NIGERIAN JOURNAL OF AFRICAN STUDIES (NJAS) VOL. 7 NO. 1, 2025 (ISSN: 2734-3146), Indexed in Google Scholar
(Email: officialnjas@gmail.com) A publication of African Studies, Nnamdi Azikiwe University, Awka, Nigeria

INTERROGATING THE EFFECTIVENESS OF NIGERIAN MILITARY CYBER WARFARE TECHNOLOGIES IN CURBING BOKO HARAM'S CYBER PROPAGANDA IN NIGERIA

Akinbile, I. O.; Chaku, S.E.; Habiba, M. & Kulugh, V.E.

Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nasarawa State. Nigeria. Correspondent email: ismailakinbile@yahoo.com

Abstract
The presence of Boko Haram insurgents in Nigeria's cyberspace has facilitated their cyber propaganda and virtual training, thereby posing a major security challenge to the nation. In response, the Nigerian military established the Cyber Command and conducted cyber operations to combat the insurgents' online activities. Following the Command's operations, it appears that Boko Haram's cyber propaganda has been reduced. To investigate this, research questions and objectives were formulated to guide the study. These objectives were addressed using descriptive statistics, while inferential statistics were employed to gain deeper insights. A sample of 100 participants was selected from an estimated population of 10,000. The participants comprised serving and retired military personnel from the Nigerian Army School of Cyber Warfare, the Nigerian Army Cyber Warfare Command, and the Ministry of Defence, as well as members of the academia and the Defence Intelligence Agency. Data were collected from both primary and secondary sources, including literature, questionnaires, and Key Informant Interviews (KIIs). The questionnaire data were analyzed using frequency counts, percentages, and mean scores to answer the research questions. Data collected from the KIIs were analyzed through thematic analysis, while the Chi-square test was used to test the hypothesis at a 0.05 significance level. The results of the Pearson Chi-square test and Likelihood Ratio indicated a statistically significant association between the employed cyber technologies and the curbing of Boko Haram's cyber propaganda. The study revealed that the Video Network Surveillance System (VNS), SVS Satellite System, and Extended Detection and Response (XDR) technologies were among the cyber warfare tools employed by the Nigerian military. It was also found that the major strengths of these technologies include tracking and blocking Boko Haram's cyber propaganda videos. The study recommends that the military ensure personnel develop cyber skills and the ability to interface effectively with technical experts to improve the human–machine interface. The study concludes that there is a need for adequate cyber technology for defensive operations in order to effectively protect Nigeria's cyberspace from Boko Haram's cyber attacks.
Keywords: Cyber Warfare Technology, Nigerian Military, Boko Haram Insurgency

Introduction

Terrorism has become a household word as there is no nation that is completely immune from its effects. The trend of globalization which includes technology has significantly influenced the spate of terrorism, as the event in one country has direct or indirect effects on other countries (John, 2002**)**. The 21st-Century Boko Haram is acquiring technological skills that enable them to engage in extremely destructive acts such as the spread of new doctrines, falsehood and blackmail, report by US Army Training and Doctrine Command cited in Ogunlana (2019). Mahmood **(2017)** opines that Boko Haram social media activities are more than propaganda, they are leveraging on social media technology such as YouTube, Twitter for recruitment, virtual training, and fund raising**.** According to Kate (2018), Nigeria has itself suffered from numerous incidents of cyber-terrorism by Boko Haram after they migrated to the internet.

To curb the group cyber activities, Nigerian government developed systematic measures and intervention policies. To this extent, the Federal Government of Nigeria (FGN) enacted the National Cyber Security Policy and Strategy in 2014, while in 2015; the FGN enacted the Cybercrime Prohibition and Prevention Act. To consolidate on these efforts and mitigate attack in Nigerian Army (NA) space, the former Chief of Army Staff, Lt Gen TY Buratai (rtd) launched the Nigerian Army Cyber Warfare Command in 2017. The Command is to ensure the NA cyberspace is secured through the employment of cyber warfare technologies against threat to National Security.

The integration of cyber technology into military Code Operations has emerged as a transformative force, reshaping the strategies employed by Nigerian Armed Forces. Therefore, Northeast landscape of conflict has now witnessed a profound shift with the induction of cyber technology. These technologies have become integral to military operation, offering unprecedented opportunities in the realm of national security. Therefore, the study

interrogated the effectiveness of the cyber technology employed by the Nigerian military against Boko Haram's cyber propaganda.

Literature Review

Conceptualizing Cyber Warfare Technology

Cyber warfare technology represents a paradigm shift in the nature of conflict, leveraging digital tools and techniques to achieve strategic objectives in the virtual domain. Noel and Reith (2021) trace cyber warfare technology back to the early days of computing in the mid-20th century. As computers became increasingly interconnected through networks such as ARPANET, the precursor to the modern internet, the potential for using these networks for military purposes became evident. Anthimos (2017) posits that one of the earliest examples of cyber warfare technology can be found in the concept of "cybernetic warfare," which emerged in the 1960s and 1970s. Today, cyber warfare technology has been driven by advancements in computing, telecommunications, and information technology. In today's interconnected world, nearly every aspect of modern life relies on digital infrastructure, thus, state and non-state actors alike uses this infrastructure as a potent tool to project power, disrupt adversaries and advance their interests.

The concept of cyber warfare technology encompasses a broad range of capabilities in offensive cyber operations, defensive cyber security measures, and the development of advanced cyber weapons. Offensive cyber operations involve the use of digital tools to infiltrate, disrupt, or sabotage adversary networks and systems. These operations can target critical infrastructure, government institutions, military networks, and private enterprises, with the aim of causing disruption, espionage, or destruction. If these tools were adequately used, Maza, et al may not have opined that blocking Boko Haram financial network in Lake Chad, North East Nigeria poses difficulties, (2020).

Defensive cyber security measures, on the other hand, involve protecting one's own networks and systems from cyber-attacks, employing techniques such as encryption, firewalls, and intrusion detection systems to safeguard sensitive information and prevent unauthorized access. The development of cyber weapons including malware, viruses, and other malicious software, represents a significant aspect of weapon used in cyber warfare technology. These weapons can be deployed to exploit vulnerabilities in adversary systems, steal sensitive data, or disrupt critical services (Steven, 2018). The proliferation of cyber weapons has generated concerns of a widespread damage and disruption from cyber-attacks, with some experts warning of the possibility of a "cyber Pearl Harbor" or "cyber 9/11" scenario in which a large-scale cyber-attack results in catastrophic consequences (Steven, 2018).

Scholars have offered various perspectives on the implications of cyber warfare technology for national security and international relations. Some argue that cyber warfare represents a new form of warfare that transcends traditional boundaries, blurring the lines between military and civilian targets and challenging established norms of conflict. Others contend that cyber warfare introduces new risks and uncertainties into the international system, as state and non-state actors seek to exploit vulnerabilities in cyberspace for strategic advantage.

Martin (2009) argues that cyber warfare technology presents both opportunities and challenges to national security. In his book "Cyber deterrence and Cyber war," Martin explores the dynamics of cyber conflict and the potential for cyber weapons to deter adversaries from engaging in aggressive behavior. He suggests that while cyber weapons could be used to inflict significant damage on adversaries, their effectiveness as a deterrent depends on factors such as attribution, escalation risks, and the resilience of adversary networks.

Thomas and Peter (2012) analyze the historical evolution of cyber warfare technology and the possibility of cyber warfare. Rid (2012) argues that 'despite growing fears of cyber warfare, the likelihood of a full-scale cyber war breaking out between major powers is low'. Instead, he contends that most cyber incidents are better understood as acts of espionage, sabotage, or criminal activity rather than acts of war. In addition to scholarly perspectives, policy makers, military leaders and governments around the world are investing heavily in cyber capabilities, strengthening cyber security defenses to protect against cyber threats.

Research Methodology

The study employed mixed method research design. The sample size for the study was determined by Yamane's (1967) formula. The instruments used for data collection include questionnaire and KIIs. The data collected through questionnaire were subjected to descriptive and inferential statistics while thematic/content analysis was used to analyze data collected from KII. The research design was descriptive in nature; therefore simple percentage and central tendency were used to achieve objectives 1 and 2, which were to investigate the nature of the cyber technologies employed by the Nigerian military in combating Boko Haram Insurgency; examine the strengths of the cyber technologies and its effect on military cyber operation in Nigeria.

In addition, Inferential Statistics was further used to gain more insight into the survey data collected as it was employed to achieve objective 2. However, Thematic Analysis was used to achieve objective one, which is to categorize the cyber technologies employed in curbing Boko Haram's cyber propaganda.

Data Presentation and Analysis

Table 1: Employed Cyber Technology

S/N	Cyber Technology	Response	Percentage
1.	IDS/IPS	12	24
2.	SVS Satellite System	22	44
3.	VNS	4	8
4.	XDR	12	24
	Total	**50**	**100**

Source: Researchers' Field Work and Analysis, 2024.

The SVS Satellite Technology which received the highest response is used to improve communication and enhance combat coordination. As shown in the table above, 44% of the respondents confirmed SVS Satellite to be a wildly employed cyber technology in the Nigerian military. However, 8% of the responses opined the VNS as one of the cyber technology in the Nigerian military. This technology is used to monitor network for suspicious activity and identify malicious actors, while Instruction Detection System/ Instruction Prevention System (IDS/IPS) technology and XDR technology received 24% each from the respondents. The former helped to block, monitor network activity for malicious behavior or potential threat while the later detect and respond to threat actors.

Table 2: Effectiveness of the Employed Cyber Technology in HADIN KAI Cyber Operation

Serial	Item	SD	D	N	A	SA	Mean Score	Decision
1.	The ability to identify malicious actors	4	6	24	60	85	3.5	Accepted
2.	The ability to communicate and enhance combat coordination.	3	8	24	60	100	3.9	Accepted
3.	The ability to degrade Boko Haram cyber network capability.	3	8	24	64	95	3.8	Accepted
4.	The ability to track and block cyber propaganda videos by Boko Haram.	2	8	27	68	90	3.9	Accepted

Source: Researchers' Field Work and Analysis, 2024.

In assessing the effectiveness of cyber technology in Operation HADIN KAI, the responses regarding identifying malicious actors, enhancing cyber communication, degrading Boko Haram cyber recruitment capability and tracking and blocking cyber propaganda videos by Boko Haram indicate a positive perception among the surveyed population. A significant majority of respondents, comprising 252, agreed with the view. This suggests a consensus among the participants that the cyber actions adopted have been the strength in achieving their intended objectives. Additionally, 370 of the respondents strongly agreed with the view. On the contrary, 30 of participants disagreed with the statement while 12 respondents strongly disagreed. However, 99 provided a neutral response. The decision confirmed that the views presented in the table were accepted as significant during the operation.

Cross Tabulation of the Cyber Technologies Employed in Operation HADIN KAI

The cross tabulation in table 3 shows the perception of the respondents on how the employed cyber technologies have curbed Boko Haram's cyber propaganda.

Table 3: Respondents' Perceptions on the Employed Cyber Technology and Curbing Boko Haram Cyber Propaganda in Cross Tabulation

Degrading of BHT Cyber Propaganda	Agree	Disagree	Neutral	Strongly Disagree	Strongly Agree	Total
SVS Satellite System	27	4	2	0	11	44
(IDS/IPS, VNS, XDR)	76	13	12	2	7	110
Total	103	17	14	2	18	154

Source: Researchers' Field Work and Analysis, 2024.

The data captured in the table above is a cross-tabulation of responses related to the perceived extent to which Boko Haram insurgency's cyber propaganda in the Nigeria have been curbed based on different cyber technologies employed either in isolation or combined effort. The data is organized into categories of agreement, disagreement, neutral stance, strongly disagree, and strongly agree.

In the employment of only "SVS Satellite System" for curbing BHT cyber propaganda, a total of 44 respondents participated in the survey. Among them, 27 agreed that the System was instrumental in locating Boko Haram cyber activities, 4 disagreed, 2 were neutral, and none of the respondents strongly disagreed while 11 strongly agreed. In the employment of "SVS Satellite System in combination with VNS, IDS/IPS and XDR" category, there were 110 respondents. Of these, 76 agreed, 13 disagreed, 12 were neutral, 2 strongly agreed and 7 respondents strongly disagreed in this category.

The combined total, across both technologies includes 154 responses, with 103 agreeing, 17 disagreeing, 14 being neutral, 2 strongly disagreeing, and 18 strongly agreeing. This cross-tabulation provides an overview of the distribution of opinions on the success of operations in curbing the cyber activities of Boko Haram in the study area with regards to the two major categories of technologies employed, which are SVS Satellite System and a combination of SVS Satellite System with VNS, IDS/IPS and XDR, highlighting the varying degrees of agreement or disagreement among the respondents.

Hypothesis 1

There is no statistically significant association between the cyber technology employed and BHT cyber propaganda.

Chi square Test on Employed Cyber Technology and BHT Cyber Propaganda

The chi-square test was conducted to assess the statistical significance of the relationship between the cyber technology employed and curbing BHT cyber propaganda. The results are presented in Table 4.

Table 4: Chi-Square Test on Employed Cyber Technology and BHT Cyber Propaganda

Chi-Square Test	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.031a	4	0.017
Likelihood Ratio	11.669	4	0.020
N of Valid Cases	154		

Source: Researchers' Field Work and Analysis, 2024.

a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .57.

Pearson Chi-Square: The calculated chi-square value is 12.031a with 4 degrees of freedom, resulting in an asymptotic significance (p-value) of .017.

Likelihood Ratio: The likelihood ratio chi-square value is 11.669 with 4 degrees of freedom, and the asymptotic significance is 0.020. These values indicate that there was a statistically significant association between the cyber technologies employed and the curbing of BHT propaganda, as both p-values are less than the conventional

significance level of 0.05. Therefore, based on the chi-square test, the curbing of Boko Haram's propaganda in the area of operations appears to be significantly influenced by the type of cyber technologies employed.
This therefore affirms that there is a significant difference in the performance of operations that use single tool and those that use a combination of variant cyber tools in curbing Boko Haram cyber activities during cyber operation. Table **5** provides measures of association between single employed cyber technology and combined cyber technology.

Table 5: Measures of Association

Symmetric Measures	Value	Approximate Significance
Phi	0.280	0.017
Cramer's V	0.280	0.017
N of Valid Cases	154	

Source: Researchers' Field Work and Analysis, 2024.
Phi: The calculated Phi coefficient is 0.280, and the approximate significance is 0.017.
Cramer's V: The Cramer's V coefficient is also 0.280, with an approximate significance of 0.017.

These measures of association further support the findings from the chi-square test, indicating a strong association between the types of cyber technology employed (single or combined) and the perceived success of operations. The p-values bellow the significance level of 0.05 suggests that the relationship was statistically significant. Therefore, based on these measures, there is a strong evidence to conclude that the success of operations in degrading the activities of Boko Haram is significantly associated with the choice between the application of a single cyber tools and combined variants tools.

Virtual interview with Cdr Boyen and Dr Zannah Boguma (16 October, 2024, Kaduna and Borno States), provide positive assessments of the cyber warfare technology of the Nigerian military, suggesting the approach adopted in the HADIN KAI has achieved its objective, has the military been able to curtail the menace of the group's cyber propaganda and threat. The study also incorporates Retired Brig Gen Olabode's viewpoint on the importance of political elements and good governance in complementing military successes (virtual interview 22 October, 2024, Abuja).

In all, the result of the effectiveness of the approaches adopted in the Code Operation as shown in table **5** indicate that combine variants of cyber tools in cyber operation will have more success when compared with solely cyber tools strategy.

Conclusion

The study assessed the cyber warfare technologies employed by the Nigerian military in curbing Boko Haram's cyber propaganda in Nigeria. The analysis revealed several areas of effectiveness. These include locating and intercepting cyber threats, identifying and monitoring malicious actors, degrading Boko Haram's cyber recruitment capabilities, and tracking and blocking the group's cyber propaganda videos. The study identified these capabilities as essential tools for defensive cyber operations and national security. It further emphasized the need for adequate cyber technology for defensive combat operations to effectively protect Nigeria's cyberspace against Boko Haram's cyber threats and enhance national security.

Recommendations

Based on the findings of this study, the following key recommendations are proposed:

i. The military should ensure personnel develop cyber skills and the ability to interface with technical experts to function effectively and perfecting the human-machine interface.
ii. The Federal Government and military should commence the review of cyber security training for personnel to reflect and test their knowledge in cyber technology and evaluate their effectiveness in detecting and mitigating cyber threat as being practice in developed nations.
iii. Government should procure up-to-date and additional cyber defensive technology for the military to enhance their Operation. Also, infrastructure for timely maintenance of cyber equipment should be put in place to ensure effectiveness and accuracy of use.
iv. The military should partner with university and private sector for training, development and design of cyber tool for defensive military operation.

References

Ahmed F.F and Abah P.O (2014). Determinant of Food Security and Low-Income House Earners in Maiduguri Metropolis of Borno State. Asian Journal of Social Science and Humanities vol.3 (1) February 2014. Retrieved from http/www.ajssh.leena-luma.co.JSSHPDFFs. Last Accessed July 2024.

Anthimos, T. (2017). Cyber Warfare and Discourse. DOI:10.1007/978-3119-50847-2 retrieved from https:/www. Researchgate.net/publication.htm.on 19 April 2024.

Human Right Watch, (2020). Gruesome Boko Haram Killings in Northeast Nigeria Authorities Should Prioritize Civilian Protection. Retrieved from https://www.hrw.org/news/2020/12/01/gruesome-boko-haram-killings-northeast-nigeria Last Accessed June 2024.

John, F M. (2002). Impact of Terrorism on Globalization and Vicie-Versa. https://scholars.smu.edu/till/vol36/iss1/9.(Accessed on 19 March 2024).

Kate, O, F.(2018). Nigerian Cyber Warfare Command: Waging War in Cyber Space, retrieved from https://www.fores.com/sites/kateoflahhertyuk/2018/11/2 html on 23 Apr 24.

Mahmood, O.S (2017). More than Propaganda: A Review of Boko Haram's Public Messgae. Institute for Security Studies West African Report 20 March 2017. https://issafrican.s3.amazonaws.com/site/uploads/war20pdf. (Accessed on 14 July 2024).

Maza, D., Umut, K., & Aksit, S. (2020) Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case Study of Boko Haram. *Retrieved 6 June 2020 from https://doi.org/10.1177/2158244020934494-Sage -Journals-June -2020*.pdf.

Martin, C.L (2009**). Cyber deterrence and Cyber war.** Retrieved from https://www.amazon.com/Cyberdeterrence-Cyberwar-Martin-C-Libicki/dp/0833047345#immersive-view_1736678688743. (Accessed on 2 June 2024).

National Population Census (2006). Borno State Population retrieved from https://zodml.org.borno.state. (Accessed on 19 April 2024).

Noel,G.E, & Reith, M.G (2021). Cyber Warfar Evolution and Role in Modern Conflict. Journal of information warfare vol 20, No.4. 20th Anniversary Edition pp. 30-44 retrieved from https://www.jstor.org/stable/27125011 on 20 April 2024.

Ogunlana, S,O. (2019). Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies.Journal of Strategic Security Vol. 12, No. 1 (2019), pp. 72-106 Published by: University of South Florida Board of Trustees Stable URL: https://www.jstor.org/stable/10.2307/26623078.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies 35/1, S-32; retrieved from https://www.tandfonline.com/doi/abs/10.1080.01402390.2011.608939. Accessed on 6 April 2024.

Stevens, T. (2018), Cyber Weapons: Power and the Governance of the Invisible retrieved from https://www.reasercgate.net/publication on 19 April 2024.

Thomas, R., & Peter M (2012). Cyber Weapons, the RUSI journal, Volume 157,-issue 1, retrieved from https://www.nsf-journal,hr/online-issues/focus/id/1317.

Yamane, T. (1067) Statistics, An Introductory Analysis, 2nd Ed, New York Harper and Row.