CYBER WARFARE IN THE RUSSIA-UKRAINE CONFLICT: AN EMERGING THREAT TO INTERNATIONAL PEACE AND SECURITY (2022-2025)

BY

TIKUECHUKWU KAMBILI ANENE-ARINZE

GOU/U22/IRE/657

DEPARTMENT OF POLITICAL SCIENCE AND INTERNATIONAL RELATIONS,
FACULTY OF MANAGEMENTAND SOCIAL SCIENCES,
GODFREY OKOYE UNIVERSITY THINKERS CORNER ENUGU,
NIGERIA

JULY 2026.

DECLARATION

I, Tikuechukwu Kambili Anene-Arinze, hereby declare that this research project titled: “Cyber Warfare in theRussia-Ukraine Conflict: An Emerging Threat to International Security and Peace (2022–2025)” was written and presented by me in the Department of Political Science and International Relations, and has not been presented elsewhere for the purpose of obtaining any degree or certificate. All sources of information used in this study have been duly acknowledged and referenced.

_____ _____

TIKUECHUKWU KAMBILI ANENE-ARINZE DATE

APPROVAL PAGE

This research project titled "Cyber Warfare in the Russia–Ukraine Conflict: An Emerging Threat to International Security and Peace (2022–2025)" has been carefully read, supervised, and approved as meeting the requirements for the award of a Degree in the Department of International Relations, Godfrey Okoye University, Enugu State, Nigeria.

_____ _____

REV. SR. DR. LUCY UMEH **DATE**

(Project Supervisor)

_____ _____

PROF. BARR. SAMUEL UGWUOZOR **DATE**

Department of International Relations

_____ _____

PROF. JOHN ODO **DATE**

Dean, Faculty of Management and

Social Sciences

_____ _____

External Examiner **DATE**

DEDICATION

I dedicate this project to Almighty God for His grace, wisdom, strength, and guidance throughout the course of this study.

ACKNOWLEDGEMENTS

First and foremost, I give all thanks and praise to Almighty God for His endless mercy, wisdom, protection, and unwavering grace throughout the course of my academic journey.

I owe a profound debt of gratitude to my amiable and dedicated supervisor, Rev. Sr. Dr. Lucy Umeh whose patience, guidance, and immense knowledge in research writing greatly shaped this work. Her constant availability, valuable corrections, and direction at every stage of this study made the entire process smoother and more rewarding. I sincerely pray that God continues to bless and uplift her abundantly.

I am equally grateful to all the lecturers in the Department of Political Science and International Relations who have impacted my academic and personal life positively over the past four years. Your teachings, mentorship, and encouragement have contributed immensely to my growth. In a special way, I also acknowledge the immense support of the Dean of the Faculty of Management and Social Sciences, Prof. John Odo and Prof. Barr. Samuel Ugwuozor, my esteemed Head of Department, for his fatherly support, guidance, and inspiration throughout my stay in the department.

My sincere appreciation also goes to Rev. Sr. Dr. Lucy Umeh, Dr. Kingsley Ezechi, Dr. N.C Mbaeze, Mr. Okonkwo W.O, Dr. Alex Ogbonnya, Dr. Amadi Cletus, Mr. Anthony Onyishi, Dr. (Mrs.) Fransisca Ifedi, Rev. Fr. Dr. Ikenna Ogbuka, Prof. Ochioha, and Mr. Ajibo C.C. whose contributions and encouragement I will always cherish.

Furthermore, I deeply appreciate the Secretary of the Department of Political Science and International Relations, Mrs. Chioma, whose assistance and support contributed significantly to my academic progress and overall educational experience.

To everyone who contributed directly or indirectly to the success of this work, I remain sincerely grateful. May God bless and reward you all abundantly.

I also wish to express my heartfelt gratitude to my beloved family for their immeasurable love, prayers, sacrifices, and unwavering support throughout my academic journey. My deepest appreciation goes to my wonderful mother, Mrs. Nkiru Anene-Arinze, whose constant encouragement, care, and dedication have been a great source of strength and motivation to me. I am equally grateful to my siblings, Chidubem Anene-Arinze, Munachimso Chelsea Anene-Arinze, and Chimbusomma Nnenna Anene-Arinze, for their love, understanding, and moral support throughout this period. My sincere thanks also go to my aunty and role model, Mrs. Obi Nwokedi, for her kindness, encouragement, and support, as well as to my grandmother, Mrs. Nneka Enwezor, whose prayers and wise counsel have continually inspired me. I am also deeply thankful to my uncle, Ossy Enwezor, for his encouragement and support during my years of study.

Special appreciation also goes to my dear friends, Amarachi Judith, Samson Okosi, Mmesoma, and Agu Goodnews, whose friendship, support, motivation, and prayers contributed immensely to making this academic journey a successful and memorable one. May God richly bless and reward you all abundantly.

TABLE OF CONTENTS

ABSTRACT

This study examined cyber warfare in the Russia–Ukraine conflict as an emerging threat to international peace and security between 2022 and 2025. The study focused on how cyber warfare threatened international peace and how cyber security strategies affected the crisis between Russia and Ukraine during the period under study. The research was motivated by the increasing use of cyber operations in modern interstate conflicts and the growing vulnerability of global digital infrastructure and international security systems. The study adopted Structural Realism (Neorealism) as its theoretical framework and utilized an ex-post facto research design. Data were collected through secondary sources, including academic journals, cybersecurity reports, policy documents, institutional publications, and international media reports. Data analysis was conducted using content analysis, supported by historical and comparative methods. Findings revealed that cyber warfare significantly threatened international peace and security by targeting critical infrastructure such as government institutions, communication systems, energy facilities, banking networks, and digital platforms, thereby increasing geopolitical tensions and risks of escalation within the international system. The study further found that cyber warfare generated transnational spill-over effects that disrupted multinational corporations, global communication systems, and international economic activities beyond the immediate conflict zone. In addition, findings showed that cyber security strategies significantly affected the Russia–Ukraine crisis, as Ukraine's cyber resilience, strengthened through international cooperation, intelligence sharing, and cloud-based security systems, reduced the effectiveness of several cyber attacks during the conflict. The study recommended stronger international cyber governance frameworks, improved cyber diplomacy, enhanced cooperation among states and international organizations, and increased investment in cyber defense mechanisms and digital infrastructure protection.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The international system has witnessed a radical change in the nature of warfare. Kinetic military action and acquisition of territory, the type of warfare that prevailed in the past, has smaller and smaller been complemented (and in others, supplanted) by non-kinetic forms of warfare, especially cyber warfare. The development of digital technologies, the spread of cyberspace, and an increasing dependence of states on information and communication technologies have established new spheres of vulnerability and conflict (Kello, 2023; Nye, 2024). Subsequently, cyber space has become a vital space of power projections, strategic competition as well as conflict among states.

Cyber warfare can be defined as the application of digital attacks to interfere, harm, or destroy the information systems, infrastructure, or network of an enemy by a state or non-state for either political or military purposes (Schmitt, 2023). Cyber operations unlike in normal warfare can be conducted under the level of armed confrontation and hence can be hard to identify, assign liability as well as control by the prevailing international laws. This ambiguity has increased the understanding of escalation, miscalculation and the undermining of international peace and security (UNIDIR, 2024).

One of the longest and most prominent cases of cyber warfare in the recent international relations is the conflict between Russia and Ukraine. Cyber operations have been instrumental ever since the annexation of Crimea in 2014, part of an overall Russia-Ukraine conflict that is now supported by military, economic, and informational means. Cyber attacks on vital

infrastructure, government agencies, financial infrastructure, and media platforms have repeatedly been launched against Ukraine (Greenberg, 2023; Microsoft, 2024). Large-scale outages of power systems, malware comprising data wipers, and organized disinformation efforts are just a few examples of how cyber weapons were used strategically in the confrontation.

The Russian-Ukraine case of cyber warfare between 2014 and 2024 has seen an increase in the level of scale, sophistication, and intensity. The early days of cyber operations were mostly espionage-driven and disruption-driven, whereas subsequent stages were destructive malware and coordinated strategies of cyber-kinetic attacks, especially after the full-scale invasion by the Russians in 2022 (Rid, 2024; NATO CCDCOE, 2023). The developments highlight the increased normalization of cyber warfare as a tool of state power.

Cyber warfare does not end with the direct parties being fought. Cyber activities are usually transnational and story into third states and non state actors thus posing a threat to international stability. The cyber war can weaken world peace without a declaration of war, as the attacks of world supply chains, communication networks, and multinational corporations show (EU Cybersecurity Agency, 2024). Thus, the Russia-Ukraine conflict has taken a very special case study to comprehend the cyber warfare as a new threat to the international peace and security.

1.2 Statement of the Problem

The character of the warfare in the international system has changed dramatically, as it is no longer like a traditional kinetic conflict but a non-kinetic one, especially cyber warfare. The increase in digital technology and the dependence of states on information systems has established new areas of vulnerability and strategic competition (Kello, 2023; Nye, 2024). Cyber warfare as the digital attacks used to destabilize or harm an opponent (politically or militarily)

can be practiced at a level that does not involve the armed conflict, which is why it is challenging to detect, attribute, and manage (Schmitt, 2023; UNIDIR, 2024).

The confrontation between Russia and Ukraine is one of the most visible instances of the protracted cyber warfare. The cyber operations have been used to augment military and political plans since 2022 and have been used to attack key infrastructure, government systems, and communication networks (Greenberg, 2023; Microsoft, 2024). These actions have shifted out of primitive espionage and disruption to more devastating and effective cyber-kinetic means, especially after the 2022 escalation (Rid, 2024; NATO CCDCOE, 2023).

Although cyber warfare is increasingly important, it has significant regulatory issues. Attribution is challenging, which undermines accountability and deterrence (Schmitt and Vihul, 2023), and the current system of international law, developed to address kinetic warfare, does not offer much guidance on cyber operations (UN General Assembly, 2024). Cyber warfare, therefore, allows states to cause immense harm without eliciting direct military response.

Additionally, the transnational impact of cyber operations is frequent, as it interferes with the global systems, making the miscalculation and escalation particularly possible (EU Cybersecurity Agency, 2024). Russia-Ukraine conflict hence points to cyber warfare as a dynamic and continuing menace to international peace and security.

1.3 Research Questions

1. How has Cyber warfare in the Russia-Ukraine Conflict threatened International peace between 2022 – 2025?

2. How has the Cyber Security Strategy influenced the crisis between Russia-Ukraine from 2022-2025?

1.4 Objectives of the Study

This Study has both broad and Specific Objectives. The broad objective remains Cyber warfare in the Russia - Ukraine Conflict: An emerging threat to international peace while the specific objectives are:

1. To Examine whether Cyber Warfare in the Russia - Ukraine Conflict threatened international peace between 2022 - 2025
2. To verify whether the Cyber Security Strategy affected the Crisis between Russia - Ukraine between 2022 - 2025.

1.5 Significance of the Study

This study is significant both theoretically and practically, particularly within the discipline of International Relations and the broader field of security studies.

Theoretically, the paper makes a contribution to the existing body of research on the subject of global security by enhancing the concept of cyber warfare as a new variation of war and peace that breaks the conventional war and peace definition. Although the literature so far focuses on cyber security and cyber threats, overall, there are limited works that offer a longitudinal study of the cyber warfare in a particular interstate conflict within a remarkable time frame. This paper addresses this gap by analysing the development of the problem of cyber operations and its persistence and prolongation in 2022-2025, thereby providing a more profound insight on the problem of cyber warfare as a long-term strategy implementer and not a pattern of individual episodes.

Moreover, the study contributes to theoretical discussion in the sphere of International Relations by proving that cyber warfare makes current theories of power, deterrence, and conflicts to be more complex. The historical security theories manifestly occurred within the framework of kinetic warfare and territorial war, but the cyber warfare spans borders, beneath the threshold of an armed conflict, and is not necessarily associated with some obvious attribution. The case of cyber warfare in the Russia-Ukraine conflict empowers this study to make empirical contributions to the debate over hybrid warfare, security dilemmas, and the dynamism of threats to international peace. In the case of undergraduate students and future researchers, the study will be the background information that leads to the next research in exploring the issue of cyber conflict, digital security, and modern warfare.

Practically, the study is pertinent to policymakers, international organizations and security practitioners who would be interested in averting conflict escalation and international peace. It brings out the analysis of cyber operations during the Russia-Ukraine conflict by pointing at how cyber warfare is capable of affecting critical infrastructure, undermining state structures and causing all society to be full of instability without necessarily involving the use of physical force. The dynamics of these dynamics are also important in understanding by states trying to create beneficial approaches in cyber defense and the resilience of the digital environment that is becoming more digitalized and globalized.

In addition, the research has practical implications when it comes to the formulation of global regulations and legal provisions that will govern the cyberspace. By revealing the shortcomings in the current international humanitarian law and collective security processes to deal with cyber warfare, the research presupposes how important it is that the rules, norms, and mechanisms of

accountability at the international level should be demonstrated more clearly. The implications of the findings can be used to inform future deliberations on cyber governance, and confidence-building provisions as well as cooperative security arrangements in an international organization. In the end, the research also makes a contribution to the practical work of minimizing tensions related to cyber-related issues, enhancing the international cyber stability, and protecting the international peace and safety.

1.6 Scope of the Study

The paper is concerned with the example of cyber warfare during the 2022-2025 conflict between Russia and Ukraine. The time frame starts with the start of the confrontation when the art of the annexation of Crimea by Russia started in 2014 and concludes with the events that are taking place until 2025, such as the various cyber activities related to the full-scale military increase that started in 2022.

The thematic scope of the report encompasses cyber operations sponsored and / or affiliated by the state, comprising cyber spying, cyber sabotage, causing havoc in critical infrastructure as well disruption in the information warfare that is enabled through digital platforms. This special focus is put on cyber attacks affecting government entities, energy systems, financial systems, and communication infrastructures, and its repercussions on the international peace and security.

Geographically speaking, the issue of the study will focus on Russia, and Ukraine but also the rest of the international situation, such as, cyber spillover to third states, international organizations, and international digital infrastructure. The paper takes the IR lens of the analysis

(focusing more on security, relationship of power and the use of international institution instead of technicalities of cyber activities).

On the methodological level, the research will be based on secondary data consisting of academic journals, policy reports, cybersecurity analysis, and publications of international organizations. There is no access to classified information and a primary technical analysis of the forensic analysis because of data inaccessibility and attribution problem in cyber warfare.

1.7 Operational Definition of Terms

For clarity and consistency, the following key terms are operationally defined as they are used within the context of this study:

1. Cyber Warfare:

The term cyber warfare is used in this research to refer to the intentional deployment of cyber operations by a state or state-sponsored entity and target to interrupt, degrade, manipulate, or destroy the digital infrastructure, information systems, or networks of another state to achieve political, military, or strategic goals. In the context of the Russia-Ukraine war, cyber warfare involves cyber intelligence operations, cyber sabotage, malware installation, denial-of-service operation, and synchronized digital operations carried out in parallel to the conventional warfare activities.

2. International Peace:

In this research, international peace refers to a state of condition where the relations between states are marked by the lack of armed conflict of large scale, international stability, and the productive management of conflicts through institutional and diplomatic means. The study

operationalises international peace through the association and analysis of the role of cyber warfare in fostering instability, risk of escalation and breaking of trust in the international system.

3. Cyber Security:

In this research, the term cyber security means the set of policies, strategies and technical provisions that states and other international actors have implemented to ensure that digital systems, networks, and data remain untouched, distorted, or hacked by unapproved persons, groups, or organizations. Addressing cyber security in the context of the Russia-Ukraine conflict, it refers to the national and international measures to prevent, mitigate, and respond to the hostile, cyber-based activities.

4. Hybrid Warfare:

Operationally, hybrid warfare refers to the synchronized action of a standard military force with non-kinetic capabilities including cyber operations, misinformation, economic pressure, along with diplomatic manipulation to reach strategic tasks. In this paper, hybrid warfare refers to a more comprehensive warfare strategy used in the conflict between Russia and Ukraine in which cyber warfare is one of its key aspects.

5. Critical Infrastructure:

Critical infrastructure is any system and assets that failure would have grave repercussions on national security, economic stability and even lives of people. Critical infrastructure in this paper encompasses energy grids, financial systems, government databases, communication systems and transportation systems that are targeted by cyber operations in the Russia-Ukraine conflict.

6. State-Sponsored Actors:

The state-sponsored actors refer to the participants of cyber activities who carry cyber activities with a direct, approving, or strategic backing of a state. In the frame of this research, the term will encompass military units in cyber operations, intelligence agencies, and other related non-state organizations that have participated in cyber operations connected to the Russia-Ukraine conflict.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1 Conceptual Review

The theoretical basis of the research paper is on four concepts that are closely associated with each other adhering to cyber warfare, cyber security, hybrid warfare and international peace and security. These ideas are the key to the development of the digital conflict as a strategic tool of statecraft and how the conflict between Russia and Ukraine demonstrates more extensive changes in the international security realm. This part defines these concepts and places them in the frame of the contemporary academic debate as well as modern events in the world.

2.1.1 Cyber Warfare

Cyber war has emerged as one of the most controversial terms in the current security studies. In its simplest definition, cyber war involves the application of digital tools and cyber potentials by states or state-sponsored entities to accomplish their strategic goals through interference, debilitation, manipulation, or destruction of the information systems and infrastructure of an adversary (Schmitt, 2023). Nonetheless, researchers have not reached consensus on the point at which cyber operations amount to war.

The literature with early views the cyber activities mainly as espionage or sabotage. However, emerging literature has viewed cyber warfare as a consistent and tactical instrument that should be part of state conflict practice (Kello, 2023; Rid, 2024). Cyber warfare as opposed to the old system of war does not require the use of physical violence. Rather, it focuses on information,

communications networks, financial systems, and crucial infrastructure to generate strategic outcomes, without the usual battlefield interactions.

Ambiguity is one of the characteristics of cyber war. Attribution is technically difficult and politically virulent. As Nye (2024) notes, this ambiguity lets states act in what is commonly termed as the grey zone - a place between peace and war in which states behave in an antagonistic way yet are not at the level of armed conflict. Such a grey-zone effect dilutes deterrence mechanism and international law responses.

The dispute between Russia and Ukraine is now seen as one of the most popular studies on cyber war. Ukraine has been subject to perennial cyber activities, such as power grid cyber attacks, government databases, banking, and military communications (Greenberg, 2023; Microsoft, 2024). After the complete invasion in 2022, there was an increase in cyber operations, with malicious programs, including wipers, used together with kinetic military attacks. This integration, according to scholars, reflects the process of the normalization of cyber warfare as a daily tool of interstate warfare (NATO CCDCOE, 2024).

Cyber warfare has increased around the world and not only has been limited to the issue between Russia and Ukraine. Large countries such as the United States, China, and Iran have taken on additional offensive cyber capabilities to integrate it into their military doctrine (UNIDIR, 2024). This more general tendency indicates the topicality of the given research: the conflict in Russia and Ukraine is not a one-time situation but an embodiment of a more general shift in the very nature of warfare. This study places the concept of the cyber warfare in a ten-year cycle of metamorphosis of the international security practices by analyzing this conflict that took place in 20142024.

Notably, cyber warfare directly affects the key thesis of this undertaking a challenge to international peace. Since cyber operations can cause economic disturbance, political upheavals as well as infrastructure destruction without necessarily incurring military aggression, they erode the distinction between war and peace to the point of establishing a persistent state of insecurity in the international system.

2.1.2 Cyber Security

Cyber security describes the prevention policies, institution and technology that helps guard digital systems, networks, and information against unauthorized access, disruptiveness, or assault. In the framework of International Relations, cyber security has become a highly relevant national, international security concern and transferred beyond the technical field (Nye, 2024).

Researchers underline that cyber security is not only the technology of defense but a issue of state resilience and the ability to act strategically. UNIDIR (2024) notes that cyber security currently dictates the equilibrium of power between states because countries that had well-developed cyber-based capabilities have offensive and defensive capabilities. This poses great effects to the stability of the world.

Securitization of cyberspace is also a recent topic in literature. Cyber threats are being increasingly depicted by the governments as a matter of national survival and interest, and, in such a way, the military presence is spread into the digital space (Kello, 2023). This securitization affects the budgetary allocations, defense policies and international relations.

The cyber security in the conflict between Russia and Ukraine was under the persistent pressure. The resilience of Ukraine to cyber attacks, achieved due to national reforms and alliances, has become a popular topic of discussion because despite numerous cyber attacks leading to

disruption of the entire infrastructure, Ukraine was able to withstand them (Microsoft, 2024; EU Cybersecurity Agency, 2024). This shows the impact of cyber security capacity on the results of a conflict.

In addition, cyber security is a global issue. The Russia-Ukraine conflict has been associated with cyber attacks that impact multinational corporations and third-party states, and it is an example of how digital infrastructure is interconnected (Greenberg, 2023). These spillover effects demonstrate the fact that national security, not only cyber security, can be swept away by the vulnerabilities of cyber security, which is the main issue of the given study.

2.1.3 Hybrid Warfare

Hybrid warfare refers to the integration of regular military action with non-conventional tools such as cyber warfare, false information and economic pressure, and political pressure to pursue strategic aims (Hoffman, 2023). The notion disputes conventional conceptualizations of war as being kinetic.

The latest research presents hybrid warfare as a characteristic of the conflicts in the twenty-first century (Rid, 2024). Cyber warfare is regarded as one of the pillars of the hybrid approaches since it enables states to undermine their opponent internally before or during military conflict.

The conflict between Russia and Ukraine is a demonstration of hybrid warfare in action. Since 2014, the military action has been supplemented by cyber operations, and the federal elections, as well as information environment and institutions trust, have been undermined (Kostyuk and Zhukov, 2023). A combination of cyber-attacks and disinformation campaigns depicts how technology increases psychological and political aspects of war.

The hybrid warfare tactics have become more or less common all over the world. The documents adopted by NATO and the EU policy in 2023-2024 highlight the increased risk of hybrid action that reinforces cyber operation with the use of economic and informational means (NATO CCDCOE, 2024). This expanded awareness of the problem makes this research problem all the more relevant: cyber warfare cannot be discussed separately, but rather as a component of complex strategic rivalry.

In this project, hybrid warfare will be relevant because it puts cyber operations in the context of further development of the one-level conflict and strategic pressure. It assists in the explanation of how cyber warfare aids destabilization without the fully established conventional war.

2.1.4 International Peace and Security

International peace and security traditionally refer to the prevention of armed conflict and the maintenance of stability through diplomacy, international law, and collective security mechanisms. However, the rise of cyber warfare has challenged this traditional framework.

The international peace and security are traditionally the process of the prevention of armed conflict by means of diplomacy, international law, and the collective security system. This model has however been put to test by emergence of cyber warfare.

More current-day scholarship claims that cyberspace operations establish a scenario of a state of never-ending engagement, such that states are constantly competing on the border of an armed conflict (Nye, 2024). This conflicts with the dichotomous nature of war and peace and draws onto a low-level confrontation.

It has been recognized on associated expert groups including the United Nations General Assembly (2024) that the dynamics of escalation and issues of attribution combined with the lack of binding international norms make cyber threats an issue concerning international stability. In the absence of iselfevident guidelines on cyber conduct, the states are likely to interpret cyber events as the initial stage in the military aggression, which renders the possibility of an accidental escalation even greater.

The conflict between Russia and Ukraine brings out the aspect of how the war can be internationalized through cyber warfare. International organizations, financial systems, global supply chain have been targets of cyber attacks proving that cyber conflict is rarely limited within the territorial boundaries (EU Cybersecurity Agency, 2024). These spill over effects further justify the suggestion that cyber warfare is not a bi-lateral problem alone but a systemic danger to global peace.

Through the analysis of cyber warfare in this larger conceptual framework, the research helps us to comprehend that digital war transforms international peace and security in the modern world.

2.2 Thematic Review

This part will be a review of scholarly debates pertaining to the thematic topics according to the research questions that guide this research. The review is not a simple description of what has happened, but it addresses the scholarly debate about the nature, development, consequences, and the legalization of cyber warfare, especially in the environment of the war between Russia and Ukraine (2022-2025).

2.2.1 Forms of Cyber Warfare in the Russia-Ukraine Conflict

Numerous literatures have confirmed the existence of various types of cyber war that were used in the conflict between Russia and Ukraine. This encompasses cyber spying and numerous destructive malware code releases, infrastructure sabotage, interference with satellite communications and organized disinformation (Greenberg, 2023; NATO CCDCOE, 2024; Microsoft, 2024).

According to scholars, the conflict illustrates the ability of cyber warfare to go beyond the intelligence collection to operational and strategic interference. Initial activities (2014-2016) mainly consisted of cyber espionage and intrusion of lesser infrastructure. Nevertheless, the 2015 and 2016 attacks on the power grid of Ukraine are considered to be historic, as one of the first reported instances of disruption of physical infrastructure on a large scale due to cyber operations (Rid, 2024). This stretched out the distinction of digital and kinetic outcomes.

Later advances broadened the horizons of the sphere of cyber tools. The malware attack in 2017 NotPetya is generally considered to constitute a watershed event in the literature on cyber conflicts thanks to its unintended global economic impacts (Kelleher, 2023). Though the malware was aimed at Ukrainian systems it was spread throughout the world with corporations in Europe and North America being affected. This justified the research anxieties regarding cyber spillover and the collective character of digital infrastructure.

After the escalation in 2022, the literature records a higher level of synchronization between cyber operations and traditional military approach. Wiper malware, communications sabotage, and premeditated cyber attacks have been reported to have been conducted prior to ground entries, which shows intentional incorporation into the military operations (Microsoft, 2024;

NATO CCDCOE, 2024). According to the scholars, this is an indication that cyber warfare is no longer just the case of isolated disruption but is institutionalized state strategy.

Although a lot of incidents have been documented, a significant portion of research has been conducted on an individual high-profile attack instead of examining the trends over time. The study is significant in the sense that it combines these forms over the ten year span and uncovers patterns in the structure and not just events.

2.2.2 Evolution of cyber warfare in the Conflict.

Modern literature is becoming more conceptualising cyber war in the Russia-Ukraine war as evolutionary, not static. Researchers distinguish between three stages, namely experimental destabilization (2014-2016), systemic escalation (2017-2021), and integrated cyber-kinetic warfare (2022-2024) (Nye, 2024; Rid, 2024).

The first wave of cyber activities was carried out mainly as a tool of political manipulation and interference. These actions were usually clandestine, reconnoiterative, and aimed at experimenting with any weaknesses of Ukrainian systems. Nevertheless, with the further progression of the conflict, the magnitude and complexity of cyber attacks rose dramatically.

In the systemic escalation stage there were increased destructive intent and transnationally. NotPetya made it clear that economic damage caused by cyber weapons can be produced on the global level, which has radically changed the way in which policymakers and scholars evaluated the threats posed by cyber attacks (Greenberg, 2023). The cyber attack revealed wider discussions as to whether or not cyber activity must be considered an act of war necessitating international law.

The phase after 2022 is a qualitative change. The amalgamation of the cyber and kinetic operations, according to scholars, is an indicator of doctrinal adaptation (NATO CCDCOE, 2024). Both alleged cyber attacks were also aimed at disabling logistics, causing disruption of command-and-control systems, and molding information environments before the actual physical offensives. This integration indicates the growing cyber doctrine within the enlarged military policy.

Moreover, the literature mentions the growing professionalization and institutionalization of cyber units into state security points of the world (UNIDIR, 2024). The lessons experienced in the Russia-Ukraine conflict are also being applied to defense policy making across the world, implying that what can be perceived here may not be an isolated evolution but rather a systemic change.

Nonetheless, although these stages of evolution have been identified by scholars, there are limited findings that offer a longitudinal evaluation process of 2014-2024. This paper fills this analytical lapse by constructing continuity and change over a ten-year period.

2.2.3 Cyber warfare as a threat to International Peace and Security

One of the main arguments in the current security research is whether cyber warfare is a structural danger to international peace or just a novel field of strategic rivalry. According to scholars like Nye (2024), cyber operations encompass a long-lasting instability due to a lack of trust and fueled by false perception whilst making deterrence more difficult.

In contrast to traditional warfare cyber operations are usually not easily attributed, and thus any retribution is both politically dangerous and legally questionable. Such ambiguity enhances risks

of escalation. United Nations General Assembly (2024) has recognised that cyber operations may disrupt international peace by affecting the countries through undermining the sovereignty and the protection of critical infrastructures.

Cyber warfare is a contributing factor to systemic instability as is the case in the Russia-Ukraine conflict. Cyber operations, which are related to the conflict, have targeted international corporations, financial institutions, and even satellite communication networks, thus extending the effects of the conflict even without being limited to geographical borders (EU Cybersecurity Agency, 2024). This proves the fact that cyber war is not geographically constrained.

Another point that has been made by scholars is that cyber warfare makes the perpetual low-level hostility routine. According to Kello (2023), this is a state of unpeace since states are engaged in a digital conflict but without a formal war. This constant competition has put the traditional collective security mechanisms established to react to open military aggression in question.

Nevertheless, there are also scholars who argue that cyber warfare has not provided casualties and destruction comparable to conventional wars yet and must not be exaggerated as the existential threat (Rid, 2024). The debate is still unresolved to this effect and raises the need to be cautious in the empirical evaluation, which is what this study attempts to present.

2.2.4.Adequacy of International Legal and Institutional Frameworks.

The last significant theme is whether or not there is enough international law in place to govern cyber warfare. The general principles are contained in international humanitarian law (IHL), the UN Charter, and customary international law but the application of these principles to cyberspace is debated (Schmitt, 2023).

The Tallinn Manual 2.0 is an interpretative guidance, but not binding. In the meantime, negotiations in the UN community via the Open-Ended Working Group (2023-2024) show that there is a wide difference in opinion between states concerning the sovereignty within cyberspace, countermeasures, and mechanisms of joint response (UNIDIR, 2024).

Researchers believe that the presence of legal ambiguity in the field of cyber activity as a strategic incentive because the states have an opportunity to maneuver around causing hostile actions without activating any disciplined legal repercussions (Nye, 2024). Such a lax enforcing atmosphere might encourage violent conduct.

Through Russia-Ukraine conflict, reactions to cyber attacks have mostly been diplomatic denunciation, sanctions and attribution instead of court proceedings. This is an indication of institutional constraints to the formulation of norms into mechanisms.

Although literature accepts the existence of such gaps in regulation, there remains little agreement on how to enhance in the international cyber governance without violating sovereignty or augmenting geopolitical rivalry. This paper does this by connecting legal incompetence directly to the risks at large towards international peace.

2.3 Theoretical Review

In this section, there is a review of the key theoretical approaches that apply to the issue of cyber warfare and its consequences to international peace. It discusses Structural Realism, the Security Dilemma Theory, and Liberal Institutionalism. Although each of three viewpoints brings insightful analytical understanding, Structural Realism will be the main point of reference in the

current study since it has given the most comprehensive explanation regarding state behavior in the Russia-Ukraine cyber conflict.

2.3.1: Structural Realism (Neorealism)

Neorealism as Structural Realism is one of such dominant theories of International Relations. The theory advanced most famously by Kenneth Waltz posits that the international system is anarchic, that is, there is no central power that is above and above states that makes rules and ensures security. Consequently, states are left to exist in self-help system in which the main goal is existence (Waltz; Mearsheimer; recent talks in Nye, 2024).

Structural Realism explains state behavior by the international system structure other than its internal nature. Since states cannot rely on each other completely, they are in constant power-cumulative endeavours in a bid to ensure their survival. This causes competition, arms race and the repetition of war.

The Structural Realism has been applied to the cyberspace by the recent scholarship. Researchers believe that online capabilities have turned out to be new tools of relative power in anarchic order (Kello, 2023; Rid, 2024). Offensive and defensive capabilities in cyber are a heavy investment in states due to the increase in strategic benefits without the need to provoke a conventional war.

Structural Realism is a very powerful explanation in the framework of the conflict between Russia and Ukraine. In this sense, one can consider that the application of cyber operations by Russia can be seen as an attempt to preserve the influence in the region and prevent the

perceived geopolitical encroachment. Cyber war is an instrument of power maximization that is rational in an anarchical environment.

In addition, Structural Realism is applicable in understanding the reason international legal norms represent a weak restraining effect. Under anarchic system international law is followed subject to national interest. States might prefer relative gains to normative obligations where it views the use of cyber operations as a means to gain strategic advantage and at minimal immediate costs (Nye, 2024).

Since Structural Realism represents the aspect of power contest, strategic calculation and systemic insecurity, this paper shall be pegged on this theory in its understanding of the role of cyber warfare in instability and threat to international peace.

2.3.2 Security Dilemma Theory

A theory closely linked with realism, the Security Dilemma Theory elaborates that the actions of the state to enhance its security can inadvertently hurt the security of others and thus lead to the cycles of suspicion and upsurge.

A security dilemma is unnecessary in cyberspace as the issue of uncertainty and attribution fuels the problem. Cyber capabilities are sometimes concealed as compared to conventional weapons, and countermeasures may seem no different than offensive placement (Kello, 2023). Such ambiguity renders the states unable to comprehend the motives of digital actions.

Recent literature suggests that the Russia-Ukraine cyber war provides an example of a dilemma at the digital security level. Cyber defense on one part can be seen as offensive operations

preparation, which leads to an equal counterpart (NATO CCDCOE, 2024). An addition of cyber units to military doctrine adds another perception that there is even more threat.

Also, since cyber operations are usually conducted at the level lower than that of armed conflict, the retaliation levels are ambiguous. This may result in the permanentpersistential confrontation, making the state of long-term instability even higher without the actual war.

Although the Security Dilemma theory is appropriate in explaining the dynamics of escalation and mistrust in cyberspaces, it fails to explain the structural power rivalry in the making of cyber capabilities comprehensively. This is why in this study, it is a complement of Structural Realism and not a substitute.

2.3.3 Liberal Institutionalism

Liberal Institutionalism focuses on the use of international institutions, norms and cooperation in the reducing of conflict. As per this school of thought, institutions even within an anarchic system are able to minimize the uncertainty, initiate cooperation, and enhance the stability.

Liberal Institutionalism concerns itself with initiatives undertaken by the United Nations and other international organizations to come up with the norms that can regulate the responsible behavior of states in the cyber space (UN General Assembly, 2024; UNIDIR, 2024). Efforts to establish the consensus on cyber governance have been manifested in initiatives like the Open-Ended Working Group.

Nonetheless, according to scholars, institutional development has been gradual and disjointed. The formation of obligatory cyber laws has been curtailed by lack of agreement on sovereignty,

attribution and countermeasures by the major powers (Nye, 2024). These institutional shortcomings are apparent in the Russia-Ukraine conflict, where despite the discussion of the norms, cyber operations are not ceasing.

Liberal Institutionalism helps explain why regulatory frameworks struggle in a competitive geopolitical environment. However, it tends to assume that cooperation is achievable when mutual interests align. In highly polarized conflicts, such as the Russia–Ukraine case, structural power politics often override institutional constraints.

Thus, while Liberal Institutionalism provides valuable insights into governance efforts, it does not fully capture the competitive dynamics driving cyber warfare.

2.4 Empirical Review

1. Beska, Solomiia (2025) Cyber Resilience in Ukraine: The Response to Cyber Threats in the Hybrid Warfare. In this dissertation, the changing institutional and strategic reaction to persistent Russian cyber aggression of 2014-2025 in Ukraine is examined with reference to such important cyber incidents as the BlackEnergy (2015), the NotPetya (2017), and the Kyivstar (2023) cyberattacks. In the framework of cyber resilience in Ukraine, the study followed institutional learning and strategic adjustment using longitudinal case study and document analysis. Beska has discovered that Ukraine cyber defenses developed by reacquiring adaptation as opposed to a planned approach and collaborated with international partners and reference to the effective model of cyber protection as in Estonia. The author suggests the need to reinforce coherent national cyber approaches and integrate best practices at the international level in order to improve resiliency in the case of cyber threat in the future.

2. Khoirunnisa, Cristy Sugiati (2024) -- Cyber Warfare Strategies during the Russian-Ukraine war (2021-2022): What to Expect on the National Security Front and the Modern Warfare. This university study found in Universitas 17 Agustus 1945 Jakarta examined the DDoS attacks and other cyber tactics by Russia and Ukraine in the 2021-2022 phase of the conflict based on a descriptive approach to qualitative research. In a research done by Khoirunnisa, the author discovered both sides conducted actions through cyber which they used to interrupt communications and government systems, greatly affecting the strategic stability. The research finds that cyber warfare is now part of national security planning in contemporary inter-state conflicts and suggests more defensive coordination of national and international levels.

3. Juutilainen, Jari (2022) Cyber Warfare: A Component of the Russo-Ukrainian War in 2022. Juutilainen researched about 800 reported cyberattacks on Ukraine in this academic thesis after the Russian invasion of the country in 2022. Referring to the case documentation and descriptive analysis, the paper emphasized the frequency, the targets, and the means of cyberattacks that are combined with kinetic warfare. Results underline that cyber activities went further than disrupting infrastructure to strategic degradation of the Ukrainian infrastructure. The thesis finds that cyber warfare has evolved into a complementary field of contemporary warfare that needs new legal and policy countermeasures.

4.Broekstra, Aaron (2024) Digital Battlegrounds: Assessing the effects of cyber warfare on international humanitarian law in the Russian-Ukraine War. The thesis of Peace and Conflict Studies written by Broekstra viewed legal and ethical issues in cyber warfare and specifically the protection of civilians under the International Humanitarian Law (IHL). The study based on qualitative case-studies and incorporating the 2022 asylum ambuscade computer-based attacks

on refugees and humanitarian organization identified some critical gaps in the existing legal standards that were not effective in addressing cyber harms. It suggests the enlargement of IHL and cyberlaw frameworks with an aim of elaborating cyber incidents affecting civilians.

5. Sani, Abuh Ibrahim et al. (2025) -- Qualitative Analysis of Cybers case Nigeria: measuring the readiness of this country against state-sponsored cyber attacks: the comparison of cybersecurity policy modifications, incident response systems, and international collaboration. This paper assessed the cybersecurity policy and the cybersecurity incident response strategies in Nigeria, South Africa and Kenya using comparative policy analysis. The results indicated that although Nigeria has embraced the necessary initial policies on cybersecurity, institutional failures, minimal capacity to act technically, and lack of cooperation between states and regions make it incapable of preparing against state-sponsored cybersecurity attacks. The authors suggest the increased capacity building, regional coordination, and standardized legal framework as the means of strengthening national cyber defense and international coordination.

6. Evelyn (2025, Nigerian Journal) -- Evaluation of the Geopolitics Implications of Offensive Cyber Operations. This is an empirical study published in the West African International Security Studies Journal and used documentary analysis to evaluate motivations and effects of state-sponsored cyberattacks during international conflicts. It discovered that offensive cyber activity has turned into a higher-order geopolitical rivalry as opposed to criminal activities in isolation. To sum up, the paper comes to the conclusion that diplomatic and legal and technical methods should be incorporated into the cybersecurity policies in order to alleviate the tension and the challenges to the international peace.

7. Muzayan Haq, Muhammad Yasir et al. (2023) -- Evaluating the Actions of Network Operators to Improve Digital Sovereignty and Network Resilience: A Longitudinal Study in the War between Russia and Ukraine. This study entailed longitudinal network measurement analysis to examine how network operators used infrastructure in response to the conflict as a way of defending the concept of digital sovereignty. It discovered that proactive migration of infrastructure and increasing redundancy will offset conflict-related disruption. The authors suggest the structurally resistent networks and cross-national technical collaboration in terms of protection of cyberspace integrity in case of interstate conflicts.

8. Malikussaid and Sutiyo (2025) - The Effect of the Russia-Ukraine conflict on the cloud computing risk landscape. This is a systematic qualitative synthesis which investigated the role of geopolitical factors in managing the risk of cloud computing in the case of the conflict between Russia and Ukraine. The research study established that the conflict has led to the acceleration of cyber incident risk awareness, policies of localization of data, and sovereign cloud adoption in 40 or more countries. The authors suggest a multi-layer model of governance that combines the geopolitical risk factor to enhance IT security policy and cloud resilience.

9. Derbyshire, Richard et al. (2025) -- From Protest to Power Plant: Making Sense of the place of Escalatory Hacktivism in Cyber Conflict.This new paper examines the ways in which, as of geopolitical conflicts occurring after 2022, hacktivist groups no longer stopped at DDoS and leaks and instead targeted operational technology (OT) of critical infrastructure. The authors conducted a comparative analysis and discovered that hacktivism created a grey zone between activism and cyber warfare, which create further threats to national security. They suggest the

better definition of non-state cyber actors and specific policy actions to reduce destabilizing effects.

10. Gerard et al. (2024) -- Information Narrative Detection and Evolution Modeling on Telegram in the middle of the war between Russia and Ukraine. Based on computational discourse analysis, this paper discussed how information stories, on Telegram, were formed in the course of the conflict and the effect they had on the general opinion. The study established that the narrative-based transitions had a profound influence on the community feeling and the international reactions, which indicates the nonlinearity of cyber-enabled discourse operations in conflict dynamics. The authors suggest including narrative surveillance in the work on cybersecurity so that the psychological aspects of cyber conflict could be predicted and addressed.

11. Al-Billeh, T. (2025) -- The International Framework of Cyber-Attacks that takes place under the international law. This was an empirical legal research project that examined the application of the international humanitarian law (IHL) on cyberattacks. According to the legal reasoning and the comparative analysis, Al-Billeh observed the lack of effective enforcement measures that prosecute cyber aggression and which leads to legal ambiguity, which proves to promote aggressive state conduct in the cyberland. The paper will end by suggesting a higher fortification of the treaties and a proper understanding of the jurisdictional standards to bring cyber mercilessors to book.

12. Melella, C. (2024) — *Disjointed Cyber Warfare: Internal Conflicts Among Russian Intelligence Agencies* This exploratory study examined the coordination (or lack thereof) among Russia's intelligence units (GRU, SVR, FSB) in cyber operations. Using organizational analysis,

the research found internal competition and technical disparities hinder cohesive cyber efforts, which may explain lower than expected strategic impact. The author recommends improved inter-agency coordination to enhance cyber effectiveness in interstate conflict contexts.

2.5 Summary of Literature and Identified Research Gap

As indicated by the literature that has been reviewed in this chapter, cyber warfare has become a core aspect of the modern interstate conflict. Conceptual debates indicate that cyber warfare has transformed into a fringe technical problem into strategic tool of statecraft, which can cause chaos to vital infrastructure, affect mass perception and manipulate military results. There is a wide consensus among scholars that cyberspace has become a fifth domain of operation in war in the same way as land, sea, air and space. Nonetheless, there are still discussion boards on the categorization, baseline, and future consequences of cyber conflict.

The thematic review reveals that the fight between Russia and Ukraine is one of the most studied instances of a protracted cyber war in the contemporary history. According to the empirical literature, various types of cyber operations, such as espionage, malicious malware software, infrastructure sabotage and synchronous information activity can be distinguished. The literature also confirms that, during this conflict, cyber war has combined over the period between 2014 and 2024 as it becomes more of an exploratory digital disruption into integrated cyber-kinetic operations facilitating conventional military campaigns.

It is also in the face of this comprehensive documentation that some gaps in analysis abound.

To begin with, most of the existing scholarship is dispersed. Isolated high-profile cases are subject to many studies, including the power grid attacks in 2015 or the NotPetya malware outbreak, but not put in the context of a longitudinal study. Synthesis of cyber operations is done

very little through the entire ten years (2022-2025) to determine structural continuity and change between the years.

Second, although multiple studies discuss the technical complexity or legal aspects of cyber warfare, limited literature also discusses these developments in relation to the issue of international peace and system stability on a larger scale. Cyber warfare is typically understood as a cybersecurity problem or a legal regulation question, but even less commonly as a structural problem to the stability of the international system. This leaves a vacuum in comprehending the role of creating digital competition in global power relations, threat of escalation, and transnational security operations.

Third, much theoretical perspective on cyber conflict in general, including Structural Realism, Security Dilemma Theory, or Liberal Institutionalism, has been applied in practice, but little has been integrated in the assessment of the Russia-Ukraine situation over a period of one decade. Most of the researches are mainly descriptive with fewer investigations based on theories thus discouraging depth in explanations.

Moreover, the discussion still goes on concerning the seriousness of cyber warfare as the threat. According to some scholars, cyber activities have not yet crossed the threshold of catastrophic violence hence should not be exaggerated to the level of existential threats. Others argue that trust, the established institutions, and the normalization of the hostility that has always existed in the international system are all destroyed by the cumulative impacts of constant cyber competition. Such disagreement highlights the necessity to propose additional systematic study.

CHAPTER THREE

METHODOLOGY

3.1 THEORETICAL FRAMEWOK

Structural Realism (Neorealism)

3.1.1 Exponents of Structural Realism

Structural Realism, also called Neorealism, is mostly linked to the writings of Kenneth Waltz, who worked out the theory in systematic form in his masterpiece Theory of International Politics (1979). Waltz changed the object of realism concern not with human nature and state leadership but with the structure of the international system itself, which determines the eventual actions of states.

Waltz holds the position of the international system that is characterized by anarchy, i.e. the lack of a central authority above states. In this system, states are functionally similar units that are distinguished primarily by their capabilities. Consequently, balance of power within the system turns out to be the major factor that determines the outcomes in international affairs.

John Mearsheimer is another key player who developed the theory in terms of the Offensive Realism. Mearsheimer believes that the states are not simply in search of survival but instead

seek regional or global hegemony in order to maximize their security. His interpretation is more aggressive, but much of this is defensive orientation by Waltz, but both theorists believe that power competition is an inevitable occurrence in an anarchic system.

Modern theorists like Joseph Nye have applied the realist approach to the cyber domain, and they believe that cyber capabilities are a novel form of power in the international system (Nye, 2024). This development reveals Structural Realism is still relevant in explaining new forms of conflicts like cyber warfare.

3.1.2 Assumptions of Structural Realism Structural

Realism consists of a number of assumptions underlying the behavior of the states in the international system. To begin with, the international system is anarchic. No overall force could superimpose rules or ensure security. This lack of centralization forces states to act on their own in order to guarantee their survival.

Second, there is a self-help system of states. No external authority can guarantee protection so that each state is forced to depend upon its abilities, which can be military, economic or technological intervention to ensure its interests. This self-help mechanism has now comprised of cyber capabilities in the modern age.

Third, survival is the main objective of states. Whether there is an ideological or political difference, all states put their survival first. This is a common goal that motivates states to amass power and minimize vulnerability.

Fourth, relative gains are a concern to the states as opposed to absolute gains. Differently put, states not only measure their development based on their own development but also compare them to others. This brings about competition at all times, one state gains and another state feels like it has been defeated.

Fifth, Structural Realism emphasizes the issue of security dilemma. The measures implemented by one state in order to make its security better, like better cyber defense or the creation of offensive cyber capabilities, can be perceived as a threat by the rest of the states. This results in mutual moves that augment tension even in cases where no state plans to cause conflict.

These assumptions are especially applicable in the case of cyber warfare. Invisibility and ambiguity of cyber capabilities make the situation even more unpredictable, as the goals of states to differentiate between defensive and offensive intentions become even more challenging. This makes cyberspace further enhance the dynamics of mistrust and competition of the international system.

3.1.3 Application of Structural Realism to the Study.

The research is supported by Structural Realism in that it has the most detailed explanation of cyber warfare as a strategic tool of state action in an anarchic international system.

Applied to the situation of the war between Russia and Ukraine, cyber warfare can be considered as a logical continuation of power rivalry. Structural Realist point of view would suggest that the use of cyber functions by Russia is not an accidental or technological event but a strategic measure to retain influence, undermine an enemy and restructure the balance of power in the region.

Cyber war fits into the self-help principle, in which states derive and execute cyber capabilities to ensure their interests in the absence of assured protection. The initiative by Ukraine to build its cyber defenses with international alliances is also an indication of the need to improve the survival of the country in a competitive system.

In the cyber world, security dilemma can also be seen. Any defensive cyber actions, including network fortification or intelligence scouting, could be seen as offensive preparations, which adversaries would respond to. This forms a circle of increasingness that runs in a nightless cycle, sometimes below the level of armed conflict.

Additionally, Structural Realism defines why the legal and institutional systems of the international law fail to control the cyber warfare. In anarchic system, adherence to the international norms depends on state interests. States are less likely to be bound by the rule of law where cyber operations offer a strategic edge at relatively cheap cost and risk of failure. This would contribute to highlighting why cyber attacks have remained a persistent problem even with continued global denunciations and creation of cyber norms.

Notably, the theory gives one a clue on how cyber warfare is a menace to international peace. Instead of causing large-scale destruction instantly, cyber operations create a state of continuous instability, a lack of trust between states, and a certain threat of erroneous decision-making. This is a state that has been explained by the scholars as unending strategic competition whereby there is conflict even without the direct declaration of war.

Through Structural Realism, this paper goes beyond the descriptive explanations of cyber incidents and rather elucidates the concept of cyber warfare as a system phenomenon based on the framework of international politics. It proves that the cyber conflict is not an exceptional case and it is a logical consequence of the states acting in a competitive and anarchic international system.

3.2 Hypotheses

1. Cyber warfare in the Russia–Ukraine conflict has not undermined international peace between 2022-2025.

2. Cyber Security Strategy has affected the crisis between Russia-Ukraine from 2022-2025

3.3 Research Design

The research was anchored on ex-post facto research design. The design is deemed suitable in the current research since it is based on examination of events that have already taken place without manipulations or any form of control of variables by the researcher. Ex-post facto research is strongly employed in social sciences and International Relations, especially the research when subject of interest, like conflicts, state behavior, and policy outcomes, cannot be easily manipulated in the laboratory because they are complex and real-life variables.

Considering the scope of the present research, the examples of cyber warfare in the Russia-Ukraine conflict of 2014-2024 can be discussed as historical and current phenomena that cannot be altered or manipulated by the author of the research. The research thus uses the available information to analyze the connection between cyber warfare and its effects on international peace. Through this design, the study can be in a position to examine the cause and effect relationships in a retrospective way especially how cyber operations have led to instability, risk of escalation, and disruptions of the international system.

Moreover, the ex-post facto design enables a systematic review of patterns, trends and results of cyber warfare within a specified period of time. It allows the researcher to study the development of cyber strategies, their application by state actors, and their impact on the geopolitical

processes in general. It is particularly pertinent in light of the fact that cyber warfare exists in complex and interdependent systems where direct testing is impossible and moral.

It is also appropriate in terms of design since it will allow the use of secondary sources of data like academic publications, cybersecurity reports, policy documents, and institutional records. The sources are informative and verifiable, detailing the cyber incidents, the response of the state, and the response of the international community, which contributes to better reliability and validity of the study.

Moreover, ex-post facto approach is consistent with the theoretical approach of Structural Realism that has been employed in this research. As the theory focuses on the observed state behaviour in an anarchic international system, historical data can be used to explain the operation of cyber warfare as a means of power struggle in a more correct manner.

In general, the ex- post facto research design offers a sound methodological basis to the current study as it will allow conducting the comprehensive and objective analysis of cyber warfare in Russia vs. Ukraine conflict and its effect on the international peace and security.

3.4 Method of Data Collection

This study employed secondary sources of data like academic articles about cyber conflict, academic theses, dissertations, cybersecurity technical reports, international organizations publications, governmental cyber policy reports, databases of conflicts where needed, and official international media archives. These sources were chosen as they offer detailed and reliable information about the essence, development, and consequences of cyber warfare in the context of the Russia-Ukraine conflict.

Appropriateness of secondary data in this study is on the grounds that activities of cyber warfare are usually confidential and delicate such that primary data collection can be challenging and in most instances unrealistic. Consequently, the dependence on written and peer-reviewed materials will enable a more credible and verifiable study of cyber attacks, governmental activities, and foreign reactions.

Moreover, the information used in this research is up-to-date and valid starting from 2022 and up through 2025, which will be both historical and relevant. This period allows the investigator to trace the development of cyber warfare over time as it is in its primitive forms up to the more integrated forms, thus facilitating the examination of the entire effects of cyber war on the international peace and security.

3.5 Method of Data Analysis

This research used content analysis, which was backed by historical and comparative methods of analysis. Data were systematically analyzed and interpreted through content analysis to find major patterns including trends in cyber escalation, cyber operations types, institutional responses, and international diplomatic responses in the context of Russia-Ukraine conflict.

Moreover, the historical analysis was applied to track the development of cyber warfare during the following years, 2014 to 2024. This method allowed the study to identify the variations in the scale, sophistication, and strategic application of cyber operations at various stages of the conflict.

Moreover, the effectiveness of institutional and international reaction to cyber war was compared to analyze how well it was managed. Through the comparison of various policy responses, law

regimes, and strategic responses the study offers a more subtle picture of the advantages and constraints of international responses to cyber conflict regulation.

To increase the credibility and reliability of the findings, the study embraced triple data validation by utilizing various sources of data. This methodology guarantees that an analysis is made based on a pooling of evidence thus making the analysis robust.

.

3.6 Logical Framework

Table 3.1: Logical Framework of the Study

Research Question	Hypothesis	Major Variables	Empirical Indicators	Method of Data Collection	Sources of Data	Method of Analysis
How has cyber warfare in the Russia–Ukraine conflict threatened international peace between 2022–2025?	1	Independent Variable: Cyber Warfare (Cyber Operations) Dependent Variable: International Peace	Frequency of cyber attacks, infrastructure disruption, cyber escalation trends, impact on communication systems, geopolitical tensions	Documentary method (Secondary Data)	Academic journals, cybersecurity reports, policy documents, international organization publications, global media archives	Content analysis, supported by historical analysis
How has cyber security strategy affected the crisis between Russia and Ukraine from 2022–2025?	2	Independent Variable: Cyber Security Strategy Dependent Variable: Crisis Dynamics (Conflict Intensity/Stability)	National cyber defense measures, resilience of digital infrastructure, response strategies, international cyber cooperation, reduction or escalation of attacks	Documentary method (Secondary Data)	Government policy documents, cybersecurity reports, academic literature, institutional publications	Content analysis, supported by comparative analysis

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 Analysis of Hypothesis One

1: Cyber warfare in the Russia–Ukraine conflict has not undermined international peace between 2022 till 2025.

Cyber warfare is one of the most visible and apparent ways in which it has an impact on international peace and security in the modern international system, and the Russia–Ukraine conflict is one of them. Cyber operations in the 2022-2025 timeframe became more multifaceted and increasingly strategic tools that had an impact on state stability, critical infrastructure or global geopolitical relations. The cyber operation is a major component of the military conflict, highlighting the increasing importance of cyberspace as a venue of inter-state conflict.

In the conflict, one important aspect of cyber warfare that contributed to the destabilisation of international peace was attacks against critical infrastructure. In 2022, after the recent escalation of the conflict, Ukrainian government bodies, communication systems, banking systems and energy infrastructure were victims of several cyberattacks allegedly executed by the Russian side. Microsoft (2024) reports that malicious actors used malware and destructive wiper attacks against Ukrainian public institutions and ministries prior to and in conjunction with kinetic military operations. Such online operations and operations were carefully executed to disrupt administrative mechanisms, hinder communications and create ambiguity and disruptions within the Ukrainian state system.

The attacks on Ukraine's energy sector is another example of the destabilizing impact of cyber warfare. The eagerness to see cyber attacks against power infrastructure produce physical and

psychological effects akin to real-world military attacks is noteworthy, as revealed by scholars like Rid (2024) and Greenberg (2023). The conflict caused disruptions in power supplies, undermine public confidence, and heightened humanitarian pressures. Unlike traditional warfare these cyber operations were conducted with degrees of difficulty in attribution, making direct retaliation more challenging and added to uncertainty in the international system.

Moreover, cyber warfare also played a major role in the dynamics of escalation in the conflict. Cyber operation adopted into military warfare led to the emergence of hybrid warfare, where cyber operations assisted battlefield missions. NATO CCDCOE (2024) reports coordinated attacks in cyber space have often been seen as precedents to kinetic attacks, such as communication network and intelligence system disruption. With the aim of this synchronization, the reality of war and peace became somewhat indistinguishable, establishing a continuous state of strategic confrontation.

Russia – Ukraine war has also triggered global spill-over effects of cyber warfare beyond the theater of war. While the primary target of the NotPetya malware attack was Ukrainian systems, it had a significant impact on multinational organizations and institutions around Europe and North America, resulting in billions of dollars in damages (Greenberg, 2023). This was proof that cyber warfare has transnational effects which can have a significant impact on the global economy and global interconnected systems. Cyber conflict therefore was no longer a bilateral affair, between Russia and Ukraine, but has become a challenge to world peace.

Also, the cyber operations escalated geopolitical tensions between different countries. Western countries, especially NATO nations and the EU, saw Russian cyber operations as a growing challenge to collective security. The perception fostered cyber defense cooperation and enhanced strategic competition as well as tightened sanctions in place against Russia and the West. In sum,

Nye concludes, cyberspace is an arena of constant strategic competition, a space in which states carry out constant low-level confrontation, and one in which the use of the force is not in doubt. This can make the likelihood of miscalculation and unintended escalation higher.

The issue of attribution further undermined international peace during the conflict. Another significant aspect of cyber warfare is the inability to definitively trace attacks back to the originator or individual(s). According to Schmitt &Vihul (2023), attribution issues reduce the effectiveness of deterrence as the states have time to carry out hostile cyber activities without facing immediate responsibility. In the context of the Russia–Ukraine conflict, charges of cyber aggression were very often refuted, leading to greater distrust and diplomatic tension prevailing in the international community.

Furthermore, in the context of the conflict, neither international law nor international institutional bodies are functioning effectively to control cyber operations. International humanitarian law (IHL) bodies were first developed to align with the laws of armed conflict and only offer limited guidance for cyber operations conducted before the threshold of armed conflict (UN General Assembly, 2024). The legal implications of proportional response, sovereignty violations and accountability were unclear because of this institutional weakness. As a result, the world of cyber warfare morphed into a relatively lax regulatory framework, and the potential for cyber war became commonplace among states.

In the eyes of Structural Realism, cyber warfare continues to be a feature of the Russia–Ukraine conflict today, because the international system is anarchic in nature. Without a better authority having the power to enforce the rules effectively, states use self-help to win a strategic advantage. Russia's use of cyber means can thus be interpreted as a general sign of power struggle which faces the purpose of smashing opponents and maintaining geopolitical leverage.

Likewise, Ukraine's cooperation efforts in the field of cyber security with Western countries are aimed at survival and strengthening security within the framework of competition in the international arena.

The same can be said for cyber warfare and how it contributes to instability even when it isn't used in a manner where full-scale direct confrontation between major powers occurs. States view cyber operations as relatively low cost strategic tools that can create considerable disruption without posing "hot buttons" to some of the more direct aspects of conventional warfare. This would ensure ongoing competition in cyberspace and continue to promote an environment of insecurity and distrust among states.

The current Russia–Ukraine war, then, shows how cyber warfare has greatly contributed to the deteriorating peace of the international community between 2022 and 2025. Cyber operations led to: infrastructural disruption, geopolitical tensions, transnational instability, institutional uncertainty and escalation risks in the international system. The struggle has become a strategic one with far-reaching consequences for world peace and security in cyberspace.

The above analysis indicates that the hypothesis that reads ‘Cyber warfare in the Russia–Ukraine conflict has not undermined the international peace within the period of 2022-2025’ is hereby rejected. The study takes it as a given that cyber warfare had a significant effect on international peace and security during the period covered.

4.2 Analysis of Hypothesis Two

Hypothesis Two

2: Cyber Security Strategy has affected the crisis between Russia–Ukraine from 2022 till 2025.

Cyber Security Strategy had a significant influence on the direction, intensity and governance of the Russia–Ukraine conflict (2022-2025). The game showed that in this kind of war, arms will not be decisive anymore, but instead, strategic advantages will be gained through cyber resilience and cyber coordination, as well as technological preparedness. Today, cyber strategies in both Russia and Ukraine more and more are being used not just in order to defend but to get intelligence, disrupt strategies, communicate and gain influence in the international arena.

Enhancement of the country's cyber resilience, which had occurred after previous cyber attacks since 2014, was one of the most crucial elements of Ukraine's cyber security strategy. BlackEnergy and NotPetya attacks were only two of the previously published cyber incidents that highlighted the need for cyber reforms in Ukraine's digital infrastructure and forced the nation to overhaul its cyber defense structure. Microsoft (2024) notes that Ukraine greatly enhanced its cyber defense coordination, thanks to collaboration with Western cyber security organizations, NATO cyber activities, and European digital security organizations. They were especially key since the escalation of the conflict in 2022.

One of Ukraine's primary concerns in its cyber security strategy was infrastructure protection, response to cyber incidents in a timely manner and cooperation in the field of cyber security with foreign countries. Governmental institutions Ops adopted cloud based data protection systems

and decentralized communication networks, trying to minimize such destructive cyberattacks. Ukraine's cyber defense was another strategic enabler for Russian cyber operations that helped contain their impact, as scholars Beska (2025) have put it. Despite the consistent pressure during the digital attacks, Ukraine was able to preserve the performance of key governmental and communication services.

In addition, the international cyber cooperation played a major role in the conflict. Ukraine was given technical and intelligence assistance, cyber defense support, and assistance from NATO members, European Union, private cybersecurity organizations as well as Western technology companies. This international cooperation added to Ukraine's capacity to identify, control and mitigate cyber incidents. The EU Cybersecurity Agency (2024) states that cooperative cyber defense systems facilitated better real-time threat detection, boosting digital resilience against coordinated attacks.

There was also a large-scale cyber strategy in the conflict on the part of Russia. The Russian cyber operations aimed to compromise communication systems, satellite infrastructure, financial institutions and government networks, which were intended to be used to weaken the Ukrainian state capacity and assist in other military operations. Cyber operations were more commonly woven into the concept of hybrid warfare, alongside military operations and information ones, which NATO CCDCOE (2024) noted. The following represent some of the ways in which cyber warfare is becoming institutionalized as part of military thinking today.

Nevertheless, despite of Russia's huge cyber capabilities, scholars believe that several cyber big failures predicted have not happened as expected because Ukraine was more ready to face cyber attacks and had external support. Many of the hopes for cataclysmic cyber paralysis were quashed by defensive adaptation and response and by infrastructure redundancy, Greenberg

(2023) writes. It indicates that the solutions to cyber security strategy can significantly shape the contribution and dynamics of cyber conflict.

The battle also showed how critical cyber resilience is for the stability of nations in the event of conflict. However, Ukraine's cyber security measures successfully limited the impact of attacks on public administration, financial and energy systems. In this context, cyber defense became a direct link with the survival of the State and the continuity of society. Such a capacity ensured the continuity of communication, monetary transactions and institutional stability during times of conflict.

In addition, the conflict had impacts on international diplomatic and strategic relations through cyber security strategy. The aid to Ukraine from the west was viewed by the Russians as a component of a wider shift in geopolitics that was aimed at Russian interests. This contributed to further strategic rivalry and strengthened security dilemma outlined in Structural Realism. Defensive measures were seen as an attack on cyber protection and were viewed as strategic maneuvering, adding to the suspicion of opposing actors.

The war also showed that the current cyber security systems failed in certain aspects. Yet, in spite of the evolution of cyber security, international organizations did not have universal binding and effective cyber governance frameworks to properly control cyber operations. Collective enforcement mechanisms were restricted by attribution issues, variable legal norms and geopolitical competition. In turn, cyber strategies were still strongly based on national capabilities, cooperation and technological advantage, as opposed to international law.

Structural Realists would argue that the cyber security tactics that Russia and Ukraine have employed are both examples of the self-help principle of the international system. Without the

assurance of international institutions, states engaged in technological capability, strategic alliances and cyber preparedness to ensure their survival and strategic advantage. Cyber security then was an extension of power politics in the anarchic international structure.

The growing focus on cyber defense and offensive cyber activities by states can also be attributed to Structural Realism. Survival and relative gains are the main concerns of the states, which makes cyber preparedness a key tool in achieving strategic balance in a situation of uncertainty and competition. The Russia–Ukraine conflict is a good example of the fact that cyber security strategy has become an integral part of modern geopolitical competition.

The analysis, therefore, was able to prove the impact of the cyber security strategy on the Russian Ukrainian crisis in 2022-2025. The intensity of cyber operations, and the overall stability of the conflict environment, was affected by cyber defence mechanisms, international cyber cooperation, strategic adaptation, and resilience planning.

Based on the findings above, the hypothesis which states that “Cyber Security Strategy has affected the crisis between Russia–Ukraine from 2022 till 2025” is hereby accepted. The conclusion of the study is that during the historical timeframe examined, cyber security strategy significantly influenced the dynamics, the management and the results of the conflict between Russia and Ukraine.

4.3 Discussion of Findings

4 Additional Empirical Evidence on Cyber Warfare

Recent verified cybersecurity reports confirm that cyber warfare has become a central feature of modern geopolitical conflicts. The Russia–Ukraine war demonstrated how cyber operations can influence military coordination, national stability, communication systems, and international

diplomatic relations. Cyberattacks targeting energy systems, banking infrastructure, and governmental communication channels revealed the vulnerability of highly digitalized states during periods of strategic confrontation.

Furthermore, the conflict revealed the increasing dependence of states on international cyber cooperation and technological resilience. Western allies, private cybersecurity companies, and international organizations provided critical support to Ukraine in the form of threat intelligence, cloud protection, incident response mechanisms, and digital infrastructure defense. These efforts greatly reduced the effectiveness of destructive cyber operations and strengthened Ukraine's ability to maintain institutional continuity despite persistent attacks.

Verified Source	Key Finding	Importance to Study
Microsoft Digital Defense Report (2024)	Over 600 million cyberattacks were recorded daily worldwide.	Shows the growing scale of cyber warfare.
NATO CCDCOE (2024)	Cyber operations support hybrid military warfare.	Explains cyber integration into conflict strategy.
ENISA Report (2024)	Cyber incidents affect cross-border infrastructure.	Demonstrates global spill-over effects.

Source: Microsoft Digital Defense Report (2024), NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and European Union Agency for Cybersecurity (ENISA).

1. The study found that cyber warfare in the Russia–Ukraine conflict significantly undermined international peace between 2022 and 2025. Cyberattacks on government institutions,

communication systems, energy infrastructure, and financial networks created instability within Ukraine and increased geopolitical tensions internationally. The findings further revealed that cyber warfare produced transnational spill-over effects that affected multinational organizations, international communication systems, and global economic activities beyond the immediate conflict zone. The study also established that attribution difficulties, weak international cyber regulations, and the integration of cyber operations into hybrid warfare contributed to uncertainty, escalation risks, and threats to global peace and security.

2. The study also found that cyber security strategy significantly affected the Russia–Ukraine crisis from 2022 till 2025. Ukraine's improved cyber resilience, international cyber cooperation, cloud protection systems, intelligence sharing, and rapid response mechanisms greatly reduced the impact of Russian cyberattacks and ensured institutional continuity during the conflict. The findings revealed that cyber security strategies became an important part of military operations, national defense, diplomacy, and geopolitical competition. Furthermore, the study established that international technical assistance and cyber defense cooperation from NATO members, the European Union, private cybersecurity firms, and allied states strengthened Ukraine's capacity to resist cyber aggression and influenced the overall dynamics, management, and stability of the conflict.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This study identified the cyber warfare as an emerging threat in the Russia- Ukraine conflict in the period 2022-2025. The study was aimed at the question of the impact of cyber warfare on international peace and the impact of cyber security strategy on the Russia–Ukraine conflict during the period of the study.

The study was done based on Structural Realism as theoretical approach and ex post facto research design. Secondary data sources (academic journals, cybersecurity publications, policy documents and publications from international organizations) were used. Qualitative content analysis with historical and comparative approach was used in analyzing data.

Research showed that cyber warfare was a major threat to international peace in terms of disruptions of infrastructure, geopolitical tension and transnational instability. The study also revealed that the conflict had a significant dynamic and outcome influenced by the cyber security strategy.

In summary, it has been shown in this study that cyber warfare is a significant part of modern-day interstate conflicts and is emerging as a threat to international peace and security.

5.2 Conclusion

Conclusions indicate that cyber warfare is actually a complete revolution in the concept of warfare and international security relations in the modern era. The ongoing Russia-Ukraine

conflict has shown how cyber operations are becoming tools of war with the potential to impact geopolitical dynamics, military operations, and state stability, both within Ukraine and globally.

This study also suggests that cyber security is a key factor in determining state resilience and strategic survival in modern conflicts. Yet, international law and international institutional mechanisms are still not satisfactory for effective regulation of cyber warfare.

Cyber conflict has continued because from a Structural Realist point of view the international system is anarchic and competitive, with states constantly aiming for strategic advantage by technological means.

5.3 Recommendations

1. The governments of Russia and Ukraine, alongside international organizations such as the United Nations and NATO, should strengthen international cyber diplomacy and establish binding cyber warfare regulations to prevent cyber attacks on critical infrastructure, civilian institutions, and communication systems. This would help reduce the threat cyber warfare poses to international peace and security between 2022 and 2025.

2. Russia and Ukraine should improve and expand their cyber security strategies through stronger cyber defense systems, intelligence sharing, international cooperation, and rapid response mechanisms against cyber threats. Effective cyber security strategies can reduce the escalation of the crisis, protect national security interests, and promote stability during the Russia-Ukraine conflict from 2022 to 2025.

REFERENCES

Al-Billeh, T. (2025). The international framework of cyber-attacks under international law. *Journal of Cyber Law and International Security*, 12(2), 44–61.

Beska, S. (2025). Cyber resilience in Ukraine: The response to cyber threats in hybrid warfare (Master's thesis). University of Warsaw.

Broekstra, A. (2024). Digital battlegrounds: Assessing the effects of cyber warfare on international humanitarian law in the Russian-Ukraine war (Master's thesis). Utrecht University.

Derbyshire, R., Coleman, P., & Evans, T. (2025). From protest to power plant: Making sense of the place of escalatory hacktivism in cyber conflict. *Journal of Strategic Cyber Studies*, 8(1), 77–95.

European Union Agency for Cybersecurity. (2024). Threat landscape report 2024. ENISA.

Evelyn, O. (2025). Evaluation of the geopolitical implications of offensive cyber operations. *West African International Security Studies Journal*, 6(1), 31–49.

Gerard, M., Alexei, V., & Thomas, P. (2024). Information narrative detection and evolution modeling on Telegram during the Russia–Ukraine war. *International Journal of Cyber Communication*, 11(3), 102–124.

Greenberg, A. (2023). *Tracers in the dark: The global hunt for the crime lords of cryptocurrency. Doubleday.*

Hoffman, F. G. (2023). Conflict in the 21st century: *The rise of hybrid wars*. Potomac Institute Press.

Juutilainen, J. (2022). Cyber warfare: A component of the Russo-Ukrainian war in 2022 (Bachelor's thesis). Finnish National Defence University.

Kelleher, C. (2023). Cyber spillover and global digital vulnerability after NotPetya. *Cyber Security Review*, 15(2), 55–72.

Kello, L. (2023). *The virtual weapon and international order*. Yale University Press.

Khoirunnisa, C. S. (2024). Cyber warfare strategies during the Russian-Ukraine war (2021–2022): National security and modern warfare (Undergraduate thesis). Universitas 17 Agustus 1945 Jakarta.

Kostyuk, N., & Zhukov, Y. (2023). Invisible digital front: Cyber operations in the Russia–Ukraine conflict. *Journal of Conflict Studies*, 18(4), 221–239.

Malikussaid, M., & Sutiyo, A. (2025). The effect of the Russia–Ukraine conflict on the cloud computing risk landscape. *International Journal of Information Security and Cloud Computing*, 9(1), 67–84.

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton.

Melella, C. (2024). Disjointed cyber warfare: Internal conflicts among Russian intelligence agencies. *Journal of Intelligence and Cyber Operations*, 5(2), 88–104.

Microsoft. (2024). Defending Ukraine: Early lessons from the cyber war. Microsoft Digital Security Unit.

Muzayan Haq, M. Y., Rahman, A., & Ibrahim, S. (2023). Evaluating the actions of network operators to improve digital sovereignty and network resilience during the Russia–Ukraine war. *International Journal of Network Security*, 21(4), 301–319.

NATO Cooperative Cyber Defence Centre of Excellence. (2023). Cyber threats and hybrid warfare in Eastern Europe. NATO CCDCOE.

NATO Cooperative Cyber Defence Centre of Excellence. (2024). Cyber operations and strategic escalation in the Russia–Ukraine conflict. NATO CCDCOE.

Nye, J. S. (2024). Cyber power and national security in the digital age. Oxford University Press.

Rid, T. (2024). Cyber war will not take place (Updated ed.). Oxford University Press.

Sani, A. I., Okeke, P., & Bello, M. (2025). Qualitative analysis of cyber preparedness in Nigeria against state-sponsored cyber attacks. *African Journal of Cyber Policy and Security*, 7(2), 91–110

Schmitt, M. N. (2023). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2023). International cyber law and state responsibility in cyberspace. *Harvard International Law Review*, 64(1), 145–168.

United Nations General Assembly. (2024). Developments in the field of information and telecommunications in the context of international security. United Nations.

United Nations Institute for Disarmament Research. (2024). Cyber stability and international peace. UNIDIR.

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.