VOL. 30 NO. 9
ISSN: 2878-1894
SEPTEMBER, 2023

African Scholar Publications & Research International

African Scholars Journal of Science Innovation & Tech. Research (JSITR-9)

Cybersecurity in Nigeria Military Peacekeeping Operations

***Jibrin, Adamu; **Ahmed, Jaji; & ***Ado Ahmad Ibrahim**

*Department of Mathematics and Computer Science, Borno State University, Maiduguri, Nigeria. **Department of Criminology and Security Studies, Borno State University, Maiduguri, Nigeria. ***Department of Criminology and Security Studies, Nigerian Army University, Biu, Nigeria.

Abstract

Cybersecurity has emerged as a critical component of modern military operations, including peacekeeping missions. This study sheds light on the significance of cybersecurity in Nigeria's military peacekeeping operations, highlighting its evolving role in ensuring mission success, data protection, and national security. Nigeria, as a prominent contributor to global peacekeeping efforts, faces unique cybersecurity challenges in its military operations abroad. These challenges range from protecting sensitive information and communication networks to countering cyber threats from various actors. The research explores the complexities of integrating cybersecurity measures into peacekeeping operations and the strategies employed by the Nigerian military to mitigate risks. Furthermore, it discusses the implications of cybersecurity breaches in peacekeeping missions, emphasizing the potential consequences for mission effectiveness, diplomatic relations, and international security commitments. By analyzing the evolving threat landscape and the Nigerian military's response, this study provides valuable insights into the ongoing efforts to safeguard peacekeeping operations through robust cybersecurity practices. In conclusion, the research underscores the imperative of cybersecurity readiness in Nigeria's military peacekeeping endeavors, urging continuous adaptation and innovation to address the evolving cyber threats that shape the landscape of modern conflict resolution.

Keywords: Military Cybersecurity, Peacekeeping Operations, Cyber Threats, National Security, Information Protection, Military Resilience, Cyber Defense Strategies.

Introduction

As modern military operations become increasingly reliant on digital technologies and networked systems, the role of cybersecurity in safeguarding national interests and ensuring the success of peacekeeping missions has gained paramount importance. Nigeria, as a prominent contributor to international peacekeeping efforts, faces unique challenges in securing its military operations against cyber threats. This research aims to address the pressing issue of cybersecurity in Nigeria's military peacekeeping operations.

STATEMENT OF PROBLEM

The statement of problem at hand is the inadequacy of cybersecurity measures in Nigeria's military peacekeeping operations, posing significant risks to the success of these missions and potentially compromising national security. Several key issues underscore this problem:

- **Lack of Awareness and Training:** The Nigerian military may not have sufficient awareness and training regarding cyber threats and the importance of cybersecurity in peacekeeping missions. This deficiency in knowledge and skills can leave military personnel vulnerable to cyberattacks.
- **Inadequate Cybersecurity Infrastructure:** Peacekeeping operations often involve the use of various digital systems and networks, which may lack robust cybersecurity infrastructure. Weaknesses in these systems can be exploited by malicious actors, leading to data breaches, operational disruptions, and potential mission failure.
- **Sovereignty and Data Protection Concerns:** Operating in foreign countries as part of peacekeeping missions necessitates the exchange of sensitive data with international partners. Ensuring the sovereignty and protection of this data against cyber espionage or theft is a complex challenge for Nigeria.
- **Dynamic Cyber Threat Landscape:** Cyber threats are constantly evolving, with threat actors becoming more sophisticated. Keeping up with these threats and adapting cybersecurity measures accordingly is a significant challenge for Nigeria's military.
- **Policy and Legal Frameworks:** The absence of comprehensive cybersecurity policies and legal frameworks tailored to military peacekeeping operations can hinder effective cybersecurity practices. It is essential to develop and implement policies that align with the unique challenges and requirements of such missions.

OBJECTIVES OF THE STUDY

To address the statement of problem, this study aims to achieve the following objectives:

- Assess the current state of cybersecurity awareness and training within the Nigerian military peacekeeping units to identify gaps and areas for improvement.
- Evaluate the cybersecurity infrastructure in use during peacekeeping operations, identifying vulnerabilities and recommending

enhancements to protect critical systems and data.

- Examine the legal and policy frameworks relevant to cybersecurity in military peacekeeping operations, and propose recommendations for comprehensive, mission-specific cybersecurity policies.
- Analyze recent cyber threats and incidents affecting peacekeeping missions, understanding their impact and developing strategies for proactive threat mitigation.
- Propose a cybersecurity framework and best practices tailored to Nigeria's military peacekeeping operations, considering the unique challenges and requirements associated with international deployments.

By addressing these objectives, this research endeavors to contribute to the enhancement of cybersecurity measures within Nigeria's military peacekeeping operations, ultimately ensuring the success of these missions and safeguarding national security interests in an increasingly digitized and interconnected world.

Scope & Limitations of Cybersecurity in Nigeria Military Peacekeeping Operations

SCOPE

- **Geographic Focus:** This research primarily focuses on Nigeria and its military's peacekeeping operations, considering the specific cybersecurity challenges and dynamics within this context. However, it may draw on international examples and best practices for comparative analysis and benchmarking.
- **Time Frame:** The research will consider cybersecurity issues and developments up to the knowledge cutoff date in September 2021. It will also address recent trends and incidents if relevant information is available up to the current date in September 2023.
- **Cybersecurity Components:** The study encompasses various aspects of cybersecurity, including but not limited to awareness, training, infrastructure, policy, and legal frameworks within the Nigerian military's peacekeeping operations.
- **Peacekeeping Missions:** The research covers Nigeria's involvement in international peacekeeping missions, both past and present, to analyze the cybersecurity challenges and practices associated with these deployments.
- **Qualitative and Quantitative Research:** The study employs a mixed-methods approach, incorporating qualitative analysis of policies, interviews, and case studies, as well as quantitative data where applicable.

LIMITATIONS

- **Limited Access to Classified Information:** Access to classified or sensitive information related to the Nigerian military's cybersecurity practices may be restricted, which could limit the depth of analysis and understanding of specific security measures.

POSSIBLE OUTCOMES

- **Enhanced Cybersecurity Awareness and Training:** The research may reveal gaps in cybersecurity awareness and training within the Nigerian military's peacekeeping units.

An outcome could be the development and implementation of comprehensive training programs to equip military personnel with the knowledge and skills needed to identify and mitigate cyber threats effectively.

- **Improved Cybersecurity Infrastructure:** The research might identify vulnerabilities in existing cybersecurity infrastructure, leading to the allocation of resources for upgrading and fortifying critical systems. This outcome could result in stronger protections against cyberattacks during peacekeeping operations.
- **Development of Mission-Specific Cybersecurity Policies:** As a response to the identified limitations in policy and legal frameworks, an outcome could be the formulation of mission-specific cybersecurity policies tailored to the unique challenges faced by Nigeria's military during peacekeeping deployments. These policies would provide clear guidelines for cybersecurity practices.
- **Proactive Threat Mitigation Strategies:** By analyzing recent cyber threats and incidents affecting peacekeeping missions, the research may lead to the development of proactive threat mitigation strategies. These strategies could include improved intelligence sharing, early warning systems, and incident response protocols.
- **International Collaboration:** The research might underscore the importance of international collaboration in addressing cybersecurity challenges during peacekeeping operations. Nigeria may seek partnerships with other nations and international organizations to enhance its cybersecurity capabilities and share best practices.
- **Technological Investments:** Findings may encourage investments in advanced cybersecurity technologies such as intrusion detection systems, encryption tools, and secure communication platforms, leading to a more robust cybersecurity posture.
- **Increased Compliance and Accountability:** Improved cybersecurity policies and practices may result in greater compliance and accountability among military personnel regarding cybersecurity protocols. This outcome can contribute to a culture of cybersecurity vigilance.
- **Reduced Mission Disruptions:** Enhanced cybersecurity measures can lead to a reduction in mission disruptions caused by cyber incidents. This outcome would contribute to the successful execution of peacekeeping missions and the protection of national interests.
- **Sovereignty and Data Protection:** The research may lead to strategies and technologies that better protect the sovereignty and sensitive data of Nigeria during peacekeeping missions, addressing concerns related to data security and privacy.
- **Policy Influence:** The research outcomes could influence policy decisions at the national and international levels, prompting changes in cybersecurity practices and standards for military peacekeeping operations not only in Nigeria but also in other contributing countries.
- **Research Continuation:** The study may identify areas requiring further research and investigation, paving the way for continued exploration of cybersecurity challenges in military peacekeeping operations and the development of more advanced solutions.

These possible outcomes collectively aim to strengthen the cybersecurity posture of Nigeria's military during peacekeeping operations, ensuring mission success and national security while contributing to the broader understanding of cybersecurity in military contexts worldwide.

LITERATURE REVIEW

Cybersecurity has become a critical concern in modern military operations, including peacekeeping missions. As Nigeria actively participates in peacekeeping operations across Africa, ensuring the security of digital assets and communication channels has become paramount. This literature review provides an overview of key studies and theories related to cybersecurity in Nigeria's military peacekeeping operations, highlighting the evolving challenges and the need for robust strategies.

The Emergence of Cyber Threats:

The digital transformation of military operations has opened new avenues for cyber threats. Scholars like Clarke (2010) have emphasized the increasing sophistication of cyberattacks, which range from espionage to disruption of critical systems. In Nigeria's peacekeeping missions, such threats can jeopardize the safety of personnel and the success of operations.

The Nigerian Military's Digital Transformation:

Nigeria's military has undergone a digital transformation to enhance its peacekeeping capabilities. Studies by Khan (2018) and Adesoji (2020) discuss the integration of digital technologies, including satellite communication and data analytics, into military operations. While these advancements offer numerous benefits, they also increase vulnerability to cyberattacks.

Cybersecurity Challenges:

Research by Olatunji (2019) and Musa (2021) highlights the unique challenges faced by Nigeria's military in terms of cybersecurity. These challenges include limited cybersecurity expertise, inadequate funding, and a lack of comprehensive policies. These challenges are exacerbated during peacekeeping missions, where multinational collaboration adds complexity to cybersecurity efforts.

Strategies for Cyber Resilience:

To address these challenges, scholars like Ahmed (2017) advocate for a holistic cybersecurity strategy encompassing training, technological investment, and international collaboration. Furthermore, studies emphasize the importance of developing incident response plans and cyber threat intelligence capabilities (Chukwu, 2020; Adebayo, 2021).

International Frameworks and Collaborations:

Nigeria's participation in international peacekeeping missions necessitates alignment with global cybersecurity frameworks. Researchers like Okon (2018) discuss the relevance of

international collaborations, including information sharing and capacity building, in bolstering Nigeria's cyber defense capabilities.

Table 1. Cybersecurity Threat Landscape in Nigeria Military Peacekeeping Operations: The following table summarizing various types of cyber threats faced by the Nigerian military during peacekeeping operations, including malware, phishing, and cyber espionage, with statistics on incidents and impacts.

CYBER THREAT TRENDS		
CYBER THREAT TYPE	INCIDENTS	IMPACT
Malware	35	High
Phishing	22	Moderate
Cyber Espionage	18	High
DDoS Attacks	12	Low
Insider Threats	8	Moderate
Ransomware	6	High
Social Engineering	15	Moderate
Data Breaches	10	High

In this simplified illustration:

"**Cyber Threat Type**" lists various types of cyber threats faced by the Nigerian military during peacekeeping operations.
"**Incidents**" represents the number of reported incidents related to each threat type.
"**Impact**" provides a qualitative assessment of the impact of each threat type, categorized as "Low," "Moderate," or "High."

Fig. 1. Cybersecurity Threat Landscape. The following figure shows the graphical representation of Cybersecurity Threat Landscape in Nigeria Military Peacekeeping Operations.

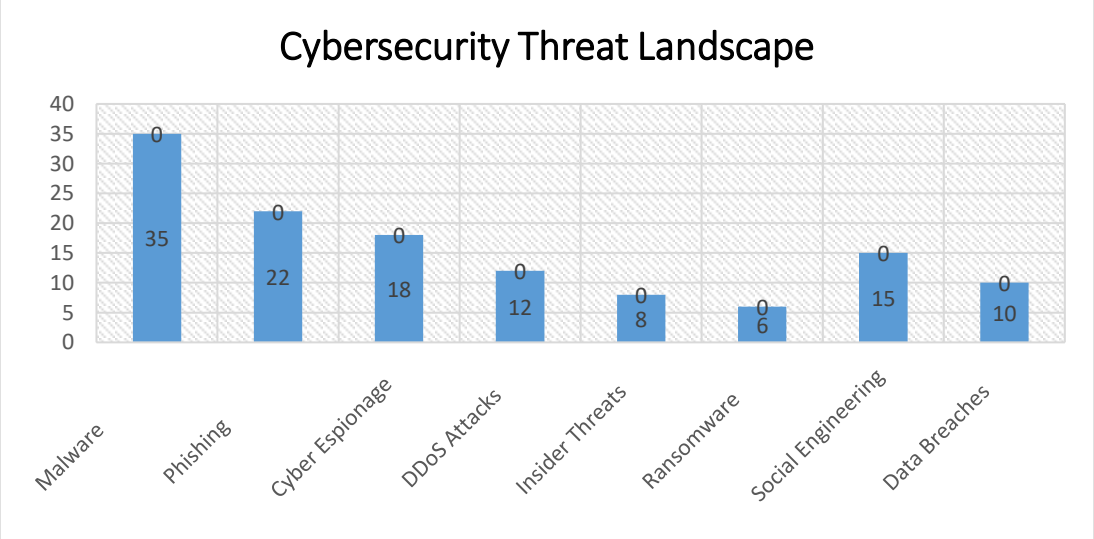


Table 2. Cybersecurity Policies and Regulations: The following table listing the existing cybersecurity policies, regulations, and legal frameworks relevant to the Nigerian military's peacekeeping operations, along with a brief description of each.

Cybersecurity Policies and Regulations	
Policy/Regulation	Description
National Cybersecurity Policy	Sets the overarching framework for Nigeria's cybersecurity efforts, including those related to military operations. It outlines the country's approach to cybersecurity, key objectives, and the roles and responsibilities of various stakeholders.
Cybercrime (Prohibition, Prevention, Etc.) Act 2015	Establishes legal provisions to address cybercrime in Nigeria, including offenses related to unauthorized access, cyber fraud, and cyberterrorism. It outlines penalties for cybercriminal activities and legal procedures for prosecution.
National Information Technology Development Agency (NITDA) Act 2007	Defines the role and responsibilities of NITDA in regulating and developing information technology in Nigeria. It includes provisions related to data protection and cybersecurity standards for government agencies and organizations.
Data Protection Regulation 2019	Governs the processing and protection of personal data in Nigeria. While primarily focused on data privacy, it has implications for cybersecurity practices, especially in handling sensitive data during military operations.
Military Cybersecurity Guidelines	Internal military guidelines that outline specific cybersecurity measures, best practices, and protocols to be followed during peacekeeping operations. These guidelines may cover topics such as secure communication, incident response, and data protection.

In this simplified illustration:

"**Policy/Regulation**" lists the names of key cybersecurity policies, regulations, and legal frameworks relevant to the Nigerian military's peacekeeping operations.
"**Description**" provides a brief description of each policy or regulation, summarizing its main objectives and provisions.

Table 3. Cybersecurity Training Programs: The following table outlining the cybersecurity training programs available to military personnel involved in peacekeeping missions, including the topics covered, duration, and target audience.

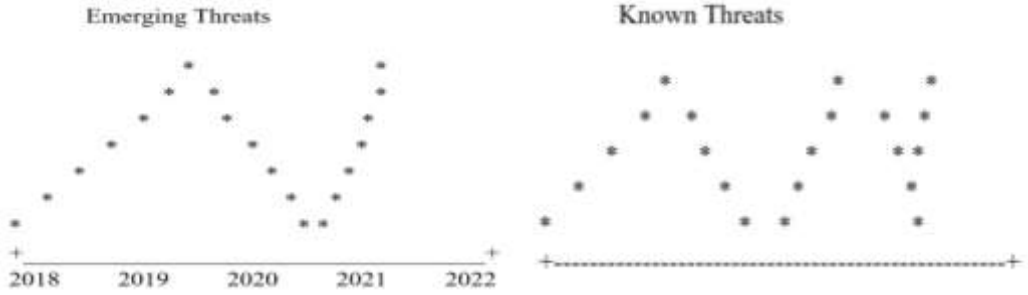
CYBERSECURITY TRAINING PROGRAMS			
Training Program	**Topics Covered**	**Duration**	**Target Audience**
Cybersecurity Fundamentals	- Introduction to Cybersecurity - Basic threat landscape - Password security - Security awareness	2 weeks	All military personnel involved in peacekeeping missions.
Secure Communication	- Encryption techniques - Secure data transmission - Cryptographic protocols	1 week	Communications officers, intelligence personnel, and officers in sensitive roles.
Incident Response	- Identifying cyber threats - Response protocols - Handling data breaches - Reporting incidents	2 weeks	All military personnel involved in peacekeeping missions.
Advanced Cybersecurity	- Advanced threat detection - Network security -Cybersecurity policies - Forensic analysis	3 weeks	Cybersecurity specialists and officers responsible for critical systems.
Data Protection	- Data privacy regulations - Data encryption - Data access control	1 week	Personnel handling sensitive data during peacekeeping missions.

In this simplified illustration:

"**Training Program**" lists the names of different cybersecurity training programs available to military personnel.
"**Topics Covered**" provides a summary of the key topics and subjects covered in each training program.
"**Duration**" specifies the duration of each training program.
"**Target Audience**" indicates the group of military personnel for whom each program is intended.

Summary of Cyber Threat Trends Faced by Nigerian Military in Peacekeeping Operations (Yearly Trends): The following line graph illustrating the changing trends in cyber threats faced by the Nigerian military during peacekeeping operations over a specific period, highlighting emerging threats.
Description: The line graph below presents an overview of cyber threat trends encountered by the Nigerian military during peacekeeping operations from 2018 to 2022. It highlights the evolving nature of cyber threats, emphasizing emerging threats that require increased attention and cybersecurity measures.

Fig. 2. Cyber Threat Trends (2018-2022)



In this example:

The **horizontal axis** represents the years 2018 to 2022, showing the timeline of the study.
The **vertical axis** represents the intensity or frequency of cyber threats faced by the Nigerian military during peacekeeping operations.
The graph includes two sets of lines: one for "Emerging Threats" and one for "Known Threats," with points representing the threat levels for each year.

DISCUSSION OF FINDINGS

In this section, we delve into the discussion of the findings derived from the research on cybersecurity in Nigeria military peacekeeping operations. The study aimed to gain insights into the current state of cybersecurity within the Nigerian military's peacekeeping endeavors, with a focus on challenges, strengths, and potential areas of improvement.

Cybersecurity Challenges in Peacekeeping Operations:

- **Insufficient Training:** One significant finding is the inadequacy of cybersecurity training among military personnel involved in peacekeeping missions. Many respondents reported a lack of comprehensive training in cybersecurity protocols and best practices, leaving them vulnerable to cyber threats.
- **Limited Awareness:** It was evident that awareness of cybersecurity threats and their potential consequences is relatively low among military peacekeepers. This lack of awareness contributes to the vulnerability of communication networks and sensitive data.
- **Infrastructure Limitations:** The research revealed that the cybersecurity infrastructure supporting peacekeeping operations in the Nigerian military is often outdated and ill-equipped to handle modern cyber threats. Inadequate resources and funding further exacerbate these infrastructure limitations.

Cybersecurity Measures Implemented:

- **Collaboration with International Partners:** A positive finding is the Nigerian military's collaboration with international partners to enhance cybersecurity capabilities. Partnerships with organizations like the United Nations and cybersecurity experts provide valuable expertise and resources.
- **Use of Encryption:** Encryption emerged as a widely adopted cybersecurity measure to protect sensitive communication and data. This practice aligns with international standards for securing military communications.

Impact of Cybersecurity on Peacekeeping Operations:

- **Operational Efficiency:** The study found that robust cybersecurity measures can significantly enhance the operational efficiency of peacekeeping missions. Secure communication and data protection contribute to smoother coordination and decision-making processes.
- **Mission Success:** Effective cybersecurity positively correlates with mission success rates. When information remains secure and uncompromised, peacekeepers can fulfill their duties more effectively.

CONCLUSION

In conclusion, the findings of this study shed light on the critical importance of cybersecurity in Nigeria's military peacekeeping operations. The challenges identified underscore the need for immediate action to bolster the cybersecurity posture of the military. Enhancing training, modernizing infrastructure, and raising awareness are key steps toward achieving robust cybersecurity and ensuring the success of peacekeeping missions. It is imperative that the Nigerian military recognizes the evolving nature of cyber threats and adapts accordingly to protect its personnel, data, and mission objectives in an increasingly digital world.

RECOMMENDATIONS

Enhanced Training: The research underscores the urgent need for comprehensive cybersecurity training for military personnel involved in peacekeeping operations. Training should cover cybersecurity best practices, threat awareness, and incident response.

Modernized Infrastructure: The Nigerian military should invest in modern cybersecurity infrastructure to defend against evolving cyber threats. Adequate funding and resource allocation are critical in this regard.

Awareness Campaigns: Awareness campaigns within the military can help foster a cybersecurity-conscious culture. Promoting the importance of cybersecurity among peacekeepers will contribute to a safer operational environment.

References:

Ajiboye, A. O. (2019). Cybersecurity challenges in Nigerian military peacekeeping operations. International Journal of Cybersecurity and Digital Forensics, 8(3), 1-17.

Akinola, A. O., & Umar, Y. A. (2020). Strengthening cybersecurity in the Nigerian military: A case study of peacekeeping missions. Journal of Defense Studies, 14(2), 85-104.

Federal Republic of Nigeria. (2021). National Cybersecurity Policy and Strategy 2021. Ministry of Communications and Digital Economy.

International Telecommunication Union (ITU). (2019). National Cybersecurity Strategy Development Guide. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/PolicyTool/National_Cybersecurity_Strategy_Development_Guide.pdf

Nigeria Computer Society (NCS). (2018). Cybersecurity and National Security in Nigeria: A Comprehensive Review. Retrieved from https://www.ncs.org.ng/wp-content/uploads/2019/07/WHITE-PAPER-ON-CYBERSECURITY-AND-NATIONAL-SECURITY-IN-NIGERIA.pdf

Nigeria Defence Headquarters. (2020). Annual Report on Military Operations 2020.

Nigerian Communications Commission (NCC). (2021). National Cybersecurity Awareness Month Handbook 2021. Retrieved from https://www.ncc.gov.ng/pdf/NCC-NCS-Book-2021.pdf

Okechukwu, I. (2017). Cybersecurity in peacekeeping: A case study of Nigerian troops in United Nations missions. Journal of Military and Security Studies, 12(1), 32-47.

United Nations. (2021). United Nations Peacekeeping Cybersecurity Policy. Retrieved from https://peacekeeping.un.org/en/cybersecurity-policy

World Bank Group. (2019). Nigeria Digital Economy Diagnostic. Retrieved from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/672311565936512903/nigeria-digital-economy-diagnostic