Cyber Warfare And National Security: Imperative For Naval Operations

Abdullahi Muhammad Ahmed
Nigerian Navy, Nigeria
munikoko@yahoo.com

Adamu Hussaini
Towson University, USA
ahussa7@students.towson.edu

Alhassan Abdulhamid
University of Bradford, UK
a.abdulh2@bradford.ac.uk

***Abstract*—The increase in the reliance on an application of digital technologies in the 21st Century has triggered several cyber threats that threaten national security in various dimensions. To keep at pace with the dynamics of the global information domain, nations are increasingly developing cyber capabilities and integrates these capabilities into hybrid warfare in accordance with the changing character of warfare. The interplay of defensive and offensive cyber capabilities brought to fore the new paradigm of safe guarding own digital technologies against adversaries' attack and at the same time exploiting the vulnerabilities. The employment of cyber-warfare within the paradigm of national security involves the activities in cyberspace which centred around the use of Information and Communication Technology (ICT) weapons for offensive and defensive operations by state and non-state actors against other nation-states or non-state actors. Accordingly, Advanced navies have developed their capacities to defend maritime assets and infrastructure against cyber-attacks by state and non-state actors. The Federal Government of Nigeria (FGN) has, over the years, made concerted efforts to develop the capacity of the Nigerian Navy (NN) to defend the maritime assets against any threats, including cyber-related attacks, for enhanced national security. However, the cyber warfare capabilities of the NN remain limited, thereby making Nigeria's Maritime Environment (NME) vulnerable to cyber-attacks with negative implications on national security. The desire to explore ways of developing the NN capabilities in cyber warfare for naval operations is the motivation of this research. The major problem is that the cyber warfare capability of the NN to defend the nation from the maritime sector is low due to inadequacies or outright lack of requisite cyber tools. The study was descriptive research and integrated both qualitative and quantitative data. The data were collected from primary and secondary sources. The research proffered strategies including formulation of NN cyber warfare policy, creation of a cyber warfare directorate and special recruitment and training of naval cyber warriors.**

***Index Terms*—Cybersecurity, cybercrime, national security, Naval Operations, security**

I. Introduction

The increase in the reliance on an application of digital technologies in the 21st Century has triggered several cyber threats that threaten national security of various nations. To mitigate threats emanating from the cyber domains, nations are increasingly developing cyber capabilities and integrates the capabilities into a holistic hybrid warfare for their national defence. The interplay of defensive and offensive cyber capabilities brought to fore the new paradigm in the ever changing character of war which is now known as cyber-warfare. The employment of cyber-warfare within the paradigm of national security involves the activities within the cyberspace which centred around the use of Information and Communication Technology (ICT) weapons for offensive and defensive operations by state and non-state actors against other nation-states or non-state actors [1]. Accordingly, armed forces leverage the cyber warfare capabilities to protect their technological assets against malicious attacks [2] by both domestic subversive organisations, hostile intelligence services or other cyber adversaries to enhance national security. National security entails providing for human needs and protecting a nation's territorial integrity, core values and interests against aggression. This also covers human security, political stability as well as maintenance of law and order. Therefore, efforts to counter any attempt to use cyberspace to disrupt or attack national assets, especially maritime resources, are vital to deter any aggression. In this regard, nations have continued to explore ways and means to develop the cyber warfare capabilities of their navies in order to enhance their national security [3].

In 2010, the United States (US) Navy established the Fleet Cyber Command (FCC), followed by the reactivation of the US Tenth Fleet to serve as a force provider for the FCC to conduct cyber warfare [4]. The Tenth Fleet comprises over 16,000 personnel, including ethical hackers and other cyber professionals. The Tenth Fleet also deployed platforms with Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) capability for cyber warfare operations towards enhanced national security in the US [5]. In South Africa (SA), in 2017, there were cyber-attacks against Maersk that led to the shutdown of terminals at Port Elizabeth [6]. This prompted the SA Navy (SAN), in 2018, to partner with the SA Department of Defence Directorate of Information Warfare and Cyber Command Centre to develop a maritime cyber warfare strategy [7]. The strategy focused on cyber-related Research and Development (R&D) and solutions against cyber piracy and cyber terrorism in the SA territorial waters for enhanced national security. Thus, US Navy and SA Navy efforts are aimed at improving cyber warfare for enhanced national security [3].

In Nigeria, the rise in cyber activities brought about a corresponding increase in cyber threats. For instance, activities of cyber attackers led to the hacking and defacing of Defence Headquarters (DHQ) and the Nigerian Navy (NN) websites in 2012 [8]. The cyber attacks prejudice the image of the defence sector and, by extension, undermined national security

979-8-3503-2028-2/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00239

in Nigeria [9]. In response to the rise in cyber threats, the Federal Government of Nigeria (FGN) enacted the Cybercrime Prohibition and Prevention Act (CPPA) in 2015 [10]. The enactment of the CPPA was followed by establishing a Nigeria Computer Emergency Response Team (ngCERT) in the Office of the National Security Adviser (ONSA). The CPPA mandated organisations, including the NN, to always report cyber attacks to ngCERT. Accordingly, the Nigerian Army (NA) established the NA Cyber Warfare Command (NACWC). Although Nigeria's maritime assets are vulnerable to cyber attacks, the NN's cyber warfare capabilities in policy, infrastructure, and human capacity is at infancy stage.The purpose of this study is to proffer workable strategies to develop the capabilities of the NN in cyber warfare for enhanced national security in Nigeria [11].

The remainder of this paper is organized as follows. First, section II introduces the background of cyber warfare-related terms and national security. Next, section III explores literature related to cyber warfare in the navies and national security. Then, section IV proffered strategies to overcome the challenges militating against the development of cyber warfare in the NN for enhancing national security in Nigeria. Finally, it presents and analyses the data related to issues associated with cyber warfare in the NN and national security in Nigeria in Section V, along with conclusions in Section VI.

II. Background: Conceptual Definition

The key variables in this study are cyber warfare as the independent variable and national security as the dependent variable. First, these variables are conceptualized and the relationship between them is established subsequently.

A. Cyber Warfare

Cyber warfare can be defined as an activity of units, institutions, state or non-state actors or well-trained individuals operating within cyberspace using computer-related assets and infrastructure to conduct offensive and defensive operations. It can also be defined as a criminal intent conducted by state or non-state actors using computers to attack digital infrastructure [12] or obstruct other computers or networks within cyberspace for malicious, political, religious, military, economic or strategic motives [13]. This definition covers the offensive, defensive, criminal and incidental intents of cyber warfare by states or non-state actors [14].

B. Cyberspace

Cyberspace refers to the virtual computer world, more specifically, an electronic medium used to facilitate online communication. Cyberspace typically involves an extensive computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities [15].The technical wonder of cyberspace promises to bring together the two strands of the new naval power—economic gain and ideological conviction—in a creative way that will revolutionize the course of maritime combat in the future [3].

C. Cyber Warrior

A cyber warrior is a person who engages in cyber warfare, whether for personal reasons or out of patriotic or religious belief. Cyber warfare is pursued either to defend computers and information systems or attack them. Cyber-warriors may also discover more effective ways to secure a system by identifying its vulnerabilities through hacking and other methods and fixing them before other hackers do. He must possess special knowledge and expertise in computer networking, programming, and security. Some examples of the skills needed include information gathering skills and offensive/Defensive skills that are computer network operation which provides for Computer Network Attacks (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE) [16].

D. Cyber Dominance

The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. It can also be viewed as a situation in the cyber domain in which the desired representation of cyber reality is completely realized despite an adversary's efforts. Cyberwar is the struggle for cyber dominance, and all of the measures we employ to win the war fall under the umbrella of cyber warfare. [17]

E. National Security

Retter et al. [18] viewed national security as the blend of human, material resources, technology and military that might protect a state, its territories, and its people from physical assault by an external force. According to Retter et al. (2020), national security also protects economic and financial assets, maritime assets, commercial activities, and critical infrastructure from attacks emanating from foreign or domestic sources, which may undermine, erode, or eliminate these interests. Retter et al. (2020) further stated that the protection of maritime assets could be achieved through naval domain awareness and maritime policing operations. The view covers protecting a nation's interests using technology and naval operations, which are the thrust of this study. It is appropriate and therefore adopted for this paper.

F. Relationship between Cyber Warfare and National Security

The attributes of cyber warfare include using computer-related assets and infrastructure by well-trained individuals and state or non-state actors or institutions to conduct offensive, defensive, criminal and incidental intents by state or non-state actors in cyberspace. On the other hand, the attributes of national security include the protection of commercial and financial assets, the economy, and critical infrastructure from attacks through policing operations and maritime domain awareness. Effective conduct of offensive and defensive operations in cyberspace by well-trained individuals and institutions using robust infrastructure would protect commercial, financial assets, the economy, and critical infrastructure and improve maritime policing operations and maritime domain awareness of a state against adversaries. Conversely, the poor conduct of offensive or defensive operations in cyberspace could expose the state's systems and assets to cyber threats or cyber-attacks. This could influence critical infrastructure, commercial, and financial assets and undermine maritime domain awareness and policing operations. This implies that the development of cyber warfare by a state actor enhances national security, while poor or non-application of cyber warfare by a state actor undermines national security.

G. Nigerian Security and Cyber Warfare

The recorded cases of Denial of service and malware attacks, coupled with the rise in cyber-related threats in Nigeria as illustrated In Fig. 2, necessitated a response by the FGN with the formulation of the National Cybersecurity Policy and Strategy (NCPS) in December 2014 [8], [19], [20]. This was followed by enacting Cybercrime (Prohibition, Prevention, etc.) Act (CPPA) in 2015. In addition, the Act established ngCERT under the ONSA to counter cyber threats in Nigeria. However, it is noteworthy that the NN need to enact and draw her cyber warfare policy that could have provided guidelines for cyber warfare in Nigeria's Maritime Environment (NME) [21].

By 2018, Boko Haram had advanced using social media for cyberterrorism activities. As a result growing reliance on cyberspace by Boko Haram to conduct cyber terrorism, the NA became the first Service in the AFN to establish a NACWC as an institutional framework for cyber warfare. In the NME, non-state actors such as militants and sea pirates also utilise cyberspace for cyber-related threats in the Niger Delta region. The NN, however, does not have such an institutional framework that could have been used for coordinating and executing cyber warfare in the NME. In August 2020, NN witnessed cyber attacks that affected 1190 electronic mail (email) accounts. Two months after the email incident, precisely in October 2020, Nigeria saw an unprecedented protest by the youth tagged EndSARS. Initially, the protest was against police brutality in Nigeria until criminals, including hacktivist groups, hijacked it. One "hacktivist" group called Anonymous conducted cyber attacks against government websites during the EndSARS protests. In response to the email hacking and the threats from the "hacktivist" group, the NN initiated various engagements to enhace her cyber capabilities. Notably, some initiatives in capacity building of its personnel in cyber security is ongoig. Additionally, cyber awareness of personnel on cyber-related activities become part of the NN annual schedule calendar of events. Nevertheless, despite these efforts, the level of technical capacity in NN for cyber warfare operations remains a serious concern. The overview has brought out some key issues that need to be discussed.

III. Related Work

Several works of literature related to cyber warfare in the navies and national security. The majority of the literature differs in context and approach. Accordingly, the literature of Odeyinde (2018) [22], Greenberg (2019) [23] and Jasper (2020) [24] were reviewed. The aim is to identify gaps which the study intends to fill.

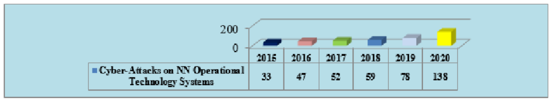


Fig. 1. Trend of Cyber Attacks on NN In The Last 10 Years

Odeyinde (2018) [22] stated that the Armed Forces of Nigeria (AFN)'s capacity to conduct cyber warfare was low. According to his research, the low capacity was due to the lack of a cyber warfare policy and inadequate human capacity, among other challenges. Therefore, the researcher recommended, among others, that the DHQ should formulate a cyber warfare policy. Although Odeyinde's work was on cyber warfare in the AFN, he focused more on cyber warfare in the NA and NAF than the NN, which is the focus of this study.

Greenberg (2019) [23], in his book titled *"Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers"*, revealed how the world started to witness cyber attacks. Some of the cyber-attacks identified by Greenberg include the 2014 cyber attacks against the US utility companies, NATO, and electric grids in Eastern Europe. He further mentioned the 2017 malware NotPetya unleashed by Sandworm in Russia's military intelligence agency to penetrate, disrupt, and paralyze some of the world's largest businesses, such as shipping companies in Ukraine. Unfortunately, although the author captured offensive cyber warfare by Russia's military, cyber operations in the maritime environment were not covered in the book, which is the focus of this study. .

Jasper (2020) [24],In his book titled *"Russian Cyber Operations: Coding the Boundaries of Conflict*", he noted that Russia utilized a hybrid of cyber attacks and information warfare to achieve its offensive operations, such as the 2016 US Presidential Elections interference and the 2017 NotPetya ransomware attack against Ukraine by Russia. Therefore, the author offers a strategy to the affected nations to develop robust plans of action critical to mount a durable defence against Russian cyber campaigns effectively. The author's work, however, does not provide how Russia's offensive cyber campaign affects other nations' maritime interests, which is the focus of this study.

IV. Cyber Warfare in the Nigerian Navy

The study has proffered strategies to overcome the challenges militating against the development of cyber warfare in the NN for enhancing national security in Nigeria. These include the formulation of NN cyber warfare policy, the creation of a cyber warfare directorate in the NN and special recruitment and training of naval cyber warriors. These strategies are discussed subsequently.

A. Formulation of Nigerian Navy Cyber Warfare Policy

Formulating an NN cyber warfare policy would mitigate the challenge of the non-existence of cyber warfare policy. The objective of this strategy is for the NN to have clear policy guidelines for developing and applying offensive and defensive cyber warfare. The policy would provide approaches for the NN to improve its capacity and readiness regarding workforce and institutional and infrastructural development for cyber warfare. The policy would also provide guidelines for the NN to articulate rules and regulations on using portable, electronic and other computer-related devices such as Universal Serial Bus (USB flash drives) to prevent cyber threats. In this regard, the policy could suggest computer specifications without serial ports for naval activities. In addition, the policy would provide guidelines on integrating Fourth Industrial Revolution (4IR) technologies or Industry 4.0 in cyber warfare in the NN.

Furthermore, the policy could provide guidelines on how NN could extend its cyber warfare operations to protect assets in the NME from cyber attacks for enhanced national security. The NHQ could task the Policy and Plans (PPLANS) Branch to formulate NN cyber warfare policy to cover all the areas as mentioned above. The resources required for developing the policy, particularly funding and logistics, could be provided by the NHQ. Specifically, the PPLANS could reach out to ONSA, DHQ, Ministry of Defence (MOD), and NACWC through Army Headquarters (AHQ) to understudy their cyber-related activities to facilitate policy formulation.

B. Nigerian Navy Cyber Warfare Directorate

From Fig. 1, the cyber attacks on NN operational technology rose from 33 in 2015 to 138 in 2020. The rise in malicious attacks undermined NN information security and national security in Nigeria. Additionally, for instance, the NN, NIMASA and NPA recorded several cyber attacks on their websites, respectively, disrupting activities that undermined national security as shown in Table I . The development of cyber warfare would enable the NN to conduct cyber warfare against hacktivists that intrude on its information system assets. This would improve maritime policing operations for enhanced national security in Nigeria. In addition, the creation of a cyber warfare directorate in the NN would mitigate the challenge of the non-establishment of the NN CWC. This strategy aims to have a dedicated institution charged with all activities related to cyber warfare in the NN and the NME in general. Considering cyber warfare's complex, secrecy and dynamic nature, creating a cyber warfare directorate would enable the NN to effectively conduct cyber warfare in the NME for enhanced national security in Nigeria. The Directorate would focus on proper planning and coordination of all activities related to cyber warfare and implement proposed policy documents on cyber warfare in the NN. The Directorate could be headquartered at NHQ and have units at all NN commands and other maritime agencies where NN is present. Therefore, the proposed organogram of the Directorate is designed. To achieve this, the NHQ could task the Training and Operation (TOPS) Branch to develop modalities for creating a cyber warfare directorate in the NN. The resources required for the creation of the Directorate, especially funding and logistics, could be provided by the NHQ.

C. Capacity Building of Naval Cyber Warriors

Special recruitment and training of naval cyber warriors would mitigate the challenge of limited cyber warriors. This strategy aims to ensure that personnel with requisite knowledge and skills in cyber warfare are recruited into the NN to improve the conduct of offensive and defensive cyber warfare operations in the NME. The special recruitment could involve the employment of civilians irrespective of age but have relevant certifications in ethical hacking, network and software security, and other related cyber professions. The NHQ could task the TOPS Branch to articulate the number of personnel with cyber warfare qualifications required to be recruited and trained for the proposed cyber warfare directorate every year. The funding for the TOPS to carry out this task could be provided by NHQ. The NHQ could, after that, reach out to MOD to forward the special recruitment and training of naval cyber warriors to the Presidency for approval. The special recruitment and training funding could be included in the NN annual budget approval and release.

V. Technical Discussion and Result

This section presents and analyses the data related to issues associated with cyber warfare in the NN and national security in Nigeria. The issues include cyber warfare policy and institutional framework, and technical capacity. These are discussed subsequently.

A. Cyber Warfare Policy

Cyber warfare policy outlines guidelines, direction, standardization and course of action for cyber warfare. In an ideal situation, the existence of a comprehensive and adequate cyber warfare policy would outline the procedures for cyber offensive and defensive operations in the maritime domain by the navies for enhanced national security [25]. In global best practices, navies such as the Iranian Navy, Russian Navy and US Navy have dedicated policies for cyber warfare in the maritime domain [26]. In the NN, the existing policy documents to possibly conduct cyber warfare are the NCPS 2021 and CPPA of 2015 [27]. Also, the NN relies on Signal Documents that are often sent to its formations for cyber-related programmes [28]. According to [29], the NN Signal Documents provided guidelines for the NN to respond to malicious attacks, especially computer viruses discovered from the 1190 email accounts affected in 2020. This also enabled the NN to carry out administrative functions towards defending the nation's territorial waters for enhanced national security. Despite this, [30] rated the existing policy documents as inadequate for cyber warfare in the NN. He noted that none of the policies captured cyber warfare, which is about conducting offensive and defensive operations, as the Iranian Navy practised in 2019 by shutting down US drones in the Strait of Hormuz through cyber offensive operations. O.B. Daji

TABLE I
Cyber Attacks on Government Websites in the Nigerian Maritime Environment

Year	2015	2016	2017	2018	201 9	2020
NN	17	24	31	37	41	45
NIMASA	7	13	20	22	25	29
NPA	5	9	16	18	21	25

[31] stated that the NN does not currently have a dedicated cyber warfare policy for offensive and defensive operations in the NME. F.F. Ogu [32] posited that the non-existence of NN cyber warfare policy is limiting the capacity of the NN to establish itself in cyberspace for the defence of NME towards enhanced national security. Cyber warfare policy is thus a significant consideration for cyber warfare in the NN towards enhanced national security in Nigeria. According to Ajijola [26], the non-existence of a cyber warfare policy has limited the capacity of the NN to respond to high-level cyber attacks from within and outside the country. He noted that in 2012, for instance, the NN website was hacked and defaced by Boko Haram agents without any resistance through offensive or defensive actions by the NN. This was due to a lack of cyber warfare policy that could have provided guidelines or incident response plans against cyber attacks. Ohunenese [33] also noted that the non-existence of cyber warfare policy has made it difficult for the NN to dominate the cyberspace of the NME in its constitutional role of defending Nigeria's territorial waters. As a result, maritime agencies have continued to record cyber-attacks. Ajijola [26] also stated that the non-existence of cyber warfare policy impedes the development of a mission, infrastructure, human resources, and People Process and Technology (PPT) for cyber warfare in the NN. He further noted that the non-existence of policy has led to a lack of clear provisions for the defence of e-commerce. The non-existence of a cyber warfare policy is thus a challenge to developing cyber warfare in the NN towards enhanced national security in Nigeria.

B. Institutional Framework

The institutional framework facilitates the conduct of cyber warfare operations for enhanced national security. Ideally, a navy requires adequate and functional institutions to conduct offensive and defensive cyber warfare operations, train personnel and embark on cyber awareness programmes. In global best practices, the Russian Navy, Chinese Navy and Iranian Navy have been developing quite impressive institutions to conduct cyber warfare against networks of other navies [34]. In addition, section 41 (1) of the CPPA 2015 empowered ONSA to provide technical support to the NN on cyber security. Also, the Directorate of Cyber Security (DCS) and Directorate of Cyber Operations Centre (DCOC) at the DSA protect NN from cyber attacks (M.S. Usman, personal communication, 5 January 2021).

Furthermore, the Directorate of Communication Information Technology (DCIT) at Naval Headquarters (NHQ) keeps an update on NN computer-related assets. The institutional measures aimed to improve the NN's cyber capabilities for enhanced national security.ONSA, DCOC and DCS were able to thwart a series of possible cyber attacks against NN networks. Similarly, relevant institutions were able to foil cyber attacks against NN networks in the NME. These efforts also prevented attacks against critical information systems for enhanced national security.

Notwithstanding these developments, one naval expert rated the institutional capacity for NN cyber warfare inadequate. He noted that the NN does not have a Cyber Warfare Command (CWC) like that of the NACWC to coordinate all activities related to cyber warfare for enhanced national security. He stated that the existing institutional framework is inadequate for effective cyber warfare in the NN. The institutional framework is, therefore, crucial to cyber warfare in the NN for enhanced national security in Nigeria. Daji (2021) noted that the non-establishment of CWC has made it difficult for the NN to conduct offensive and defensive cyber operations. According to Moses (2020), the non-establishment of CWC has made it difficult for the NN to combat cyber attacks from pirates, pipeline vandals, "hacktivists", and other threats in the NME. Another expert stated that the non-establishment of CWC has made it difficult for the NN to coordinate all activities related to cyber warfare in the NME. As a result, the situation has continued to undermine maritime security and, by extension, national security in Nigeria. Non-establishment of CWC is thus a challenge of developing cyber warfare in the NN for enhanced national security in Nigeria.

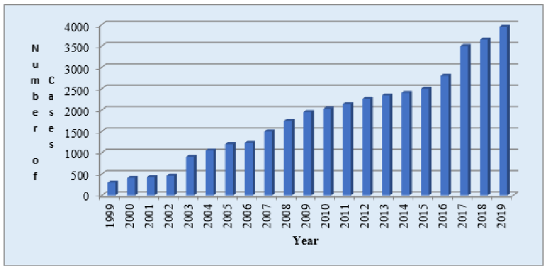


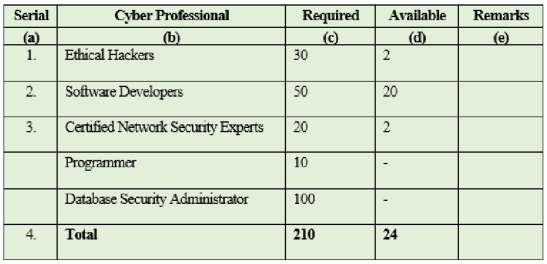
Fig. 2. Cyber Related Attacks In Nigeria

C. Technical Capacity

Technical capacity provides qualitative manpower needed for cyber warfare in an organization. Ideally, effective technical capacity guarantees the requisite know-how in cyber operations. Globally, navies train their personnel in ethical hacking and software development for cyber warfare. For example, according to [32], in 2015 and 2016, NN trained 2 of its personnel in cyber security. As a result, the personnel could manage NN ICT assets from cyber attacks. Also, according to

[35] in 2019, the NN trained 2 personnel on ethical hacking to improve cyber warfare capability.

Consequently, the NN personnel were able to block over 2302 possible attacks on NN email networks [36]. As of January 2021, the NN had 4 personnel certified in cyber security for cyber warfare operations. However, it noted that the technical capacity at NN is only suited to protect ICT assets from cyber-attacks and not adequate for offensive operations, which are crucial for cyber warfare. He further noted that the NN required at least 30 cyber experts or cyber warriors but had only 4 personnel trained in cyber security. This implies that the technical capacity is inadequate for cyber warfare in the NN for enhanced national security in Nigeria as shown in Fig. 3. The NN's technical expertise for cyber offensive and defensive operations is insufficient. Technical capacity is, therefore, a major consideration for cyber warfare in the NN towards enhanced national security in Nigeria. Adaji (2021) [27] attributed the inadequacy to limited cyber warriors such as ethical hacking, network security, information security experts and other cyber professionals. According to Bashir (2021) [35], as of February 2021, NN had trained only 3 warriors comprising 2 ethical hackers and information security experts out of at least 30 cyber warriors required, as shown in Fig. 3. He noted that the situation had created gaps in certified information systems security and ethical hacking expertise. The situation has made it possible and even easy for hackers to penetrate the NN assets without any resistance. Details of cyber expertise required for cyber warfare in the NN are shown in Fig. 3. This has undermined maritime policing operations and national security in Nigeria. Limited cyber warriors, therefore, constitute a challenge to cyber warfare in the NN for enhanced national security in Nigeria. The issues and challenges discussed have made it necessary to consider the implications of cyber warfare in the NN for enhanced national security in Nigeria.



Serial	Cyber Professional	Required	Available	Remarks
(a)	(b)	(c)	(d)	(e)
1.	Ethical Hackers	30	2	
2.	Software Developers	50	20	
3.	Certified Network Security Experts	20	2	
	Programmer	10	-	
	Database Security Administrator	100	-	
4.	**Total**	**210**	**24**	

Fig. 3. NN Cyber Workforce

VI. Conclusions

The study appraised cyber warfare in the NN and national security in Nigeria. The key variables established a direct relationship between cyber warfare and national security. The study overviewed cyber warfare and national security in Nigeria and brought about cyber-related threats to NN and DHQ by Boko Haram elements. The study thus observed that the NN could not develop its cyber warfare effectively because the cyber warfare policy to provide guidelines remained unavailable. Similarly, the NN did not have the institutional framework for executing cyber warfare operations. Furthermore, technical capacity was found inadequate, hindering the development of cyber warfare in the NN for enhanced national security in Nigeria. Data analysis showed that developing cyber warfare in the NN has positive implications for enhanced national security in Nigeria. These implications include the protection of critical information infrastructure and maritime policing operations. However, identified challenges of developing cyber warfare in the NN towards enhanced national security in Nigeria include the non-existence of cyber warfare policy, non-establishment of CWC and limited cyber warriors. The study proffered some strategies to overcome the challenges of developing cyber warfare in the NN for enhanced national security in Nigeria. The NHQ could formulate NN cyber warfare policy to provide guidelines for executing cyber warfare by the NN towards enhanced national security in Nigeria. The NN could also create a cyber warfare directorate for an adequate institutional framework for cyber warfare. Special recruitment and training of naval cyber warriors would improve the NN's technical capacity for cyber warfare.

A. Disclaimer

This paper represents the authors' opinions and is the product of intellectual research. It is not meant to represent the position or opinions of the NN, AFN or its Members, nor the official position of any staff members

References

[1] D. Serpanos and T. Komninos, "The cyberwarfare in ukraine," *Computer*, vol. 55, no. 7, pp. 88–91, 2022.

[2] A. Hussaini, B. Zahran, and A. Ali-Gombe, "Object allocation pattern as an indicator for maliciousness-an exploratory analysis," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 2021, pp. 313–315.

[3] M. J. Flynn, "Cyberspace and naval power," *Journal of Advanced Military Studies*, vol. 13, no. 2, pp. 167–181, 2022.

[4] D. M. Activity, "U.S. Fleet Cyber Command/U.S. TENTH Fleet Search Fleet Cyber CommandU.S. TENTH FLEET:Search," https://www.fcc.navy.mil/, 2022, [Online; accessed 3-November-2022].

[5] E. Castillo, "Information sharing within the fltcybercom/c10f organization," Naval Postgraduate School, Tech. Rep., 2020.

[6] K. Muronga, M. O. Letebele, P. L. Binda, and S. M. Smith-Godfrey, "Towards secure maritime transport in south africa: An investigation of cybersecurity readiness of organisations," 2019.

[7] D. Reva, "Maritime cyber security getting africa ready," *ISS Africa Report*, vol. 2020, no. 29, pp. 1–16, 2020.

[8] K. OMONOBI, "Terrorists hack into DHQ, Navy websites," https://www.vanguardngr.com/2012/09/terrorists-hack-into-dhq-navy-websites/, 2012, [Online; accessed 3-November-2022].

[9] C. N. I. B. Yusuf *et al.*, "Cyber threats and national security in nigeria: Challenges and options," *NDC E-JOURNAL*, vol. 13, no. 2, pp. 131–146, 2014.

[10] A. Alasa, "A legal analysis of cybercrimes and cybertorts: Lessons for nigeria," *Available at SSRN 3560905*, 2019.

[11] B. Sule, U. Sambo, and M. Yusuf, "Countering cybercrimes as the strategy of enhancing sustainable digital economy in nigeria," *Journal of Financial Crime*, no. ahead-of-print, 2022.

[12] A. Hussaini, C. Qian, W. Liao, and W. Yu, “A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems,” in *2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*. IEEE, 2022, pp. 597–604.

[13] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[14] P. Akarcay and G. Ak, “Rethinking cyber warfare: Timeless, normless and unconstrained,” *IKSAD Journal*, vol. 4, no. 9, pp. 195–214, 2018.

[15] L. C. T. D. Howard and J. d. A. da Cruz, “Like the sea, so cyberspace: A brief exploration of establishing cyberspace norms through a maritime lens,” *Journal of Advanced Military Studies*, vol. 13, no. 2, pp. 142–153, 2022.

[16] M. L. Ferretti, T. Richards, J. G. Irons, and K. Richards James, “The dimensionality of the cyber warrior,” in *International Conference on Human-Computer Interaction*. Springer, 2022, pp. 326–339.

[17] M. P. Fischerkeller, E. O. Goldman, and R. J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press, 2022.

[18] R. Lucia, “Relationships between the economy and national security:Analysis and considerations for economic security policy in the Netherlands,” ”https://www.rand.org/pubs/research$_reports/RR4287.html/$”$, year = 2020, note = $”$[Online; accessed14 - January - 2022]$”.

[19] M. A. Baballe, A. Hussaini, M. I. Bello, and U. S. Musa, “Online attacks types of data breach and cyber-attack prevention methods,” *Current Trends in Information Technology*, vol. 12, no. 2, pp. 21–26p, 2022.

[20] D. G. DATONG, “Cyber-terrorism: Nigeria’s payment system infrastructural readiness,” 2018.

[21] O. Oke, “An appraisal of the nigerian cybercrime (prohibition, prevention etc) act, 2015,” *Available at SSRN 2655593*, 2015.

[22] O. Olufemi Babajide, *Cyber Warfare and National Security in Nigeria: The Armed Forces of Nigeria in Perspective*. A Research Project Submitted to National Defence College Nigeria., 2018.

[23] A. Greenberg, *Sandworm: A new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers*. Anchor, 2019.

[24] S. Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. Georgetown University Press, 2022.

[25] S. Garba, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[26] A. Ajijola, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2021.

[27] A. Adaji, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2021.

[28] O. S.O, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[29] M. Oamen, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[30] E. Eji, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[31] D. O. B, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[32] F. Ogu, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[33] S. Ohunenese, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.

[34] R. D. Thiele, “Game changer–cyber security in the naval domain,” *The Institute for strategic, political, security and economic consultancy (ISPSW), Berlin, Germany*, 2018.

[35] B. M.M, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2021.

[36] S. I. A, “Cyber Warfare and National Security: Imperatives for the Nigerian Navy,” Personal Communication, 2020.