© Journal of Security Management, Policy & Administration, Nigerian Defence Academy, Kaduna. Vol. 3, No. 3, 2026 ISSN: 2971-7973
Available on https://jsmpa.com.ng. IBIAMA Tonye Furo & OGUNLEYE O. Adebayo

The Role of Leadership in Enhancing Military Cybersecurity and Information Management Systems: A Study of the Nigerian Army Cyberwarfare Command

By

IBIAMA Tonye Furo

&

OGUNLEYE Olutosin Adebayo

Department of History and War Studies, Nigerian Defence Academy, Kaduna.

Abstract

This study examined the role of leadership in enhancing Information Management Systems (IMS) in the Nigerian Army. It investigated the cybersecurity leadership strategies employed in the NA and assessed their effectiveness in enhancing information management in military systems. The study anchored on the Transformational Leadership Theory and adopted a convergent parallel mixed-methods design to select Nigerian Army formations with cybersecurity and information management responsibilities. A sample of 404 respondents was purposively selected from an estimated population of 10,000 personnel using a multi-stage sampling approach. Quantitative data were collected from 386 respondents through structured questionnaires, while qualitative data were obtained through 18 key informant interviews. Quantitative data were analysed using descriptive statistics, while qualitative data were subjected to thematic analysis. Findings from both strands were triangulated to provide a comprehensive understanding of cybersecurity leadership practices within the NA. The findings revealed that the NA utilises a combination of situational, authoritative and transformational leadership strategies in managing cybersecurity operations, with situational and transformational leadership being the most dominant. The findings also showed that respondents perceive cybersecurity leadership as a critical factor associated with the effectiveness of IMS and NA. The study recommends the institutionalisation of a cybersecurity leadership development framework and the establishment of an integrated cybersecurity coordination and incidence response system in the NA for improved IMS.

Keywords: Cybersecurity, Information Management Systems, Nigerian Army, Military Effectiveness, National Security.

1. INTRODUCTION

Increase in the rate of overreliance on technology has necessitated a crucial need for ensuring privacy, maintaining organizations operations and protecting sensitive data in recent times. This has led to development of strategies that can provide strong security postures against malicious attacks to protect internet connected systems such as hardware, software and data from cyber-threats (Hasib, 2021; Northouse, 2021). Keeping up with threat intelligence, new technologies and security trends required in cybersecurity is a challenging task, which can only be executed by the strategic role of organisational leadership (Gonzales, 2014; Stanciulescu & Beldman, 2019). This has led to the emergence of cybersecurity leadership to guide organisations in protecting their systems from cyberattacks, which immobilise and disrupt organisations' system or sensitive data.

To guard against cybersecurity threats and protect its information systems, the NA has taken commendable steps to enhance its cybersecurity capacity. A notable stride is the establishment of the Nigerian Army Cyber Warfare Command (NACWC) in 2018. This initiative aligned with the 2014 National Cybersecurity Policy and Strategy which aimed to protect national data, networks and information systems, while also countering online radicalization and terrorist propaganda (O'Flaherty, 2018). However, persistent issues such as inadequate personnel training, an overdependence on technological tools without robust human oversight and insufficient funding have limited the NACWC's effectiveness (Okafor, 2019; Agwu, 2021). These shortcomings have left the NA's Information Management Systems (IMS) vulnerable to increasingly sophisticated cyber threats and risks compromising sensitive military data and weakening operational integrity.

Evidence of these vulnerabilities is apparent in high-profile breaches. For instance, in 2017, Boko Haram insurgents disrupted the NA's recruitment process by compromising its website (Murtala, 2023). In 2021, a cyberattack on the Nigerian Defence Academy (NDA) led to an online crisis that eroded public trust in the military's capacity to secure its digital infrastructure (Agwu, 2021). Similarly, coordinated online disinformation during the 2020 #EndSARS protests damaged the Army's public image and credibility (Chukwuma, 2021). More recently,

in October 2023, Boko Haram reportedly breached critical NA servers, leading to temporary operational disruptions (Amos, 2023).

These recurring cyber-attacks highlight structural weaknesses within the NACWC (Nwokedi, 2020; IISS, 2022). The International Institute for Strategic Studies (IISS) (2022) also observes that Nigeria's military cyber strategy remains underdeveloped when compared to global standards, underscoring an urgent need for reform (IISS, 2022). These deficiencies expose the NA to threats that could disrupt command and control, endanger personnel and undermine national security. The problem is further exacerbated by a growing reliance on digital technologies in military operations, logistics, intelligence and information management. While this digital shift enhances operational efficiency, it also expands the NA's exposure to cyber threats (Smith et al., 2021 Johnson, 2023). Without updating studies in the cybersecurity leadership strategies in the NA and their effectiveness to improve on information management systems, these digital systems remain susceptible to attacks.

A leadership-oriented approach is therefore critical for building a robust and adaptive cybersecurity framework capable of responding to dynamic digital threats. However, available literature emphasizes the technical aspects of military cybersecurity without giving sufficient attention to the role of leadership in shaping cybersecurity culture, preparedness and resilience in military institutions. Neglecting the leadership dimension in cybersecurity undermines the NA's capacity to prevent data breaches, safeguard operational integrity and maintain public confidence. To address these critical vulnerabilities and fill this evident gap in military literature, this study seeks to evaluate the specific cybersecurity leadership strategies adopted by the Nigerian Army and assess their institutional effectiveness to establish a robust framework for strengthening IMS in the NA.

1.1 LITERATURE REVIEW

1.1.1 Leadership and Military Cybersecurity

The rapid digitalisation of military operations has transformed cybersecurity from a purely technical concern into a strategic leadership responsibility. Modern armed forces rely

extensively on interconnected information systems for intelligence gathering, command and control, logistics, communications, surveillance, and operational planning. This has resulted in the emergence of cybersecurity leadership as a critical determinant of organisational resilience and operational effectiveness. Thus, rather than merely overseeing technological infrastructure, military leaders are increasingly expected to formulate cybersecurity strategies, establish governance structures, develop cyber-resilient organisational cultures and coordinate responses to evolving cyber threats (Northouse, 2021; Gonzales, 2014).

Leadership within cybersecurity encompasses the ability to influence organisational behaviour towards achieving secure information environments through strategic vision, resource mobilisation, policy implementation and personnel development. According to Bass (1999), transformational leaders inspire innovation, encourage continuous learning and motivate organisational members to adapt to rapidly changing environments. These characteristics are particularly relevant within military cybersecurity, where threat landscapes continuously evolve and require adaptive decision-making. Similarly, situational leadership enables commanders to adjust leadership behaviours according to operational circumstances, while authoritative leadership facilitates rapid decision-making during cyber incidents requiring immediate responses. Collaborative leadership, on the other hand, promotes knowledge sharing, inter-agency cooperation and collective problem-solving, all of which are increasingly recognised as essential components of contemporary cyber defence (Northouse, 2021).

Military organisations worldwide have recognised leadership as an essential element of cybersecurity capability. The United States Cyber Command (USCYBERCOM), for example, combines strategic leadership with integrated cyber operations to coordinate defensive and offensive cyber capabilities across the Department of Defence (Healey, 2013). Likewise, India's Defence Cyber Agency, Brazil's Cyber Defence Command, and South Africa's cyber defence initiatives emphasise leadership-driven coordination, institutional learning and strategic governance in responding to cyber threats (Shoard, 2020; Parenty & Domet, 2019; Adesina, 2020). These developments demonstrate that effective cybersecurity extends beyond technological sophistication to encompass strategic leadership capable of fostering

organisational adaptability and resilience.

Although existing studies acknowledge the importance of leadership in cybersecurity, much of the literature concentrates on leadership styles or technological capabilities independently, with limited attention to how leadership influences cybersecurity governance mechanisms that ultimately improve organisational performance. This study therefore conceptualises leadership as the strategic antecedent of cybersecurity governance within military organisations.

1.1.2 Cybersecurity Governance as a Strategic Leadership Function

Cybersecurity governance refers to the structures, policies, processes and accountability mechanisms through which organisations manage cyber risks and protect information assets. Effective governance ensures that cybersecurity objectives are integrated into organisational strategy, supported by adequate resources, monitored through performance indicators and implemented across all operational units (Microsoft, 2022; IBM, 2022).

Leadership plays a fundamental role in cybersecurity governance by establishing strategic priorities, formulating institutional policies, allocating resources, coordinating stakeholders and promoting accountability throughout the organisation. Rather than functioning as an isolated technical activity, cybersecurity governance requires continuous executive oversight to ensure organisational preparedness against emerging threats. Effective leaders institutionalise cybersecurity through comprehensive governance frameworks such as risk assessment, policy enforcement, personnel training, incident response planning, vulnerability management and organisational learning.

Research consistently demonstrates that organisations possessing strong cybersecurity governance structures experience fewer successful cyberattacks, faster incident response and greater organisational resilience (IBM, 2022). Leadership commitment influences cybersecurity awareness programmes, investment decisions, technological modernisation, compliance with security standards and collaboration across organisational units. Consequently, cybersecurity governance serves as the mechanism through which leadership

translates strategic intent into operational cybersecurity capability.

Within military organisations, governance assumes even greater significance because cybersecurity failures may compromise national security, military intelligence, command structures and operational continuity. Effective governance therefore requires close coordination among military leadership, cybersecurity specialists, intelligence units, communications departments and operational commanders. However, studies examining cybersecurity governance within African military institutions remain limited, particularly regarding how leadership influences governance effectiveness. This study addresses this contextual gap by examining cybersecurity governance within the Nigerian Army.

1.1.3 Cybersecurity Governance and Information Management Systems Effectiveness

Information Management Systems (IMS) constitute the technological backbone supporting military decision-making, intelligence management, communications, logistics, surveillance, and operational coordination. The effectiveness of these systems depends not only on technological infrastructure but also on the quality of cybersecurity governance that protects them against evolving cyber threats. Effective cybersecurity governance enhances Information Management Systems through ensuring confidentiality, integrity, availability, accessibility and resilience of organisational information assets. Confidentiality safeguards sensitive military information from unauthorised disclosure, integrity protects information from manipulation or corruption, while availability ensures uninterrupted access to critical information during military operations. These dimensions determine the overall effectiveness of Information Management Systems within defence organisations.

Leadership-driven governance mechanisms such as cybersecurity policies, personnel training, cyber risk management, resource allocation, continuous monitoring, vulnerability assessments and coordinated incident response contribute significantly to improving system reliability and resilience. Research indicates that organisations implementing comprehensive governance frameworks achieve higher levels of system security, improved information sharing, greater user confidence and more effective cyber incident management (IBM, 2022; Microsoft, 2022).

In military environments, effective Information Management Systems facilitate secure intelligence exchange, protect operational communications, enhance interoperability among military formations and minimise disruptions caused by cyberattacks. On the other hand, weak governance exposes information systems to malware, ransomware, espionage, insider threats, and operational disruptions capable of compromising national defence capabilities. Thus, cybersecurity governance represents the critical institutional mechanism through which leadership enhances Information Management Systems effectiveness.

1.1.4 Information Management Systems and Military Operational Readiness

Military operational readiness refers to the capability of armed forces to effectively execute assigned missions through the availability of personnel, equipment, intelligence, logistics, communications, and command systems. Contemporary military operations depend heavily on reliable Information Management Systems that provide commanders with timely, accurate and secure information for strategic and tactical decision-making.

Effective Information Management Systems strengthen operational readiness by enabling secure command and control, rapid intelligence dissemination, coordinated force deployment, logistical efficiency, and uninterrupted communication during military operations. Information superiority has become a decisive factor in modern warfare, where cyberattacks increasingly target communication networks, command systems, intelligence databases, and critical military infrastructure. Consequently, the resilience of Information Management Systems directly influences operational effectiveness, mission success, and national security.

Studies on military cyber operations demonstrate that cyber incidents capable of disrupting information systems may delay operational decisions, compromise intelligence assets, interrupt command structures, and reduce military responsiveness during crises (Healey, 2013; IISS, 2022). On the contrary, organisations possessing resilient Information Management Systems demonstrate greater operational continuity, faster incident recovery, improved situational awareness, and enhanced mission effectiveness.

Within the Nigerian Army, increasing reliance on digital technologies for intelligence gathering, operational planning, logistics management, and communications has heightened the strategic importance of secure Information Management Systems. However, recurring cyber incidents targeting military infrastructure highlight persistent vulnerabilities capable of undermining operational readiness. Strengthening Information Management Systems therefore represents a strategic requirement for enhancing military preparedness against increasingly sophisticated cyber threats.

1.2 EMPIRICAL REVIEW

Empirical evidence increasingly supports the relationship between leadership, cybersecurity governance, and organisational performance. Gonzales (2014) reported that organisations characterised by proactive cybersecurity leadership demonstrate stronger governance structures, improved policy implementation, and enhanced cyber resilience. Similarly, Northouse (2021) argues that transformational leadership enhances organisational adaptability by encouraging innovation, continuous learning, and strategic responsiveness to emerging challenges.

Within military contexts, Healey (2013) observed that leadership integration within USCYBERCOM significantly strengthened command coordination and cyber defence capabilities through centralised governance and strategic planning. Studies examining India's Defence Cyber Agency and Brazil's Cyber Defence Command similarly emphasise leadership commitment as a prerequisite for effective cybersecurity governance and institutional resilience (Shoard, 2020; Parenty and Domet, 2019).

Nigerian studies have similarly identified leadership, cybersecurity awareness, personnel training, and organisational coordination as important determinants of information security (Agwu, 2021; Iyanu-Oluwa & Ayoola, 2022). However, these studies primarily focus on technical cybersecurity practices, awareness programmes, or information security management without empirically examining the pathways through which leadership influences cybersecurity governance, Information Management Systems effectiveness, and ultimately

military operational readiness. Furthermore, empirical evidence specifically addressing cybersecurity leadership within the Nigerian Army Cyber Warfare Command remains extremely limited.

Studies predominantly examine cybersecurity from technical, technological, or engineering perspectives, while leadership processes influencing cybersecurity governance remain insufficiently explored. Most available evidence originates from developed countries such as the United States, the United Kingdom, and other NATO member states, with limited empirical evidence from African military institutions, particularly the Nigerian Army. Previous studies largely employ qualitative case studies, policy analyses, or technical assessments, with relatively few mixed-method investigations examining the interrelationships among leadership, cybersecurity governance, Information Management Systems effectiveness, and military operational readiness.

To address these gaps, this study used a conceptual model in which leadership styles influence cybersecurity governance, cybersecurity governance enhances Information Management Systems effectiveness and effective Information Management Systems improve military operational readiness. Guided by Transformational Leadership Theory, the model provides an integrated framework for understanding how leadership contributes to military cyber resilience through organisational governance and information management capabilities.

1.3 THEORETICAL FRAMEWORK

This study is anchored on Transformational Leadership Theory developed by Burns (1978) and extended by Bass (1985; 1999). The theory explains how leaders inspire innovation, organisational learning and adaptability to achieve organisational goals. It is particularly relevant to military cybersecurity, where leaders are expected to provide strategic direction, strengthen cybersecurity governance, build personnel capacity and promote organisational resilience. The study argues that effective leadership enhances cybersecurity governance, which improves Information Management Systems (IMS) and ultimately strengthens military operational readiness. The theory therefore provided a suitable framework for examining the

relationship between leadership, cybersecurity governance, IMS effectiveness, and operational readiness within the Nigerian Army.

1.4 RESEARCH METHODOLOGY

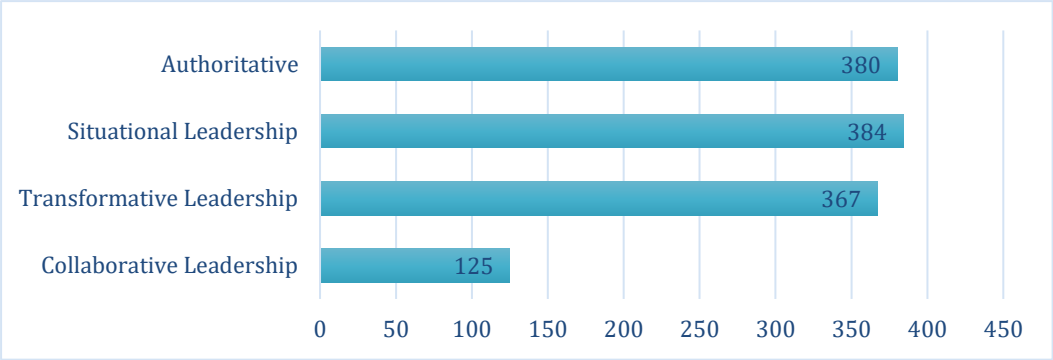
This study employed a mixed-methods design and multi-stage sampling approach to investigate the role of leadership in strengthening cybersecurity and IMS within the NA. The target population comprised military personnel engaged in cybersecurity and information management functions. Based on an estimated population of 10,000 personnel (AHQDPM ,2022; AHQMS, 2024), a sample size of 404 respondents was determined using Slovin's formula at a 95% confidence level and a 5% margin of error, including an allowance for non-response. Purposive sampling technique was used to select six formations in the Nigerian Army with key responsibilities for cybersecurity, information management, communications and cyber training, namely the Nigerian Army Cyber Warfare Command (NACWC), Nigerian Army Cyber Warfare School (NACWS), Nigerian Army Signals Corps (NASC), Directorate of Army Data Processing (DADP), Headquarters 7 Division Maiduguri and Headquarters 81 Division Lagos. The total population of the study was shared among the selected formations using stratified sampling and simple random sampling techniques was used to select survey participants for quantitative data collection. For qualitative data collection, purposive and snowball sampling were employed to identify 18 key informants for interviews. A total of 386 valid responses were obtained for quantitative data indicating a 95.5 per cent validity on obtained and reviewed questionnaires.

Data were collected from both primary and secondary sources (Mbachu, 2023). Primary data were obtained through structured questionnaires administered to personnel across the selected formations and through key informant interviews with officers occupying strategic, operational and technical cybersecurity positions. Secondary data were derived from military policy documents, operational reports, doctrinal publications, academic literature and other relevant records. Quantitative data were analysed using the Statistical Package for the Social Sciences (SPSS), with results presented using descriptive statistics such as frequencies and percentages. Qualitative interview data were transcribed, coded and analysed thematically to identify

recurring patterns relating to leadership practices, cybersecurity governance and information management. Findings from the different data sources were triangulated to enhance the credibility and robustness of the results. The validity of the research instruments was strengthened through expert review, pilot testing and Cronbach's Alpha to evaluate internal consistency. A reliability coefficient of 0.82 was achieved, while ethical approval was obtained from the appropriate authorities. Participation was voluntary and all respondents provided informed consent, with confidentiality and anonymity maintained throughout the study.

1.5 RESULTS/FINDINGS

Figure 1: Respondents' View on Current Cybersecurity Leadership Strategies Utilized in the NA (N=386)



Source: Field Survey 2025

As shown in Figure 1, cybersecurity leadership within the NA is characterised by a multi-strategy approach that combines directive, adaptive, and transformational leadership practices. Quantitative results show that situational leadership (99.5%), authoritative leadership (98.4%), and transformational leadership (95.1%) are the most frequently utilised approaches in cybersecurity management. In contrast, collaborative leadership recorded substantially lower utilisation (32.4%), suggesting that cybersecurity decision-making within the Army remains largely centralised and command-driven.

The dominance of situational and transformational leadership suggests that cybersecurity

leaders recognise the dynamic nature of cyber threats and the need for flexibility in responding to emerging vulnerabilities. The high prevalence of authoritative leadership further reflects the hierarchical structure of military institutions, where rapid decision-making and command compliance are essential for operational effectiveness. However, the relatively limited use of collaborative leadership indicates that opportunities for cross-unit coordination, knowledge sharing and participatory decision-making may not be fully leveraged within the NA cybersecurity architecture.

Qualitative findings reinforce these observations. Participants consistently described cybersecurity leadership as adaptive rather than fixed, with leadership approaches varying according to operational circumstances and threat environments. Key informants emphasised that transformational leadership is particularly important for anticipating emerging threats, promoting innovation and driving organisational change, while authoritative leadership becomes necessary during crisis situations that require immediate responses. Participant 15, a 43-year-old, male instructor serving in NACWC explains:

> The threat landscape is dynamic; thus, the NA adopts holistic strategies in combating such. Therefore, there is no fixed leadership strategy or pattern followed in this school or in combating cybersecurity threats in the NA (Interview, 2025).

This was confirmed by Participant 10, another instructor with the NACWC,

> Transformational leadership is utilized in NA cybersecurity leadership, because ideally we anticipate changes since we operate in a dynamic terrain, however, authoritative leadership strategy is utilized where competing priorities hinders the effectiveness of a response effort (Interview, 2025).

The convergence of quantitative and qualitative findings therefore demonstrates that cybersecurity leadership in the NA is largely responsive and context-driven, with leaders employing different approaches depending on operational demands. This flexibility represents

a strategic strength in a rapidly evolving cyber environment.

Table 1: Percentage Distribution of Respondents' view on Effectiveness of Existing Cybersecurity Leadership Strategies in Enhancing IMS in the NA (N=386)

How effective are the existing Cybersecurity Leadership Strategies in Enhancing IMS in the NA	Yes	No	Don't Know	Total (N=386) %=100
The computers, servers, mobile devices, electronic systems, networks and data used in my unit are reliable and safe from malicious attacks	150	171	65	386
	38.9	44.3	16.8	100
The current IMS in my unit effectively protects sensitive data from unauthorised access	201	99	86	386
	52.1	25.6	22.2	100
The IMS in my unit are user friendly and easy to navigate (I can access it, if need be)	226	108	52	386
	58.5	28	13.5	100
Our IMS allows for quick and effective response to cybersecurity incidents	156	140	91	386
	40.4	36	23.6	100
Proactive leadership in cybersecurity has led to improved security of our IMS	274	45	67	386
	71	11.7	17.3	100
Leaders in my unit effectively manage cyber risk regularly, thereby enhancing the security of our IMS	200	112	74	386
	51.8	29	19.2	100

Leadership ensures that adequate resources are allocated for the security of IMS in my unit	196	112	81	386
	50.8	29	20.2	100
Leadership led cybersecurity awareness training has improved the overall security of our IMS	241	76	69	386
	62.4	19.7	17.9	100
Do you think the success of Information Management in your unit is linked to cyber security leadership strategies utilized in your unit?	365	2	19	386
	94.6	0.5	4.9	100

Source: Field Survey, 2025

Table 1 presents respondents' views on the effectiveness of existing cybersecurity leadership strategies in enhancing Information Management Systems (IMS) in the Nigerian Army, based on responses from 386 participants.

The findings show mixed perceptions regarding the security of ICT infrastructure, as *44.3%* of respondents believed that the computers, servers, mobile devices, networks, and data in their units are not adequately protected from malicious attacks, while *38.9%* considered them secure.

A majority (*52.1%*) agreed that the current IMS effectively protects sensitive data from unauthorised access, and *58.5%* reported that the systems are user-friendly and easy to navigate. However, only *40.4%* believed that the systems enable quick and effective responses to cybersecurity incidents, suggesting room for improvement in incident response.

Respondents generally expressed confidence in cybersecurity leadership. About *71.0%* agreed that proactive leadership has improved the security of IMS, *51.8%* believed leaders effectively manage cyber risks, and *50.8%* indicated that leadership provides adequate resources for securing IMS. In addition, *62.4%* agreed that leadership-led cybersecurity awareness training has strengthened the overall security of Information Management Systems.

Most importantly, *94.6%* of respondents affirmed that the success of Information Management Systems in their units is linked to the cybersecurity leadership strategies adopted. Overall, the findings indicate that effective cybersecurity leadership is widely perceived as a key factor in improving the security and performance of Information Management Systems within the Nigerian Army.

The study further assessed the effectiveness of cybersecurity leadership in improving Information Management Systems (IMS) within the NA. Findings shown on Table 1 reveal that leadership interventions have contributed positively to several dimensions of information management, particularly cybersecurity awareness, risk management, resource allocation, and system protection. Notably, 71.0% of respondents agreed that proactive cybersecurity leadership has improved the security of IMS, while 62.4% reported that leadership-driven cybersecurity training has enhanced system security. Similarly, 51.8% indicated that leaders effectively manage cyber risks, and 50.8% acknowledged adequate resource allocation toward information security initiatives.

These findings suggest that leadership has played a significant role in building cybersecurity awareness and fostering institutional resilience. The positive assessment of training initiatives highlights the importance of human capacity development in strengthening cybersecurity posture, while the moderate ratings for risk management and resource allocation indicate ongoing efforts to institutionalize cybersecurity governance within the NA. Together, these findings demonstrate that leadership influences cybersecurity outcomes not only through policy formulation but also through the provision of resources, oversight and organisational support.

Despite these positive outcomes, the findings reveal notable weaknesses in the effectiveness of existing IMS. Less than half of respondents (38.9%) considered information technology assets within their units to be reliable and adequately protected from malicious attacks. Similarly, only 40.4% reported that their IMS supports rapid and effective responses to cybersecurity incidents. These results point to persistent technological and operational vulnerabilities that could undermine the NA's ability to detect, respond to, and recover from cyber threats. The

relatively low confidence in system reliability and incident response capability suggests that leadership efforts, while beneficial, have not yet translated into comprehensive cybersecurity resilience across all formations.

The study also identified moderate performance in access control and system usability. Although 52.1% of respondents agreed that their IMS effectively protects sensitive information from unauthorised access, a substantial proportion remained unconvinced of the systems' security effectiveness. Likewise, while 58.5% considered the systems user-friendly and accessible, the remaining respondents reported challenges relating to usability and accessibility. Respondents views show that improvements in cybersecurity governance have not been matched by equivalent advances in technological modernisation and user-centred system design.

Qualitative evidence provides further insight into these outcomes. Interview participants highlighted sustained investments in cybersecurity awareness programmes, personnel training, vulnerability assessments, and proactive security measures. Respondents also reported ongoing efforts by the NACWC to strengthen cyber preparedness through continuous system monitoring and periodic security upgrades. These initiatives demonstrate a commitment to continuous improvement and indicate that cybersecurity leadership is increasingly embedded within the NA organisational culture.

Most significantly, an overwhelming majority of respondents (94.6%) affirmed that the effectiveness of IMS within their units is directly linked to cybersecurity leadership practices. This finding underscores the central role of leadership as a determinant of cybersecurity performance and information system effectiveness. The result suggests that improvements in leadership capacity, strategic direction, coordination mechanisms and personnel development are likely to generate corresponding improvements in IMS outcomes. Overall, the evidence indicates that while cybersecurity leadership has substantially enhanced IMS within the NA persistent challenges relating to technological infrastructure, inter-unit collaboration and incident response capabilities continue to constrain the achievement of a fully resilient cybersecurity environment.

1.6 DISCUSSION OF FINDINGS

This study revealed that the NA employs a combination of situational, authoritative, transformational, collaborative and participative leadership approaches in managing cybersecurity and IMS. Quantitative findings revealed that situational leadership (99.5%), authoritative leadership (98.4%) and transformational leadership (95.1%) are the most frequently utilised approaches, while collaborative leadership (32.4%) is comparatively less employed. This suggests that cybersecurity leadership within the NA is characterised by a hybrid leadership model that combines military command structures with adaptive and transformational approaches required for managing contemporary cyber threats.

The prominence of transformational leadership aligns with Bass' (1999) Transformational Leadership Theory, which posits that effective leaders inspire followers to transcend routine expectations, embrace innovation and adapt to changing environmental demands. The cybersecurity environment is inherently dynamic, requiring leaders who can anticipate emerging threats, motivate personnel and drive continuous organisational learning. The high prevalence of transformational leadership identified in this study suggests that NA cybersecurity leaders recognize the need to cultivate innovation, adaptability and strategic foresight in responding to increasingly sophisticated cyber threats. This supports Northouse (2021), who argues that transformational leaders are particularly effective in environments characterised by uncertainty, complexity and rapid technological change.

1. The findings also demonstrate the continued relevance of authoritative leadership within the military context. While transformational leadership encourages innovation and adaptability, military organisations operate within established command structures that often require rapid decision-making and strict compliance with directives. The high utilisation of authoritative leadership therefore reflects the operational realities of cybersecurity management within a military institution, where timely responses are critical to preventing or mitigating cyber incidents. This corroborates Healey's (2013) and Mohammed and Mohamad (2019) observation that military cyber operations

frequently require centralised command and control mechanisms to ensure coordinated responses to cyber threats.

2. Qualitative findings further reveal that cybersecurity leadership within the NA is flexible and context-specific rather than rigidly attached to a single leadership style. Key informants emphasised that leadership approaches vary according to operational requirements and threat conditions. This finding reinforces the principle of intellectual stimulation, a core component of Transformational Leadership Theory, which encourages leaders to adopt innovative and adaptive solutions to emerging challenges. The ability of cybersecurity leaders to switch between transformational, situational and authoritative approaches reflects a pragmatic leadership orientation that enhances organisational resilience in an evolving threat environment. However, the relatively low adoption of collaborative leadership suggests the existence of institutional barriers to information sharing and collective decision-making. From a transformational leadership perspective, this finding is noteworthy because transformational leaders are expected to foster collaboration, trust and shared commitment to organisational goals. The limited utilization of collaborative leadership may therefore constrain the full realization of transformational leadership outcomes within the NA's cybersecurity architecture. This observation highlights the need for greater inter-unit cooperation and enhanced stakeholder engagement to strengthen organizational learning and cyber resilience. The findings suggest that cybersecurity leadership in the NA is increasingly transitioning from a purely command-and-control model toward a more adaptive and transformational framework. This study therefore extends the findings of O'Flaherty (2018) and Iyanu-Oluwa and Ayoola (2022) by demonstrating that cybersecurity leadership in the NA is not solely dependent on hierarchical authority but increasingly incorporates transformational principles aimed at enhancing organizational adaptability and cyber resilience.

On the effectiveness of existing cybersecurity leadership in enhancing IMS in the NA, findings reveal that cybersecurity leadership has contributed significantly to strengthening IMS within

the NA. Although several challenges remain. While respondents acknowledged improvements in cybersecurity awareness, risk management and information protection. Concerns were raised regarding technological reliability, incident response capability and system resilience. For instance, only 38.9% of respondents considered information technology assets within their units to be adequately protected from malicious attacks, while only 40.4% reported that their IMS supports rapid and effective responses to cybersecurity incidents. These findings suggest that despite leadership efforts, significant infrastructural and operational vulnerabilities persist within the Army's cybersecurity ecosystem.

The observed weaknesses in system reliability and incident response capability may partly be explained by limitations in technological modernization and institutional coordination. Transformational Leadership Theory emphasizes the role of leaders in creating a compelling vision for change and mobilizing organizational resources to achieve strategic objectives. The relatively low confidence in system reliability suggests that leadership initiatives have not yet been fully translated into technological upgrades capable of supporting resilient cybersecurity operations. This finding supports Gonzales (2014) and Koleoso (2019), who argue that effective cybersecurity outcomes require both strategic leadership and sustained investments in technological infrastructure.

Despite these challenges, the findings reveal positive outcomes associated with leadership-driven cybersecurity initiatives. A substantial proportion of respondents reported that proactive cybersecurity leadership has improved IMS security (71%), enhanced cyber risk management (51.8%), and facilitated cybersecurity awareness training (62.4%). These findings reflect the transformational leadership dimensions of inspirational motivation and idealised influence. Through proactive engagement, strategic communication and capacity-building programmes, leaders have demonstrated commitment to improving cybersecurity awareness and cultivating a culture of information security across the organisation. Such actions are consistent with Bass' (1999) assertion that transformational leaders inspire followers to embrace organizational goals and develop a shared commitment to institutional success.

The findings also demonstrate moderate success in protecting sensitive information and improving system usability. More than half of the respondents agreed that their IMS effectively protects sensitive information from unauthorised access and is relatively user-friendly. These outcomes suggest that leadership interventions have contributed positively to information governance and accessibility. Nevertheless, the persistence of significant proportions of respondents expressing concerns about system security and usability indicates the need for continued investments in technological infrastructure and personnel training. From a transformational leadership perspective, this highlights the importance of individualised consideration, whereby leaders continuously identify and address the developmental needs of personnel to improve organisational performance.

The most significant finding of this study is that 94.6% of respondents linked the success of IMS within their units directly to cybersecurity leadership strategies. This overwhelming level of agreement provides strong empirical support for the study's theoretical proposition that leadership is a critical determinant of cybersecurity effectiveness and information system resilience. The finding validates the central assumptions of Transformational Leadership Theory, which maintains that effective leadership can influence organisational outcomes by shaping culture, motivating personnel, encouraging innovation, and driving institutional change. It also supports the arguments of Gonzales (2014) and Koleoso (2019), who identify leadership as a foundational element in building resilient cybersecurity systems.

This demonstrates that cybersecurity leadership has become a critical enabler of information management effectiveness within the Nigerian Army. While existing leadership strategies have generated measurable improvements in cybersecurity awareness, risk management and information protection, achieving a fully resilient cybersecurity environment will require stronger collaboration, enhanced technological modernisation, improved incident response mechanisms and sustained transformational leadership capable of driving continuous organisational adaptation to emerging cyber threats. This correlation was also supported by literature, including Agwu (2021) and NCSC (2022), all of which stress the importance of proactive leadership in building effective cybersecurity systems.

1.7 CONCLUSION

This study examined the role of cybersecurity leadership in enhancing Information Management Systems (IMS) within the Nigerian Army (NA), with particular focus on the leadership strategies employed in managing cybersecurity and their effectiveness in strengthening information management outcomes. The findings revealed that the NA adopts a combination of situational, authoritative and transformational leadership approaches in addressing cybersecurity challenges, with transformational and situational leadership emerging as the most prominent strategies. The study further established that proactive leadership practices, including cybersecurity awareness training, capacity development, cyber risk management, policy implementation and resource allocation, have contributed positively to the security and effectiveness of IMS across the NA. However, the findings also revealed persistent challenges, including limited collaborative leadership, inadequate inter-unit information sharing, weaknesses in incident response capability and concerns regarding the reliability and resilience of some information systems.

The study concludes that effective cybersecurity leadership is a critical determinant of IMS effectiveness within the NA. While technological investments remain important, sustainable cybersecurity resilience depends largely on leadership capacity to inspire innovation, promote organisational learning, strengthen coordination and drive institutional adaptation to emerging cyber threats. Anchored on Transformational Leadership Theory, the study demonstrates that leadership practices characterised by strategic vision, intellectual stimulation, capacity building and proactive engagement significantly influence cybersecurity outcomes. In doing so, the study fills an important gap in the existing literature, which has largely focused on technical dimensions of military cybersecurity while paying limited attention to the leadership factors that shape cyber resilience and information management effectiveness in military organisations, particularly within the Nigerian context. The study therefore contributes empirical evidence on the relationship between cybersecurity leadership and information management effectiveness and provides a leadership-centred framework for strengthening cyber resilience in military institutions.

1.8 RECOMMENDATIONS

Based on the study's findings, the following recommendations are proposed to strengthen cybersecurity leadership and Information Management Systems (IMS) in the Nigerian Army:

The Nigerian Army Headquarters should establish a structured leadership development framework that emphasises situational and transformational leadership. This can be achieved through scenario-based training, leadership simulations, and continuous professional education tailored to cyber environments. By institutionalising adaptive and innovative leadership practices, commanders will be better equipped to anticipate emerging threats and inspire organisational resilience.

The Nigerian Army Cyber Warfare Command (NACWC) should formalise authoritative leadership practices into clear incident response protocols. This involves codifying rapid decision-making procedures, defining chain-of-command responsibilities, and embedding accountability mechanisms during cyber crises. Such protocols will ensure that authoritative leadership is applied consistently, reducing delays in operational recovery and strengthening command integrity during emergencies.

The Directorate of Army Data Processing (DADP) and Signals Corps (NASC) should create collaborative structures such as joint cyber task forces, inter-unit coordination platforms, and knowledge-sharing hubs. These mechanisms will expand the currently limited use of collaborative leadership, encourage cross-unit cooperation, and foster collective problem-solving. By leveraging diverse expertise, the Army can enhance its cyber defence posture and reduce vulnerabilities caused by siloed operations.

The Nigerian Army Cyber Warfare School (NACWS) should lead continuous cybersecurity awareness campaigns and training programs across all formations. These should focus on emerging threats, safe digital practices, and resilience-building exercises. Since the study found that leadership-led training significantly improved IMS security, institutionalising such

programs will sustain personnel readiness, reduce human error, and strengthen the Army's cyber culture.

The Ministry of Defence, in collaboration with Army leadership, should establish a dedicated cybersecurity budget line. This funding should cover infrastructure upgrades, personnel development, and investment in advanced cyber defence technologies. Addressing resource gaps identified in the study will ensure that IMS remain reliable, user-friendly, and resilient against malicious attacks, thereby safeguarding operational readiness and national security.

References

Adesina, O.S. (2020). Enhancing Nigeria's Cybersecurity Capabilities: The Role of the Nigerian Cyber Command. African Security Review, 29(3), 270-285

Agwu, E. (2021). The Impact of Cybersecurity on National Defence Systems. African Journal of Science and Technology, 17(2), 45-581

AHQ (2012) Report on the Establishment of the Directorate of ICT. Abuja: Nigerian Army Headquarters.

AHQ (2017) Annual Report 2017 Abuja: Nigerian Army Headquarters.

AHQ (Army Headquarters). (2012). *Policy directive on ICT integration in the Nigerian Army*. Abuja: Nigerian Army Headquarters.

AHQ DPM (2020) Annual Report: 2020

AHQ MS (2024) Annual Report 2024

Amos, J. (2023). Cyber warfare and modern military operations in Nigeria. *Journal of Defence Studies*, 15(2), 44–59.

Bass, B.M. (1999). Two decades of research and development in transformational leadership.

European Journal of Work and Organizational Psychology, 8(1), 9-32

Chukwuma, O. (2021). Digital misinformation and military perception in Nigeria. *Security Journal of West Africa*, 9(1), 33–47.

Cybersecurity Infrastructure Security Agency (2021). Russia-Ukraine Cyber Espionage Reports. Retrieved from https://usa.gov.cisareport2022.

Gonzales, A. (2014). *Security convergence: Managing enterprise security risk*. *Journal of Security Administration*, 37(1), 12–27.

Gonzales, J. (2014). Leadership styles in military settings and their influences on program satisfaction. Being a MSc thesis submitted to the Graduate Faculty Georgia Southern University

Hasib, A. (2021). Cybersecurity and cyberwar: What everyone needs to know. New York, NY: Oxford University Press.

Healey, J. (2013). The Role of USCYBERCOM in National Defence. Retrieved from https://www.reuters,com

International Business Machines Corporation (2022). Threat Intelligence Index: Identity Attacks Strain Recovery Ttime for Breaches in Middle East and Africa. IBM2022.

International Institute for Strategic Studies (2022). Cyber-capabilities and National Power. IISS Report, Nigeria, Cybersecurity 2022 2(8)

Iyanu-Oluwa, T. and Ayoola, O (2022). Information security governance: Leadership and the Nigerian context. African Journal of Information Systems, 13(4), 245-260.

Johnson, M. (2023). Leadership in the digital age: Cybersecurity and military operations. London, England: Routledge.

Koleoso, O. (2019). Evolution of information systems in the Nigerian Army. *Nigerian Journal*

of Military Studies, 7(1), 50–67.

Mbachu, O. (2023). Social Science Research Methods: For Policy and Strategic Studies. 3rd ed Medusa Academic Publishers Limited, Nigerian Defence Academy, Kaduna.

Microsoft (2022). How Nigeria is tackling cybersecurity challenges. TechCabal. Retrieved from https://techcabal.com/articles/nigeria-cybersecurity

Mohammed and Mahammad (2019). Strategic governance for cybersecurity leadership in public organizations. *Journal of Information Policy and Cybersecurity*, 11(3), 77–93.

Morgan S, (2022) cybercrime to Cost the World $10.5 Trillion Annually by 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damage-costs-10trillionby2025

Murtala, A. (2023). Army Trains Personnel in Cyber Warfare. Punch Newspaper 24 Oct 23

National Cyber Security Centre (NCSC). (2022). *Operational collaboration for national cyber resilience: Framework for Defence agencies*. London: NCSC.

Northhouse, P.G. (2021). Leadership Theory and Practice (8th ed). Thousand Oaks, CA: Sage Publications.

Nwokedi, C, (2020). Organizational Gaps in Cybersecurity: A Nigerian Perspective International Journal of Cyber Criminology, 13 (1), 54-67

O'Flaherty, K. (2018). The Nigerian Cyber Warfare Command: Waging War in Cyberspace. Retrieved from https://forbes,com/sites/kateoflaherty

Okafor E.E. (2019). Cybersecurity awareness and training in Nigeria's military: Current challenges and future prospects. International Journal of Cyber Criminology, 13 (1), 34-47

Parenty, T.A. and Domet, J.L. (2019). Cybersecurity and Critical Infrastructure Protection in Brazil: A Case Study on the 2016 Rio Olympic Games. Journal of strategic Security, 11(1), 31-50

Shoard, A. (2020). India's Intelligence Agencies. Manas Publications.