ASSESSING THE CHALLENGES OF NIGERIAN MILITARY CYBER WARFARE TECHNOLOGIES IN COMBATING BOKO HARAM'S CYBER ACTIVITIES 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 migration of Boko Haram insurgents to Nigeria's cyberspace has become a major security challenge to the nation due to their increasing cyber activities. In response, the Nigerian military has employed various approaches, including the use of cyber technology. Despite these efforts, Boko Haram's online propaganda, virtual training, and recruitment activities have persisted. To investigate this development, research questions and objectives were formulated to guide the study. The 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. Others included 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). Questionnaire data were analyzed using frequency counts, percentages, and mean scores to answer the research questions. Data collected from KIIs were analyzed through thematic analysis, while the Chi-square test was used to test hypotheses at a 0.05 significance level. The results of the Pearson Chi-square Test and the Likelihood Ratio indicated a statistically significant association between combating Boko Haram's cyber activities and the use of non-offensive cyber technology. The study found that Video Network Surveillance System (VNS), SVS Satellite System, and Extended Detection and Response (XDR) were among the cyber warfare technologies employed by the Nigerian military in combating Boko Haram's cyber operations. However, the study also found that major shortcomings of the cyber technologies include operating systems that do not support combat and intelligence operations, as well as security gaps in installation and configuration. The study concludes that there is a need to procure offensive cyber technologies for combat operations in order to effectively defeat Boko Haram in cyberspace. It also recommends that the military ensure its personnel develop advanced cyber skills and the capacity to interface with technical experts to enhance the human–machine interface.
Keywords: Cyber Warfare Technology, Nigerian Military, Boko Haram Insurgency, North-East

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) opined 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.

In spite of the success recorded by the Nigerian military, Boko Haram Insurgency (BHI) still conduct networking and propaganda, according to Ogunlana (2019). With these, it seems the military effort and its cyber warfare technologies appear to be challenged with some inherent shortcomings. However, majority of the studies conducted only examined the military operations on the outward without investigating military cyber warfare technology, what technology was employed in Nigerian military cyber operations to mitigate the effect of the Boko Haram? Did it fail and why it failed to achieve the expected results? This creates a gap the study intends to

fill. Hence, a need exists for a study to unravel the shortcomings of cyber technology of the Nigerian military in combating BHI. Therefore, the study assessed the challenges of the cyber technology employed by the Nigerian military against Boko Haram's cyber activities.

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) traced 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 tools 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) argued 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) analyzed 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, developing offensive cyber capabilities to protect against cyber threats.

Methodology

Mixed method research design was employed in the study. 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. 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 combating Boko Haram's cyber activities.

Data Presentation and Analysis

Table 1: Cyber Technologies of the Nigerian Military

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 obtained result in table 1 shows that 44% of the respondents confirmed SVS Satellite System as one of the cyber technologies of the military. Technology which received the highest response is used to improve communication and enhance combat coordination 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: Shortcoming of the Employed Cyber Warfare Technology

Serial	Item	SD	D	N	A	SA	Mean	Decision
Score								
1.	The System is not design for offensive cyber operation.	3	4	18	56	125	4.1	Accepted
2.	The technology is prone to intrusion by hackers, also not design for offensive cyber operation.	7	12	24	48	85	3.5	Accepted
3.	The OS is not design to support combat intelligence operation.	5	4	18	52	120	3.9	Accepted
4.	The technology could not be effectively applied because of security gap in the OS's design, installation or configuration.	4	12	15	48	115	3.8	Accepted

Source: Researchers' Field Work and Analysis, 2024.

From the survey result, 204 per cent of the respondents agreed that the issues presented in table 2 were shortcoming of the cyber warfare technology employed by the military. This suggests that most participants believed that legal/technical gap, not design for offensive cyber operation, OS not supporting combat, intelligence operation and security gap in installation or configuration as major shortcomings. Interestingly, 445 respondents strongly agreed with the view, while 32 participants disagreed with the view. Another 75 provided a neutral response. Only 19 respondents strongly disagreed with the statement. The decision confirmed that the view presented in the table were significant shortcoming that could hamper the operation.

Effect of Combating Boko Haram Cyber Activities with a Non Offensive Cyber Technology

Table 2 revealed that the employed cyber technology was not design for offensive cyber operation. Therefore, it is identified as a crucial shortcoming**,** prompting its selection as a metric for this investigation. The primary objective was to investigate the effect of combating Boko Haram's cyber activities with a non-offensive cyber technology. To rigorously test the hypothesis, the researchers employed a non-parametric Chi-square test, providing a robust statistical method for the analysis. The results of this investigation were presented in Table 3, Table 4, and Table 5 with each contributing valuable insights into the relationship between the identified shortcoming and BHT cyber activities. These tables, as part of the broader study, facilitated the testing of the null hypothesis asserting that conducting offensive operation with a non-offensive cyber technology on Boko Haram's cyber activities will affects military cyber combat operation.

Table 3: Respondents' Perceptions on Combating Boko Haram Cyber Activities with a Non Offensive Cyber Technology in Cross-tabulation

BHT Cyber Activities	Agree	Disagree	Neutral	Strongly Disagree	Strongly Agree	Total
IDS/IPS	22	5	8	4	11	50
VNS, XDR and SVS Satellite System	9	16	12	10	3	50
Total	**31**	**21**	**20**	**14**	**14**	**100**

Source: Researchers' Field Work and Analysis, 2024.

Table 3 illustrates respondents' perception of cyber tools not deployable for combat operation against Boko Haram's cyber activities a cross-tabulation. The table breaks down responses into categories of agreement, disagreement, neutrality, strongly agreement and disagreement.

In the context of IDS/IPS, substantial portion of respondents, constituting 22 individuals, opined that the tool is not appropriate for offensive cyber warfare. Hence is a challenge. This acknowledgment was disagreed by 5 respondents, 8 expressed neutrality, 4 strongly disagree while 11 strongly agreeing, resulting in a total of 50 respondents in this category. In the context of VNS, SVS Satellite System and XDR, the data paints a different picture. A lower number, specifically 9 respondents, agree that the combined cyber tools are appropriate for offensive cyber warfare. Surprisingly, 16 respondents disagree, 12 expressed neutrality, 10 strongly disagree while 3 strongly agreeing, resulting in a total of 50 respondents in this category. These results underscore the need for further analysis to understand the relationship between the shortcoming and combating BHT activities.

Hypothesis One

Ho: There is no statistical significant relationship between combating BHT cyber activities and non-offensive cyber technology.

Table 4: Chi-square test on the effect of combating Boko Haram Cyber Activities with a Non-Offensive Cyber Technology

Chi-Square Test (2-sided)	Value	Df	Asymptotic Significance
Pearson Chi-Square	18.294a	4	.000
Likelihood Ratio	28.555	4	.000
N of Valid Cases	50		

Source: Researchers' Field Work and Analysis, 2024.

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 2.00.

The table above presents the results of a Chi-square test aimed at examining the statistical significance of the relationship between the shortcoming and combating BHT cyber activities. The Pearson Chi-square Test yielded a chi-square value of 18.294 with 4 degrees of freedom, resulting in an asymptotic significance (2-sided) of 0.000, which is less than level of significance of 0.05. Similarly, the Likelihood Ratio Test produced a chi-square value of 28.555with 4 degrees of freedom and a significance level of 0.000. Both tests indicate a statistically significant association between the shortcoming and combating BHT cyber activities.

The significance levels obtained from both tests, below the commonly used threshold of 0.05, suggest that the observed relationship is unlikely to be a result of random chance. This statistical significance provides strong evidence that there is indeed a meaningful association between non-offensive cyber technology and combating BHT cyber activities.

The results of the Chi-square tests affirm the presence of a statistically significant relationship between the shortcoming and combating BHT cyber activities. Interview with Maj Gen Wahab (Rtd), confirmed the statistical findings that the use of cyber tools not design for offensive combat operation in such circumstance would challenge the effectiveness of the military operation. Further analysis was needed to understand the degree of association for operational planning and decision-making.

Table 5: Degree of Associations

Symmetric Measures (2-sided)	Value	Asymptotic Significance
Cramer's V	0.706	.000
N of Valid Cases	50	

Source: Researchers' Field Work and Analysis, 2024.

Table 5 presents the measure of association, Cramer's V, to quantify the strength and statistical significance of the relationship between the shortcoming and combating BHT cyber activities. Crammer' V yielded a value of 0.706, indicating a substantial degree of association between these variables. The approximate significance levels for Cramer's V was 0.000, falling below the conventional threshold of 0.05. This low p-value suggests that the observed association is unlikely to be a result of random chance, affirming the statistical significance of the relationship.

The Cramer's V, an extension of phi coefficient suitable for larger contingency tables, highlighted a robust and meaningful connection between the shortcoming and combating BHT cyber activities. The consistency in results across these measures reinforces the reliability of the findings. The results were further given insight by the respondents. Some military scholar's notable, KII 1 argued that, the non use of cyber offensive tools in military cyber operations may be due to lack of technical expertise in cyber weapon design.

Regarding technical expertise and non use of offensive tools in cyber operation, Dr Zannah Boguma, a key informant sees it as a response to evolving circumstances (virtual interview on 16 October, 2024, Borno States), while Brig. Gen B. C Olabode (Rtd) adds depth to this perspective, explaining that fluid and unpredictable situations may affect strategic decision, (virtual interview on 22 October, 2024, Abuja). The perspectives offered by these key informants provide a comprehensive understanding of the challenges and intricacies involved in cyber operations. Each informant brought a unique viewpoint shaped by their roles, experiences, and observations. In all, the result of combating Boko Haram cyber activities with a non-offensive cyber technology is little or no disruption or sabotage on adversary networks and systems. These operations cannot target critical infrastructure or platform hosting adversary. This therefore emphasizes the importance of highlighting shortcomings for effective planning and execution of military operations.

Conclusion

The study assessed the cyber warfare technologies of the Nigerian military in combating Boko Haram's cyber activities in Nigeria. The assessment revealed several shortcomings, including legal and technical gaps, tools not designed for offensive cyber operations, operating systems that do not support combat and intelligence operations, and security vulnerabilities in installation or configuration. The study observed that combating Boko Haram's cyber activities with non-offensive cyber technologies would have little or no disruptive impact on the group's networks and systems. It further emphasized the need to employ offensive cyber technologies to effectively defeat Boko Haram in cyberspace.

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 its operating system and evaluate their effectiveness in detecting and mitigating cyber threat as being practice in developed nations.

iii. Government should procure up-to-date cyber offensive technology for the military to enhance their Operation.

iv. The military should partner with university and private sector for training, development and design of cyber tool for offensive 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.