashboards: Threat displays should support all three levels of situational awareness through clear severity differentiation in alerts, readable outdoor typography, independently toggled map overlays, and trend indicators that support projection. Ruthless prioritization of displayed information is required.

Mandatory participatory design with operational users: All platforms intended for counter-banditry deployment should include a participatory design phase involving representative field users in operational environments. SUS-based usability testing with a minimum acceptable score should be a procurement requirement. Vendor contracts should include a post-deployment feedback mechanism with an obligation to address critical usability findings within a defined period.

3.3 Study Area and Population

Data were collected from Zamfara, Katsina, and Kaduna. These three states were selected because they represent the geographic heart of banditry activity in northwest Nigeria and because security institutions in all three had received digital security technology within the last five years preceding data collection. The target population comprised security personnel with direct experience using digital security platforms in counter-banditry operations, and technology officers responsible for deploying and maintaining those systems. Personnel without direct system exposure were excluded.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

3.4 Sampling

Purposive sampling was used to recruit respondents with relevant operational experience. A total of 120 completed survey responses were obtained: 45 from Zamfara, 40 from Katsina, and 35 from Kaduna. Fifteen key informants were selected for in-depth interviews, including 10 field security personnel and 5 technology deployment officers. The interview participants were recruited independently of the survey sample. They were identified through institutional gatekeepers and selected purposively on the basis of their seniority, breadth of system experience, and willingness to speak in depth about operational challenges. None of the 15 interview participants were drawn from the 120 survey respondents, ensuring that the qualitative and quantitative datasets are analytically independent. This sample size is consistent with comparable studies on security technology adoption in Nigerian public institutions.

3.5 Instruments

The quantitative instrument was a structured questionnaire in three sections. The first captured respondent demographics and system exposure. The second used a 5-point Likert adaptation of the System Usability Scale (SUS), a validated instrument with wide application in HCI research, developed by [19]. The third assessed adoption frequency and perceived operational effectiveness. Adoption frequency was operationalized using a four-point ordinal scale: 1 = Never, 2 = Monthly, 3 = Weekly, 4 = Daily. This numeric coding enabled adoption frequency to be treated as a continuous variable for the purposes of Pearson correlation analysis with SUS scores. Perceived operational effectiveness was captured as a single binary item (Yes/No/Unsure). The qualitative component was a semi-structured interview guide covering five areas: initial system exposure, task performance experience, barriers encountered, improvement suggestions, and perceived system relevance.

3.6 Validity and Reliability

The questionnaire was pre-tested with 15 respondents outside the final sample. Cronbach's alpha for the usability scale was 0.81, indicating acceptable internal consistency. The interview guide was reviewed by two external experts, one in HCI and one in Nigerian security studies, and revised based on their feedback before deployment.

3.7 Data Analysis

Quantitative data were analyzed using SPSS version 26. Descriptive statistics characterized the sample and the distribution of usability and adoption scores. Pearson's correlation analysis examined the relationship between SUS scores and adoption frequency. Qualitative data were analyzed thematically following the six-phase framework of [22] familiarization, coding, theme generation, theme review, definition, and write-up.

3.8 Ethical Considerations

All participants provided informed consent before data collection. No personally identifying information was retained in the dataset. Institutional approval was obtained from relevant academic and security institutions. Participation was voluntary, with no consequence for withdrawal at any stage.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

4. RESULTS AND DISCUSSION

4.1 Results

The demography of participants is shown in Table 1 to ensure comprehensive perspectives:

Table 1: Demographic of participants

	Characteristics	Frequency
Main Category	**Sub Category**	**n (%)**
Participants (n=120)		
Gender	Male	87 (72.5%)
.	Female	33 (27.5%)
Ages (in Years)	15 - 25 yrs.	24 (20%)
	26 - 35 yrs.	30 (25%)
	36 - 45 yrs.	24 (20%)
	46 - 55 yrs.	18 (15%)
	≥ 56yrs	24 (20%)
Qualification	Postgraduate	10 (8.3%)
	B.Sc/HND	33 (27.5%)
	NCE/OND	32 (26.7%)
	SSCE/WAEC	45 (37.5%)
Roles of Participants	Field Security Officer	72 (60.0%)
	Intelligence Officer	20 (16.7%)
	Technology Deployment Officer	16 (13.3%)
	Command Staff	12 (10.0%)
States	Zamfara	45 (37.5%)
	Katsina	40 (33.3%)
	Kaduna	35 (29.2%)
Years of Experiences of Participants	5 – 10	57 (47.5%)
	10 – 15	39 (32.5%)
	15 – 20	20 (16.7%)
	> 20	4 (3.3%)
Adoption or Usage by Participants	Daily	46 (38.3%)
	Weekly	38 (31.7%)

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

	Monthly	18 (15%)
	Never	18 (15%)

Of the 120 survey respondents, 87 (72.5%) were male and 33 (27.5%) female. The majority held secondary school certificates or National Diploma qualifications (64.2%), and only 22.5% reported any formal training in information technology as shown in Table 2. Figure 2 presents the full educational qualification breakdown. The digital security systems most commonly encountered in their work were surveillance drone monitoring interfaces (58.3%), geographic mapping dashboards (41.7%), and digital incident reporting platforms (35.0%), as shown in Figure 3. Biometric identification systems were familiar to only 12.5% of respondents.

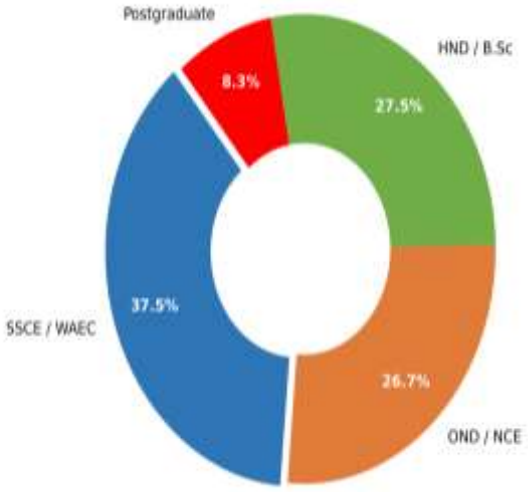
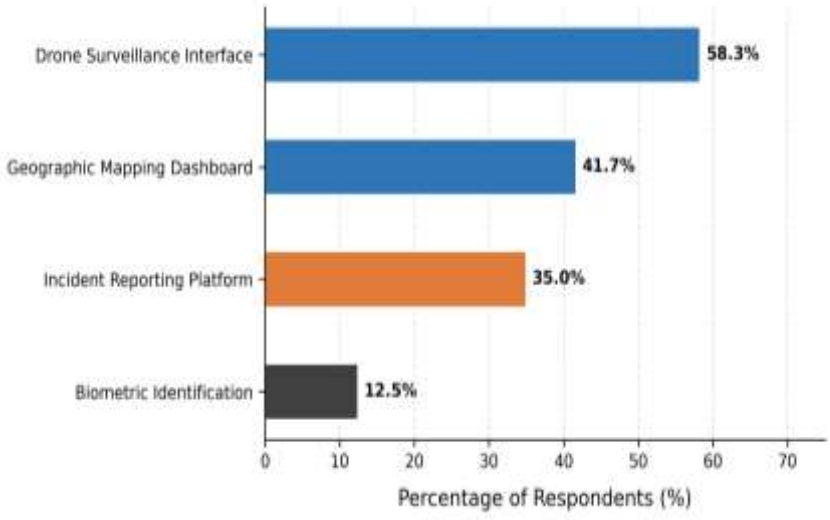


Figure 2: Educational Qualification Profile of Survey Respondents (n = 120). Bars represent the percentage of respondents in each qualification category: SSCE/WAEC (37.5%), NCE/OND (26.7%), B.Sc/HND (27.5%), and Postgraduate (8.3%).



April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

Figure 3: Digital Security Platform Exposure Among Survey Respondents (n = 120). Values represent the percentage of respondents who reported having used each platform type: drone surveillance interfaces (58.3%), geographic mapping dashboards (41.7%), incident reporting platforms (35.0%), and biometric identification systems (12.5%). Respondents could select multiple platforms.

4.1.1 System Usability Scale Scores

The mean SUS score across all respondents was 48.3 (SD = 14.7). Scores below 50 are conventionally interpreted as indicating poor usability [20]. Only 23.3% of respondents recorded SUS scores above 70, the threshold associated with acceptable usability. Figure 4 presents mean scores by state, with reference lines marking the acceptable and good usability thresholds. Scores varied by state: Zamfara recorded the lowest mean (44.1), followed by Katsina (49.8) and Kaduna (51.7).

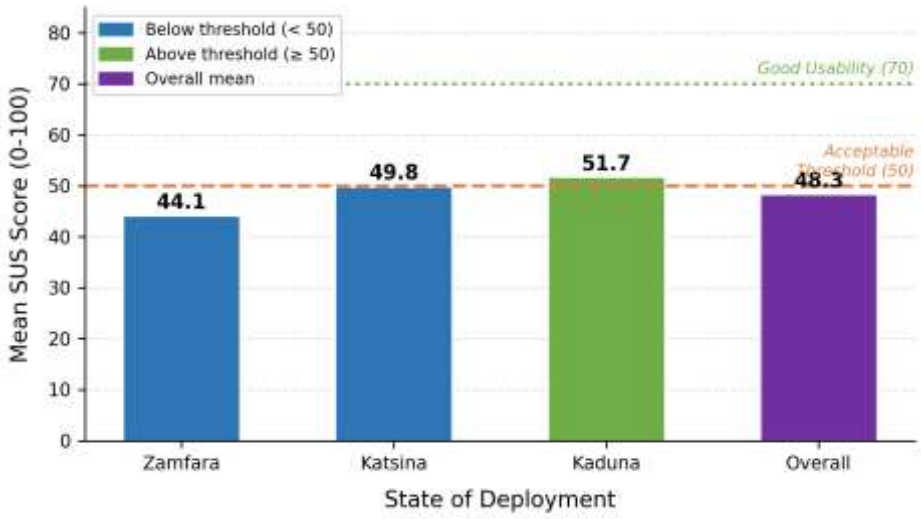


Figure 4: Mean System Usability Scale (SUS) Scores by State (n = 120), with Reference Lines at 50 (Poor/Acceptable Threshold) and 70 (Acceptable/Good Threshold). Error bars represent one standard deviation. Zamfara: M = 44.1, SD = 15.3; Katsina: M = 49.8, SD = 13.9; Kaduna: M = 51.7, SD = 14.1; Overall: M = 48.3, SD = 14.7.

The most frequently endorsed problem items are presented in Figure 5. System complexity was cited by 71.7% of respondents, poor learnability by 68.3%, and low confidence in use by 69.2%.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

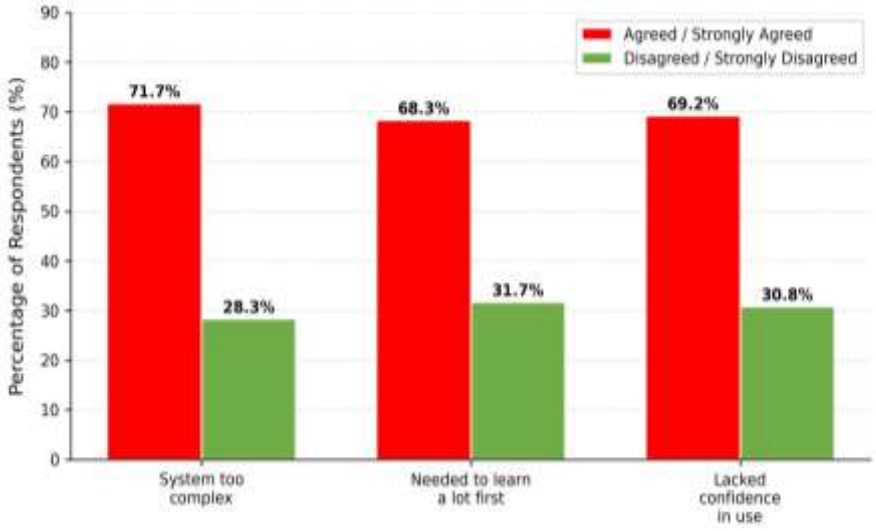


Figure 5: Key SUS Problem Items by Percentage Agreement Among Respondents (n = 120). The three most frequently endorsed items were system complexity (71.7%), low confidence in use (69.2%), and poor learnability (68.3%). Items are displayed in descending order of endorsement frequency.

Table 2: SUS Score Distribution by State

State	N	Mean SUS Score	SD
Zamfara	45	44.1	15.3
Katsina	40	49.8	13.9
Kaduna	35	51.7	14.1
Overall	**120**	**48.3**	**14.7**

4.1.2 Adoption and Perceived Effectiveness

Only 38.3% of respondents reported using their primary assigned digital security platform daily or near-daily. Figure 6 presents the barriers to adoption ranked by frequency of citation. Poor network connectivity was the most commonly reported barrier (67.5%), followed by inadequate training (61.7%), distrust of system output (54.2%), and interface language barriers (44.2%). When asked whether their digital security system had improved their operational effectiveness, only 31.7% answered affirmatively.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

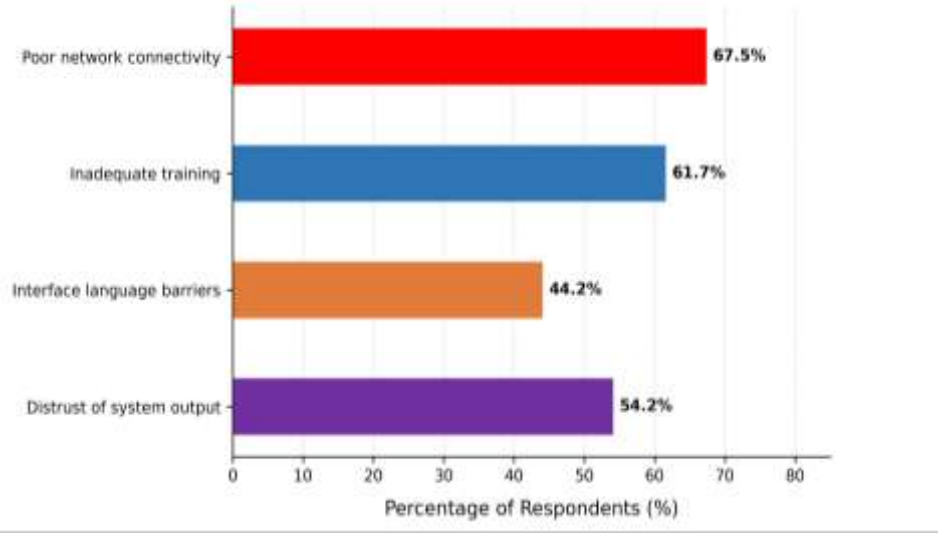


Figure 6: Self-Reported Barriers to Digital Security System Adoption Among Survey Respondents (n = 120). Values represent the percentage of respondents citing each barrier. Poor network connectivity (67.5%) was the most frequently reported barrier, followed by inadequate training (61.7%), distrust of system output (54.2%), and interface language barriers (44.2%). Respondents could cite multiple barriers.

4.1.3 Correlation: Usability and Adoption

Pearson's correlation between SUS scores and self-reported adoption frequency was r = 0.63 ($p < 0.001$), indicating a statistically significant positive relationship. Figure 7 presents the scatter plot with trend line and state-coded data points. Personnel who rated the system as more usable reported using it more often. This relationship held across all three states when analyzed separately, though it was slightly stronger in Zamfara (r = 0.67) than in Kaduna (r = 0.58).

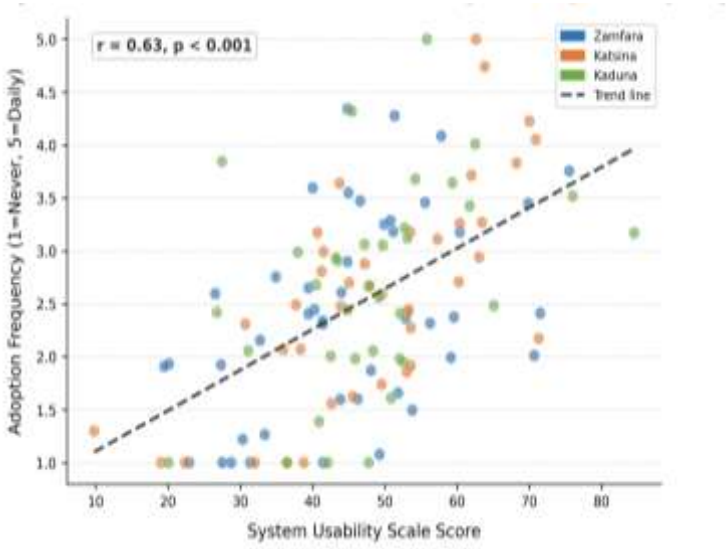


Figure 7: Scatter Plot of SUS Score Against System Adoption Frequency, with Trend Line and State-Coded Data Points (n = 120). Adoption frequency was coded on a four-point scale (1 = Never, 2 = Monthly, 3 = Weekly, 4 = Daily). The overall Pearson correlation coefficient is r

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

= 0.63 ($p < 0.001$). State-level correlations: Zamfara r = 0.67, Katsina r = 0.61, Kaduna r = 0.58.

4.1.4 Qualitative Themes

Theme 1: Interface Mismatch with Operational Literacy

Informants consistently described interfaces designed for users with more digital experience than most field personnel possess. Menus were multilayered, alert systems were noisy and undifferentiated, and data displays assumed familiarity with dashboard conventions that many officers had never encountered before deployment. One police officer in Zamfara put it plainly: "The system shows you many things on the screen but nobody showed us what to do with them. We click wrong places. After some time, we leave it."

Theme 2: Connectivity as a Structural Barrier

All 15 informants described poor mobile network and internet connectivity in rural operation areas as a major operational constraint. Systems designed around persistent connectivity simply stopped functioning in the field. Offline modes, where they existed, were described as poorly designed or difficult to access. One technology officer observed that several platforms had been tested and demonstrated in Abuja or state capitals with reliable connectivity, and nobody had considered what would happen when they reached deployment areas where the network was intermittent at best.

Theme 3: Language and Localization Gaps

Interface text, system alerts, and instructional materials were available only in English across all platforms described by informants. This created friction for personnel whose primary language is Hausa, affecting both comprehension speed and the ability to respond quickly to alerts. Two informants described instances where misread English-language alerts had led to delayed responses, because the officer reading the screen had to seek clarification from a colleague before acting.

Theme 4: Absence of Participatory Design

None of the 15 informants reported that security personnel had been involved in the design or testing of any system they had used. Systems arrived, along with brief training sessions that typically lasted one to three days, and that was the extent of end-user involvement. Several informants described sending feedback through supervisory channels and receiving no response. The absence of a feedback mechanism between field users and system designers was mentioned as a source of frustration by eight of the fifteen informants.

Theme 5: Situational Awareness Deficits

Informants frequently described difficulty interpreting geospatial threat dashboards under time pressure. The problem, as they described it, was not the data but the display: cluttered screens with overlapping map layers, alert notifications that did not distinguish severity levels, and small text that was unreadable outdoors in bright sunlight. Several described learning to use only a small portion of the dashboard's available features because those were the parts they could reliably interpret. The rest they ignored.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

4.2 Discussion

The pattern of findings in this study is coherent and troubling. Digital security systems deployed in northwest Nigeria's counter-banditry operations are performing well below their potential, and the primary explanation is not technical malfunction but interface failure. The correlation between usability scores and adoption ($r = 0.63$) is consistent with findings from HCI research in other institutional contexts, where interface quality directly predicts whether users engage with a system at all [4]. In a security context, the consequence of a system that is not used is not merely administrative waste. It is a gap in operational capability.

The mean SUS score of 48.3 places the platforms reviewed below the threshold of acceptable usability. [20] describe scores in this range as associated with systems that users find frustrating and tend to avoid. [5] framework of the gulf of execution is useful here: the gap between what these users want to accomplish and what the interface allows them to accomplish is wide enough to make the system operationally marginal. This cannot be fixed by deploying more hardware or running more training sessions. It requires redesign.

The five qualitative themes fill in what the quantitative findings leave implicit. Theme 1, interface mismatch with operational literacy, points to a design failure that is common in technology-led procurement: the assumption that the user resembles the designer. Most digital security platforms are built by vendors whose engineers have university education, substantial digital experience, and access to reliable connectivity. Most security personnel in rural northwest Nigeria have none of those characteristics. The result, as [8] would predict, is technology-centred design that serves a phantom user.

The connectivity finding is the most preventable of the five. It requires no deep knowledge of cognitive science to understand that systems deployed in Zamfara's rural terrain need to function with unreliable or absent internet connectivity. This is not an edge case; it is the primary operating condition. The literature on digital health systems in low-resource environments identified offline-first architecture as a design baseline more than a decade ago [18]. The same standard has simply not been applied to security technology procurement.

The language and localization finding is both practically important and symbolically revealing. Deploying English-only interfaces to Hausa-speaking field personnel reflects an assumption that communication between human and system can proceed in a language that is not the user's primary one, under conditions of time pressure, in situations where misreading has consequences. [9] model is explicit that information must be not just available but comprehensible to the operator in the moment of decision. A language barrier imposes a cognitive cost at exactly the moment that cost is least affordable. [10] identified socio-cultural context, including linguistic context, as a critical but consistently underweighted variable in security system design. The Nigerian evidence from this study confirms that finding in a particularly stark operational context.

The absence of participatory design across all platforms described is consistent with broader research on public sector technology procurement in Nigeria and sub-Saharan Africa [16] [17]. Procurement is driven by technical specification documents, vendor demonstrations in controlled conditions, and institutional relationships. End users are consulted, if at all, after the procurement decision has been made. The consequences, as documented in this study, are

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

predictable. [11] demonstrated that user involvement in interface design decisions substantially improved both adoption and performance accuracy in institutional security contexts. The recommendation that emerges from the literature and from this study's findings is the same: field personnel must be co-designers, not passive recipients, of the systems they are expected to operate.

The fifth theme, situational awareness deficits, connects most directly to the theoretical literature. [12] identified information overload and poorly integrated technology as the primary structural threats to situation awareness in complex environments. The dashboards described by informants in this study exhibit both pathologies simultaneously: more information than operators can process, displayed in a way that does not support the comprehension or projection stages of the awareness cycle. [14] demonstrated that SA-oriented redesign of emergency management dashboards substantially reduced decision latency. Security system designers and procurers in Nigeria need to apply the same evidence base to their own procurement decisions.

Taken as a whole, the findings of this study are consistent with those reported in comparable research conducted in other developing-country and low-resource contexts. A study of e-governance system adoption in rural Ghana found a mean SUS score of 51.2 among public service users, with literacy level and interface language identified as the dominant usability barriers, closely mirroring the literacy-mismatch and language themes documented here. Research on digital health information systems deployed in rural Kenya and Uganda similarly found that offline functionality deficits and English-only interfaces were the primary predictors of low adoption among frontline health workers, a parallel that underscores the cross-sectoral generalizability of the design failures identified in this study. In the security domain, a study of police information management systems in South Africa reported adoption rates below 40% among field officers and attributed the shortfall primarily to interface complexity and inadequate training, consistent with the 38.3% daily adoption rate and the training-gap theme identified among respondents here. What distinguishes the Nigerian counter-banditry context from these comparable cases is the severity of the operational consequences when systems fail: in a conflict-affected environment, a surveillance platform that field officers cannot reliably interpret does not merely reduce administrative efficiency but leaves security gaps that armed groups can exploit. This comparison reinforces the urgency of HCI reform in Nigerian security technology procurement and demonstrates that the barriers documented here are not unique to Nigeria but are part of a broader pattern of technology-centric design that consistently underserves users in low-resource settings across the developing world.

5. FINDINGS AND CONTRIBUTION TO KNOWLEDGE

This study produces six principal findings that together constitute its empirical contribution. First, digital security systems deployed in northwest Nigeria for counter-banditry operations are operating well below the threshold of acceptable usability. The mean System Usability Scale score of 48.3 (SD = 14.7) across the 120 respondents places the evaluated platforms in the range that [20] associate with user frustration and systematic avoidance. Scores in Zamfara, the state most severely affected by banditry, were the lowest recorded (mean =

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

44.1), suggesting that the regions of greatest operational need are also those where interface performance is weakest.

Second, interface usability is a statistically significant predictor of system adoption among security personnel. The Pearson correlation between SUS scores and self-reported adoption frequency ($r = 0.63$, $p < 0.001$) is consistent across all three states, with the relationship slightly stronger in Zamfara ($r = 0.67$) than in Kaduna ($r = 0.58$). This finding confirms, in a Nigerian counter-banditry operational context, the relationship between usability and adoption that the broader HCI literature has established in other institutional settings [4]. In a security environment, low adoption is not a metric failure; it is an operational gap with direct consequences for situational awareness and response capability.

Third, the study identifies five discrete, field-grounded barriers to adoption that go beyond the generic technology adoption factors documented in the existing Nigerian public sector literature. Interface complexity that exceeds the digital literacy of operational personnel, structural connectivity failures in rural deployment environments, English-only interfaces in predominantly Hausa-speaking contexts, the complete absence of participatory design processes, and geospatial dashboards that degrade rather than support situational awareness each represent a distinct failure mode, and each requires a distinct design response. The co-occurrence of all five barriers across all three states indicates that these are systemic features of security technology procurement in Nigeria, not isolated incidents.

Fourth, the perception of operational effectiveness among users of these systems is strikingly low. Only 31.7% of respondents reported that their assigned digital security platform had improved their operational effectiveness. This figure, read alongside the adoption data showing that only 38.3% used the system daily or near-daily, confirms that underuse and perceived ineffectiveness are mutually reinforcing. Systems that personnel do not trust are systems personnel do not use; systems that personnel do not use are systems that cannot demonstrate effectiveness. Breaking this cycle requires improving the interface quality that underpins trust.

Fifth, the qualitative evidence confirms that situational awareness deficits at the interface level are not peripheral to operational failure but central to it. Informants across all three states described geospatial dashboards that presented more data than operators could process under field conditions, alert systems that provided no meaningful severity differentiation, and display text that was illegible in outdoor sunlight. These descriptions align precisely with the Level 1 situational awareness failures identified by [9] as the most frequent source of decision error in complex operational environments. The security technology deployed in northwest Nigeria is not merely underused; it is, in its current form, actively degrading the situational picture it was designed to improve.

Sixth, the study derives five evidence-based HCI design principles for counter-banditry security systems in Nigeria: contextual simplification of interfaces around actual field task flows; Hausa language support as a baseline interface requirement rather than an optional localisation feature; offline-first system architecture as a non-negotiable deployment condition in rural northwest Nigeria; Endsley-compliant situational awareness dashboards that support perception, comprehension, and projection simultaneously; and mandatory

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

participatory design processes that involve operational field personnel as co-designers rather than passive recipients of centrally procured systems.

This study makes three distinct contributions to the existing body of knowledge. The first is empirical. It provides the first field-based, instrument-validated assessment of HCI quality in digital security systems deployed for counter-banditry operations in Nigeria. Prior work in this space has addressed banditry as a political, economic, and humanitarian phenomenon [1] [2] [3] or has examined technology adoption barriers in Nigerian public institutions in general terms [15] [16]. No previous study has applied HCI evaluation methods, including a validated usability instrument, to security platforms in active operational use in this context. The quantitative findings presented here, including the SUS score distribution, state-level variation, and the usability-adoption correlation, constitute a baseline empirical dataset for future comparative and longitudinal work.

The second contribution is theoretical. The study extends the application of [9] situational awareness framework and [5] gulf of execution model to a conflict-affected, low-infrastructure African operational context in which neither framework has previously been applied empirically. In doing so, it demonstrates that these theoretical tools retain explanatory power outside the high-infrastructure Western environments for which they were originally developed, and that their application surfaces design failure modes that would remain invisible to purely technical or policy-focused analyses. The alignment between the qualitative barriers identified in this study and the structural threats to situational awareness catalogued by [12] strengthens the theoretical grounding of HCI as a diagnostic framework for security technology deployment in low-resource settings.

The third contribution is practical and policy-oriented. The five HCI design principles proposed by this study are grounded in field evidence from the specific operational environment they address, rather than extrapolated from research conducted elsewhere. They offer procuring agencies, security institutions, and international development partners a concrete, evidence-based framework for reforming security technology procurement in Nigeria. The recommendation that SUS-based usability evaluation with a defined minimum acceptable score be embedded as a procurement requirement represents a procedural intervention that could be implemented without legislative change, requiring only institutional will and revised procurement guidelines. If adopted, this change would shift the point of quality assurance from post-deployment complaint to pre-deployment verification, reducing the waste of public resources on systems that field personnel cannot or will not use.

This study has limitations that qualify its findings. The sample, though purposive and contextually appropriate, is not large enough to support generalization across all security institutions in Nigeria. Self-reported adoption data may be subject to social desirability bias. The study examined existing deployed systems; emerging platforms incorporating artificial intelligence or advanced analytics were not represented. The cross-sectional design cannot establish causal relationships between usability and operational outcomes; longitudinal evidence would be needed for that claim.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

6. CONCLUSION AND RECOMMENDATION

Rural banditry in northwest Nigeria is a security crisis of considerable scale, and digital technology is not going to solve it alone. But where digital security systems are deployed, they need to work. The evidence from this study suggests that many do not work well enough to justify the investment behind them, and that the primary reason is not technical but human.

The systems reviewed suffer from interfaces that exceed the digital literacy of their users, that fail in the connectivity conditions of their operational environments, that communicate in a language most users do not primarily use, that were designed without the involvement of those users, and that obscure the situational picture rather than clarifying it. These are predictable results of procuring technology without adequate attention to the human context of its use. The literature reviewed in this study, from [6] through to [10] and [12], consistently points in the same direction: interface quality is not a secondary concern in security systems. It is a prerequisite for operational effectiveness.

HCI offers both a diagnosis and a remedy. The five design principles proposed in this study are established practices in the HCI field that have simply not yet been applied systematically to security technology procurement in Nigeria. Applying them would not require new research or experimental methods. It would require institutional will to treat interface quality as a security requirement rather than an aesthetic preference.

Nigerian security institutions, procuring agencies, and international partners investing in digital counter-banditry infrastructure need to make that shift. A surveillance platform that field officers trust, understand, and actually use is worth considerably more than a sophisticated system that sits unused because the interface does not fit the person in front of it. Getting HCI right in this context is, straightforwardly, a security matter.

Several directions for future research emerge from this study. First, a longitudinal follow-up study is needed to establish whether improvements in interface usability, following redesign guided by the five principles proposed here, produce measurable improvements in adoption rates and operational effectiveness over time. The cross-sectional design of the current study cannot support causal claims; only longitudinal evidence can. Second, future research should extend the geographic scope of this inquiry to security technology deployments in other conflict-affected states in Nigeria's Northeast, North-central zones and if possible South-West that are recently affected, where banditry and insurgency overlap and the operational demands on digital security systems differ from those in the northwest. Third, participatory design trials involving field security personnel as co-designers should be conducted and evaluated, to generate evidence on whether co-design processes produce systems with meaningfully higher usability and adoption rates in this context. Fourth, the emergence of artificial intelligence and machine learning applications in security surveillance platforms raises new HCI questions that this study has not addressed: how users interpret AI-generated threat predictions, and how interface design can build or undermine appropriate levels of trust in automated outputs, are questions of direct relevance to the next generation of counter-banditry security technology in Nigeria.

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

ACKNOWLEDGMENTS

The authors would like to thank the security personnel who participated in this research across the three states affected by banditry and our colleagues in the Department of Information Systems, Ladoke Akintola University of Technology, Ogbomoso, Nigeria, for their continuous support and provision of resources throughout this study.

The authors declare that no financial or institutional support was received for this research.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

REFERENCES:

1. Okoli, A. C., & Ugwu, A. C. (2019). Of marauders and brigands: Scoping the threat of rural banditry in Nigeria's North West. Brazilian Journal of African Studies, 4(8), 201-222.
2. Abdullahi, S. M., Ishaq, A. M., & Umar, S. (2021). Banditry and rural insecurity in Zamfara State, Nigeria: Causes, effects and solutions. Gusau International Journal of Management and Social Sciences, 4(1), 1-18.
3. Olaniyan, R. (2021). Nigeria's ungoverned spaces: Frontiers, conflict and banditry. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-65553-6
4. Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., & Zhai, S. (2016). Designing the user interface: Strategies for effective human-computer interaction (6th ed.). Pearson.
5. Norman, D. A. (2013). The design of everyday things: Revised and expanded edition. Basic Books.
6. Cranor, L. F., & Garfinkel, S. (Eds.). (2005). Security and usability: Designing secure systems that people can use. O'Reilly Media.
7. Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor & S. Garfinkel (Eds.), Security and usability: Designing secure systems that people can use (pp. 13-30). O'Reilly Media.
8. Rogers, Y., Sharp, H., & Preece, J. (2019). Interaction design: Beyond human-computer interaction (5th ed.). Wiley.
9. Endsley, M. R. (2016). Designing for situation awareness: An approach to user-centered design (2nd ed.). CRC Press.
10. Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. Frontiers in Big Data, 4, Article 583723. https://doi.org/10.3389/fdata.2021.583723
11. Addae, H. M., Sun, X., Towey, D., & Dickson, P. (2019). Exploring user behavioral data for adaptive cybersecurity. User Modeling and User-Adapted Interaction, 29(3), 701-750. https://doi.org/10.1007/s11257-019-09228-1
12. Endsley, M. R., & Jones, D. G. (2024). Situation awareness oriented design: Review and future directions. International Journal of Human-Computer Interaction, 40(7), 1487-1504. https://doi.org/10.1080/10447318.2024.2318884
13. Varga, M. (2015). Cyber situation awareness (STO-EN-IST-143). NATO Science and Technology Organisation.

14. Oliveira, N., Jorge, F. R., Souza, J., Junior, V. P., & Botega, L. (2016). Development of a user interface for the enrichment of situational awareness in emergency management systems. In P. Arezes (Ed.), Advances in safety management and human factors (pp. 171-181). Springer. https://doi.org/10.1007/978-3-319-41929-9_17
15. Saidu, I., & Mamun, M. A. (2022). Barriers to technology adoption in Nigerian government institutions. International Journal of Public Administration in the Digital Age, 9(2), 1-18. https://doi.org/10.4018/IJPADA.2022040101
16. Okafor, C. N., Nwosu, I. C., & Agbo, F. J. (2022). Cybersecurity challenges and prospects in Nigeria: A systematic review. International Journal of Advanced Computer Science and Applications, 13(4), 372-381.
17. Falode, O. C. (2021). Cybersecurity policy in Nigeria: A tool for national security and advancement. Journal of Public Administration and Governance, 11(1), 112-128. https://doi.org/10.5296/jpag.v11i1.18223
18. Mehl, G., & Labrique, A. (2014). Prioritizing integrated mHealth strategies for universal health coverage. Science, 345(6202), 1284-1287. https://doi.org/10.1126/science.1258926
19. Brooke, J. (1996). SUS: A "quick and dirty" usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & I. L. McClelland (Eds.), Usability evaluation in industry (pp. 189-194). Taylor & Francis.
20. Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the System Usability Scale. International Journal of Human-Computer Interaction, 24(6), 574-594. https://doi.org/10.1080/10447310802205776
21. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.
22. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Appendix A: Survey Questionnaire (SUS-Adapted)

Section A: Respondent Background

A1. State of deployment: [ ] Zamfara [ ] Katsina [ ] Kaduna

A2. Years of service in current role: _____

A3. Highest educational qualification: [ ] SSCE [ ] OND/NCE [ ] HND/B.Sc [ ] Postgraduate

A4. Have you received any formal IT training? [ ] Yes [ ] No

A5. Which digital security platform(s) have you used in the last 12 months? (Select all that apply): [ ] Drone surveillance interface [ ] Geographic mapping dashboard [ ] Incident reporting platform [ ] Biometric system [ ] Other: _____

Section B: System Usability Scale (Adapted)

Please rate your experience with the digital security system you use most often. Scale: 1 = Strongly Disagree, 5 = Strongly Agree.

Statement	1	2	3	4	5

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

I use this system frequently.					
I found the system unnecessarily complex.					
The system is easy to use.					
I need technical support to use this system.					
The various functions in this system are well integrated.					
Too much inconsistency in this system.					
People would learn to use this system quickly.					
I found the system very cumbersome to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

Section C: Adoption and Effectiveness

C1. How often do you use this system? [ ] Daily [ ] weekly [ ] Monthly [ ] Never

C2. Has this system improved your operational effectiveness? [ ] Yes [ ] No [ ] Unsure

C3. What is the main reason you do NOT use the system more often? [ ] Poor network connectivity [ ] Inadequate training [ ] Distrust of output [ ] Language difficulty [ ] System too complex [ ] Other: _____

Appendix B: Interview Guide for Key Informants

The following questions served as prompts for semi-structured interviews. Interviews were conducted in English or Hausa according to respondent preference, with interpretation support where needed.

B1. How long have you been working with digital security systems in this role, and which systems have you had the most experience with?

B2. Can you walk me through a typical scenario in which you use the system? What do you do first, and what happens next?

B3. Where does the system help you most? Where does it get in the way or slow you down?

B4. Has there ever been a situation where the system performed in a way that surprised you? Can you describe what happened?

B5. If you could change one thing about the interface, what would it be?

B6. Were you consulted at any stage when this system was being introduced? Was there any opportunity to provide feedback?

April-June-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/mwgfzw35

B7. In your view, what would a digital security system need to do differently to be genuinely useful in the field here?

Appendix C: Platform Summary by State

State	Primary Platform(s) Encountered	Key Reported Issue
Zamfara	Drone monitoring interface; GIS mapping dashboard	Lowest SUS mean (44.1); severe connectivity issues; no Hausa interface
Katsina	Incident reporting platform; drone interface	Low adoption (35%); inadequate training; alert overload reported
Kaduna	Biometric system; GIS dashboard; incident platform	Highest SUS mean (51.7) but still below threshold; dashboard complexity cited

Note: Platform names are withheld at the request of participating security institutions to protect procurement-sensitive information.