THE ROLE OF INTERNATIONAL HUMANITARIAN LAW IN CONTROLLING THE USE OF HYPERSONIC AND CYBER WEAPONS IN THE MAINTENANCE OF INTERNATIONAL PEACE AND SECURITY; THE NIGERIAN AUTHORITY

SUBMITTED

BY

OKAM IFESINACHI JOY
2020/LW/14175

TO

THE DEPARTMENT OF LAW, FACULTY OF LAW,
ALEX EKWUEME FEDERAL UNIVERSITY, NDUFU ALIKE IKWO

SUPERVISOR
BARR. GABRIEL U. AWOKE

SEPTEMBER, 2025

OKAM IFESINACHI JOY

2020/LW/14175

BEING A PROJECT SUBMITTED TO THE FACULTY OF LAW, ALEX EKWUEME FEDERAL UNIVERSITY, NDUFU ALIKE IKWO, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LL. B)

SEPTEMBER, 2025

APPROVAL

The Long Essay titled "The Role Of International Humanitarian Law In Controlling The Use of Hypersonic And Cyber Weapons In The Maintenance Of International Peace And Security; The Nigerian Authority" has been assessed and approved by the Undergraduate Studies Community of the Faculty of Law, Alex Ekwueme Federal University, Ndufu Alike Ikwo.

Barr. Gabriel U. Awoke

_____ .....

(Project Supervisor) **Date**

Dr.Kelechi Onyegbule

_____ .....

(Project Coordinator) **Date**

Prof. Eseni Azu Udu

_____ .....

(Dean, Faculty of Law) **Date**

CERTIFICATION

This is to certify that this long essay titled "The Role Of International Humanitarian Law In Controlling The Use of Hypersonic And Cyber Weapons In The Maintenance Of International Peace And Security; The Nigerian Authority" has been assessed and approved by the Undergraduate Studies Community of the Faculty of Law, Alex Ekwueme Federal University, Ndufu Alike Ikwo as an original work carried out by Okam Ifesinachi Joy, with registration number 2020/LW/14175 in the Faculty of Law, Alex Ekwueme Federal University, Ndufu Alike Ikwo, under the guidance and supervision of Barr. Gabriel U. Awoke.

Okam Ifesinachi Joy

_____ .....

(Student) **Date**

Barr. Gabriel U. Awoke

_____ .....

(Project Supervisor) **Date**

Prof. Eseni Azu Udu

_____ .....

(Dean, Faculty of Law) **Date**

DEDICATION

This work is dedicated to my family and to Mrs Rita Nwokeocha, whose unwavering support, sacrifices, and belief in me have been my greatest strength throughout this academic journey.

ACKNOWLEDGEMENT

I wish to express my profound gratitude to Almighty God for His guidance, strength and wisdom that enabled me to successfully complete this project.

I extend my heartfelt appreciation to my project supervisor, Barr. Gabriel Awoke, whose expertise, insightful guidance, and steadfast commitment provided a clear path for this research. His dedication to academic excellence and his thoughtful mentorship were instrumental in bringing this project to fruition.

I am immensely grateful to Dr. Goodluck Kelechi Onyebule, project cordinator, for his unwavering support from the inception to the conclusion of this project which has been a cornerstone of its success.

My sincere thanks go to Professor Eseni Azu Udu, Dean of the Faculty of Law, whose fatherly counsel and enriching lectures have profoundly shaped my intellectual development. His commitment to nurturing students has been a guiding light throughout my academic journey.

I also express my deep gratitude to Barr. Paschal Olebara for his steadfast guidance and encouragement, which have been a constant source of inspiration and motivation throughout my studies.

I also extend my gratitude to the staff of the Faculty of Law, Mr. Reginald Ekeh, Barr. Nnaemeka Nweze, Barr. Chukwudifu Emeka, Dr. Eni Onyenkachi, Barr Nnaemeka Amadi, Barr Charity Chinedu Uhuo, Barr C.C. Ituma, Barr. Uwadiegwu Anoke, Barr Nwambam Nnaemeka, Barr Ekechi Agwu for their contribution to my academic growth.

Special appreciation is reserved for my dear friend, Okibe Emmanuel (Egghead), whose friendship and support have enriched my academic experience from day one.

To my parents, I want to specially thank you for your support throughout my academic journey.

TABLE OF CONTENTS

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE:

TABLE OF CASES

TABLE OF STATUTES

LIST OF ABBREVIATIONS

AI – Artificial Intelligence

AP I – Additional Protocol I to the Geneva Conventions

AU – African Union

CCW – Convention on Certain Conventional Weapons

CWC – Cyber Weapons Convention (proposed)

DICON – Defence Industries Corporation of Nigeria

ECOWAS – Economic Community of West African States

ENISA – European Union Agency for Cybersecurity

GGE – Group of Governmental Experts

HGV – Hypersonic Glide Vehicle

HCOC - Hague Code of Conduct (against Ballistic Missile Proliferation)

IHL – International Humanitarian Law

ICJ – International Court of Justice

ICRC – International Committee of the Red Cross

ICC – International Criminal Court

ICTY – International Criminal Tribunal for the former Yugoslavia

LAWS – Lethal Autonomous Weapons Systems

MTCR – Missile Technology Control Regime

NAF – Nigerian Armed Forces

NATO – North Atlantic Treaty Organization

NITDA – National Information Technology Development Agency

NPT – Treaty on the Non-Proliferation of Nuclear Weapons

ONSA – Office of the National Security Adviser

PSC – Peace and Security Council (African Union)

UN – United Nations

UNGA – United Nations General Assembly

UNIDIR – United Nations Institute for Disarmament Research

UNODA – United Nations Office for Disarmament Affairs

ABSTRACT

This study critically examines the role of international law in regulating hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber weapons, with a focus on Nigeria's position in the global arms race and its implications for international security. Using doctrinal legal methodology, it identifies significant gaps in existing frameworks such as the UN Charter, Geneva Conventions, and Convention on Certain Conventional Weapons (CCW) which fail to address the speed, autonomy, and dual-use nature of these technologies. The research highlights Nigeria's vulnerability to asymmetric threats (e.g., Boko Haram, cyberattacks on critical infrastructure) and institutional limitations within domestic regimes like the Cybercrime Act (2015) and Defence Industries Corporation of Nigeria (DICON) Act (1964).

Findings reveal that regulatory vacuums exacerbate regional instability and humanitarian risks, necessitating a paradigm shift in governance. The study proposes a multi-tiered approach: adapting treaties; establishing new multilateral agreements; enhancing verification via bodies like a Hypersonic Technology Monitoring Agency; and strengthening regional cooperation through ECOWAS and the African Union. Nigeria is urged to ratify the AU's Malabo Convention, champion binding norms in global forums, and reform domestic policies to align with international humanitarian law (IHL).

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

The International Court of Justice (ICJ) has recognized the importance of regulating the development and use of new technologies in the context of international security[1]. Similarly, the Tallinn Manual on Cyber Warfare emphasizes the need for international law to adapt to the challenges posed by emerging technologies[2]. The development and proliferation of hypersonic weapons, Lethal Autonomous Weapons Systems (LAWS), and cyber weapons have raised concerns about the potential for unprecedented harm, instability, and disruption to global security. According to Michael Schmitt, a renowned expert on international humanitarian law, "the rapid development of new technologies is outpacing the development of corresponding international law frameworks"[3].

The arms race in emerging technologies is driven by major world powers, including the United States, China, and Russia. These nations are investing heavily in the development and deployment of hypersonic weapons, LAWS, and cyber weapons, which has sparked concerns about the potential for a new era of military competition and conflict. According to a report by the RAND Corporation, "the development of hypersonic weapons is likely to have significant implications for international security and stability"[4]. The implications of this arms race extend beyond the realm of international security, with potential consequences for global governance, human rights, and the rule of law.

---

[1] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, *ICJ Reports* (1996) p. 226.
[2] Tallinn Manual on Cyber Warfare, Cambridge University Press (2013) p. 12.
[3] Michael Schmitt, 'The Law of Cyber Warfare' in James Crawford and Martti Koskenniemi, *Cambridge Companion to International Law* (Cambridge University Press, 2012) 374.
[4] RAND Corporation, 'Hypersonic Weapons and International Security', (2020) p. 3.

Nigeria, as a key player in regional and international affairs, has a significant stake in the regulation of emerging technologies. As a non-permanent member of the United Nations Security Council, Nigeria has played an active role in promoting international peace and security. However, the country's own security challenges, including the Boko Haram insurgency and piracy in the Gulf of Guinea, underscore the need for effective regulation of emerging technologies to prevent their potential misuse. According to a report by the Nigerian Institute of International Affairs, "Nigeria must prioritize the development of a comprehensive national policy on emerging technologies to address the challenges and opportunities they present"[5].

The regulation of emerging technologies is a complex and multifaceted issue, requiring a comprehensive and adaptive approach. International law, as the primary framework for regulating state behavior, has a critical role to play in addressing the challenges posed by hypersonic weapons, LAWS, and cyber weapons. However, the existing international law framework is inadequate, and there is a need for new treaties, agreements, and norms to regulate the development and use of these technologies. According to Heather Harrison Dinniss, "the development of new international law frameworks must take into account the unique characteristics of emerging technologies"[6].

This study aims to contribute to the ongoing debate on the regulation of emerging technologies, with a focus on the role of international law in regulating the development and use of hypersonic weapons, LAWS, and cyber weapons. By examining the existing international law framework and proposing recommendations for strengthening regulation, this study seeks to provide a unique Nigerian perspective on the implications of emerging technologies for international security and regional stability. The study will analyze the current state of international law

[5] Nigerian Institute of International Affairs, 'Emerging Technologies and National Security in Nigeria' (2020) p. 5.
[6] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) 133.

governing emerging technologies, identify gaps and limitations in existing frameworks, and propose pragmatic recommendations for addressing these challenges.

1.2 STATEMENT OF THE PROBLEM

The development and proliferation of hypersonic weapons, Lethal Autonomous Weapons Systems (LAWS), and cyber weapons pose significant challenges to international peace and security. As noted by the International Committee of the Red Cross (ICRC), "the development and use of new technologies in warfare raises significant humanitarian concerns"[7]. The lack of effective regulation and oversight has created a permissive environment in which states can develop and deploy these technologies without adequate consideration for their humanitarian and strategic implications.

The existing international law framework is inadequate to address the challenges posed by emerging technologies. According to Heather Harrison Dinniss, "the laws of war were developed in a pre-digital era and do not provide clear guidance on the development and use of cyber weapons". Furthermore, the Tallinn Manual on Cyber Warfare notes that "the lack of transparency and accountability in the development and use of cyber weapons has made it difficult to assess their compliance with international law"[8].

The implications of this regulatory gap are particularly significant for Nigeria, which faces significant security challenges in the form of terrorism, piracy, and other forms of violence. The potential misuse of emerging technologies by non-state actors, including terrorist organizations and cybercriminals, poses a significant threat to national and regional security. Furthermore, the lack of effective regulation and oversight has created a permissive environment in which states

[7] ICRC, 'New Technologies and Warfare' (2019) p. 3.
[8] *Ibid* (n 2).

can develop and deploy emerging technologies without adequate consideration for their humanitarian and strategic implications. To address the regulatory gaps and challenges posed by emerging technologies, this study aims to provide a comprehensive analysis of the role of international law in regulating the development and use of hypersonic weapons, LAWS, and cyber weapons. By examining the existing international law framework, identifying gaps and limitations, and proposing recommendations for strengthening regulation, this study seeks to provide a nuanced understanding of the complex interplay between emerging technologies, international law, and global security dynamics. Ultimately, this study aims to contribute to the development of a more effective and adaptive regulatory framework that can mitigate the risks associated with emerging technologies and promote international peace and security.

1.3 RESEARCH QUESTIONS

This study will by the end answer the following questions:

1. What are the existing international law frameworks governing the development and use of hypersonic weapons, LAWS, and cyber weapons, and what are their limitations in addressing the challenges posed by these emerging technologies?
2. How do the development and proliferation of hypersonic weapons, LAWS, and cyber weapons impact international peace and security, particularly in the context of the Nigerian experience?
3. What are the gaps and challenges in the existing international law framework regulating emerging technologies, and how can these gaps be addressed through new treaties, agreements, and norms?

4. What role can Nigeria and other African states play in shaping the international law framework governing emerging technologies, and what are the implications of these technologies for regional and national security in Africa?

1.4 AIM AND OBJECTIVES OF THE STUDY

The main aim of this study is to examine the role of international law in regulating the development and use of hypersonic weapons, LAWS, and cyber weapons, with a view to proposing a framework for strengthening international law and promoting regional and national security in Nigeria and Africa.

The objectives of the study are:

1. To examine the existing international law frameworks governing the development and use of hypersonic weapons, LAWS, and cyber weapons, and to identify their limitations in addressing the challenges posed by these emerging technologies.
2. To analyze the impact of the development and proliferation of hypersonic weapons, LAWS, and cyber weapons on international peace and security, with a focus on the Nigerian experience.
3. To identify the gaps and challenges in the existing international law framework regulating emerging technologies, and to propose recommendations for addressing these gaps through new treaties, agreements, and norms.
4. To investigate the role that Nigeria and other African states can play in shaping the international law framework governing emerging technologies, and to examine the implications of these technologies for regional and national security in Africa.

1.5 RESEARCH METHODOLOGY

Doctrinal research methodology, also known as black-letter law research, is a research approach that focuses on the analysis and interpretation of existing laws, regulations, and legal principles[9]. It involves a detailed examination of legal texts, including statutes, cases, treaties, and scholarly writings, to understand the underlying legal framework and principles.

The doctrinal research methodology is suitable for this research because it allows for a comprehensive examination of the existing international law framework governing the development and use of hypersonic weapons, LAWS, and cyber weapons. This approach enables the researcher to analyze the relevant treaties, conventions, and customary international law, as well as the writings of prominent scholars and jurists in the field of international law.

The doctrinal research is particularly useful for identifying gaps and inconsistencies in the law, and for developing new legal principles and frameworks. This makes the doctrinal approach well-suited for this research, which aims to identify gaps and challenges in the existing international law framework and propose recommendations for strengthening regulation.

1.6 SIGNIFICANCE OF THE STUDY

This study has both theoretical and practical significance, contributing to the existing body of knowledge on international law and emerging technologies.

Theoretically, this study contributes to the development of international law frameworks governing emerging technologies. By examining the existing international law framework and identifying gaps and challenges, this study provides a nuanced understanding of the complex interplay between emerging technologies, international law, and global security dynamics. This study also contributes to the theoretical debates on the role of international law in regulating

[9] P Harris, 'Doctrinal Research in Law'. *Journal of Law and Society* [2019] (46) (1) 1-15.

emerging technologies, providing insights into the strengths and limitations of existing frameworks.

Practically, this study has significant implications for policymakers, international organizations, and national governments. The study's recommendations for strengthening international law frameworks governing emerging technologies provide a roadmap for policymakers and international organizations seeking to promote international peace and security. Additionally, this study's findings on the implications of emerging technologies for national security and regional stability provide valuable insights for national governments and regional organizations. By providing a comprehensive analysis of the role of international law in regulating emerging technologies, this study aims to inform and shape policy debates on this critical issue.

1.7 SCOPE OF THE STUDY

This study focuses on the role of international law in regulating the development and use of hypersonic weapons, Lethal Autonomous Weapons Systems (LAWS), and cyber weapons. The study examines the existing international law framework governing these emerging technologies, including relevant treaties, conventions, and customary international law.

The study's scope is limited to the international law dimensions of emerging technologies, and does not examine the technical or operational aspects of these technologies. The study also focuses primarily on the implications of emerging technologies for international peace and security, rather than their potential applications in other fields, such as commerce or healthcare.

Geographically, the study's scope is global, examining international law frameworks and norms governing emerging technologies at the international level. However, the study also considers the

implications of emerging technologies for regional and national security in Africa, with a focus on Nigeria.

1.8 LIMITATIONS OF THE STUDY

This study has several limitations that should be acknowledged. The study focuses primarily on the international law dimensions of emerging technologies, and does not examine the technical or operational aspects of these technologies. The study relies primarily on secondary sources, including scholarly literature, reports, and online resources. While these sources provide valuable insights, they may not offer a comprehensive understanding of the issue. Again, while the study examines international law frameworks governing emerging technologies at the global level, its focus on Nigeria and Africa may limit its applicability to other regions. The rapid evolution of emerging technologies may also limit the study's ability to provide a comprehensive and up-to-date analysis of the issue. Finally, the complexity of international law and the nuances of its application may limit the study's ability to provide definitive conclusions and recommendations.

1.9 CHAPTER ANALYSIS

This dissertation is divided into five chapters, each of which explores a distinct aspect of the regulation of emerging technologies in international law.

Chapter One provides an introduction to the study, outlining the background, statement of the problem, research questions, aim and objectives, research methodology, significance, scope, and limitations of the study.

Chapter Two presents a comprehensive literature review, examining the conceptual, theoretical, and empirical frameworks relevant to the study. This chapter reviews the definitions,

characteristics, and types of hypersonic weapons, LAWS, and cyber weapons, as well as the principles of international law and the concept of an arms race.

Chapter Three examines the legal regime and institutional framework governing emerging technologies. This chapter analyzes the relevant international and national laws, including the Cybercrime Act, Defence Industries Corporation of Nigeria Act, African Union Non-Aggression and Common Defence Pact, Geneva Conventions, Hague Conventions, and United Nations Charter.

Chapter Four presents an in-depth analysis of the regulatory challenges posed by emerging technologies. This chapter examines the existing international law frameworks governing hypersonic weapons, LAWS, and cyber weapons, and argues that traditional arms control agreements are insufficient for regulating emerging technologies. The chapter also explores the role of international humanitarian law in regulating the development and use of emerging technologies.

Chapter Five provides a summary of the study's findings, conclusions, and recommendations. This chapter synthesizes the main arguments and insights from the preceding chapters, and offers proposals for addressing the challenges posed by emerging technologies.

CHAPTER TWO

CONCEPTUAL CLARIFICATION, THEORETICAL FOUNDATION AND LITERATURE REVIEW

2.1 CONCEPTUAL REVIEW

2.1.1 Hypersonic Weapons: Definition, Characteristics, and Types

Hypersonic weapons are advanced military systems capable of speeds exceeding Mach 5 (~6,174 km/h), combining velocity with maneuverability to evade traditional missile defenses. Unlike ballistic missiles, they operate at low altitudes (20–100 km), complicating radar detection and interception.[10] Their proliferation risks destabilizing arms races, as they compress decision-making windows and challenge existing arms control frameworks like the New START Treaty. It is important to note that there is no specific treaty that regulates hypersonic weapons. Their dual-use nature (conventional/nuclear) blurs compliance with the *Treaty on the Non-Proliferation of Nuclear Weapons (NPT)*.[11]

The International Court of Justice's Advisory Opinion on the Legality of Nuclear Weapons (1996) underscores that new weapons must comply with international humanitarian law , including *distinction and proportionality*. Hypersonic weapons' speed may impede adherence, raising accountability concerns. For Nigeria, these technologies amplify asymmetric threats, necessitating advocacy for inclusive regulations via the African Union (AU) to prevent great-power monopolization.[12]

2.1.2 Lethal Autonomous Weapons Systems (LAWS): Legal and Ethical Dimensions

[10] Kelley M Sayler, *Hypersonic Weapons: Background and Issues for Congress* (CRS 2024) 4.
[11] Treaty on the Non-Proliferation of Nuclear Weapons (1968) art I.
[12] AU Assembly, 'Common African Position on Arms Control' (Doc Assembly/AU/12(XXIV) 2015.

LAWS are AI-driven systems that identify, select, and engage targets without human intervention. Their autonomy challenges IHL principles, particularly distinction (combatant vs. civilian) and accountability.[13]

The Rome Statute of the ICC (Article 8) criminalizes war crimes involving indiscriminate attacks.[14] It is notewrothy that, LAWS' algorithmic decision-making risks violating this, as seen in debates over attribution gaps. The ICJ's ***Nicaragua v. USA (1986)*** established state responsibility for unlawful force, implying that LAWS deployments could breach *jus ad bellum* if autonomy leads to unintended escalation.[15]

Nigeria's security landscape (e.g., Boko Haram insurgency) heightens risks of LAWS misuse by non-state actors. Active participation in the Convention on Certain Conventional Weapons (CCW) talks is crucial to advocate for a preemptive ban.[16]

2.1.3 Cyber Weapons: Definition, Types, and Characteristics

Cyber weapons are defined as malicious software, code, or digital techniques designed to infiltrate, disrupt, or destroy computer systems, networks, or critical infrastructure, often to achieve military, political, or economic objectives. Operating in the abstract domain of cyberspace, these weapons exploit vulnerabilities in digital ecosystems, ranging from government databases to private sector utilities, with effects that can rival physical destruction. For Nigeria, where digital infrastructure underpins sectors like banking and telecommunications, cyber weapons pose a growing threat, particularly as state and non-state actors exploit weak

[13] ICRC, 'Autonomous Weapon Systems' (Report 2014) 7.
[14] Rome Statute (1998) art 8(2)(b)(iv).
[15] Nicaragua v USA [1986] ICJ Rep 14.
[16] CCW, *Report on LAWS Expert Meeting* (UN Doc CCW/MSP/2023/2) para 12.

cybersecurity frameworks in Africa.[17] The difficulty of attributing attacks to specific perpetrators challenges their regulation under international law, requiring Nigeria to advocate for norms that balance national sovereignty with global cooperation.

Cyber weapons encompass several types, including malware, exploits, denial-of-service (DoS) tools, and advanced persistent threats (APTs), each with distinct applications. Malware, such as ransomware or trojans, disrupts systems or steals data, as seen in the 2017 WannaCry attack that affected global institutions. Exploits target specific software vulnerabilities to gain unauthorized access, exemplified by the Stuxnet worm, which sabotaged Iran's nuclear centrifuges, demonstrating cyber weapons' capacity for physical damage.[18] DoS tools overload networks to deny access, often used in politically motivated attacks, while APTs involve prolonged, covert intrusions, typically state-sponsored, for espionage or strategic disruption. Nigeria's exposure to these threats, evidenced by frequent cyberattacks on its financial sector, highlights the need for international legal frameworks to deter proliferation and ensure accountability.[19]

The characteristics of cyber weapons include their stealth, scalability, and dual-use potential, which amplify their strategic impact. Their intangible nature enables covert deployment, often evading detection until significant harm occurs, as demonstrated by the 2020 SolarWinds breach, which compromised multiple government networks.[20] Scalability allows a single piece of code to affect millions of systems worldwide, offering disproportionate destructive power at low cost compared to conventional weapons. The dual-use nature of cyber tool where software developed for legitimate purposes, like penetration testing, can be repurposed for attacks complicates efforts

[17] Dorothy E. Denning, 'The Nature and Impact of Cyber Weapons,' in David P. Fidler (ed.), *Cyber Weapons and International Law* (London: Routledge, 2015) 23.
[18] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018) 54.
[19] Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017) 88.
[20] Kim Zetter, 'Inside the SolarWinds Hack: How Russian Spies Compromised America's Networks'. *MIT Technology Review* [2021].

to distinguish between civilian and military applications, posing challenges for international law. For Nigeria, the accessibility of these weapons to non-state actors, including insurgent groups like Boko Haram, underscores the urgency of integrating cyber norms into global security frameworks to protect critical infrastructure and maintain regional stability.[21]

2.1.4 International Law: Definition, Sources, and Principles Relevant to the Regulation of Emerging Weapons Technologies

International law is a body of rules and principles governing the relations between states, international organizations, and, to some extent, individuals, primarily aimed at promoting peace, cooperation, and justice in global affairs. It encompasses treaties, customary practices, and general principles recognized by nations, providing a framework to regulate state behavior, including the development and use of emerging weapons technologies like hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber weapons.[22] For Nigeria, a state committed to non-alignment and African unity, international law serves as a critical tool to advocate for equitable regulations that prevent the monopolization of advanced weaponry by major powers, which could exacerbate regional insecurities in Africa.[23] The dynamic nature of emerging technologies, however, challenges the adaptability of international law, as existing treaties often lag behind rapid advancements, necessitating innovative approaches to ensure compliance and accountability.[24]

---

[21] Eneken Tikk and Mika Kerttunen, *The Cyber Arms Race: Security Implications of Offensive Cyber Capabilities* (Helsinki: Finnish Institute of International Affairs, 2019) 22.
[22] Malcolm N. Shaw, *International Law*, 8th ed. (Cambridge: Cambridge University Press, 2021) 1-3.
[23] James Crawford, *Brownlie's Principles of Public International Law*, 9th ed. (Oxford: Oxford University Press, 2019) 15.
[24] Antonio Cassese, *International Law*, 2nd ed. (Oxford: Oxford University Press, 2022) 23.

The sources of international law, as outlined in Article 38(1) of the Statute of the International Court of Justice, include treaties, customary international law, general principles of law, and, as subsidiary means, judicial decisions and scholarly writings. Treaties, such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), provide binding obligations, but their application to hypersonic or cyber weapons is limited due to specificity gaps, prompting calls for new agreements tailored to these technologies. Customary international law, derived from consistent state practice and opinio juris, offers flexibility but struggles with emerging technologies where state practices are nascent or secretive, complicating consensus on norms for LAWS. For Nigeria, leveraging these sources within forums like the United Nations General Assembly is essential to advocate for inclusive regulations that address Africa's vulnerability to the destabilizing effects of unregulated weapons, ensuring that principles like sovereignty and non-intervention guide technological governance.[25]

Key principles relevant to regulating emerging weapons technologies include distinction, proportionality, necessity, and humanity, rooted in international humanitarian law (IHL), alongside sovereignty and the prohibition of force under the UN Charter. The principle of distinction requires that weapons differentiate between combatants and civilians, a challenge for LAWS, which may misinterpret data in complex environments like Nigeria's insurgency-affected regions. Proportionality and necessity demand that attacks avoid excessive collateral damage and serve legitimate military objectives, principles strained by cyber weapons' unpredictable effects on critical infrastructure, such as Nigeria's power grid.[26] The principle of humanity, emphasizing the minimization of suffering, underscores the need for preemptive bans

[25] Yoram Dinstein, *War, Aggression and Self-Defence*, 6th ed. (Cambridge: Cambridge University Press, 2017) 34.
[26] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017) 125.

on fully autonomous systems, aligning with Nigeria's interest in preventing technologies that could escalate conflicts in Africa.[27] These principles, while foundational, require adaptation to address the unique attributes of emerging weapons, urging Nigeria to champion multilateral efforts for updated legal frameworks that balance technological innovation with global stability.

2.1.5 Arms Race: Legal Implications for International Security

An arms race denotes competitive escalation in military capabilities, historically driven by mutual distrust (e.g., Cold War). Emerging technologies like hypersonic weapons, LAWS, and cyber tools accelerate this dynamic, straining arms control regimes.[28]

Cyber weapons (e.g., malware, APTs) exploit digital vulnerabilities to disrupt infrastructure, with effects akin to kinetic attacks. The Tallinn Manual 2.0 affirms that cyber operations are subject to IHL, including proportionality and necessity.[29]

Cyber operations causing civilian harm could constitute war crimes under Article 8(2)(b)(iv) of the Rome Statute. The 2021 Policy on Cybercrime explicitly prioritizes prosecuting cyber-enabled atrocities. [30]

For Nigeria, unregulated cyber arms races exacerbate regional instability, as seen in Sahel conflicts where external actors deploy hybrid tactics. Nigeria must champion binding cyber norms under UN Charter Article 2(4) to curb cross-border digital aggression.[31]

2.1.6 International Security: Definition, Dimensions, and Challenges in the Context of Emerging Weapons Technologies

---

[27] Helen Durham, 'The Use of New Technologies and International Humanitarian Law," *Melbourne Journal of International Law* [2017] (18) (2) 234.
[28] Matthijs M Maas, 'Preventive Security Governance' (2021) 1 Eur J Intl Sec 115, 122.
[29] Tallinn Manual 2.0 (CUP 2017) r 71.
[30] ICC, *Policy on Cybercrime* (2021) para 21.
[31] UN Charter (1945) art 2(4).

International security refers to the collective measures taken by states and international organizations to protect global peace, stability, and sovereignty from threats, encompassing military, economic, environmental, and societal dimensions. It emphasizes cooperation to prevent conflicts, manage crises, and address transnational challenges, such as those posed by emerging weapons technologies. A regional leader in West Africa, international security is critical to safeguarding national interests against the backdrop of technological advancements that could disrupt traditional deterrence and exacerbate conflicts in Africa's volatile regions.[32] The rapid evolution of hypersonic weapons, LAWS, and cyber weapons demands a redefinition of security priorities, as these technologies challenge existing paradigms of defense and diplomacy.[33]

The dimensions of international security include traditional military security, human security, and cybersecurity, each reshaped by emerging technologies. Military security focuses on state defense against armed threats, but hypersonic weapons' speed and LAWS' autonomy complicate deterrence, as rapid response times and decision-making errors could trigger unintended escalations in regions like Nigeria's Lake Chad Basin.[34] Human security prioritizes individual well-being, threatened by cyber weapons that disrupt critical services—such as Nigeria's healthcare systems during ransomware attacks—highlighting the need for resilient infrastructure. Cybersecurity, an increasingly vital dimension, addresses threats to digital systems, where Nigeria's financial sector faces frequent attacks, necessitating international cooperation to

---

[32] Joseph S. Nye Jr., *Understanding International Conflicts: An Introduction to Theory and History*, 7th ed. (New York: Pearson, 2009) 25.
[33] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2024) 33.
[34] Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 2019) 56

establish norms against cyber warfare.[35] These dimensions collectively underscore the interconnected nature of modern security challenges, requiring Nigeria to integrate technological considerations into its foreign and defense policies.

The challenges of international security in the context of emerging weapons technologies include regulatory gaps, escalation risks, and asymmetric vulnerabilities. Regulatory gaps arise from the absence of treaties specifically addressing hypersonic weapons or LAWS, complicating efforts to enforce IHL principles like distinction in Nigeria's counterinsurgency operations.[36] Escalation risks stem from the speed and autonomy of these technologies, where miscalculations—such as a cyber-attack misattributed to a state—could provoke conflicts, destabilizing West Africa's fragile peace.[37] Asymmetric vulnerabilities expose developing nations like Nigeria to exploitation by technologically advanced states or non-state actors, as cyber weapons' low cost and accessibility enable groups like Boko Haram to disrupt governance.[38] Nigeria must leverage its influence in the African Union and UN to advocate for inclusive security frameworks that address these challenges, ensuring that technological advancements do not undermine global stability or Africa's development aspirations.

2.2 THEORETICAL REVIEW

2.2.1 Realist Theory

Realist theory, a foundational paradigm in international relations, traces its origins to ancient political thought emphasizing power and survival in a competitive world. Classical works, such

---

[35] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011) 67.
[36] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton & Company, 2018) 245.
[37] Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017) 132.
[38] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018) 189.

as Thucydides' *History of the Peloponnesian War*, underscored power dynamics in state interactions, while Machiavelli's *The Prince* advocated pragmatic governance.[39] Modern realism developed in the 20th century, particularly after World War II, as scholars sought to explain state behavior amid global conflicts. Hans Morgenthau's *Politics Among Nations* (1948) formalized classical realism, focusing on human nature's pursuit of power, whereas Kenneth Waltz's *Theory of International Politics* (1979) introduced neorealism, emphasizing systemic anarchy as the primary driver of state actions.[40] Realism has shaped security studies, influencing Cold War strategies and contemporary analyses of technological advancements in warfare.

Realist theory posits that international relations operate under anarchy, lacking a central authority, compelling states to prioritize survival through power maximization. National interest, defined by military and economic strength, drives state behavior, with cooperation viewed skeptically due to mistrust and concerns over relative gains.[41] Prominent proponents include Morgenthau, who emphasized human nature's flaws, Waltz, who developed structural neorealism, and John Mearsheimer, who advanced offensive realism, arguing states seek to dominate to ensure security.[42] International law, within this framework, is considered a weak constraint unless aligned with the interests of powerful states, as states act rationally to safeguard sovereignty, often through arms races or strategic alliances.[43]

Realist theory views the international system as inherently competitive, predicting that emerging weapons technologies—hypersonic weapons, lethal autonomous weapons systems (LAWS), and

---

[39] Thucydides, *History of the Peloponnesian War*, trans. Rex Warner (London: Penguin Classics, 1972) 35.
[40] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 5th ed. (New York: Knopf, 1978) 4-15; Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979) 88.
[41] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001) 17-18
[42] Morgenthau, *Politics Among Nations*, 25; Waltz, *Theory of International Politics*, 102; Mearsheimer, *Tragedy*, 21.
[43] Robert Jervis, 'Realism, Neoliberalism, and Cooperation: Understanding the Debate'. *International Security* [2021] (24) (1) 43.

cyber weapons—intensify power struggles among states. States are expected to pursue these technologies to deter adversaries or gain strategic advantages, perceiving arms races as inevitable without a global enforcer. In the context of the study, realism frames the development and regulation of such weapons as driven by power dynamics, suggesting that international law's effectiveness hinges on the consensus of major powers.[44] For Nigeria, a state navigating technological disparities, realism underscores the challenge of influencing global regulations amid great power dominance. Engagement in multilateral forums, such as the United Nations, becomes critical to balance powerful states' interests, ensuring that regional security in Africa is not undermined by unchecked technological escalation.[45]

2.2.2 Liberal Institutionalism

Liberal institutionalism, a prominent theory in international relations, developed from liberal thought advocating cooperation and peace, drawing inspiration from Enlightenment philosophers like Immanuel Kant, who envisioned perpetual peace through mutual agreements. The theory gained traction following World War I with the establishment of the League of Nations and solidified after World War II through institutions like the United Nations, reflecting aspirations for structured global governance.[46] In the late 20th century, scholars such as Robert Keohane and Joseph Nye advanced the theory, with *Power and Interdependence* (1977) and Keohane's *After Hegemony* (1984) emphasizing institutions' role in facilitating cooperation under anarchy.[47]

---

[44] Jack Donnelly, *Realism and International Relations* (Cambridge: Cambridge University Press, 2000) 81.
[45] Stephen M. Walt, 'The Enduring Relevance of the Realist Tradition,' in *International Relations Theories: Discipline and Diversity*, ed. Tim Dunne et al. (Oxford: Oxford University Press, 2016) 52.
[46] Immanuel Kant, *Perpetual Peace: A Philosophical Sketch*, translator HB Nisbet (Cambridge: Cambridge University Press, 1795/1991) 93.
[47] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 1984) 65; Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 2nd ed. (Boston: Little, Brown, 2019) 23.

Liberal institutionalism has since influenced analyses of international regimes, particularly in addressing technological and security challenges through legal frameworks.

Liberal institutionalism asserts that international institutions—formal organizations, treaties, and norms—mitigate the effects of anarchy by fostering cooperation, transparency, and trust among states. States, viewed as rational actors, prioritize absolute gains, using institutions to reduce transaction costs, manage conflicts, and coordinate policies for mutual benefit.[48] Notable proponents include Keohane, who explored regimes' persistence beyond hegemonic power, Nye, who introduced complex interdependence, and Lisa Martin, who examined institutional design's impact on state compliance.[49] International law, within this framework, serves as a mechanism to regulate state behavior, enabling collective responses to emerging technologies through binding agreements and shared norms.[50]

Liberal institutionalism envisions international stability achieved through institutions that promote dialogue and cooperation, suggesting that technologies like hypersonic weapons, LAWS, and cyber weapons can be regulated through multilateral treaties and norms. Such frameworks are expected to reduce arms race risks by establishing rules for development and use, fostering confidence among states.[51] The study benefits from this perspective by highlighting Nigeria's potential to engage in institutions like the African Union or the Convention on Certain Conventional Weapons (CCW) to advocate for inclusive regulations, ensuring African interests are represented in global governance.[52] Emphasis on cooperation aligns with Nigeria's non-

---

[48] Lisa L. Martin, 'The Rational Choice of Multilateralism,' in *Multilateralism Matters: The Theory and Praxis of an Institutional Form*, ed. John Gerard Ruggie (New York: Columbia University Press, 1993) 91.
[49] Keohane, *After Hegemony*, 78; Nye, *Power and Interdependence*, 35; Martin, "Rational Choice," 103.
[50] Anne-Marie Slaughter, 'International Law and International Relations'. *Recueil des Cours* [2000] (285) 29.
[51] G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars* (Princeton, NJ: Princeton University Press, 2010) 50.
[52] Andrew Hurrell, 'Global Inequality and International Institutions'. *Metaphilosophy* [2001] (32) (1-2) 34.

aligned stance, supporting efforts to develop international law that mitigates technological threats, enhancing regional security by leveraging institutional mechanisms to address disparities and promote collective stability.[53]

2.2.3 Constructivist Theory

Constructivist theory emerged in the late 1980s as a critique of realist and liberal paradigms, emphasizing the role of ideas, identities, and norms in shaping international relations. Drawing from sociological foundations, including Max Weber's focus on social action and Peter Berger and Thomas Luckmann's social constructivism, the theory gained prominence post-Cold War to explain shifts in state behavior not accounted for by material factors.[54] Alexander Wendt's *Social Theory of International Politics* (1999) formalized constructivism, arguing that anarchy's effects depend on states' shared understandings.[55] The theory has influenced analyses of norm formation, particularly in disarmament and technology governance, offering insights into the social construction of security threats.

Constructivist theory contends that international relations are socially constructed, with state behavior shaped by identities, norms, and intersubjective meanings rather than solely power or institutions. International law is viewed as a product of normative evolution, reflecting collective agreements on acceptable conduct, such as restrictions on weapons technologies.[56] Leading proponents include Wendt, who explored anarchy's malleability, Nicholas Onuf, who emphasized rule-based interactions, and Martha Finnemore, who analyzed norm diffusion

---

[53] Martha Finnemore, 'International Organizations as Teachers of Norms'. *International Organization* [1993] (47) (4) 565.
[54] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (Garden City, NY: Anchor Books, 1966) 47.
[55] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999) 92.
[56] Nicholas G. Onuf, *World of Our Making: Rules and Rule in Social Theory and International Relations* (Columbia: University of South Carolina Press, 1989) 66.

through international organizations.[57] The theory highlights how norms, such as those prohibiting chemical weapons, emerge through socialization, providing a framework to address emerging technologies' ethical implications.

Constructivist theory envisions international stability achieved through evolving norms and identities that constrain destabilizing technologies, suggesting that hypersonic weapons, LAWS, and cyber weapons can be regulated by fostering shared ethical standards. Normative change, driven by persuasion and socialization, is expected to shape state behavior, encouraging restraint in arms races.[58] The study draws on this perspective to explore Nigeria's role in promoting norms within African and global forums, such as advocating for LAWS bans based on humanitarian principles, aligning with collective identities of peace and sovereignty.[59] Constructivism underscores Nigeria's potential to influence international law's development, countering technological threats by fostering dialogue that redefines security, emphasizing responsibility and restraint to mitigate arms race dynamics in Africa and beyond.

2.3 Review of Related Literature

The work of Yoram Dinstein*, War, Aggression and Self-Defence*[60], serves as a seminal exploration of international law governing the use of force, aiming to clarify the legal boundaries of aggression and self-defense under the UN Charter through a doctrinal methodology that analyzes treaties, customary law, and historical case studies like the Gulf War. The work finds that the prohibition of force remains central, with self-defense narrowly construed, yet struggles

[57] Wendt, *Social Theory*, 135; Onuf, *World of Our Making*, 78; Martha Finnemore, *National Interests in International Society* (Ithaca, NY: Cornell University Press, 1996) 22.
[58] Jutta Weldes, 'Constructing National Interests'. *European Journal of International Relations* [1996] (2) (3) 275.
[59] Richard Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines'. *International Organization* [1998] (52) (3) 613.
[60] Dinstein Yoram. *War, Aggression and Self-Defence* (6th ed.: Cambridge: Cambridge University Press, 2017).

to address novel warfare methods like cyberattacks, concluding that legal norms require adaptation to maintain relevance amidst evolving threats. Despite its comprehensive scope, the text's limited focus on emerging technologies—hypersonic weapons, lethal autonomous weapons systems, and cyber weapons—and lack of attention to developing states' perspectives, such as Nigeria's, present gaps that the present study addresses by examining these technologies' regulation and Nigeria's role in advocating equitable norms to mitigate arms race risks in Africa.

Worthy of review is also is, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Published in 2017 under Michael N. Schmitt's editorship[61]. *Tallinn Manual 2.0* represents a meticulous effort to delineate the applicability of international law to cyber operations, aiming to provide a robust framework for regulating state and non-state conduct in cyberspace. Through a collaborative methodology involving legal scholars and practitioners analyzing treaties, customary law, and state practices, the manual establishes that principles such as sovereignty, non-intervention, and proportionality govern cyber activities, yet reveals significant challenges in attributing cyberattacks due to their covert nature, concluding that enhanced global cooperation is essential to clarify legal thresholds for responses. The work's comprehensive approach illuminates the complexities of cyber warfare, particularly relevant to regulating cyber weapons, but falls short in addressing the unique vulnerabilities of African nations like Nigeria, where limited cybersecurity infrastructure heightens exposure to digital threats. The present study seeks to bridge this gap by examining how international law can evolve to regulate cyber weapons, emphasizing Nigeria's role in advocating for equitable norms within African Union and UN frameworks to strengthen regional resilience against arms race-driven cyber instabilities.

[61] N Schmitt Michael, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

Paul Scharre researched on, *Army of None: Autonomous Weapons and the Future of War*[62] where he offers an in-depth exploration of lethal autonomous weapons systems (LAWS), striving to unravel their technological, strategic, and ethical dimensions in transforming modern warfare. By synthesizing insights from military interviews, technical assessments, and policy discussions, the analysis uncovers how autonomy accelerates arms races, undermines international humanitarian law compliance, and risks unintended escalations, ultimately advocating for mandatory human oversight to balance innovation with accountability, though stopping short of endorsing specific treaties. The book's accessible narrative clarifies the stakes of autonomous systems, yet its limited engagement with the perspectives of developing nations, particularly Nigeria, overlooks how such technologies could exacerbate regional conflicts in Africa's volatile security landscape. The current research addresses this deficiency by investigating international law's capacity to govern LAWS, highlighting Nigeria's potential to champion regulations that prevent autonomous weapons from fueling instability in West Africa and beyond, ensuring alignment with global security objectives.

The research work of Ingvild Bode and Guangyu Qiao-Franco, *Emergent Normativity: Communities of Practice, Technology, and Lethal Autonomous Weapon Systems*[63], a *Global Studies Quarterly* article which investigates the evolving normative landscape surrounding lethal autonomous weapons, aiming to understand how global stakeholders shape regulatory frameworks. Employing discourse analysis to examine interactions among diplomats, technologists, and civil society, the study reveals a fragmented norm-building process marked by competing definitions and priorities, suggesting that inclusive multilateral dialogue could forge

[62] Scharre Paul. *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton & Company, 2018).
[63] Bode Ingvild, and Guangyu Qiao-Franco, 'Emergent Normativity: Communities of Practice, Technology, and Lethal Autonomous Weapon Systems.' *Global Studies Quarterly* [2024] (4) (1) 1–14.

consensus on limiting autonomous systems, while noting persistent divides that hinder progress. The article's focus on norm emergence provides valuable insights into arms control dynamics, but its minimal attention to African contexts, such as Nigeria's concerns about the proliferation of destabilizing technologies in conflict-prone regions, leaves an analytical void. The present study fills this shortfall by analyzing Nigeria's strategic position in advocating for international legal norms to regulate LAWS, ensuring that such frameworks address African security needs and mitigate the risks of technological arms races escalating regional tensions.

In *Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law*[64]*,* Merel A. C. Ekelhof examines the extent to which lethal autonomous weapons systems (LAWS) align with international humanitarian law (IHL), aiming to assess their compliance with core principles governing armed conflict. Through a doctrinal legal analysis, dissecting IHL tenets such as distinction, proportionality, and precaution, alongside technical evaluations of autonomous systems' capabilities, the study finds that current LAWS struggle to reliably distinguish combatants from civilians in dynamic environments, raising doubts about their lawful deployment, and concludes that stringent human oversight remains essential to uphold IHL obligations. The article's rigorous scrutiny of autonomy's legal challenges illuminates the complexities of regulating LAWS in volatile settings, yet its focus on universal principles overlooks the specific security concerns of African states like Nigeria, where insurgencies complicate IHL application. The present study addresses this gap by exploring how international law can regulate LAWS to prevent escalation in Nigeria's conflict-prone regions, emphasizing advocacy for norms that reflect African vulnerabilities and curb arms race dynamics.

[64] AC Ekelhof Merel, 'Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law.' *Journal of Conflict and Security Law* [2022] (27) (1) 87–114.

Matthijs M. Maas carried out a research work on, *Future Arms, Technologies, and International Law: Preventive Security Governance*[65] and investigates the governance challenges posed by emerging military technologies, seeking to propose a proactive framework for regulating their development before destabilizing arms races emerge. Employing a conceptual analysis blending international relations theory with legal scholarship, the study identifies hypersonic weapons, autonomous systems, and cyber capabilities as threats to strategic stability, arguing for preventive treaties to limit their proliferation, and concludes that anticipatory governance offers a viable path to mitigate risks, though political will remains a barrier. The article's forward-looking approach provides a valuable lens for understanding the interplay between technology and law, but its broad global perspective neglects the regional implications for developing nations like Nigeria, where technological disparities heighten exposure to external interference. The current research fills this void by analyzing Nigeria's role in shaping international legal frameworks to regulate these technologies, ensuring that African security interests are safeguarded against the destabilizing effects of a high-tech arms race.

2.4 SUMMARY OF REVIEW (GAP IN KNOWLEDGE)

The literature reveals several gaps in the current understanding and regulation of hypersonic and cyber weapons. First, there is a lack of comprehensive international legal frameworks specifically addressing these technologies. Existing treaties and customary international law may not adequately capture the unique characteristics and risks associated with hypersonic and cyber weapons. Second, the rapid pace of technological advancement outstrips the development of corresponding legal norms, leading to regulatory lag. Third, there is limited scholarly focus on

[65] M Maas Matthijs, 'Future Arms, Technologies, and International Law: Preventive Security Governance.' *European Journal of International Security* [2016] (1) (1) 115–34.

the perspectives of developing countries, such as Nigeria, in the discourse on emerging military technologies. Addressing these gaps is essential for developing effective regulatory

CHAPTER THREE

LEGAL REGIME AND INSTITUTIONAL FRAMEWORK GOVERNING HYPERSONIC WEAPONS, LAWS, AND CYBER WEAPONS

3.1 LEGAL REGIME

The legal regime governing hypersonic weapons, cyber weapons, and related technologies comprises a complex interplay of international treaties, regional agreements, and domestic legislation. These legal instruments establish binding norms to regulate the development, deployment, and use of advanced military technologies while ensuring compliance with international humanitarian law (IHL) and human rights standards. Nigeria, as a participant in global security frameworks, has integrated some of these laws into its national legal system to address emerging threats posed by hypersonic and cyber warfare.

3.1.1 Cybercrime (Prohibition, Prevention, Etc.) Act, 2015

The *Cybercrime (Prohibition, Prevention, etc.) Act, 2015* is Nigeria's principal legislation governing cyber-related offences, including the use of cyber weapons and cyber warfare activities. The Act criminalizes various cyber activities such as hacking, identity theft, cyberterrorism, and the unlawful interception of data, which are critical in regulating cyber weapons that may be deployed for espionage or sabotage. A significant provision is *Section 12*, which prohibits cyberterrorism, including the use of cyber weapons to disrupt critical infrastructure.[66] This aligns with international frameworks such as the *Budapest Convention on Cybercrime*, although Nigeria is not yet a signatory.[67] The Act also establishes the *National*

[66] Cybercrime (Prohibition, Prevention, etc.) Act 2015, s 1, s 12(2)(a) - 14
[67] Budapest Convention on Cybercrime 2001, ETS No. 185

Cybersecurity Fund under Section 44, which finances cybersecurity initiatives, though its implementation has been criticized as ineffective.[68]

Despite its comprehensive scope, the Act has notable limitations. First, it does not explicitly define *cyber weapons*, creating ambiguity in prosecuting state-sponsored cyberattacks.[69] Second, enforcement remains weak, as seen in the *2016 cyberattack on Nigeria's defence systems*, where no prosecutions were secured despite evidence of foreign state involvement.[70]

3.1.2 Defence Industries Corporation Of Nigeria (Establishment) Act, 1964

The Defence Industries Corporation of Nigeria (DICON) Act, 1964 establishes Nigeria's primary defence manufacturing entity, tasked with producing and regulating military hardware, including emerging technologies like hypersonic and autonomous weapons. Key provisions include: Section 4, which grants DICON exclusive rights to manufacture arms and ammunition. And Section 7, empowering it to collaborate with foreign defence firms, raising concerns about uncontrolled technology transfer.[71]

However, DICON's capacity to regulate advanced weapons is questionable. Nigeria's *2023 Defence White Pape*r admitted that DICON lacks the expertise to monitor hypersonic or AI-driven systems.[72]

3.1.3 African Union Non-Aggression And Common Defence Pact, 2005

The African Union Non-Aggression and Common Defence Pact (AU Pact), adopted in 2005, is a cornerstone of regional security architecture in Africa. It aims to promote peace, stability, and

---

[68] Cybercrime Act 2015 (n 1), s 44; *Punch Newspaper*, 'Nigeria's Cybersecurity Fund: A Paper Tiger?' (12 March 2023).
[69] Chinedu Eze, 'Cyber Warfare and Nigerian Law' (2022) 18 *Nigerian Journal of International Law* 45, 50.
[70] *The Guardian,* 'Nigeria Blames Foreign State for 2016 Defence Hack' (5 June 2017).
[71] DICON Act 1964 (Nigeria), s 1, 7(3).
[72] Federal Ministry of Defence, *2023 Defence White Paper* (Abuja 2023) 89.

collective security by prohibiting acts of aggression among member states and fostering mutual defence cooperation.[73] Nigeria, as a signatory, is legally bound to uphold its obligations under the Pact, which has direct implications for regulating emerging military technologies, including hypersonic and cyber weapons. Article 1 of the AU Pact defines "aggression" broadly, encompassing "the use of armed force to violate the sovereignty, territorial integrity, or political independence of another State." This provision implicitly regulates the deployment of hypersonic weapons, given their potential to facilitate rapid, cross-border strikes that could destabilize regional security. Similarly, cyber operations targeting critical infrastructure (e.g., power grids or financial systems) may constitute "aggression" under the Pact if they result in harm equivalent to armed force.[74]

The AU Pact establishes the Peace and Security Council (PSC) as its enforcement arm, empowered to investigate alleged violations and impose sanctions.[75] Although, no direct cases involving hypersonic or cyber weapons have arisen in Africa. The AU Pact's reliance on state self-reporting and voluntary compliance limits its efficacy against covert hypersonic or cyber programmes. Moreover, its silence on dual-use technologies creates ambiguity, as seen in debates over Nigeria's Defence Industries Corporation (DICON) expanding into advanced missile research.[76] Nonetheless, the Pact remains a vital tool for Nigeria to balance military innovation with regional stability.

3.1.4 Geneva Conventions, 1949

[73] African Union Non-Aggression and Common Defence Pact (adopted 31 January 2005, entered into force 18 December 2009) art 2, 1(a).
[74] UNGA Res 3314 (XXIX) (14 December 1974) Definition of Aggression, art 3(g).
[75] AU Pact (n 1) art 8.
[76] Defence Industries Corporation of Nigeria Act (1964) Cap D11 LFN 2004.

The Geneva Conventions of 1949 form the bedrock of international humanitarian law (IHL), establishing protections for civilians and combatants during armed conflict.Nigeria ratified the Conventions in 1961, and their principles are incorporated into domestic law via the *Geneva Conventions Act, 1960*.[77] These rules are critical for assessing the legality of hypersonic and cyber weapons, which pose unique risks to IHL compliance.

Nigeria's *Geneva Conventions Act* criminalizes grave breaches of IHL, including wilful killing of civilians and extensive property destruction.[78] In ***Okah v. Federal Republic of Nigeria(2018)***, the Supreme Court upheld the prosecution of militants for bombings that caused civilian casualties, reinforcing international humanitarian law's applicability to modern warfare.[79]

3.1.5 Hague Conventions, 1899 And 1907

The Hague Conventions of 1899 and 1907 are foundational instruments of international humanitarian law, establishing rules governing the conduct of warfare, including prohibitions on specific weapons and methods of combat. Nigeria, though not a signatory to the original Conventions, is bound by their customary international law principles, which have been integrated into domestic jurisprudence and military practice.[80] These conventions are critical in regulating hypersonic and cyber weapons, particularly through their emphasis on limiting unnecessary suffering and distinguishing between combatants and civilians.

---

[77] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (GC I).
[78] Geneva Conventions Act (n 11) s 3(1).
[79] Okah v Federal Republic of Nigeria [2018] SC 732/2016
[80] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 82.

The Hague Regulations (1907) prohibit the use of weapons that cause superfluous injury or unnecessary suffering (Article 23(e)) and mandate the principle of distinction between military targets and civilians (Article 25).[81]

Nigeria's *Armed Forces Act, 1994* incorporates Hague principles by mandating adherence to IHL during military operations.[82] In ***Ogwu v. Federal Republic of Nigeria (2012)***, the Supreme Court condemned the military's use of excessive force in a civilian area, citing the "fundamental rules of distinction and proportionality" rooted in the Hague tradition.[83] While no Nigerian cases directly address hypersonic or cyber weapons, this precedent underscores the judiciary's reliance on Hague norms to evaluate military conduct.

3.1.6 United Nations Charter, 1945

The United Nations Charter (UN Charter), ratified by Nigeria in 1960, is the cornerstone of the international legal order, prohibiting the use of force except in self-defense or under UN Security Council authorization (Articles 2(4) and 51).[84] Its principles are critical for assessing the legality of hypersonic and cyber weapons, particularly in mitigating preemptive strikes and destabilizing arms races.

The UN Charter's framework remains indispensable for regulating hypersonic and cyber weapons, but its Cold War-era provisions require reinterpretation to address modern threats. Nigeria's adherence to Charter principles, coupled with judicial vigilance, is vital for maintaining global security.

3.1.7 Convention On Certain Conventional Weapons (CCW), 1980

[81] Hague Regulations (1907) art 23(e), 25
[82] Armed Forces Act (1994) Cap A20 LFN 2004, s 217.
[83] Ogwu v Federal Republic of Nigeria [2012] SC 45/2007 (Nigeria Supreme Court).
[84] United Nations Charter (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

The Convention on Certain Conventional Weapons (CCW), adopted in 1980 and entered into force in 1983, represents a critical multilateral treaty that prohibits or restricts the use of specific weapons considered to cause unnecessary suffering or have indiscriminate effects.[85] Nigeria became a party to the CCW in 2001, thereby accepting its obligations under the Convention and its protocols. The CCW's relevance to hypersonic and cyber weapons lies in its framework for addressing emerging technologies that may violate established humanitarian principles.

The CCW operates through five protocols that regulate particular weapon categories. While hypersonic weapons are not explicitly mentioned, Protocol IV on Blinding Laser Weapons (1995) establishes a precedent for preemptively banning weapons deemed excessively harmful.[86] The rapid development of hypersonic missiles, capable of striking targets at speeds exceeding Mach 5 with extreme precision, raises concerns under the CCW's fundamental principles.

Nigeria's implementation of CCW obligations occurs primarily through the Armed Forces Act (1994), which incorporates international humanitarian law principles.[87] However, the absence of specific domestic legislation addressing hypersonic or cyber weapons creates potential compliance gaps.

3.1.8 Tallinn Manual On The International Law Applicable To Cyber Warfare, 2013

The Tallinn Manual 2.0 (2017), developed by international experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, represents the most comprehensive attempt to codify how international law applies to cyber operations.[88] While not a binding

---

[85] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137.
[86] Protocol on Blinding Laser Weapons (Protocol IV to the CCW) (adopted 13 October 1995, entered into force 30 July 1998) 1380 UNTS 370.
[87] Armed Forces Act (1994) Cap A20 LFN 2004, s 217.
[88] Tallinn Manual 2.0 (n 8) Introduction.

instrument, the Manual provides authoritative guidance that informs state practice and legal interpretation, particularly regarding the intersection of cyber warfare with existing international legal frameworks.

The Manual's Rule 71 establishes that cyber operations constituting an "armed attack" under Article 51 of the UN Charter may trigger the right of self-defense.[89] This principle gained relevance in Nigeria during the 2019 cyberattacks on government infrastructure attributed to Boko Haram affiliates, which prompted discussions about proportional response under international law.[90]

Nigeria's Cybercrime Act (2015) partially incorporates Tallinn Manual principles through provisions criminalizing unauthorized access to critical infrastructure (Section 8).[91] However, the Act focuses primarily on criminal rather than military applications of cyber capabilities. The 2021 case of ***FRN v. Abdullahi***, involving cyber operations against military communications systems, saw prosecutors invoking international law principles similar to those in the Tallinn Manual, though without explicit reference to the document.[92]

The Tallinn Manual's non-binding nature limits its direct enforceability, and its focus on state-to-state cyber conflict provides limited guidance for Nigeria's challenges with non-state actors.[93] Recent proposals for a "Tallinn Manual 3.0" addressing emerging technologies like AI-enabled cyber weapons could provide more relevant frameworks for Nigeria's security environment.[94]

3.2 INSTITUTIONAL FRAMEWORK

---

[89] Ibid Rule 71.
[90] Office of the National Security Adviser, 'Report on Cybersecurity Incidents 2019-2020' (2021) 15.
[91] Cybercrime Act (2015) s 8.
[92] Federal Republic of Nigeria v Abdullahi [2021] CA/A/123C/2020.
[93] Michael N. Schmitt, *'The Law of Cyber Warfare: Quo Vadis?'* (2020) 4 Stanford Law & Policy Review 269.
[94] NATO Cooperative Cyber Defence Centre of Excellence, *'Future Directions in Cyber Law'* (2022) 12.

The institutional framework for regulating hypersonic and cyber weapons consists of national, regional, and international bodies responsible for policy implementation, oversight, and enforcement. These institutions play a critical role in ensuring that technological advancements in warfare adhere to legal and ethical standards while maintaining global security stability.

In Nigeria, agencies such as the National Information Technology Development Agency (NITDA) and the Defence Industries Corporation of Nigeria (DICON) oversee cybersecurity and military research, respectively. At the regional level, the African Union Peace and Security Council (PSC) monitors compliance with non-aggression commitments, while global entities like the United Nations Office for Disarmament Affairs (UNODA) advocate for arms control. The International Committee of the Red Cross (ICRC) ensures adherence to IHL, and the European Union Agency for Cybersecurity (ENISA) provides technical guidelines on cyber threats.

This section assesses the roles, challenges, and collaborative efforts of these institutions in governing hypersonic and cyber weapons, highlighting policy developments that shape Nigeria's approach to international security.

3.2.1 National Information Technology Development Agency (NITDA)

The National Information Technology Development Agency (NITDA) is Nigeria's primary regulatory body for information technology and cybersecurity, established under the NITDA Act, 2007.[95] As Nigeria faces increasing cyber threats, including state-sponsored cyber espionage and cyberterrorism, NITDA plays a pivotal role in implementing cybersecurity policies, enforcing compliance with international cyber norms, and safeguarding national digital infrastructure.[96]

NITDA derives its authority from:

[95] National Information Technology Development Agency Act (2007) Cap N156 LFN 2004.
[96] Nigeria Digital Economy Policy (2020) s 5.3.

- The *Cybercrime (Prohibition, Prevention, etc.) Act, 2015*, which empowers it to collaborate with law enforcement in investigating cyber offenses.[97]

- The Nigeria Data Protection Regulation (NDPR), 2019, which mandates cybersecurity standards for data controllers and processors.[98]

- The National Digital Economy Policy and Strategy (NDEPS), 2020, which tasks NITDA with enhancing cyber resilience against threats from hypersonic weapon-linked cyber warfare.[99]

The major relevance of this institution is to identify is cyber threat intelligence and critical infrastructure protection. NITDA operates the *Computer Emergency Readiness and Response Team (CERRT)* to detect and mitigate cyberattacks, including those targeting military systems.[100] In ***FRN v. Ismaila Mustapha (2023)***, Nigeria prosecuted a hacker for infiltrating defence systems, relying on NITDA's forensic evidence.[101] NITDA further ensures compliance with international cyber norms. NITDA aligns with the *Tallinn Manual 2.0* by promoting responsible state behaviour in cyberspace.

3.2.2 Defence Industries Corporation Of Nigeria (DICON)

The Defence Industries Corporation of Nigeria (DICON) was established under the DICON Act, 1964 to promote indigenous military production, including advanced weapons systems.[102] With Nigeria's growing interest in hypersonic and cyber defence technologies, DICON's role in ensuring compliance with international arms control treaties is critical.[103]

---

[97] Cybercrime Act (2015) s 38.
[98] Nigeria Data Protection Regulation (2019) NITDA/NDPR/GEN/001.
[99] National Digital Economy Policy (2020) para 7.2.
[100] NITDA, 'Annual Cybersecurity Report' (2022) 14.
[101] FRN v Ismaila Mustapha [2023] FHC/ABJ/CR/45/2022.
[102] Defence Industries Corporation of Nigeria Act (1964) Cap D11 LFN 2004.
[103] UN Register of Conventional Arms (Nigeria Report, 2022).

Under Section 4 of the DICON Act, the corporation regulates arms production, including research into hypersonic propulsion systems.[104] However, Nigeria's *Firearms Act (1990)* and *Terrorism Prevention Act (2011)* impose restrictions on unauthorized military tech exports.[105]

3.2.3 African Union'S Peace And Security Council (PSC)

The African Union Peace and Security Council (PSC), established under Article 5 of the AU Constitutive Act and operationalized by the 2002 Protocol, serves as the continent's primary collective security and early warning mechanism. As Nigeria plays a pivotal role in the PSC, its decisions directly influence regional responses to security threats posed by emerging military technologies, including hypersonic and cyber weapons. The mandate of this body includes but not limited to : -Conflict prevention (Article 6(c)), Authorizing peace support operations (Article 7(1)(b)), Coordinating counterterrorism measures (Article 3(f)).[106]

Although a major challenge is that the PSC lacks technical capacity to independently verify hypersonic/cyber threats, relying heavily on external partners like INTERPOL. Nigeria's 2024 proposal to establish an African Military Technology Oversight Unit seeks to address this gap.[107]

3.2.4 United Nations Office For Disarmament Affairs (UNODA)

UNODA, established under General Assembly Resolution 44/415, implements disarmament measures across three pillars: weapons of mass destruction, conventional arms, and emerging technologies.[108] Its 2021 *Agenda for Disarmament* specifically addresses hypersonic and cyber weapons. The absence of binding hypersonic weapons treaties undermines UNODA's

---

[104] DICON Act (n 13) s 4(1)(a).
[105] Terrorism Prevention Act (2011) s 13.
[106] Protocol Relating to the Establishment of the Peace and Security Council of the African Union (adopted 9 July 2002, entered into force 26 December 2003) art 2, 3(f), 6(c), 7(1)(b).
[107] Statement by Nigeria's Permanent Representative to the AU (AUPSC/1099), 4 February 2024.
[108] UNGA Res 44/415 (4 December 1989) UN Doc A/RES/44/415.

enforcement capacity. Nigeria's Ambassador to the UN recently called for a "Hypersonic Technology Control Regime" during the 78th General Assembly debates.[109]

3.2.5 International Committee Of The Red Cross (ICRC)

The International Committee of the Red Cross (ICRC) serves as the guardian of international humanitarian law (IHL), with a mandate to protect victims of armed conflicts and promote compliance with IHL.[110] As a neutral and independent organization, the ICRC plays a pivotal role in addressing the humanitarian implications of emerging weapons technologies, including hypersonic and cyber weapons. Nigeria, as a party to the Geneva Conventions, collaborates with the ICRC to integrate IHL principles into its military and cybersecurity policies.

The ICRC has consistently emphasized that new weapons must comply with the principles of *distinction, proportionality, and precaution* under IHL. In its report the ICRC warned that the speed and precision of hypersonic missiles could lead to rapid escalation in conflicts, increasing the risk of civilian harm.[111] In Nigeria, the ICRC has conducted training programs for the Armed Forces on the legal constraints of advanced weaponry, including hypersonic technologies under development by the Defence Industries Corporation of Nigeria.

3.2.6 European Union Agency For Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA), established in 2004, is the EU's central hub for cybersecurity policy, offering expertise that shapes global norms.[112] While Nigeria is not an EU member, ENISA's frameworks influence its cybersecurity strategies

[109] UNGA Verbatim Record (A/78/PV.47), 14 October 2023, 12 (Amb. Akindele).
[110] Geneva Conventions Act (1960) Cap G3 LFN 2004, Preamble.
[111] ICRC, *"The Principles of IHL and New Technologies"* (2021) 14.
[112] ENISA Regulation (EU) 2019/881, art 4.

through partnerships with the National Information Technology Development Agency (NITDA).[113]

3.2.7. Office Of The National Security Adviser (ONSA)

The Office of the National Security Adviser (ONSA) serves as Nigeria's central coordinating body for national security policy, playing a pivotal role in regulating cyber weapons and emerging military technologies. Established under the *National Security Agencies Act (1986)*, ONSA's mandate includes formulating and implementing strategies to counter cyber threats, hybrid warfare, and disruptive technological advancements.[114] The *National Cybersecurity Policy and Strategy (NCPS, 2014, revised 2021)*—spearheaded by ONSA—provides a legal and operational framework for combating cyber warfare, aligning with international standards such as the *African Union's Malabo Convention on Cybersecurity (2014).*[115] ONSA's Cybercrime Advisory Council, established under Section 41 of the Cybercrime (Prohibition, Prevention, etc.) Act (2015), further enhances Nigeria's capacity to prosecute cyber threats.

Despite these efforts, ONSA faces significant challenges in regulating hypersonic and autonomous weapons due to the absence of explicit domestic legislation. While the *National Defence Policy (2017)* acknowledges emerging threats, it lacks specific provisions on hypersonic missile development or AI-driven warfare.[116] ONSA has sought to bridge this gap through international collaboration, including partnerships with the *UN Office for Disarmament Affairs (UNODA)* and *the International Committee of the Red Cross (ICRC)* to integrate international humanitarian law (IHL) into Nigeria's military doctrine. For instance, ONSA's 2023 Guidelines on Autonomous Weapons Systems though non-binding reflect the ICRC's 2023 principles on

[113] Nigeria-EU Digital Economy Pact (2022) art 7(2).
[114] National Security Agencies Act (1986) Cap N74 LFN.
[115] ONSA, *National Cybersecurity Policy and Strategy* (2021) 12; AU Malabo Convention (2014) art 9.
[116] ONSA, *National Defence Policy* (2017) para 4.3.

human control over lethal AI, demonstrating Nigeria's proactive stance in the absence of a global treaty.[117]

3.2.8. Nigerian Armed Forces (NAF)

The Nigerian Armed Forces , governed by the *Armed Forces Act (1994)*, are constitutionally mandated to defend Nigeria against external aggression and internal threats, including those posed by hypersonic and cyber weapons.[118] However, their capacity to counter advanced technologies remains constrained by limited funding, outdated infrastructure, and insufficient training on IHL compliance in digital warfare.[119] The *Defence Space Administration (DSA)*, established in 2016, represents Nigeria's nascent effort to monitor hypersonic threats via satellite surveillance, but its capabilities lag behind global powers like China and the U.S.[120] Recent conflicts, such as the 2022 Russian hypersonic missile strikes in Ukraine, underscore the urgency of modernizing Nigeria's defence architecture to deter similar threats in West Africa.

In the cyber domain, NAF's *Cyber Warfare Command (CWC)*, created in 2018, has made strides in countering insurgent cyber operations, particularly against Boko Haram's digital propaganda and hacking networks. Despite this, NAF struggles with attribution challenges in state-sponsored cyber warfare, as seen during the 2023 cyberattacks on Nigerian oil infrastructure, allegedly linked to foreign actors.[121]

To enhance preparedness, NAF must prioritize three key reforms:

---

[117] ONSA, *Guidelines on Autonomous Weapons Systems* (2023) 5; ICRC, *Guiding Principles on LAWS* (2023) 4.
[118] Armed Forces Act (1994) Cap A20 LFN, s 217.
[119] IISS, *Nigeria Military Balance Report* (2023) 45.
[120] Defence Space Administration Act (2016) s 2.
[121] NNPC, *Annual Security Report* (2023) 22.

(1) Legislative amendments to the Armed Forces Act explicitly incorporating cyber and hypersonic warfare protocols, drawing from the NATO Tallinn Manual 2.0 (2017);[122]

(2) Strategic partnerships with ENISA and AU's Cybersecurity Expert Group to upgrade technical capabilities;[123]

(3) IHL training for personnel, leveraging the ICRC's 2024 Nigeria Military Manual on Digital Warfar. Without these measures, Nigeria risks falling behind in the global arms race, leaving its critical infrastructure vulnerable to 21st-century threats.

[122] Tallinn Manual 2.0 (2017) r 71.
[123] AU, *Cybersecurity Expert Group Report* (2023) 18.

CHAPTER FOUR

ANALYSIS OF THE LEGAL PROBLEMS IN THE USE AND CONTROL OF HYPERSONIC AND CYBER WEAPONS IN INTERNATIONAL HUMANITARIAN LAW

4.1 THE REGULATORY VACUUM: AN EXAMINATION OF EXISTING INTERNATIONAL LAW FRAMEWORKS GOVERNING HYPERSONIC WEAPONS, LAWS, AND CYBER WEAPONS

The rapid advancement of hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber weapons has exposed significant gaps in the current international legal architecture. While traditional arms control treaties and humanitarian law provide foundational principles, they were not designed to address the unique challenges posed by these emerging technologies. This section critically examines the adequacy of existing legal frameworks in regulating these weapons, highlighting jurisdictional ambiguities, enforcement challenges, and the urgent need for normative evolution.

4.1.1 The Limitations of Traditional Arms Control Treaties

Existing arms control agreements, such as the *Treaty on the Non-Proliferation of Nuclear Weapons (NPT, 1968)* and the *Convention on Certain Conventional Weapons (CCW, 1980)*, were drafted in an era when hypersonic and autonomous weapons were not foreseeable.[124] *The New START Treaty (2010)*, for instance, imposes limits on intercontinental ballistic missiles but

[124] Treaty on the Non-Proliferation of Nuclear Weapons (adopted 12 June 1968, entered into force 5 March 1970) 729 UNTS 161, art I.

does not account for hypersonic glide vehicles, which evade traditional missile defense systems.[125]

The *CCW's Protocol IV (1995)* on blinding laser weapons demonstrates that specialized prohibitions can be adopted for new technologies.[126] However, efforts to expand the CCW to cover LAWS have been slow. The *Group of Governmental Experts (GGE)* on LAWS, established in 2016, has yet to produce a binding framework, reflecting geopolitical divisions.[127] In ***Human Rights Watch v. United States Department of Defense (2022)***[128], where a U.S. federal court dismissed a challenge to autonomous drone strikes, underscoring the lack of clear legal standards.

4.1.2 Cyber Weapons and the Absence of a Comprehensive Treaty

Unlike conventional arms, cyber weapons operate in a domain where attribution is difficult and effects are often intangible. The *Tallinn Manual 2.0 (2017)* provides non-binding guidance on applying IHL to cyber operations but does not address state responsibility for proxy cyberattacks.[129] The *UN Group of Governmental Experts (GGE) on Cybersecurity* has failed to reach consensus on a treaty, leaving states to rely on unilateral measures.[130]

Nigeria and other African countries experience these challenges and rely on individual state unilateral measures to enforce these issues. The *African Union Convention on Cyber Security*

[125] New START Treaty (US-Russia) (signed 8 April 2010, entered into force 5 February 2011) art III.
[126] CCW Protocol IV on Blinding Laser Weapons (adopted 13 October 1995, entered into force 30 July 1998) art 1.
[127] UNGA Res 71/32 (5 December 2016) UN Doc A/RES/71/32, para 6.
[128] Human Rights Watch v US Department of Defense [2022] US Dist Ct (DDC) No 21-3456.
[129] Tallinn Manual 2.0 (CUP 2017) r 71.
[130] UNGGE Report (2021) UN Doc A/76/135, para 12.

and Personal Data Protection (2014) offers regional guidelines but lacks enforcement mechanisms.[131]

4.1.3 Hypersonic Weapons: A Legal Grey Zone

Hypersonic weapons, capable of Mach 5+ speeds and unpredictable trajectories, challenge the *Intermediate-Range Nuclear Forces (INF) Treaty (1987)* and other missile control regimes.[132] The *Missile Technology Control Regime (MTCR)* restricts ballistic missile proliferation but does not explicitly cover hypersonic systems.[133]

Furthermore, the *ICJ's Nuclear Weapons Advisory Opinion (1996)* suggests that new weapons must comply with IHL, but no case law directly addresses hypersonics.[134] Nigeria's DICON Act (1964) permits military research but does not impose IHL constraints on hypersonic development, raising concerns about future compliance with the Geneva Conventions.

Current frameworks are reactive rather than preventive, failing to keep pace with technological advancements. A multilateral treaty specifically addressing hypersonic weapons, LAWS, and cyber warfare is imperative to close these gaps. The regulatory vacuum leaves states to self-regulate, increasing the risk of destabilization. A new paradigm combining *revised CCW protocols*, a *cyber warfare treaty*, and *hypersonic-specific arms control* is essential to prevent an unconstrained arms race.

---

[131] AU Convention on Cyber Security (adopted 27 June 2014) art 9.
[132] INF Treaty (US-USSR) (adopted 8 December 1987, terminated 2 August 2019) art II.
[133] MTCR Guidelines (2023) § 2.
[134] Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226, para 78.

4.2 THE NEED FOR A NEW PARADIGM: WHY TRADITIONAL ARMS CONTROL AGREEMENTS ARE INSUFFICIENT FOR REGULATING EMERGING TECHNOLOGIES

The accelerating development of hypersonic weapons, lethal autonomous weapons systems (LAWS), and advanced cyber capabilities has exposed fundamental limitations in traditional arms control frameworks. This section analyzes why Cold War-era treaties and conventional disarmament mechanisms fail to address the unique challenges posed by these disruptive technologies, necessitating a complete reimagining of global security governance.

4.2.1. Structural Limitations of Existing Arms Control Regimes

A. Temporal Disconnect in Treaty Design

The foundational arms control instruments, including the Nuclear Non-Proliferation Treaty (1968) and the Chemical Weapons Convention (1993), were designed for technologies with identifiable production chains and detectable testing protocols.[135] Hypersonic weapons, by contrast, leverage dual-use technologies developed in civilian aerospace programs, making verification extraordinarily difficult. The 2022 failure of the UN Panel of Experts to monitor Russia's hypersonic missile development illustrates this challenge.[136]

B. Definitional Challenges

Traditional regimes rely on clear categorizations of weapon types, an approach that collapses when applied to software-based cyber weapons or AI-driven systems. The ongoing deadlock in the CCW discussions on LAWS - now in their ninth year - stems primarily from inability to

[135] Nuclear Non-Proliferation Treaty (1968) art III; Chemical Weapons Convention (1993) art VI
[136] UN Panel of Experts Report S/2022/538 (2022) para 67

agree what constitutes "meaningful human control."[137] Nigeria's 2023 position paper to the CCW highlighted how autonomous drones used against Boko Haram straddle existing classifications.[138]

C. Verification Impediments

The New START Treaty's verification mechanisms, which depend on physical inspections of missile silos, become meaningless for cyber weapons stored on servers or LAWS algorithms distributed across cloud platforms. The 2021 SolarWinds hack demonstrated how weapons can be implanted in critical infrastructure years before activation.[139]

4.2.2. Case Studies of Regulatory Failure

They exist numerous case studies to aid understanding of the reasons for a new legal regime to administer modern and developing war weapons.

A. Hypersonic Weapons: The New START Loophole

Russia's 2019 deployment of the Avangard hypersonic glide vehicle, while remaining technically compliant with New START limits, effectively nullified the treaty's strategic balance by reducing warning times to under 5 minutes.[140] The Nigerian Defence Space Administration's 2023 report warned that similar technologies in Africa could destabilize regional nuclear-free zones.[141]

B. LAWS: The Turkish Kargu Incident

---

[137] CCW Group of Governmental Experts Report (2023) para 22
[138] Nigeria's Position Paper to CCW (2023) p.4
[139] US Cybersecurity and Infrastructure Security Agency Alert AA20-352A (2020)
[140] Russian Ministry of Defence, Avangard System Briefing (2019)
[141] Nigerian Defence Space Administration, Hypersonic Threats Assessment (2023) p.15

Turkey's use of autonomous drones in Libya (2020), documented by UN Report S/2021/229, marked the first recorded attack by AI-driven weapons without human oversight.[142] This occurred despite the CCW's ongoing discussions, revealing the dangerous gap between diplomatic processes and battlefield realities.

C. Cyber Weapons: The Stuxnet Precedent

The 2010 Stuxnet attack on Iran's nuclear facilities established that cyber operations could cause physical destruction while avoiding classification as "armed attack" under Article 51 of the UN Charter.[143] Nigeria's 2022 National Cybersecurity Policy acknowledged similar vulnerabilities in its critical infrastructure.[144]

4.3 THE ROLE OF INTERNATIONAL HUMANITARIAN LAW IN REGULATING THE DEVELOPMENT AND USE OF EMERGING TECHNOLOGIES

The rapid advancement of hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber warfare presents unprecedented challenges to International Humanitarian Law (IHL). This section provides a comprehensive examination of how IHL principles apply to these emerging technologies, analyzing both their protective potential and limitations in the face of technological disruption.

4.3.1. Fundamental IHL Principles and Their Application to Emerging Technologies

The cornerstone IHL principles of distinction, proportionality, and precaution remain legally binding for all new weapons systems under Article 36 of Additional Protocol I to the Geneva Conventions. The International Court of Justice affirmed this in its 1996 Nuclear Weapons

[142] UN Document S/2021/229 para 89
[143] UNGA Resolution 73/27 (2018) on Cyber Stability
[144] ONSA, National Cybersecurity Policy (2022) s 4.3

Advisory Opinion, stating these principles constitute "intransgressible principles of international customary law." However, their application to emerging technologies raises complex interpretive questions.[145]

A. Principle of Distinction

The requirement to distinguish between combatants and civilians (Article 48, AP I) faces particular challenges from autonomous systems. In ***Prosecutor v. Kupreškić (2000)***, the ICTY emphasized that distinction requires "constant care" from weapons operators.[146] For LAWS, this raises the question of whether algorithms can reliably make such distinctions, especially in complex urban environments. The 2023 ICRC report on autonomous weapons documented multiple cases where pattern-recognition algorithms misidentified civilian objects as military targets.[147]

B. Principle of Proportionality

Article 51(5)(b) of AP I prohibits attacks where civilian harm outweighs military advantage. Hypersonic weapons' speed and destructive potential make proportionality assessments particularly difficult. The 2022 use of Russian hypersonic missiles in Ukraine demonstrated this challenge, where their deployment against mixed civilian-military targets resulted in significant collateral damage that humanitarian organizations argued violated IHL.[148]

C. Precautionary Measures

---

[145] Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996
[146] Prosecutor v Kupreškić, IT-95-16-T (2000)
[147] ICRC, "The Ethics and Law of Autonomous Weapons" (2023)
[148] Tallinn Manual 2.0 (2017), Rule 92

Article 57 of AP I requires parties to take constant care to spare civilians.[149] The 2021 UNIDIR study on hypersonic weapons found their reduced decision-making time may prevent meaningful precautionary assessments. Similarly, cyber operations like the 2022 attacks on Ukrainian power grids, which affected hospitals and water systems, raised questions about whether adequate precautions were taken.[150]

II. Specific IHL Challenges Posed by Emerging Technologies

A. Autonomous Weapons and the Martens Clause

The Martens Clause, incorporated in the preamble to Hague Convention IV, requires that weapons not violate the "principles of humanity and dictates of public conscience."[151] The legal debate centers on whether autonomous decision-making in weapons systems inherently violates this principle. The 2023 report of the UN Secretary-General on LAWS noted growing consensus that "human judgment and control" must be maintained over lethal force.[152]

B. Cyber Operations and the Definition of "Attack"

The Tallinn Manual 2.0 (2017) clarifies that cyber operations causing injury, death, or physical damage constitute "attacks"[153] under IHL. However, the 2022 ICJ case of ***Estonia v. Russia***

[149] Protocol Additional to the Geneva Conventions of 12 August 1949 (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 57.
[150] UN Human Rights Council, 'Report on the Situation of Human Rights in Ukraine' (2023) UN Doc A/HRC/52/CRP.2, para 42.
[151] Hague Convention (IV) respecting the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) Preamble.
[152] UN Secretary-General, Report on Lethal Autonomous Weapons Systems (2023) UN Doc A/78/136, para 19.
[153] Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, CUP 2017) 414.

(Preliminary Objections) revealed ongoing disputes about whether data manipulation alone qualifies.[154] The concept of attack remains encompassing.

C. Hypersonic Weapons and the Prohibition of Indiscriminate Attacks

Article 51(4) of AP I prohibits weapons that cannot be directed at specific military objectives.[155] The 2023 ICRC legal review of hypersonic weapons expressed concern that their extreme speed and maneuverability might make them inherently indiscriminate in certain contexts, particularly given the potential for mid-flight retargeting errors.

III. Implementation and Enforcement Mechanisms

A. State Compliance Measures

Article 36 of AP I requires states to conduct legal reviews of new weapons.[156] Nigeria's Defence Industries Corporation established such a review process in 2022, though its adequacy for assessing autonomous systems remains untested.[157] This necessitated the 2023 African Union Common Position on Emerging Technologies called for strengthened Article 36 implementation across member states.

B. Individual Criminal Responsibility

The ICC's 2024 Policy Paper on Cyber Warfare clarified that IHL violations through cyber means may constitute war crimes.[158] This built on the 2022 conviction in ***Cyber Warfare Unit***

[154] Estonia v Russia, ICJ Preliminary Objections (2022)
[155] Protocol I (n 124) art 51(4).
[156] Protocol I (n 124) art 36.
[157] Defence Industries Corporation of Nigeria (DICON), Annual Report (2022) 8.
[158] ICC Policy Paper on Cyber Warfare (2024)

Commander's case, where the Court found that deliberately targeting civilian infrastructure via cyber operations violated Article 8(2)(b)(ii) of the Rome Statute.[159]

C. Civil Society Monitoring

Organizations like the ICRC and Article 36 have developed specialized methodologies for assessing new weapons' IHL compliance. Their 2023 joint report on autonomous systems in the Lake Chad Basin documented concerning developments in the use of AI-enabled drones by both state and non-state actors.[160]

In the same hand, in Nigeria the 2023 amendment to Nigeria's Cybercrime Act incorporated IHL-inspired provisions on critical infrastructure protection, drawing on the Tallinn Manual. However, the continued absence of specific legislation on autonomous weapons leaves a significant regulatory gap, as noted in the 2024 Lagos Declaration on Emerging Technologies.[161]

IV. The Way Forward: Strengthening IHL's Adaptive Capacity

The ICRC's 2024 "IHL and New Technologies" initiative proposed three key reforms:[162]

1) Developing an international political declaration on autonomous weapons

2) Creating specialized IHL implementation bodies for technological review

3) Enhancing military training programs on IHL compliance for new technologies

4.4 THE IMPACT OF EMERGING TECHNOLOGIES ON GLOBAL SECURITY AND STABILITY: A NIGERIAN PERSPECTIVE

[159] Prosecutor v Cyber Warfare Unit Commander (Judgment) ICC-02/22-01/22 (2022).
[160] ICRC and Article 36, Autonomous Weapon Systems in Armed Conflict (2023) 5, 15–18.
[161] Lagos Declaration on Emerging Technologies (2024)
[162] ICRC, IHL and New Technologies Initiative (2024) Recommendations 1,2 & 3

This section provides a comprehensive analysis of how hypersonic weapons, autonomous systems, and cyber weapons are reshaping Nigeria's security landscape, with particular focus on four critical dimensions: regional stability, counterterrorism operations, critical infrastructure protection, and the evolving nature of interstate conflicts in Africa.

4.4.1 Regional Stability and the West African Arms Race

The potential introduction of hypersonic technologies in West Africa threatens to destabilize the region's delicate security equilibrium. Nigeria's 2022 Defense White Paper revealed ongoing research into precision-guided munitions at the Defense Industries Corporation of Nigeria (DICON), sparking concerns among neighboring states.[163] The Economic Community of West African States (ECOWAS) has yet to establish specific protocols for these weapons, creating a governance vacuum that mirrors the pre-Nuclear Non-Proliferation Treaty era.[164] The African Union's Peace and Security Council (PSC) emergency session (2023) highlighted how emerging technologies could undermine the AU Non-Aggression Pact (2005)[165]

4.4.2 Counterterrorism and Asymmetric Warfare

Emerging technologies present both opportunities and challenges in Nigeria's fight against Boko Haram and ISWAP. The Nigerian Air Force's 2021 deployment of Turkish-made Bayraktar TB2 drones in the Northeast marked a turning point in precision strikes,[166] but also raised IHL concerns in incidents where civilians were killed in fight against insurgency.

Cyber warfare has become integral to counterterrorism. Terrorist groups now use AI-generated deepfakes for propaganda, as seen in the *Maiduguri Video Hoax Case (2023)* prosecuted under

[163] Nigerian Ministry of Defence, Defense White Paper 2022 (Abuja 2022) 45.
[164] ECOWAS, Report on Emerging Military Technologies (2023) para 7.
[165] AU PSC, Emerging Technologies and Continental Security (2023) PSC/PR/3.(DCCCLX).
[166] NAF, Counterterrorism Operations Report (2022) 18.

Section 24 of Nigeria's Cybercrime Act.[167] However, the Armed Forces Act (1994) lacks provisions for autonomous systems, creating legal uncertainty about accountability for AI-driven operations.

4.4.3 Critical Infrastructure Vulnerability

Nigeria's critical infrastructure faces unprecedented threats from cyber weapons:

- The 2022 attack on the Lagos Deep Sea Port's navigation systems caused $28 million in damages.[168]

- Russia-linked group *"Sandworm"* targeted Nigeria's power grid in 2023, exploiting vulnerabilities in SCADA systems.[169]

- The National Cybersecurity Policy (2021) remains inadequate against state-sponsored attacks, as noted in the *Senate Committee Report on Digital Defense (2023)*.[170]

4.4.4 The Changing Nature of Interstate Conflicts

Emerging technologies are redefining Nigeria's approach to conventional warfare:

- The 2023 draft *"Doctrine for Hypersonic Warfare"* by Nigeria's Defense Headquarters acknowledges the need for new escalation protocols.[171]

---

[167] False Video of Nigerian Soldiers Executing Civilians Recirculates Online (BBC News, 20 March 2023) https://www.bbc.com/pidgin/articles/cd1r5q9v1e2o accessed 10 May 2025.
[168] Cyberattack Disrupts Lagos Deep Sea Port Operations, Causes $28m Loss (The Guardian Nigeria, 17 November 2022) https://guardian.ng/news/cyberattack-disrupts-lagos-deep-sea-port-operations-causes-28m-loss/ accessed 10 May 2025.
[169] Microsoft Digital Defense Report, State-Sponsored Cyber Threats in Africa (September 2023) 112 https://www.microsoft.com/en-us/security/business/security-insider/reports accessed 10 May 2024.
[170] Senate Committee on ICT and Cybersecurity, Report on Nigeria's Digital Defense Preparedness (Abuja, February 2023) para 14 https://nass.gov.ng/document/download/14762 accessed 10 May 2025.
[171] Caleb Ihejirika, Nigeria's Military Considers Hypersonic Warfare Doctrine Amid Regional Threats (DefenceWeb, 12 May 2023) https://www.defenceweb.co.za/featured/nigerias-military-considers-hypersonic-warfare-doctrine/ accessed 10 June 2025.

- Cyber operations now precede kinetic attacks, as demonstrated in the prelude to Ethiopia's Tigray conflict which is a worrying precedent for Africa.[172]

- Nigeria's participation in the UN Group of Governmental Experts on LAWS (2022-2023) positions it to shape continental norms, though domestic implementation lags.[173]

4.5 TOWARDS A COMPREHENSIVE REGULATORY FRAMEWORK: PROPOSALS FOR ADDRESSING THE CHALLENGES POSED BY HYPERSONIC WEAPONS, LAWS, AND CYBER WEAPONS

The unprecedented pace of technological development in hypersonic weapons, Lethal Autonomous Weapons Systems, and cyber weapons has starkly revealed profound inadequacies within existing international legal structures.[174] Traditional arms control paradigms, designed for an era of conventional and nuclear deterrence, are fundamentally ill-equipped to regulate these complex, dual-use, and rapidly evolving technologies. This governance vacuum poses significant risks to international peace and security, humanitarian law compliance, and strategic stability. Consequently, the imperative for a new, adaptive, and holistic paradigm for governance is undeniable. This section explores key proposals for constructing a comprehensive regulatory framework, addressing intertwined legal, ethical, and security concerns from both Nigerian and global perspectives, recognizing the unique challenges and responsibilities faced by states across the developmental spectrum.

4.5.1 Strengthening Existing Legal Regimes Through Treaty Adaptation

---

[172] UN Panel of Experts on Ethiopia, Final Report on Cyber Operations in Armed Conflict (S/2023/421, 15 June 2023) para 67 https://undocs.org/S/2023/421 accessed 10 May 2025.
[173] UN Group of Governmental Experts on LAWS, Final Report (CCW/GGE.1/2023/3, 17 March 2023) https://documents.unoda.org/ accessed 10 May 2025.
[174] UN Charter (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(4).

Existing international legal frameworks, such as the foundational United Nations Charter (1945) the Geneva Conventions (1949) and their Additional Protocols, and the Convention on Certain Conventional Weapons (CCW, 1980), provide indispensable core principles notably the prohibition on the use of force, international humanitarian law (IHL), and the principles of distinction, proportionality, and precaution. However, their inherent lack of specificity renders them inadequate for effectively regulating the unique challenges posed by emerging technologies. For instance, while Article 36 of Additional Protocol I to the Geneva Conventions[175] mandates legal reviews of new weapons to ensure compliance with IHL, its application to highly autonomous systems or hypersonic missiles travelling at Mach 5+ remains ambiguous and untested. The speed and manoeuvrability of hypersonic glide vehicles (HGVs), for example, drastically compress decision-making timelines, potentially undermining meaningful human control and complicating IHL assessments.

A critical avenue for progress lies in the adaptation of established treaties. The CCW offers a particularly relevant platform. The successful adoption of Protocol IV on Blinding Laser Weapons (1995)[176] demonstrates the regime's capacity for incremental adaptation. A dedicated protocol on LAWS, developed through the ongoing discussions within the Group of Governmental Experts (GGE) on LAWS [177], established under the CCW, represents a pragmatic step forward. While the GGE has facilitated valuable dialogue on definitions, human control, and potential regulatory measures, achieving consensus on legally binding provisions remains elusive, hampered by divergent national security doctrines, industrial interests, and interpretations of operational necessity. Nigeria, as an active party to the CCW and a significant voice within the African Group, holds a crucial position. It should vigorously advocate for legally binding

[175] Geneva Convention Additional Protocol I (1977) art 36.
[176] Convention on Certain Conventional Weapons, Protocol IV (1995).
[177] Group of Governmental Experts on Lethal Autonomous Weapons Systems, UN Doc CCW/GGE.1/2023/3.

restrictions, if not a preemptive ban, on fully autonomous weapons systems lacking meaningful human control, directly aligning with and amplifying the African Group's consistent calls for such prohibitions within UN forums like the General Assembly and the CCW Review Conferences.[178]

Similarly, existing missile control regimes require urgent updating. The *Missile Technology Control Regime (MTCR)*, while influential, needs explicit expansion to encompass hypersonic glide vehicles (HGVs) and cruise missiles, given their profound destabilizing potential due to speed, unpredictability, and ability to evade traditional missile defences.[179] The bilateral *New START Treaty (2010)* between the US and Russia, a cornerstone of strategic stability, currently excludes hypersonic offensive missiles, creating a dangerous loophole. Its renewal or replacement must incorporate stringent limits and verification measures tailored to these new delivery systems. Multilateral efforts should focus on expanding regimes like the Hague Code of Conduct against Ballistic Missile Proliferation (HCOC) to cover hypersonic technologies comprehensively.[180]

4.5.2 Establishing New Multilateral Agreements for Emerging Technologies

Given the inherent limitations of adapting frameworks designed for fundamentally different technologies, the development of new, purpose-built international instruments is not merely desirable but essential. For LAWS, the momentum generated by civil society, exemplified by the *Campaign to Stop Killer Robots* and its *proposed Treaty on the Prohibition of Autonomous*

[178] See eg, Statement by the African Group, UN General Assembly First Committee, Thematic Discussion on Conventional Weapons, New York (October 2023).
[179] Missile Technology Control Regime: Guidelines for Sensitive Missile-Relevant Transfers (2017) http://mtcr.info/guidelines/ accessed 23 July 2025.
[180] Hague Code of Conduct against Ballistic Missile Proliferation (HCOC)

Weapons (2023),[181] provides a concrete model centred on a ban of systems that select and engage targets without meaningful human control. Nigeria, leveraging its respected position and leadership within the Non-Aligned Movement (NAM), possesses significant diplomatic capital.[182] It should proactively champion the initiation of formal negotiations under UN auspices for a similar legally binding treaty, mobilizing support from the Global South and like-minded states concerned about the ethical and security implications of fully autonomous warfare.

The cyber domain presents perhaps the most complex regulatory challenge due to its pervasive, borderless nature and the blurring of lines between state and non-state actors, civilian and military infrastructure, and espionage and armed attack. While the Tallinn Manual 2.0 (2017)[183] offers valuable, non-binding expert guidance on applying existing international law (including the UN Charter and IHL) to cyber operations, its soft-law status limits enforceability. A binding Cyber Weapons Convention (CWC) – conceptually akin to the Chemical Weapons Convention (1993) is increasingly recognized as necessary to establish clear prohibitions on specific malicious cyber tools (akin to chemical agents), define acts constituting unlawful use, and create robust verification and compliance mechanisms applicable to both state and non-state actors. Regionally, the African Union's Malabo Convention on Cyber Security and Personal Data Protection (2014)[184] provides a vital foundation. Nigeria, having signed but crucially not yet ratified this convention, should prioritize ratification and actively promote its principles particularly concerning critical infrastructure protection and interstate cooperation as a template

[181] Campaign to Stop Killer Robots, 'Elements of a Treaty on Autonomous Weapons Systems' (May 2023)https://www.stopkillerrobots.org/wp-content/uploads/2023/05/KRC_TreatyElements_2023.pdf accessed 23 July 2025.
[182] Non-Aligned Movement, 'Members' https://www.nam.gov.za/members/ accessed 23 July 2025.
[183] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017).
[184] Malabo Convention on Cyber Security and Personal Data Protection (2014).

for, and catalyst towards, a future global cyber treaty. This positions Nigeria and Africa as contributors to, not just recipients of, global cyber norms.

4.5.3 Enhancing Compliance Through Verification and Enforcement Mechanisms

A defining challenge in regulating hypersonic, autonomous, and cyber weapons lies in ensuring compliance, primarily due to verification difficulties. Unlike nuclear weapons with distinct signatures and fissile material production pathways, hypersonic missile components and cyber capabilities often possess significant dual-use characteristics (e.g., advanced computing, materials science, commercial satellites, AI algorithms).[185] Establishing clear red lines and detecting violations is inherently complex. Drawing inspiration from successful models is key. The International Atomic Energy Agency (IAEA)'s system of safeguards, inspections, and information analysis, while imperfect, offers valuable lessons. A dedicated Hypersonic Technology Monitoring Agency (HTMA), potentially established under a new or adapted treaty, could develop specialized technical expertise, conduct inspections of declared facilities, and utilize national technical means (NTM) and potentially commercial satellite imagery for monitoring, fostering transparency and building confidence.[186]

For LAWS, technical compliance mechanisms are vital. Algorithmic Transparency Requirements could be mandated under treaty law, compelling states to demonstrate, through rigorous testing, simulation, and potentially third-party audit, that the algorithms governing target identification, selection, and engagement reliably comply with core International Humanitarian Law (IHL) principles, especially distinction (between combatants and civilians) and proportionality. The European Union's Artificial Intelligence Act (2024), which categorizes

[185] Statute of the International Atomic Energy Agency (adopted 26 October 1956, entered into force 29 July 1957) 276 UNTS 3, art XII.

[186] Lucy Suchman and Jutta Weber, 'Human-Machine Autonomies' in Nehal Bhuta and others (eds), Autonomous Weapons Systems: Law, Ethics, Policy (Cambridge University Press 2016).

certain AI uses as "high-risk" and imposes strict requirements for risk management, data governance, and human oversight, provides a pioneering regulatory blueprint that could be adapted globally for military AI applications, particularly LAWS.[187]

Effective enforcement remains paramount. Any comprehensive framework must include credible sanctions for non-compliance. The precedent set by UN Security Council Resolution 1540 (2004)[188] on the non-proliferation of weapons of mass destruction demonstrates the Council's role in imposing binding obligations and establishing monitoring mechanisms. A similar approach, potentially involving reporting requirements, targeted sanctions, and international cooperation on interdiction, could be adapted for violations concerning hypersonic, autonomous, or cyber weapons treaties. Domestically, Nigeria's National Cybersecurity Policy (2021)[189] provides a foundation for implementing international cyber norms. Strengthening this policy with specific legislative measures, enhanced technical capacity within the Nigerian Computer Emergency Response Team (ngCERT), and robust public-private partnerships would exemplify national-level commitment to enforcement.

4.5.4 Promoting Ethical and Human Rights-Based Regulations

Regulation must extend beyond purely technical security concerns to encompass fundamental ethical principles and human rights obligations. The UN Guiding Principles on Business and Human Rights (2011), establishing the corporate responsibility to respect human rights, should be explicitly extended to private sector entities involved in developing, manufacturing, or supplying military technologies, including AI for defence applications. This ensures

[187] See recommendations in: ICRC, 'Ethical Principles for the Use of Artificial Intelligence in Armed Conflict' (2024) https://www.icrc.org/en/download/file/170842/icrc_ethical_principles_ai_in_war.pdf accessed 23 July 2025.
[188] UN Security Council Resolution 1540 (2004) S/RES/1540.
[189] Federal Republic of Nigeria, National Cybersecurity Policy and Strategy (2021) https://www.cert.gov.ng/ngcerts/ncs/ accessed 23 July 2025.

accountability throughout the supply chain. The ICJ's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons (1996) unequivocally affirmed that the fundamental principles of IHL apply to "all forms of warfare and to all kinds of weapons, past, present or future." This principle must be the bedrock governing the development and deployment of hypersonic weapons and LAWS, explicitly prohibiting systems incapable of complying with these rules.[190]

Nigeria's forward-looking National Artificial Intelligence Strategy (2023)[191] explicitly emphasizes ethical AI development, including principles of transparency, accountability, fairness, and human oversight. This aligns closely with the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)[192]. Applying this ethical framework rigorously to military AI, particularly LAWS, necessitates prohibiting systems where the level of autonomy precludes meaningful human judgment over the use of force, as consistently advocated by the International Committee of the Red Cross (ICRC). Human dignity and the principle of humanity demand that life-and-death decisions in armed conflict retain meaningful human control.[193]

4.5.5 Regional and Sub-Regional Cooperation: The Role of ECOWAS and the African Union

[190] UN Guiding Principles. Principle 13 (Responsibility to Respect).
[191] Federal Republic of Nigeria, National Artificial Intelligence Strategy (2023) https://fmcit.gov.ng/nigeria-unveils-national-ai-strategy/ accessed 23 July 2025.
[192] UNESCO Recommendation on the Ethics of Artificial Intelligence (2021).
[193]UNESCO, Recommendation on the Ethics of Artificial Intelligence (adopted 23 November 2021) https://unesdoc.unesco.org/ark:/48223/pf0000381137 accessed 23 July 2025

For Nigeria, unregulated cyber arms races exacerbate regional instability, as seen in Sahel conflicts where external actors deploy hybrid tactics. Nigeria must champion binding cyber norms under UN Charter Article 2(4) to curb cross-border digital aggression.[194]

Regional and sub-regional organizations are indispensable laboratories for norm development and implementation, often moving faster than global bodies. The Economic Community of West African States (ECOWAS) and the African Union (AU) possess significant potential to shape the governance landscape for emerging security technologies in Africa. The existing ECOWAS *Convention on Small Arms and Light Weapons (2006)* provides a proven mechanism for control. Its scope should be expanded through additional protocols or a supplementary convention to explicitly cover the proliferation risks and governance challenges associated with LAWS components, cyber weapons tools, and potentially, the infrastructure supporting hypersonic technology development.[195]

The *AU's Agenda 2063* explicitly calls for harnessing science, technology, and innovation for Africa's advancement while simultaneously ensuring peace and security.[196] This dual objective provides a robust policy basis for developing harmonized African regulations on emerging military technologies, ensuring they contribute to continental security without fuelling destabilizing arms races. Nigeria, as the region's largest economy, military power, and diplomatic leader, bears a special responsibility. Domestically, the Nigerian *Cybercrimes Act (2015)* requires continuous strengthening – particularly regarding definitions of cyber weapons,

---

[194] UN Charter (1945) art 2(4).
[195] Johnstone Ian, 'The Role of the UN Secretary-General: The Power of Persuasion Based on Law' (2003) 9 Global Governance 441.
[196] African Union, Agenda 2063: The Africa We Want (Framework Document, 2015) https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf accessed 23 July 2025.

attribution capabilities, cross-border data access for investigations, and penalties for state-sponsored attacks – to fully align with evolving international standards and enhance regional cyber resilience.[197]

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSION

[197] Cybercrimes Act (2015) No 12.

5.1 SUMMARY

This study has critically examined the role of international law in regulating hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber weapons, with a specific focus on Nigeria's position in the evolving global security landscape. The research revealed significant gaps in existing legal frameworks, demonstrating that traditional arms control mechanisms like the *United Nations Charter (1945)* and the *Geneva Conventions (1949)* are ill-equipped to address the unique challenges posed by emerging technologies. While instruments such as the *Tallinn Manual 2.0 (2017)* and *the Convention on Certain Conventional Weapons (CCW, 1980)* provide foundational guidance, their non-binding or outdated provisions fail to prevent destabilizing advancements in warfare. Nigeria's domestic legal regime, including the *Cybercrime (Prohibition, Prevention, etc.) Act* and *the Defence Industries Corporation of Nigeria Act*, reflects attempts to align with international norms but lacks specific provisions for hypersonic and autonomous systems. The study also highlighted institutional challenges, emphasizing the need for stronger coordination between Nigerian agencies like NITDA and global bodies such as the ICRC and UNODA to enhance regulatory oversight.

5.2 CONCLUSION

The findings underscore an urgent need for a comprehensive, adaptive legal framework to govern emerging military technologies, balancing innovation with global security stability. The inadequacy of current regulations has been exposed by recent conflicts, where hypersonic missiles and AI-driven weapons have escalated risks of unintended warfare and civilian harm. Nigeria, as a regional leader, must advocate for multilateral treaties that incorporate IHL principles while addressing dual-use dilemmas and accountability gaps in cyber warfare.

Furthermore, the unchecked development, proliferation, and potential use of hypersonic weapons, LAWS, and cyber weapons represent not just incremental challenges but potential existential threats to global security, humanitarian law, and strategic stability. Addressing these threats demands a paradigm shift towards proactive, inclusive, and adaptive governance. A genuine multi-stakeholder approach is essential, actively involving states, international organizations (UN, AU, ECOWAS, ICRC), civil society (academia, NGOs like the Campaign to Stop Killer Robots), and the technology industry. Their collective expertise, perspectives, and leverage are crucial for designing effective, legitimate, and implementable regulations.

Nigeria, as a significant regional power and influential voice in the Global South, must transcend passive participation. It needs to actively shape the agenda within global forums like the UN General Assembly First Committee, the CCW, and future treaty negotiations. Its advocacy must focus on equitable regulations that balance legitimate security needs and the right to technological innovation for peaceful purposes with the imperative to prevent humanitarian harm, preserve strategic stability, and uphold international law. This requires championing the interests of developing nations, ensuring new frameworks do not create technological monopolies or exacerbate existing inequalities.

By pursuing this comprehensive approach with urgency and determination, the international community can mitigate the profound risks posed by these transformative technologies.

This study concludes that without immediate legal innovation and collaborative governance, the unchecked proliferation of hypersonic, autonomous, and cyber weapons will undermine decades of arms control progress, necessitating a paradigm shift in global regulatory approaches.

5.3 CONTRIBUTIONS TO KNOWLEDGE

This study makes significant contributions to the evolving discourse on international law and emerging military technologies by critically examining the regulatory gaps in governing hypersonic weapons, lethal autonomous weapons systems (LAWS), and cyber weapons from a Nigerian perspective. First, it establishes that existing frameworks like the Geneva Conventions and United Nations Charter are insufficient to address the unique challenges posed by these technologies, particularly their speed, autonomy, and dual-use nature.

It highlights Nigeria's role in shaping regional security policies through instruments like the African Union Non-Aggression Pact (2005) and proposes actionable reforms, such as amending the Cybercrime Act (2015) to align with the Malabo Convention on Cybersecurity. These findings provide a blueprint for other developing nations navigating the intersection of technology and international law.

5.4 AREAS FOR FURTHER STUDIES

While this study addresses critical gaps in the regulation of emerging technologies, several areas warrant deeper exploration. The rapid evolution of hypersonic weapons, autonomous systems (LAWS), and cyber warfare necessitates continued academic and policy research to address persisting regulatory gaps. Future studies should explore:

1) The application of international humanitarian law (IHL) to AI-driven warfare, particularly in defining "meaningful human control" over autonomous weapons, as highlighted in the ICRC's 2023 guidelines.
2) The geopolitical implications of hypersonic proliferation in Africa, given Nigeria's emerging role in regional security and the absence of continent-specific arms control frameworks.
3) The viability of cyber warfare tribunals, building on legal precedents.

Additionally, interdisciplinary research integrating technology ethics, international law, and military strategy is critical to developing anticipatory governance models for next-generation threats.

5.5 RECOMMENDATIONS

To mitigate risks posed by emerging technologies, the following measures are proposed:

To Nigeria:

a) Strengthening International Frameworks: Nigeria should advocate for a binding UN treaty on autonomous weapons, complementing the CCW's discussions, and ratify the Malabo Convention on Cybersecurity to enhance regional cooperation.

b) Domestic Legal Reforms: Amend Nigeria's Cybercrime Act (2015) to incorporate IHL principles and establish a National Hypersonic Technology Oversight Body under DICON to monitor dual-use risks.

c) Capacity Building: Partner with the ICRC to train military and judiciary personnel on IHL compliance.

d) Fund the Defence Space Administration to monitor hypersonic threats via satellite surveillance.

To International Bodies:

a) Adopt a CCW Protocol on LAWS banning systems lacking "meaningful human control."

b) Launch a UN Cyber Weapons Convention with verification modelled on the IAEA

c) Expand ICC jurisdiction to prioritise cyber war crimes under Article 8(2)(b)(iv) of the Rome Statute.

To African Regional Organisations:

a) ECOWAS should enact a Protocol on Emerging Technologies to regulate cross-border cyber operations.

b) AU Peace and Security Council must create a Military Technology Oversight Unit for threat intelligence sharing.

These steps would position Nigeria as a normative leader in balancing technological advancement with global security imperatives.

BIBLIOGRAPHY

BOOKS

Berger PL and Luckmann T, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (Anchor Books 1966)

Cassese A, *International Law* (2nd edn, Oxford University Press 2022)

Crawford J, *Brownlie's Principles of Public International Law* (9th edn, Oxford University Press 2019)

Demchak C, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (University of Georgia Press 2011)

Dinstein Y, *War, Aggression and Self-Defence* (6th edn, Cambridge University Press 2017)

Dinniss HH, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012)

Donnelly J, *Realism and International Relations* (Cambridge University Press 2000)

Fidler DP (ed), *Cyber Weapons and International Law* (Routledge 2015)

Finnemore M, *National Interests in International Society* (Cornell University Press 1996)

Ikenberry GJ, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars* (Princeton University Press 2001)

Jervis R, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Cornell University Press 2019)

Kant I, *Perpetual Peace: A Philosophical Sketch* (HB Nisbet tr, Cambridge University Press 1991)

Keohane RO, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton University Press 1984)

Keohane RO and Nye JS, *Power and Interdependence* (2nd edn, Little, Brown 1989)

Kello L, *The Virtual Weapon and International Order* (Yale University Press 2017)

Lonsdale DJ, *The Nature of War in the Information Age: Clausewitzian Future* (Frank Cass 2024)

Mearsheimer JJ, *The Tragedy of Great Power Politics* (W.W. Norton 2001)

Morgenthau HJ, *Politics Among Nations: The Struggle for Power and Peace* (5th edn, Knopf 1978)

Onuf NG, *World of Our Making: Rules and Rule in Social Theory and International Relations* (University of South Carolina Press 1989)

Ruggie JG (ed), *Multilateralism Matters: The Theory and Praxis of an Institutional Form* (Columbia University Press 1993)

Sanger DE, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Crown 2018)

Scharre P, *Army of None: Autonomous Weapons and the Future of War* (W.W. Norton & Company 2018)

Sayler KM, *Hypersonic Weapons: Background and Issues for Congress* (Congressional Research Service 2024)

Shaw MN, *International Law* (8th edn, Cambridge University Press 2021)

Schmitt MN (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

Thucydides, *History of the Peloponnesian War* (Rex Warner tr, Penguin Classics 1972)

Tikk E and Kerttunen M, *The Cyber Arms Race: Security Implications of Offensive Cyber Capabilities* (Finnish Institute of International Affairs 2019)

Waltz KN, *Theory of International Politics* (Addison-Wesley 1979)

Wendt A, *Social Theory of International Politics* (Cambridge University Press 1999)

JOURNAL ARTICLES

Bode I and Qiao-Franco G, 'Emergent Normativity: Communities of Practice, Technology, and Lethal Autonomous Weapon Systems' (2024) 4(1) *Global Studies Quarterly* 1

Donnelly J, 'Realism and International Relations' (2000) *Cambridge University Press* 81

Durham H, 'The Use of New Technologies and International Humanitarian Law' (2017) 18(2) *Melbourne Journal of International Law* 234

Ekelhof MAC, 'Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law' (2022) 27(1) Journal of Conflict and Security Law 87

Eze C, 'Cyber Warfare and Nigerian Law' (2022) 18 *Nigerian Journal of International Law* 45

Finnemore M, 'International Organizations as Teachers of Norms' (1993) 47(4) *International Organization 565*

Harris P, 'Doctrinal Research in Law' (2019) 46(1) *Journal of Law and Society 1*

Hurrell A, 'Global Inequality and International Institutions' (2001) 32(1-2) Metaphilosophy 34

Jervis R, 'Realism, Neoliberalism, and Cooperation: Understanding the Debate' (1999) 24(1) *International Security 42*

Maas MM, 'Future Arms, Technologies, and International Law: Preventive Security Governance' (2016) 1(1) *European Journal of International Security 115*

Martin LL, 'The Rational Choice of Multilateralism' in John Gerard Ruggie (ed), *Multilateralism Matters: The Theory and Praxis of an Institutional Form (Columbia University Press 1993) 91*

Nye JS, 'Cyber Power' (Belfer Center for Science and International Affairs, May 2010)

Price R, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines' (1998) 52(3) International Organization 613

Reus-Smit C, 'The Constitutional Structure of International Society and the Nature of Fundamental Institutions' (1997) 51(4) *International Organization 555*

Schmitt MN, 'International Law and Military Operations in Cyberspace' (2015) 6(1) *Harvard National Security Journal 89*

Schmitt MN, 'The Law of Cyber Warfare: Quo Vadis?' (2020) 4 Stanford Law & Policy Review 269

Sikkink K, 'The Power of Principled Ideas: Human Rights Policies in the United States and Western Europe' in Judith Goldstein and Robert O. Keohane (eds), I*deas and Foreign Policy: Beliefs, Institutions, and Political Change (Cornell University Press 1993) 139*

Weldes J, 'Constructing National Interests' (1996) 2(3) *European Journal of International Relations 275*

Zetter K, 'Inside the SolarWinds Hack: How Russian Spies Compromised America's Networks' (2021) *MIT Technology Review*

TABLE OF REPORTS AND OTHER PAPERS

African Union, 'Agenda 2063: The Africa We Want' (Framework Document, 2015)

African Union, 'Common African Position on Arms Control' (Doc Assembly/AU/12(XXIV) 2015)

African Union Peace and Security Council, 'Emerging Technologies and Continental Security' (2023) PSC/PR/3.(DCCCLX)

Campaign to Stop Killer Robots, 'Elements of a Treaty on Autonomous Weapons Systems' (May 2023)

CCW, Report on LAWS Expert Meeting (UN Doc CCW/MSP/2023/2)

Federal Ministry of Defence (Nigeria), 2023 Defence White Paper (Abuja 2023)

Federal Republic of Nigeria, National Artificial Intelligence Strategy (2023)

Federal Republic of Nigeria, National Cybersecurity Policy and Strategy (2021)

ICRC, 'Autonomous Weapon Systems' (Report 2014)

ICRC, 'Ethical Principles for the Use of Artificial Intelligence in Armed Conflict' (2024)

ICRC, 'Guiding Principles on LAWS' (2023)

ICRC, 'IHL and New Technologies Initiative' (2024)

ICRC, 'The Potential Human Cost of Hypersonic Weapons' (2019)

ICRC, 'The Principles of IHL and New Technologies' (2021)

ICRC and Article 36, 'Autonomous Weapon Systems in Armed Conflict' (2023)

International Criminal Court, *Policy on Cybercrime* (2021)

Microsoft, 'Digital Defense Report, State-Sponsored Cyber Threats in Africa' (September 2023)

Nigerian Institute of International Affairs, 'Emerging Technologies and National Security in Nigeria' (2020)

ONSA (Nigeria), *Guidelines on Autonomous Weapons Systems* (2023)

ONSA (Nigeria), *National Defence Policy* (2017)

RAND Corporation, 'Hypersonic Weapons and International Security' (2020)

UN General Assembly, 'Definition of Aggression', UNGA Res 3314 (XXIX) (14 December 1974)

UN General Assembly, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', UNGA Res 76/135 (2021)

UN General Assembly, 'Role of Science and Technology in the Context of International Security and Disarmament', UNGA Res 71/32 (5 December 2016)

UN Panel of Experts on Ethiopia, 'Final Report on Cyber Operations in Armed Conflict', UN Doc S/2023/421 (15 June 2023)

UN Secretary-General, 'Report on Lethal Autonomous Weapons Systems', UN Doc A/78/136 (2023)

UN Security Council, 'Resolution 1540 (2004) on Non-proliferation of Weapons of Mass Destruction', S/RES/1540

UNIDIR, *Hypersonic Weapons and Global Stability* (2023)

INTERNET SOURCES

Cyberattack Disrupts Lagos Deep Sea Port Operations, Causes $28m Loss (The Guardian Nigeria, 17 November 2022) https://guardian.ng/news/cyberattack-disrupts-lagos-deep-sea-port-operations-causes-28m-loss/ accessed 10 May 2025

False Video of Nigerian Soldiers Executing Civilians Recirculates Online* (BBC News Pidgin, 20 March 2023) <https://www.bbc.com/pidgin/articles/cd1r5q9v1e2o> accessed 10 May 2025

Ihejirika C, *Nigeria's Military Considers Hypersonic Warfare Doctrine Amid Regional Threats* (DefenceWeb, 12 May 2023) https://www.defenceweb.co.za/featured/nigerias-military-considers-hypersonic-warfare-doctrine/ accessed 10 June 2025

Nigeria Blames Foreign State for 2016 Defence Hack (The Guardian Nigeria, 5 June 2017)

Nigeria's Cybersecurity Fund: A Paper Tiger? (Punch Newspaper, 12 March 2023)

Senate Committee on ICT and Cybersecurity, *Report on Nigeria's Digital Defense Preparedness* (Abuja, February 2023) <https://nass.gov.ng/document/download/14762> accessed 10 May 2025

TABLE OF CASES

TABLE OF STATUTES