CYBER WARFARE AND TERRORISM: NIGERIAS PREPAREDNESS FOR ANY EVENTUALITY

Lakan Muhammed Zakariyyah•
Onasanya Precious Oluwapelumi•
Leke Mercy Fikayo•
Taye Z. Kabirat •
Aladodo A. Nurudeen•
Rahmat M. Imam•

Abstract

America and Israel are currently at war with Iran, Russian and Ukraine are also at war. Afghanistan is currently in shambles. Across African, especially in Nigeria, banditry, terrorism and cyber war fare is at an alarming rate. Cyber warfare has become a well-established tool in the 21st-century arsenal, employed for both offensive and defensive operations. It offers a state the potential to gain strategic advantage over adversaries without resorting to traditional kinetic warfare. Cyber-attacks prioritise achieving objectives over the specific methods employed. Using doctrinal research method, this paper undertakes a critical evaluation of the preparedness in term of the effectiveness of existing legal instruments in regulating cyber warfare and terrorism in Nigeria. Based on the analysis done in the paper, the paper finds that the current legal framework is ill-equipped to effectively regulate the vices in Nigeria. Specifically, the paper discovers that, the existing instruments for combating cyber warfare in Nigeria were mainly designed for traditional kinetic conflicts which contemporarily fail to adequately address the unique characteristics and complexities of cyber-attacks. Based on this, this paper concludes that the Nigerian government efforts against cyber warfare and terrorism are grossly inadequate. To check this, the paper among others recommends for the review/amendment of the existing legal instruments designed to regulate cyber warfare and terrorism in Nigeria.

Keywords: Legal Instruments, Cyber Warfare, Terrorism, Insurgency, Cyber-attacks

Introduction

The importance of technology in the world economy cannot be over emphasised, it forms an integral part of nation building and economy progress. Institutions, both governmental, individual and organisations are using technology especially cyber tools in their daily activities. It is consequent upon this that the new trend of cyber warfare which is a new way of waging war through technology has taken course in recent time, technology has now become the main tool and strength to nations power. This however has steered concern and fear for nations believing that as long as there is emerging cyber technology, nations will always be at war and Information technology is the main battle field.

Technology in the words of Anita has made such immense progress in the 21st century that it's now absolutely essential for governments, organisations, institutions, and even individuals in their daily lives.[1] Therefore, digital age has introduced a new and undeniable threat: cyber warfare. However, with information technology and the internet becoming central to national power, cyber-

[1]Anita Nwotite, Henry Chukwudi Okeke & Precious Orji, 'Applicability of International Humanitarian Law to Cyberwarfare' (2024) (2024) (8) (2) *Irish International Journal of Law, Political Sciences and Administration* 16.

attacks have become a constant concern, prompting nation-states to arm themselves in the digital battlefield. The 21st century has witnessed the increasing potential of such technology for military applications. This transformation has impacted the actors involved in conflict, the strategies employed, and the pervasive integration of technology into all aspects of armed conflict.[2]Modern societies are particularly vulnerable to cyber warfare due to their reliance on interconnected global and domestic information structures. A survey of major internet operators worldwide revealed a significant rise in sophisticated and malicious cyber-attacks.

Unlike traditional warfare, cyber warfare offers a diverse arsenal of attack methods, including IP spoofing, Trojan horses, Distributed Denial-of-Service (DDoS) attacks, and logic bombs. These new tools were employed, for instance, in the 2007 and 2008 DDoS attacks that crippled Estonia and Georgia respectively, incidents linked to Russia on the so-called 'digital battlefield'. Although Russian authorities had the power to investigate and prosecute these cyber hostilities, they chose not to act. Similarly, in February 2022, a group believed to be linked to Russia, the 'Actinium Group,' launched cyber-attacks against Ukrainian military and government targets.[3] The United States responded by sending cyber experts and resources to bolster Ukraine's cyber defences in the face of this cyber weaponry.[4]

These incidents highlight the real threats posed by this new domain of warfare. They offer a unique opportunity to study how cyber activities might unfold in a protracted conflict and how they influence battlefield dynamics.[5] As nations become increasingly reliant on networked infrastructure and cyberspace for critical functions, the potential targets for cyber-attacks expand significantly. Unfortunately, despite the introduction of advanced 'cyber weapons,' there is a lack of international consensus or clear rules governing their use in warfare. This ambiguity arguably confirms that the world is already experiencing cyber warfare.[6] For example, in 2009, a cyber-spy network called 'Ghost-Net' accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. Ghost-Net was reported to originate in China, although that country denied responsibility and finally in 2013, Germany revealed the existence of their 60-person computer network Operation unit. This makes it difficult for regulators to keep up with the latest development.[7]

Another challenge arises from the borderless nature of cyberspace, which renders a 'hands-off' policy potentially disruptive to cross-border transactions. Most cyber operations fall outside the legal definition of 'use of force' under *jus ad bellum.*[8] While attempt have been made to define proportional response through analogy, this approach risks creating definitional ambiguity in other contentious areas of international relations. Furthermore, there is a lack of uniformity among cyber actors regarding how to regulate the cyber domain.[9] For example, U.S. and Russia differ on a treaty for cyberspace, in the sense that while Russia favours cyber treaty, the U. S. vehemently opposed it.

---

[2]Heather Harrison-Dinniss, 'Participants in Conflict-Cyber Warriors, Patriotic Hackers and the Laws of War' in Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, Leiden, 2013) 252.

[3] Reka Szabó, 'Cyber Warfare in the Ukrainian Conflict a Determinant of the Outcome of the War?' (2022) (1) (1) *Verona Journal* 4; Microsoft Security Blog, 'Actinium Targets Ukrainian Organizations.' (2022) <www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/>accessed 11 August 2023.

[4]Ahmad Mohee, 'Cyber War: The Hidden Side of the Russian-Ukrainian Crisis' **(**2022)**<**https://osf.io/2agd3/download/?format=pdf>accessed 11 August 2023; Väljataga, A., *Cyber Vigilantism in Support of Ukraine: A Legal Analysis* (NATO Cooperative Cyber Defence Centre of Excellence Publications Tallinn 2022) 5.

[5]Tae Eun Song, *Cyber Warfare in the Russo-Ukrainian War: Assessment and Implications* (Institute of Foreign Affairs and National Security Soul South Korea 2022) 1.

[6]The German Intelligence Agency, "BND, Announced it was Seeking to Hire 130 'Hackers' for new Cyber Defence Station Unit" <https://searchsecurity.techtarget.com/definition/cyber warfare> accessed 11 August 2023.

[7] Olipede, & Chukwuonye*op.cit*. at 83.

[8] Vida MAntolin-Jenkins, 'Defining the Parameters of Cyber War Operations: Looking for Law in all the Wrong Places?' (2005) 51 *Naval Law Review* 299.

[9]Bilyana *Lilly* & Joe *Cheravitch*, The Past, Present, and Future of Russia's Cyber Strategy and Forces' in Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky, G. (eds.) *2020 12th International Conference on Cyber Conflict* **(**NATO CCDCOE Publications, Tallinn, 2020) 137.

The issue now is, what will be the hope of third world country like Nigeria when courtiers like America, United States of America and Russia are opposing the centrally regulation and control of what could later become a global catastrophic mechanism and instrument of destruction.

Divided into five sections, section two that follows the general introduction discusses cyber warfare in history, in that section, the paper also examines the changing phase from kinetic warfare to cyber warfare. In section three, the main discussion is on Nigerian cyber command (nigcybercom) activities; while in section four, it is the discussion on the terrorism and cyber warfare in Nigeria; its changing landscape as well as the analysis of whether Nigeria is winning or losing cyber warfare and terrorism that is the nucleus of discussion therein. Conclusion and recommendations constitute the final part of the paper in section five.

Cyber Warfare in History

The rise of Information and Communication Technologies (ICTs) has woven them into the fabric of human life. Their pervasiveness, coupled with society's growing reliance on cyberspace, elevates the cyber domain to a critical pillar of national function and citizen well-being.[10]This ubiquitous presence, however, has also sparked a shift in the purpose of the cyber realm, transitioning it from a facilitator of daily needs to a potential instrument of military power.

The promise of cutting through the fog of war in combat, long a dream of military strategists, fueled the concept of a Revolution in Military Affairs (RMA) built on Network-Centric. This vision, however, had not yet anticipated the rise of a new battlefield: cyberspace, while its roots can be traced back to the development of radar and Electronic Warfare Technologies (EWT).[11]The rapid proliferation of cyber-attacks has transformed cyberspace into the 'fifth dimension of war,' forcing nations to adapt their defences accordingly.

It is important to note that early cyber-attacks, emerging in the late 1980s alongside the nascent internet, were not initially viewed as acts of war or formal cyber conflict. Instead, they evolved organically alongside rapid technological advancements, often blurring the lines between espionage, hacktivism, and true warfare.[12]

Changing phase from Kinetic Warfare to Cyber Warfare: Throughout history, the battlefields where conflicts unfolded were largely confined to two distinct physical spaces: land and sea. For millennia, land served as the primordial arena of combat, where clashing armies tested their might with ever-evolving weaponry and tactics.[13]The sea, with its unique challenges and opportunities, emerged as a distinct war fighting space alongside its terrestrial counterpart.[14] The Maritime domain includes the oceans, seas, bays, estuaries, islands, coastal areas, including the littorals[15] which fall under sea as part of the kinetic warfare.

The battlefield once confined to the clash of steel on land and the roar of cannons at sea, has undergone a dramatic transformation in the wake of technological advancements. New dimensions have emerged, expanding the realm of conflict beyond physical spaces and into the ethereal realms of air and cyberspace.[16]In the 21st century, the battlefield has transcended the physical realm to encompass the ethereal expanse of cyber space. This interconnected web of information infrastructures, encompassing the internet, telecommunications networks, computer systems, and

[10]Kosmas *Pipyros*, Lilian *Mitrou*, Dimitris *Gritzalis*, &Theodore Apostolopoulos, *Cyber Operations and International Humanitarian Law: Obstacles in Applying International Law Rules in Cyber Warfare* (Information Security & Critical Infrastructure Protection Laboratory publishing Athens 2019)1.
[11]ibid.
[12]ibid.
[13]Steve *Winterfeld* & Jason Andress *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Elsevier Inc. United State 2013) 25.
[14]ibid.
[15] Deparment of Defence, 'Joint Electronic Library' (2019) <http://www.dtic.mil/doctrine/>accessed 18June 2022.
[16]Ibid.

embedded devices, has become a critical battleground. Its strategic significance necessitated its recognition as a distinct war fighting domain within the broader information environment.[17]

The Geneva Conventions, their Additional Protocols, and other existing laws under IHL primarily address the kinetic warfare domains. These domains, encompassing land, sea, air, and space constitute the traditional battlefields where physical conflict has historically unfolded.

Land Warfare

The use of land as a battleground has evolved progressively. Stone clubs gave way to spears, offering greater reach and power. Bows then surpassed spears, allowing for ranged attacks. The introduction of mounted troops granted a significant advantage over foot soldiers, further amplified by the invention of the stirrup.[18] Firearms, artillery, tanks, and machine guns revolutionized warfare, dramatically increasing the rate and range of casualties inflicted by armies, so also the use of landmine. These land war technologies have unfortunately been employed in numerous international and non-international conflicts across the globe, including Sub-Saharan Africa, the former Soviet Union, the Balkans, parts of Asia, the Middle East, and the Arab-Israeli conflict.[19]

The history of violence in Nigeria's northeast, particularly the conflict involving Boko Haram, presents a complex case of kinetic warfare within a domestic context. Boko Haram, initially known as 'Sahaba,' emerged in 1995 under the leadership of Abubakar Lawan.[20]After Lawan's departure for studies in Saudi Arabia, the group's leadership transitioned to Mohammed Yusuf, a self-proclaimed spiritual leader. Consequently, leaving the old clerics to concede the group's leadership to a self-proclaimed Nigerian spiritual leader named, Mohammed Yusuf.[21]Since its origins in Borno State, Boko Haram's activities have inflicted widespread suffering and instability across the region.[22]

The Nigerian government's primary strategy against Boko Haram has been a counter-terror military approach. Security forces, supported by civilian volunteers known as 'Civilian JTF' and local hunters, engage in armed confrontations with the insurgents his approach exemplifies the characteristics of kinetic warfare, with direct use of force on land as the primary means of conflict resolution.

It is important to note that legal frameworks like Additional Protocol II to the Geneva Conventions address the application of common Article 3 in non-international armed conflicts. However, the Protocol's scope and conditions remain specific to certain situations and cannot be applied universally to define all such conflicts.[23] Article 1 of the Additional Protocol II provides that:

> 'This Protocol shall apply to all armed conflicts which are not [of international character] and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.

Boko Haram's military capabilities have undeniably evolved over time, raising concerns about its potential transition towards a more conventional fighting force. While its exact size remains

---

[17]Department of Defence, 'Dictionary of Military and associated terms, DoD' (2010) <http://www.dtic.mil/doctrine/dod_dictionary/index.html> accessed 18 June, 2025

[18]Ibid.

[19]Kevin *P. Clements*, 'The Causes and Prevention of Violent Conflict' in *Dolgopol* Ustinia & *Gardam* Judith(eds.) *The Challenge of Conflict International Law Responds* (Martinus Nijhoff Publishers, Boston, 2006) 6.

[20] Itumo, A., & Nwefuru, N. H., 'Nigerian State and Responses to Plights of Persons Internally Displaced by Boko Haram Insurgents: Implications for Socio-Economic and Political Development' (2016)6(15) *Research on Humanities and Social Sciences* 28.

[21] ibid.

[22] Lenshie, N. E., & Yenda, H. B., 'Boko Haram Insurgency, Internally Displaced Persons and Humanitarian Response in Northeast Nigeria' (2016) 4(8) *The International Journal of Humanities & Social Studies* 143.

[23] Melzer, N., *International Humanitarian Law: A Comprehensive Introduction* (International Committee of the Red Cross, Geneva, 2016) 68.

difficult to pinpoint, it is estimated to possess thousands of armed personnel. The group has also reportedly established specialized units focused on bomb-making and other tactical operations.[24]Furthermore, reports suggest the presence of increasingly sophisticated weaponry within Boko Haram's arsenal, including armored vehicles, rocket launchers, anti-aircraft guns, and various firearms.[25] The study asserts that such an array of weaponry aligns with the characteristics of kinetic warfare, which emphasizes direct force application on land.

Sea Warfare

The open sea shares certain characteristics with cyberspace, both being vast and offering relative ease of movement for vessels or data, making it challenging for defenders to pinpoint potential threats.[26] When considering hostilities at sea, the rules diverge from land warfare due to several factors. All states have the right to navigate the high seas, and navies have historically utilized this freedom for various purposes, including disrupting enemy trade and neutral trade with the enemy.

It is significant that most international instruments regulating naval warfare emerged in the late 19th and early 20th centuries. These include, the Paris Declaration of 1856 respecting Maritime Law abolished privateering and established rules for blockades as well as prizes. Eight of the 1907 Hague Conventions, a few of which still have some relevance today, tackle different aspects of naval warfare: Hague Convention (VII) relating to the Conversion of Merchant Ships into War-Ships; Hague Convention (VIII) relative to the Laying of Automatic Submarine Contact Mines; Hague Convention (IX) Concerning Bombardment by Naval Forces in Time of War; Hague Convention (XI) Relative to Certain Restrictions concerning the Exercise of Capture in Naval War; and Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War.[27]

Air Warfare

Airpower, much like cyberspace, is a domain heavily influenced by technological advancements. Initially employed for reconnaissance in the late 19th century, airpower evolved into a powerful strike force in the 20th century. More recently, it has played a crucial role in the 'zero-casualty' war doctrine embraced by the US and its allies, seeking to minimize ground troops' involvement and prioritise airstrikes.[28]Examples of airpower in action include the 2003 invasion of Iraq, the Syrian Civil War also witnessed the devastating use of airpower in the destruction of Aleppo in 2012,[29] the 2023 Air strike of the State of Israel against Hamas in the Palestine[30]Currently, the Nigerian military employs airpower in its fight against Boko Haram in the country's northeast.[31]

The development of airpower has significantly impacted warfare, with the introduction of cluster munitions marking a potent addition to its kinetic arsenal. These weapons, deployed from aircraft or ground launchers, release numerous explosive sub-munitions that scatter over wide areas.[32]However, their indiscriminate nature and high dud rates pose significant risks to civilians and hamper post-conflict reconstruction for years after hostilities cease.[33]

Unlike naval warfare, the legal framework governing air warfare largely aligns with traditional land warfare principles, particularly regarding target selection, proportionality, and precautions in

---

[24]James *Archibong*& Michael *Ibanga* 'The Boko Haram Insurgency: Characterization and Implications Under Municipal and International Laws' in John-Mark *Iyi* and Hennie *Strydom* (eds.) *Boko Haram and International Law* (Springer International Publishing Switzerland 2018) 144.

[25]ibid.

[26]Ibid

[27]ICRC, 'Treaties, States Parties and Commentaries'<https://ihl-databases.icrc.org/ihl>accessed 26June, 2022.

[28]ibid.

[29]The Gulf War in 1991, the 1999 strikes against former Yugoslavia*; ibid.*

[30]Jim Zanotti, Jeremy M. Sharp, & Christopher M. Blanchard *Israel and Hamas October 2023 Conflict: Frequently Asked Questions (FAQs)* (Congressional Research Service, the United States, 2023) 1.

[31] Ibid

[32] Ibid

[33] To address these dangers, 2008 Convention on Cluster Munitions prohibits the use, production, acquisition, stockpiling, retention and transfer of cluster munitions; Article 1, Oslo Convention on Cluster Munitions, 2008.

attack.[34]This emphasis on protecting civilians and minimizing unnecessary suffering applies to all attacks on land, regardless of the launch platform.[35]

The legal instruments specifically dealing with the subject of air warfare include the Hague Declaration of 1907.[36]While the 1907 Hague Declaration prohibited projectiles from balloons due to concerns about targeting precision, it does not explicitly ban aerial bombardments in today's context.[37]Subsequent efforts like the Hague Rules further clarified the legal framework, though they never achieved formal ratification. Nevertheless, many of their provisions are considered customary international law, shaping the contemporary legal landscape for air warfare.[38]Furthermore, Additional Protocol I to the Geneva Conventions specifically addresses the application of existing laws and principles to air warfare, providing further clarity on permissible and prohibited conduct.[39]

Space Warfare

Space, like cyberspace, is often considered an essential enabler for other warfare domains.[40]It provides crucial infrastructure for various critical functions such as long-distance communications, command and control (C2), intelligence gathering through surveillance and reconnaissance (ISR), navigation with Global Positioning System (GPS), and even communication for phones, radios, television, and financial transactions. Additionally, space-based technologies offer vital capabilities for wide-area reconnaissance, weather forecasting, mapping, and commercial imaging.[41]This virtual space, independent of physical borders, fosters global interconnectivity, raising important legal questions about the applicability of the Geneva Conventions and their Additional Protocols to space warfare.[42]Furthermore, space serves as a prime example of integrating new technologies into the armed forces, becoming so intertwined with other domains that they have become dependent on it.

The next chapter in warfare may involve the fusion of traditional and cyber domains for offensive operations. For instance, Israel's use of a cyber-attack against Syrian space defence radar systems, creating a false image of a clear sky, effectively masked a subsequent kinetic attack.[43]

Cyber Warfare

The future of warfare may witness a significant shift from kinetic force to cyber warfare, potentially orchestrated within an artificial cyberspace domain.[44] While traditional, kinetic attacks may still play a supporting role, the emphasis could lie in sophisticated cyber operations.[45] This emerging and rapidly evolving domain presents significant advantages for technologically advanced belligerents, potentially offering a cost-effective and resource-efficient alternative to conventional military campaigns.[46]Cyberspace is increasingly recognized as a potential 'battle-space,' a virtual arena where states and non-state actors can engage in competition and power struggles.[47] This recognition underscores the potential for cyber operations to become the primary mode of conflict in the future.[48]

---

[34]Ibid
[35]Ibid
[36]Hague Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons (18 October 1907) 1 US Treaty Series 739.
[37]Rules Concerning the Control of Wireless Telegraphy in Time of War and Air Warfare (Drafted by a Commission of Jurists at the Hague, 1922–1923).
[38]Ibid
[39]Article 49(3), Additional Protocol I to the Geneva Conventions, 1945.
[40]Ibid
[41]ibid.
[42]ibid.
[43]Gary D Solis,'Cyber Warfare' (2014) 219 *Military Law Review* 7.
[44]Ibid
[45] ibid.
[46]Christina E *Bailey*, 'Cyber Warfare, An Emerging Area of State Practice' (2015) 8(1) *Creighton International and Comparative Law Journal*9.
[47]Adriano *Iaria*, *E-Emblems: Protective Emblems and the Legal Challenges of Cyber Warfare*
[48] ibid.

Cyberspace presents a unique challenge for military operations due to its inherent interconnectedness with civilian infrastructure. Military networks often rely on civilian infrastructure like undersea cables, satellites, and communication nodes.[49] Conversely, civilian systems like navigation, traffic control, and even logistical networks share the same web and communication channels as some military operations.[50]Civilian logistical chains for essential supplies, businesses, and critical infrastructure heavily rely on the same web and communication networks as some military operations.[51]This interconnectedness blurs the lines between civilian and military cyber-infrastructures, making it extremely difficult to differentiate between them and attribute responsibility for cyber-attacks.[52]

The rapid evolution of cyber skills and knowledge has outpaced the development of legal frameworks to address cyber warfare. While existing armed conflict laws attempt to grapple with this new domain, they have not yet fully adapted to its complexities. Establishing regulatory mechanisms for offensive cyber capabilities and effective verification regimes remains a significant hurdle.[53]

Nigerian Cyber Command (Nigcybercom)

In response to the growing importance of cyberspace, the Nigerian military announced plans in 2016 to establish the Nigerian Cyber Command (NIGCYBERCOM).[54]This initiative reflects the recognition of cyberspace as a new operational domain for modern warfare.[55] The Nigerian military has outlined the intended functions of NIGCYBERCOM, which include monitoring cyberspace for threats, defending Nigerian networks, and undertaking counter-attacks.[56]

In 2018, the former Nigerian President Buhari approved the establishment of the NIGCYBERCOM and in compliance with the presidential directive, the former Nigerian Chief of Defence Staff, Lieutenant General Tukur Yusuf Buratai established NIGCYBERCOM.[57] According to the Nigerian military "With the establishment of the Command the fight against terror, insurgency, armed banditry, pipeline vandalism, herdsmen and militia killings would be checkmated since real-time information would be provided to the fighting forces and commanders in the field from the highly sophisticated equipment already procured."[58]

To strengthen the newly established NIGCYBERCOM, the Nigerian military has revealed that NIGCYBERCOM is comprised of an initial 150 specially trained information and communications technology (ICT) officers and personnel drawn from across all Corps and Services of the Nigerian Army. It adds that "The Headquarters of the Cyber Warfare Command would be in Abuja even as it would also have other units in each of the geo-political zones. It is the first of its kind in Africa. Moreover, plans have been concluded to send officers and soldiers of the command to attend various courses in Countries like US, Russia and the UK."[59]

In 2021, the NIGCYBERCOM established the Nigerian Army Cyber Warfare School (NACWS) and according to a former Chief of Army Staff (COAS), Lieutenant General Faruk Yahaya: 'This development has brought to the fore, the need to properly defend the territorial integrity

[49]International Committee of the Red Cross (ICRC) 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (2015) (97)(900) *International Review of the Red Cross*1477.
[50]ibid.
[51] ibid.
[52]Ibid
[53]ibid.
[54]Flaherty, K., 'The Nigerian Cyber Warfare Command: Waging War in Cyberspace' (2018),<forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/#1e48436b2fba>accessed 1 September 2025.
[55] ibid.
[56] ibid.
[57] Kingsley Omonobi, 'Nigerian Army's Cyber Warfare Command Begins Operation' (2018) <<https:/nigerian-army's-cyber-warfare-command-begins-operation>accessed 1 September 2025.
[58] ibid.
[59] ibid.

of the nation in the cyberspace, hence, the establishment of the Nigerian Army Cyber Warfare Command (NACWC).'[60]

It is worth noting that the Digital Literacy, Internet and Core Computing Certification Course (IC3) forms an integral part of the NACWS curriculum.[61]The inaugural course enrolled 30 students drawn from various Army units within Abuja.[62]

Operation of Nigcybercom: NIGCYBERCOM has a dual mission: to undertake offensive cyber operations against cybercriminal and terrorist groups both within and outside Nigeria, and to defend critical national infrastructure from cyber-attacks.[63]

Cyber Operations against Nigeria: Boko Haram is a significant cyber threat to Nigeria's critical national infrastructure, employing tactics similar to those used by the Taliban in Afghanistan.[64]These tactics include recruiting online followers, targeting military systems, and website defacement.[65]Boko Haram's reliance on the internet for its activities creates vulnerabilities, such as opportunities for Nigerian authorities to disrupt their operations.[66]

Boko Haram also exploits cyberspace to spread religious extremism, incite violence, and coordinate attacks.[67]While the extent of their financial resources dedicated to cyber activities remains unclear, their online presence suggests an effort to recruit skilled individuals for cyber-attacks.[68]In essence, Boko Haram weaponises the ICT to further their violent agenda.[69]

Boko Haram's ability to access sensitive information remains unproven and there's limited evidence to support claims of them possessing 'world-class decryption technology.'[70]However, Boko Haram does leverage cyberspace to spread propaganda, recruit fighters, and potentially coordinate attacks because unlike traditional battlefields, cyberspace requires no specialised equipment.[71] Other groups in Nigeria that are also employing cyber operations, including Islamic State West Africa, the Movement for Unity and Jihad in West Africa, Biafra separatist and some bandits especially in the North Western part of Nigeria.

Cyber Operations carried out by NIGCYBERCOM

The establishment of the Nigerian Army Cyber Warfare School (NACWS) in 2021 marked a significant development in the Nigerian military's cyber capabilities.[72]Nigeria's focus on cyber operations stems from two key concerns: countering terrorist activity in cyberspace, and addressing the spread of disinformation and hate speech during events like the #EndSARS protests.[73]

---

[60]Onyema Nwachukwu, 'Modern Battle not Limited to Land, Air and Maritime Domain –COAS' (2021) <https://army.mil.ng/ modern -battle-not-limited-to-land-air-and-maritime-domain -coas>. accessed 1 September 2025.
[61]ibid.
[62]ibid.
[63]Ibid
[64]Freedom Onuoha, 'Understanding Boko Haram's Attacks On Telecommunication Infrastructure' in Mantzikos., I., (ed.) *Boko Haram Anatomy of a Crisis* (e-International Relations, U.K, 2013) 17.
[65]Lukman Adewale Quadri & Monsuru Olaitan Rasaq, 'Cyber Theatre a Fifth Domain of International Politics: Africa and the rest of the world in the Cyberspace' (2020) 2(2) AHBV *Akdeniz Havzası ve Afrika Medeniyetleri Der-gisi* 104.
[66]ibid.
[67] Sunday Odundare Ogunlana, 'Halting Boko Haram /Islamic State's West Africa Province Propaganda in Cyberspace with Cyber Security Technologies' (2019) 12(1) *Journal of Strategic Security* 72.
[68] ibid.
[69] ibid at 73; Idrees Mahmud Gana, Ado FatimaZahra Ibrahim, Wisdom Adeleye Oluwaseyi & Abdullahi Isah Wali, 'Cyber Warfare and National Security in Nigeria: Threats and Responses' (2024) 1(2) *Kwararafa Security Review* 103.
[70] ibid at 87; Mubarak Ahmed Mashi & Aliyu Mukhtar Katsina 'Revisiting Nigeria's National Defence Policy for A Secured Cyber Domain in the 21st Century' (2022) 12(2) *Arts and Social Science Research* 279.
[71] Ibid
[72] Okodili Ndidi, 'Army Launches Cyber Warfare Over Hate Speech.'(2020)< https://thenationonlineng.net/army-launches-cyber-warfare-over-hate-speech/>accessed 1 September 2025.
[73]ibid; Abuh Ibrahim San, & Ibrahim Yakub, 'Evaluating Nigeria's Readiness Against State-Sponsored Cyber Attacks: A Comparative Study of CyberSecurity Policies, Incident Response, and International Cooperation' (2025) 34(4) *Journal of Computational Analysis and Applications* 694.

NIGCYBERCOM's strategy to counter cyber-attacks involves integrating robust defensive measures into the National Security Strategy. This aims to build a strong shield against Boko Haram and other groups targeting Nigeria's critical infrastructure.[74]NIGCYBERCOM recognizes cyberspace as a new battleground, mirroring global concerns. However, destabilising cyber-attacks are difficult to achieve.[75] Instead, NIGCYBERCOM focuses on strengthening its encryption and decryption capabilities to address the 21st-century cyber threats posed by Boko Haram and others when it opines that "the Nigerian Army, once again, reassures all well-meaning Nigerians of its commitment to the sustenance of peace and security in Nigeria and urges members of the public for their support and understanding throughout the exercise."[76]

On the second reason, NIGCYBERCOM puts it this way "the Exercise is deliberately intended to be all-encompassing to include cyber warfare exercises designed to identify, track and counter negative propaganda in the social media and across the cyber space."[77]

One objective of NIGCYBERCOM is to prevent a repeat of the cyber-attacks that exploited the #EndSARS protests in 2020.[78]These attacks targeted critical digital infrastructure, which can be highly disruptive as it underpins many essential cyber-physical systems.

Despite being relatively new, NIGCYBERCOM is relatively preparing to defend critical infrastructure from cyber-attacks which includes systems like traffic lights, power grids, water purification plants, and medical devices, many of which are now internet-connected. A successful cyber-attack could disrupt or even destroy this critical infrastructure, potentially jeopardizing national security and public safety.[79]

Cyber warfare and terrorism: is Nigeria winning or losing

Terrorism has emerged as one of the most pressing global security challenges, exerting profound social, political, and economic consequences. In Africa, Nigeria has been a focal point of concern due to the persistent and evolving nature of its terrorist threats. Groups such as Boko Haram, ISIS-West Africa Province (ISWAP),[80] and other extremist actors have not only destabilized Nigeria but have also impacted the broader West African region, highlighting the need for comprehensive studies on this issue. From 2007 to 2016, the total economic cost of terrorism in Africa is at a minimum US$119 billion with Nigeria's economy losing up to $97 billion, the total economic impact of refugees and IDPs to Nigeria, was US$75 billion over the ten-year period, an average of 0.73% of GDP United Nations Development Program, 2019.[81] In recent years, terrorism in Nigeria has entered a new phase characterized by significant shifts in tactics and geographic reach. According to Global Terrorism Trends and Analysis Center (GTTAC) in 2023, about 3,270 casualties were caused by terrorist incidents in Nigeria. The Institute for Economics & Peace (IEP) reports that Nigeria is ranked 8th out of 163 countries in 2023, three of the 20 most fatal terrorist attacks have occurred in Nigeria, accounting for 15%. Moreover, according to the Internal Displacement Monitoring Centre (IDMC), as of 2023, there are about 3.34 million internally displaced persons (IDPs) due to conflict and violence in Nigeria.[82]

Terrorism is an illegal and violent act use or employ to intimidate the public as well as influence the government into doing what is against the law or what is not supposed to done. There are different

---

[74] ibid; Muhammad Reza Suleiman & Kayode Omojuwa, 'Strategic Intelligence and Nigeria's Diplomatic Engagements: Enhancing National Security in An Era of Transnational Threats' (2025) < https://doi.org/10.1080/18335330.2025.2467953> accessed 1 September 2025.

[75] ibid.

[76]Murtala Abdullahi, 'Nigerian Army Plans Offensive Cyber Warfare Ops' (2020) <https://humanglemedia.com/nigerian-army-plans-offensive-cyber-warfare-ops/#>accessed 1 September 2025.

[77]ibid.

[78] Ibid.

[79]Ibid

[80] Adebayo Alonge (2022). Solving the Boko Haram Menace, Adebayo Alonge, March 11, 2012. Retrieved2024-2-9, from https://adebayoalonge.com/2012/03/11/solving-the-boko haram-menace/ .

[81] Ibid

[82] Ibid

kinds of terrorism which sole aim is to destabilise the government and disorganize the country. Nigeria has long been havened for terrorists starting from the Islamic extremists called Boko Haram to Fulani Herdsmen known as the Miyeti Allah.

Recently, the rate at which kidnapping is being committed is on a very high rate, in fact, kidnapping has been turned into a lucrative business in Nigeria in which ordinary citizen are benefiting from negotiating with kidnappers on the amount of ransom demanded and the percentage due to the negotiator. In December 2025, popular Nigerian activist and security mediator Harrison Gwamnishu was arrested following allegations that he removed money from a crowdfunded ransom meant for the release of a kidnapped couple in Edo State, Gwamnishu was accused of removing ₦5.4 million from a total of ₦20 million raised by the family of Mr. and Mrs. Segiru, who were abducted on November 22, 2025, Due to the "incomplete" payment, the kidnappers reportedly released only the wife (who was pregnant) while continuing to hold the husband in captivity. Through his lawyer and public statements, Gwamnishu claimed he removed the funds as a security tactic. He alleged that he replaced the currency with "dud notes" containing tracking chips to help security forces locate the kidnappers' hideout. The victims' family on the other hand alleged that they were not informed of this "tactic" and accused him of diverting the funds for personal use. In a country where there are law enforcement agencies and military, how treasonable is it for an ordinary individual be posing himself as a negotiator between kidnappers and victims' family.

In 2023, Nigeria recorded 435 terrorist incidents resulting in 2,797 deaths, accounting for 13% of global terrorism deaths (21,615) and 23% of terrorism deaths in Africa (12,051) for the year. This indicates, compared to 2019 a 5% decrease in terrorist incidents but a 1% increase in fatalities; when contrasted with Nigeria's 2022 data, terrorist incidents dropped substantially by 31%, yet fatalities rose by 4%. Nigeria remains threatened by various terrorist groups, including the ISIS-West Africa Province (ISWAP) and Boko Haram in the North East militant groups in the North West, Fulani militants in the North Central, and the Indigenous People of Biafra (IPOB) in the South East. Furthermore, according to Table 1, 22% of the terrorist incidents in 2023 could not be attributed to any specific organisation.[83]

Terrorism threatens democratic processes and the legitimacy of government. Terrorist organisations frequently attack electoral infrastructure, materials, and officials during elections. Such actions hinder voter registration and participation and spread disinformation on social media to incite violence, reducing voter turnout. In the run-up to the 2023 general elections, 109 election-related deaths were reported, with election violence concentrated in key battleground states such as Lagos.[84] Terrorist exploit controversies surrounding election results to incite violent protests, challenge government legitimacy, and expand their influence, threatening regional peace and stability.

Secondly, terrorism exacerbates religious, ethnic, and regional divisions and rivalries. Groups like Boko Haram and ISWAP target Christians and certain Muslim sects, leveraging religious extremism to further their political agendas. Meanwhile, in the Northwest and North central regions, terrorism disguised as banditry targets farmers and ethnic minorities, exacerbating social tensions and eroding community cohesion. Additionally, the IPOB, originally a legitimate self-determination movement, has evolved into an armed separatist campaign.[85] By capitalising on nationalist sentiment, it poses a threat to political stability. These challenges reveal the extent to which terrorism disrupts Nigeria's political stability, necessitating comprehensive and strategic responses. Constraints on Economic Development Terrorism have a detrimental impact on Nigeria's economic growth. Between 2007 and 2019, the economic cost of terrorism in Nigeria amounted to $142 billion, with losses in 2019 alone accounting for 2.4% of the country's GDP. Terrorism directly causes damage to private property and public infrastructure, affecting infrastructure construction and economic operations, such as transportation, communication, and electricity supplies. In addition, terrorism indirectly affects economic development by reducing foreign direct investment, raising unemployment,

[83] Doris Dokua Sasu (2023). Economic cost of terrorism as share of GDP in Nigeria 2017-2019, Statista, September 29, 2023. Retrieved 2024-2-12, https://www.statista.com/statistics/1197872/economic-cost-of-terrorism-in-nigeria/ from .
[84] Ibid
[85] Ibid

increasing food insecurity, etc., affecting the development of various industries in Nigeria, especially agriculture, trade, and tourism. This economic instability has also contributed to social unrest and political unrest, creating a vicious circle that has limited Nigeria's overall development.[86]

It is no longer a surprise that the act of terrorism has become a normal day to day activity in Nigeria and different terrorists' groups have their own mode of operation. In Nigeria however, the common act of terrorism is kidnapping, suicide bombing and attacks on places of worship. These attacks have resulted in multiple deaths and several properties lose.

Terrorism in Nigeria has eaten deep into the system to the extent that terrorists are now having more sophisticated weapons and equipment than the Nigerian military. As a developing nation, terrorists are using drones to monitor and survey a targeted area without being caught nor challenged, Terrorists are using mobile phone to communicate with the families of the kidnapped victims without being traced nor caught, the question is how are they successfully doing all these?

Recently, the use of mobile phones and drones by terrorist groups such as Kidnappers, Boko Haram, ISWAP has become increasingly sophisticated[87]. It is believed that these groups are trying to avoid all detection by the use of off-the-shelf technology and encrypted communication, security forces however are supposed to deploy advanced multi-layered systems to trace and neutralize these threats, but reverse is the case because despite the increase of deploying cyber technology to wage war on Nigerians, the military have not been able to trace and track even a single terrorist group.

Kidnappers now make use of various technical and social engineering tactics to communicate and demand ransom from the families of their victims while evading detection by law enforcement. This is another form of cyber war in which Nigeria is losing and there has not been a way to confront this war, the rate at which the offence is being committed is increases every day and citizens are losing trust in the military system.

In light of the foregoing, it could be safely said that Nigeria is on the losing end of cyber warfare and terrorism and it seems that in case of any eventuality, Nigeria is not prepared. Not surprising, terrorist groups in Nigeria frequently operating at any time at anywhere without fear nor remorse and they are easily getting away with their nefarious activities.

Conclusion

Having analysed the serious nature of both cyber warfare and terrorism as well as the likely devastating effects of same on any nation, it is the position of this paper that putting these vices on the same balance as against the level of preparedness of Nigeria to check the menace through regulatory mechanism, it is certain that the current legal frameworks on cyber warfare and terrorism in Nigeria are inadequate to check the complexities of the contemporary intricacies attached thereto. The NIGCYBERCOM in place to take care of contemporary catastrophic situation attach with cyber warfare and terrorism is still struggling to adapt to the unique attributes of cyber warfare and terrorism in Nigeria. It is recommended thus: that provision of adequate funding for Cyber Programmes: Securing cyberspace necessitates significant investment. This paper recommends that Nigerian government should allocate more funds to sustain her cyber ware programme. Doing this will ensure optimal performance and preparedness for digital combats always; Review/amendment of the existing legal instruments designed to regulate cyber warfare and terrorism in Nigeria: Due to several shortcomings in the current legal regimes on the cyber warfare and terrorism in Nigeria, reviewing and amendment of the law to be in line with the current global best practices will be an excellent idea for the country, because same will strengthened the Nations effort in checking and preventing cyber related vices as well as persistence incidences of terrorism we are witnessing in Nigeria; Enhancing Institutional and Capacity-Building: The institutional framework for cyber war fare, terrorism and insurgency in Nigeria should be strengthened to effectively reflect the contemporary changing face of war fare, terrorism and insurgency; **and** Enhancement of the NIGCYBERCOM's Structure through the creation of Additional Service Units: The NIGCYBERCOM, established in 2018, currently

[86] Ibid

[87]https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf

comprises only the Nigerian Army Cyber Warfare (NACW) unit. This paper recommends the creation of other units such as Nigerian Navy Cyber Warfare (NNCW) and Nigerian Air Force Cyber Warfare (NAFCW) within NIGCYBERCOM, mirroring the structure of the USCYBERCOM.