THE REPUBLIC OF TÜRKİYE
SOCIAL SCIENCES UNIVERSITY OF ANKARA
THE GRADUATE SCHOOL OF SOCIAL SCIENCES

RUSSIA'S INFORMATION WARFARE POLICIES IN UKRAINE CONFLICT

Master's Thesis

İrem Güldem KARAR

PEACE AND CONFLICT STUDIES

August 2024

THE REPUBLIC OF TÜRKİYE
SOCIAL SCIENCES UNIVERSITY OF ANKARA
THE GRADUATE SCHOOL OF SOCIAL SCIENCES

RUSSIA'S INFORMATION WARFARE POLICIES IN UKRAINE CONFLICT

Master's Thesis

Irem Guldem KARAR

Prof. Dr. Murat YEŞİLTAŞ

PEACE AND CONFLICT STUDIES

August 2024

Canım aileme ve inançla sürdürdüğüm mücadeleye minnetle…

TEŞEKKÜR

Bu süreçte değerli görüşleriyle yolumu aydınlatan ve bana rehberlik eden değerli hocam Prof. Dr. Murat Yeşiltaş'a derin teşekkürlerimi sunarım. Ayrıca, manevi destekleriyle her zaman yanımda olan ve tezimin tamamlanmasına olan inançlarıyla beni teşvik eden aileme, Semra Aksu'ya ve Hatice Demirci'ye yürekten teşekkürlerimi sunarım.

TABLE OF CONTENTS

TEŞEKKÜR iv
TABLE OF CONTENTS v
ÖZET vii
ABSTRACT ix
ABBREVIATION xi
TABLE OF FIGURES xii
LIST OF TABLES xiii
1. CHAPTER 1: INTRODUCTION 1
1.1. Research Aims and Objectives 3
1.2. Research Methodology and Research Question 4
1.3. Structure of the Thesis 7
1.4. Literature Review 8
2. CHAPTER 2: CONCEPTUAL FRAMEWORK OF INFORMATION WARFARE 12
2.1. Two Types of Information Warfare 13
2.2. Three Classes of Information Warfare 16
2.2.1. Class I: Personal Information Warfare 16
2.2.2. Class II: Corporate Information Warfare 17
2.2.3. Class III: Global Information Warfare 17
2.3. History of Warfare: Agrarian Wave, Industrial Wave, Information Wave 18
2.3.1. First Wave: Agrarian Wave 18
2.3.2. Second Wave: Industrial Wave 19
2.3.3. Third Wave: Information Wave 20
2.4. Seven Forms of Information Warfare 21
2.5. Strategies of Information Warfare 25
2.6. Weapons of Information Warfare 27
3. CHAPTER 3: RUSSIAN INFORMATION WARFARE POLICIES . 30
3.1. Russian Information Warfare Concepts 30
3.1.1. Information Confrontation instead of Information Warfare 31

3.1.2. Main Terminologies Related to Information Confrontation in the Literature 33
3.1.3. Weapons of Information Confrontation 34
3.1.4. Who use Information Confrontation in Russia? 36
3.2. Historical Perspective of Russia in Information Confrontation 37
3.2.1. Information Confrontation Before the Soviet Era 37
3.2.2. Information Confrontation During the Soviet Era 39
3.2.3. Information confrontation in the Post-Soviet Era 45
3.2.4. 21st Century Developments and Gibridnaya Voyna (Hybrid War) 48
3.3. Russian Information Warfare Doctrine 57
3.3.1. 2011- Information Space Activities Concept 57
3.3.2. 2014- The Military Doctrine 60
3.3.3. 2015- 2021- Strategies of National Security 62
3.3.4. 2016- Doctrine of Information Security 67
3.3.5. Foreign Policy Concepts 69
4. CHAPTER 4: RUSSIAN INFORMATION WARFARE POLICIES IN UKRAINE CONFLICT 73
4.1. The Nature of the Conflict 73
4.2. Information Confrontation Policies of Russia in Ukraine 75
4.2.1. Information- Psychological Field: Kremlin Rhetoric 76
4.2.2. Information- Psychological Field: Social Media 93
4.2.3. Information- Technical Field: Cyberwarfare 101
5. CHAPTER 5: CONCLUSION 107
BIBLIOGRAPHY 117

ÖZET

Bilgi Harbi, yeni dönem çatışmalarını anlamak için önemli bir perspektif sunmakta ve devletlerin çatışmaları meşrulaştırmada etkili bir araç olarak kullanılmaktadır. Rusya- Ukrayna çatışması, savaşın savaş alanında değil ilk olarak insanların aklında kazanılması gerektiğini vurgulayarak bilgi harbi alanında bir kırılma noktasıdır. Rusya, bu alana özel bir önem vermiş ve kendi politikalarını geliştirerek bilgi üstünlüğünü sağlamaya çalışmaktadır. Bu, Rusya'nın Sovyetler Birliği'nin dağılmasıyla kaybettiği eski etki gücüne ulaşma arayışından kaynaklanmaktadır. Bu çerçevede, Rusya'nın Ukrayna çatışmasındaki bilgi- psikolojik ve bilgi-teknik alanlarda geliştirdiği politikalar, bilgi harbine verdiği önemi açıkça ortaya koymakta ve bu çatışma ile ortadan kaldırılmaya çalışılan güçlü Rusya algısını tekrar inşa etmeyi amaçlamaktadır. Örneğin, bilgi- psikolojik alanında Rusya alıntısını din, dil, coğrafya, batı karşıtlığı, kültür ve tarihsel anlatı üzerine kurarken, bilgi- teknik alanını genellikle siber saldırılara karşı savunma ve saldırı politikalarıyla oluşturmuştur. Bu tez, Rusya'nın Ukrayna üzerinde uyguladığı bilgi harp politikalarını inceleyerek Rusya'nın bilgi üstünlüğünü sağlaması sonucunda Ukrayna çatışmasında Rusya'nın oynadığı rolü meşrulaştırdığına dair bir bakış sunmayı hedeflemektedir.

Rusya'nın Ukrayna üzerinde uyguladığı bilgi harp politikaları hakkında Rusya'nın Ukrayna'ya yönelik tutum ve davranışını anlamak amacıyla kelimeler, resimler ve gözlemlerden veriler toplanmıştır. Literatür araştırması, çatışmaya yönelik ulusal ve uluslararası medyanın bakış açısı, sosyal medyanın kullanımı ve siber saldırılara karşı gelişen yeni teknolojilerle elde edilen veriler üzerinden bir çıkarım yapılmıştır. Fakat çatışmanın devam etmesinden dolayı yapılacak çıkarım öngörü

niteliğindedir ve tezi sonucunu kısıtlamaktadır. Elde edilen veriler doğrultusunda, Rusya'nın bilgi- psikolojik alanında oluşturduğu anlatı ve bilgi- teknik araçlarını kullanarak bu anlatının yayılması, çatışmanın daha da uzaması ve Ukrayna'ya yeterli destek sağlanmadığı müddetçe çatışmanın, Rusya'nın anlatısının benimsenerek meşrulaştırılmasının kaçınılmaz olduğu sonucuna varılmaktadır.

Anahtar Kelimeler: Bilgi Harbi, Rusya- Ukrayna Çatışması, Bilgi-Teknik, Bilgi- Psikolojik, Bilgi Harp Politikaları

ABSTRACT

Information warfare offers a crucial perspective on understanding new era conflicts and is used as an effective tool by states to legitimize the conflicts. The conflict between Russia and Ukraine marks a pivotal moment in the realm of information warfare, emphasizing that the war must be won first in people's minds, not on the battlefield. Russia has assigned special significance to this field and is trying to ensure information superiority by developing its own policies. This pursuit is driven from Russia's attempt to recover the influence it lost the following the dissolution of the Soviet Union. Within this framework, the policies developed by Russia in the information-psychological and information-technical fields during the Ukrainian conflict clearly demonstrate the importance it attaches to information warfare and aim to rebuild the perception of a powerful Russia that was trying to be eliminated by this conflict. For instance, in the information-psychological field, Russia constructs its narrative based on religion, language, geography, anti-Westernism, culture, and historical discourse, while it has generally created the information-technical field with defense and attack policies against cyberattacks. This thesis aims to examine Russia's information warfare policies in Ukraine and provide an overview of how Russia legitimized its role in the Ukrainian conflict as a result of its information superiority.

Data were collected from words, pictures and observations in order to understand Russia's attitude and behavior towards Ukraine about the information warfare policies implemented by Russia on Ukraine. An inference was made based on literature research, the perspective of national and international media on the conflict, the use of social media,

and the data obtained with new technologies developed against cyberattacks. However, due to the continuation of the conflict, the inference is predictive and limits the conclusion of the thesis. In line with the data obtained, it is concluded that Russia's narrative in the information psychological field, spread through the use of information-technical tools, prolongs the conflict further, and it is inevitable to legitimize the conflict by adopting Russia's narrative unless sufficient support is provided to Ukraine.

Keywords: Information Warfare, Russia- Ukraine Conflict, Information Technical, Information Psychological, Information Warfare Policies

ABBREVIATION

AI	Artificial Intelligence
CERT-UA	The Computer Emergency Response Team of Ukraine
CW	Cyberwarfare
C2W	Command and Control Warfare
DOD	Department of Defense
DoI	Denial of Information
D&D	Disruption and Destruction
D&M	Deception and Mimicry
EW	Electronic Warfare
EIW	Economic Information Warfare
FSB	Federalnaya Sluzhba Bezopasnoti[1]
GRU	Glavnoye Razvedyvatelnoye Upravleniye[2]
HW	Hacker Warfare
IBW	Intelligence- Based Warfare
KGB	Komitet Gosudarstvennoy Bezopasnoti[3]
MIJI	Meaconing, Intrusion, Jamming and Interference
PW	Psychological Warfare
RT	Russia Today
SUB	Subversion
SVR	Sluzhba Vneshney Razvedki[4]
UNIDIR	United Nations Institute for Disarmament Research

[1] This term is commonly used in English as Federal Security Service
[2] This term is commonly used in English as The Main Directorate of the General Staff of the Armed Forces.
[3] This term is commonly used in English as The Committee for State Security.
[4] This term is commonly used in English as Foreign Intelligence Service.

TABLE OF FIGURES

Figure 1: OIW Strategy Flowchart 14
Figure 2: Three waves of warfare 18
Figure 3: Seven Forms of Information Warfare by Libicki 21
Figure 4: Information Warfare Strategies by C. Kopp 25
Figure 5: Methods used to spread communist ideology 39
Figure 7: "If this is freedom, then what is prison" 45
Figure 8: "Conquering Space" David Pollack 1960s. 45
Figure 10: RT News 96
Figure 11: Sputnik Global News 96
Figure 12: TV Zvezda 98

LIST OF TABLES

Table 1: Information Security Threats and Mitigation Policies in the National Security Strategy of Russia..... 65
Table 2: Russia's Strategic National Priorities (2015-2021)..... 67

1. CHAPTER 1: INTRODUCTION

In order to understand the contemporary dynamics of interstate peace and conflict, it is crucial to observe the changes and trends of the era. Toffler & Toffler (1995) defines the current era of the world as the Information Age. Accordingly, developing technology and the boundless proliferation of knowledge have emerged as source of power. This new power has raised to concern about how the power, which forms the basis of international relations, will be used by various states.

The utilization of information, which forms the cornerstone of the Information Age, in interstate conflicts has given rise to a novel concept known as information warfare in the literature. Particularly following the dissolution of the Soviet Union, this phenomenon gained significance and began to be studied within the realm of international relations. Now, interstate competition based on weapon production, a legacy of the industrial revolution, has been replaced by information manipulation that shapes societies in line with the interests of states.

Since information warfare is studied in a multidisciplinary field, it has a wide scope, so it is not possible to compress it into a single definition. Nonetheless, a foundational understanding can be established through a basic definition. Information warfare entails ensuring information superiority over the opponent through the proper use of developing technology. This definition was developed by different scholars, and the theory has been enriched through diverse perspectives such as types, forms, and strategies of information warfare.

The weaponry employed in information warfare plays a pivotal role in ensuring information superiority over the opposing side. These weapons encompass a diverse array and aim to manipulate information by

damaging the software systems of the adversaries or to prevent the use of conventional weapons that work with computer software. The emergence of challenges stemming from state utilization of such weaponry has underscored the necessity for international regulation. However, since no consensus has yet been reached as to whether the use of these weapons constitutes a use of force, regulation has not been introduced. Another pressing issue is that, with the development of technologies, information can easily be seized by individuals, states or non-state actors and used in a detrimental way. For instance, the ubiquitous discourse surrounding artificial intelligence technology exacerbates concerns by enabling reputation damage through the manipulation of individuals voices or images.

States are formulating various policies specifically for information warfare. The aim of these policies is to legitimize the actions of the state by preventing the discomfort that any action taken by the state for its own interests will cause in international public opinion. In this regard, Russia stands out prominently for its policies on information warfare. Russia has primarily adopted the information warfare theory originating from the West by developing parallel concepts through its own scholars. Notably, Russia has explored analogous concepts with comparable functionalities, such as information confrontation instead of information warfare etc.

Within the scope of information warfare, it is claimed that Russia can maintain its influential position within the global power structure by attaining superiority over adversaries through psychological operations such as propaganda, disinformation, and deception. The widespread utilization of propaganda tools was observed during the Cold War. The Soviets employed information warfare tactics such as propaganda to ensure the dominance of communist ideology over liberal ideas. Despite

efforts to achieve theories like active measures or reflexive control during the Soviet era, these theories were replaced by concepts such as the Russian Federation's notion of "gibridnaya voyna" following the collapse of the USSR. Gibridnaya voyna, as articulated in Russian information warfare literature, encapsulated the concept of "hybrid war". In general, these theories have been integrated into practical frameworks in the military doctrines of the Russian Federation, strategies of national security, foreign policy concept and information security doctrines.

The policies implemented by Russia in the Ukrainian conflict generally derive their origins from historical processes and doctrines. While seeking an answer to the research question in this thesis, the information policies implemented by Russia in Ukraine will be examined under two main headings: information-psychological and information-technical. Information psychological policies will focus more on Putin's discourses and social media operations, while information technical policies will focus on Russia's cyber operations. Finally, this thesis aims to understand the effects of Russia's information warfare policies on Ukraine by examining their effects on the balance of power in the information age.

1.1. Research Aims and Objectives

The primary objective of this thesis is to explore the impact of the escalating role of information warfare in the conflict between Ukraine and Russia. Specifically, it seeks to examine the breadth and substance of Russia's information warfare strategies regarding Ukraine. Through these strategies, Russia has crafted an information warfare policy that seeks to legitimize its actions domestically and internationally. This is achieved

via a coordinated mix of information-psychological and information-technical efforts.

1.2. Research Methodology and Research Question

At the beginning of the thesis, various questions arise regarding the selection of an appropriate research methodology. These questions generally focus on where and how to obtain reliable data that is compatible with the subject of the thesis or what structure the thesis should have. Therefore, it is crucial to determine the most appropriate research method to investigate Russia's information warfare policies in the Ukraine Conflict.

In this thesis, qualitative and case study methods will be used to scrutinize Russia's information warfare policies in the Ukraine conflict. First of all, it has been determined that qualitative analysis is a suitable method for the thesis because it deals with how and why. The information warfare policies used by Russia in the Ukraine conflict will be analyzed with data obtained from official documents, Putin's speeches, media reports, and other relevant sources. Furthermore, insights derived from Russia's military doctrines, strategies of national security, foreign policy concepts, and information security doctrines will be utilized to explain the information warfare policies implemented during the Ukrainian conflict. Additionally, Putin's pre-conflict address to the nation will constitute a pivotal source for this thesis.

Information Warfare has gained popularity in multidisciplinary fields as a direct result of the ongoing tensions between Russia and Ukraine. Therefore, one of the most significant aspects that makes the Ukraine case worthy of scholarly inquiry is that Russia and Ukraine are two separate sovereign entities recognized by the United Nations. Although

information warfare applications have increased in prestige in academic discourse, especially after the 1991 Gulf War, case studies have predominantly remained limited to focusing on the conflict between state and non-state actors.

Another reason why the case study method was preferred in this thesis is to examine the usage areas of Information Warfare applications within interstate conflicts. Accordingly, the ongoing conflict between Russia and Ukraine was chosen as an on-site case study. Additionally, another motivation for choosing the case study method is to investigate the role of information warfare policies by focusing on how states' actions are tried to be legitimized in the eyes of the international public. In this thesis study, some steps were followed using the case study method. First, the information warfare implemented by Russia in former Soviet regions after the collapse of the Soviet Union was examined and how these policies were used in the conflict that started in 2022 and is still ongoing.

A conceptual framework was then created to understand the conflict between Russia and Ukraine. For example, information warfare has defensive and offensive dimensions, and Russia follows an offensive strategy by targeting Ukraine's command and control systems with cyber operations; It has been observed that the international community is trying to strengthen Russia's defense position by responding with propaganda against Russia. Defensive and offensive information warfare strategies can shape the legitimacy of the conflict or trust in the government by influencing dependent variables such as public perception.

The process of collecting data based on a concept determined by the case study method is of great importance. In order to understand Russia's information warfare policies in the Ukrainian conflict, official sources such as official documents, doctrines, foreign policy concepts, as well as

statements of government officials are used as sources. Additionally, sources such as Rand Corporation, Atlantic Council reports, academic papers, and social media activities have been utilized to understand both Russian and Ukrainian perspectives.

In addition, efforts have been made to access materials such as misinformation campaigns, cyber-attacks and social media interactions through quantitative data collection method. Supported by qualitative data from speeches, interviews and official statements of both sides, this study aims to go beyond conventional military conflicts between Russia and Ukraine. It was aimed to show which side achieves information superiority by examining the symbols and actions conveyed through the media (such as Zelensky wearing camouflage to highlight Ukraine's resistance or Russia's social media posts denigrating Ukrainian soldiers).

This thesis aims to fill the gap in the literature by analyzing Russia's practices in Ukraine by examining the effectiveness of information warfare policies in contemporary conflicts through the utilization of both qualitative and case study methods. Nevertheless, given the thesis's domain, it is imperative to examine the problem statement. Since both sides are involved in the conflict between Russia and Ukraine, studies are often viewed from a biased perspective. Within this thesis, any biased discourse will not be supported and will not be portrayal of a right or wrong side. In addition, both Russian and Western-based sources regarding information warfare are included, and Russia's information warfare policies will be inferred from reliable and valid sources.

This thesis aims to address the central research question: "What are the key elements of Russian information warfare policies in the context of the Ukraine Conflict?" To answer this, the study first defines the concept of information warfare, then traces the evolution of Russia's information

warfare policies over time. Finally, it provides a detailed analysis of Russia's information warfare policies specifically related to Ukraine, based on the collected data.

In this way, while seeking an answer to the research question, information warfare dynamics in contemporary conflicts were discussed and a more comprehensive meaning was given to the Ukrainian conflict instead of looking at it from a singular perspective.

1.3. Structure of the Thesis

This thesis structured into five primary chapters. Each chapters addresses a distinct aspect of the research topic. The initial chapter provides general structural information and includes the sections of introduction, research aims and objectives, methodology and research question, structure of the thesis, literature review. The second, third and fourth chapters of the thesis prefer an order from general to specific while seeking an answer to the research question. Consequently, the second chapter of the thesis explore the scope of information warfare concept. Within this context, since information warfare does not have a universally acknowledged definition, it has been explained how the theory is defined by different researchers. In order to enhance the concept more clearly, insights into the tools utilized in information warfare are elucidated.

Following the elucidation of the theoretical structure of information warfare understandable, Russia's information warfare policies are examined in the third part of the thesis. At the beginning, the discussion centers on the "information confrontation" theory developed by Russia in parallel with the information warfare theory, shedding light on the tools employed by Russia in information warfare and the actors responsible for

their implementation. In the rest of the chapter, Russia's information warfare policies from past to present are analyzed in detail.
Towards the end of the chapter, Russia's doctrinal documents, namely foreign policy concepts, national strategies and military doctrines, are examined and a general framework of the policies followed by Russia in information security is presented.

In the second and third chapters of the thesis, preparations for addressing the research question were completed, and in the fourth chapter, an answer was sought to Russia's information warfare policies in the Ukrainian conflict in order to answer the research question. In this context, two main parameters were emphasized: information psychological and information technological. The fifth and last chapter of the thesis summarizes the important points, states the contributions to the literature, presents some suggestions and contains the author's conclusions.

1.4. Literature Review

The literature review constitutes one of the most critical parts of the thesis. This is accomplished by utilizing appropriate, reliable and accurate sources to answer the research question. In this thesis, different aspects of information warfare were touched upon and the drawing upon the contributions of numerous researchers. In this way, by synthesizing the insights gleaned from these scholarly endeavors, this study aims to illuminate contemporary events by contextualizing from past to present day manifestation. However, Information warfare, as a field of study based on manipulative data, allows the truth to be presented and interpreted in various ways. This situation is particularly evident in the Ukraine-Russia conflict. The sources used were manipulated in

accordance with the parties' information warfare and arranged to suit their own interests. For this reason, it causes difficulties in accessing reliable information while searching for suitable sources for the thesis.

In the thesis, the framework of information warfare was defined by Libicki in his book "What is Information Warfare" in 1995, with seven different forms of information warfare. Libicki's work highlights the complexity and diversity of the field. This book is an important mainstream book for understanding the different strategic aspects of information warfare by creating a conceptual framework. Libicki's classification of information warfare into seven forms, from cyber warfare to economic information warfare, provides a comprehensive understanding of the multifaceted nature of information warfare.

Toffler & Toffler's book "War and Anti-War" (1993) focuses on the historical development of information warfare and writes about the transition to the information age in contemporary societies and the effects of this transition on war and war strategies. They also argue that the information age offers a different paradigm from the agricultural and industrial eras and draw attention to the change in the nature of war in this context. The book provides an in-depth analysis to understand the shape information warfare took in the 1990s and is an important resource for grasping the historical evolution of information warfare and understanding how information warfare strategies are shaped today. This study presents a perspective on how war transitioned from industrial to information warfare in modern times, while also emphasizing the transformation in today's war strategies.

Schwartau's book "Information Warfare" (1994) examines the different dimensions of information warfare in detail. The author emphasizes the need for a detailed analysis of information warfare not

only from its military dynamics but also from its economic, political and social dimensions. The book also shows cyber security, manipulation and propaganda as the three main points of information warfare. In his book, Schwartau offers a comprehensive perspective on information warfare as he examines information warfare in legal, ethical and cultural areas. Therefore, it is one of the main reference sources for information warfare.

Timothy L. Thomas's works are among the main sources of the thesis. In particular, many different articles and books he wrote on the military strategies of the Soviets and Russia constitute an important part of the research. It is noteworthy that Thomas, in his article "Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice" (2004), categorizes the tools Russia uses in information warfare and puts them into a certain structure. Apart from this, Thomas's examination of the effects of the 2008 events on information warfare in his article "Russian Information Warfare Theory: The Consequences of August 2008" (2010) is an important source of information for the thesis. Thomas's book "Kremlin Control: Russia's Political-Military Reality" (2019) is also emphasized in the thesis as a critical reference source for understanding Russia's political and military reality.

Today, the main source for understanding Russia's modern war strategies is Fridman's work called "Russian Hybrid Warfare" (2018). Fridman analyzes Russia's hybrid war strategies, which include the use of traditional military force along with contemporary warfare methods such as manipulation, propaganda, and cyberattack. This research significantly enhances our understanding of the impact of Russia's information warfare policies.

In addition to these studies, recent literature has also examined the developing structure of information warfare within the framework of

modern technological advances. Trifonov, Nakov and Mladenov (2018) discuss the effects of artificial intelligence on cyber threat intelligence and modern cyber warfare techniques in their study titled “Artificial Intelligence in Cyber Threats Intellegence”. Wright (2020), in his article titled “The Future of Cyber Conflict”, was used to discuss the future of cyber conflicts and modern cyber warfare techniques. Zeitzoff (2017) in his study titled “How Social Media is Changing Conflicts” discusses the effect of social media in conflicts and its role in the spread of propaganda to the public. Additionally, Zabrodskyi et al. (2022) in their report titled “Preliminary Lessons in Covential Wrafighting from Russia’s Invasion of Ukraine”, they emphasize the use of information warfare in traditional war strategies in the context of Russia’s invasion of Ukraine. It contributes to providing a comprehensive view of the latest studies and the latest developments in the war and supports the arguments of the thesis.

2. CHAPTER 2: CONCEPTUAL FRAMEWORK OF INFORMATION WARFARE

There is a war out there, old friend, a world war.
And it is not about who's got the most bullets.
It's about who controls the information:
... what we see and hear, how we work, what we think.
It's all about the information! (Robinson,1992).

In this section, definitions of some researchers who have considered information warfare as a concept, especially after the 1990s, are included. Due to the broad nature of information warfare, many researchers from different fields have developed their own concepts by approaching this issue from different perspectives. This thesis includes definitions of information warfare at the political level, which can be parallel to the information warfare policies implemented by Russia within the framework of the Ukrainian war.

Firstly, the defensive and offensive types of information warfare were examined, and then Winn Schwartau's personal, corporate and global information warfare were discussed. Alvin and Heidi Toffler, who defined information warfare in the historical development of warfare, talked about the transition to the information warfare era in the 21st century in the historical transformation of information warfare. The seven forms determined by Martin C. Libicki are explained and C. Koop's strategic approach to information warfare is examined, aiming to form the basis of policies in the Russia-Ukraine war. Finally, the variety of weapons used in information warfare is mentioned, with the goal of offering an extensive view on how these policies are applied in contemporary conflicts like the Russia and Ukraine situation.

One of the notable topics that have garnered recent attention and led to the formulation of national strategies is Information Warfare. Nonetheless, a fundamental challenge associated with this emerging concept lies in the absence of a universally accepted definition. Even agreement on alternative terminology, such as cyberwar, netwar, information war-based war, knowledge-based war, command and control warfare, and information age conflict, has not been reached. As a result, achieving a unified technical, theological, or political definition is challenging.

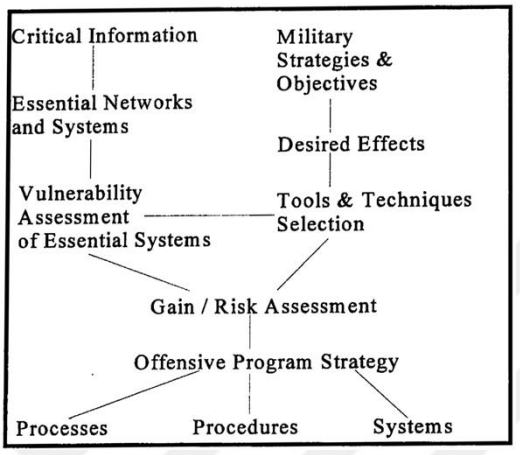
The US Department of Defense provides the most commonly cited definition of information warfare in existing literature. According to US Department of Defense, these actions involve protecting one's information systems from exploitation, corruption, or destruction while simultaneously targeting an adversary's systems to gain an information advantage. This strategy seeks to achieve information superiority in line with national military objectives by affecting adversary information systems while safeguarding one's own (DeVries, 1997).

The Department of Defense not only defines information warfare but also looks at it more broadly and divides it into two types.

2.1.Two Types of Information Warfare

According to DoD, Information Warfare consists of both offensive and defensive components. When determining the national strategies of countries concerning Information Warfare, a coherent strategy should be proposed in both types. It is essential to create an advanced organizational chart and countries should formulate policies in accordance with this chart.

Figure 1: OIW Strategy Flowchart



Source: (Elam,1996, p.83)

To begin with, offensive information warfare is defined as any activity aimed at disrupting or dismantling an adversary's information system. The initial phase of the strategy theme created in offensive information warfare is the acquisition of "critical information" by countries. The collected critical information feeds itself with "essential networks and systems". Nonetheless, the weakness in this system is found with the "vulnerability assessment of essential system". On the other side of the offensive strategy, which is also highlighted in the table, the "desired effect" on the opponent is delineated through "military strategies and objectives". As a result of the vulnerability assessment, it is necessary to choose the appropriate tool and technique. This process allows for the identification of potential gains and risks, culminating in the development of an offensive program strategy (Elam, 1996).

The offensive information warfare strategy theme is built around determining tools and techniques. Tool and technique can be analyzed in

many different forms. While physical offensive information attacks can be carried out by attacking command centers, telephone switches or microwave towers, the opponent can also be neutralized with psychological offensive information attacks such as propaganda messages. For instance, the propaganda message can be spread as desired through media and tools such as video morphing. Friendly troops can use misinformation, as well as carefully prepared audio and video footage, to trick enemy forces or even the opponent's home front into believing something is happening that is not. (DeCaro, 1994). All of these find a place in traditional forms of offensive information warfare. While phreaking form is mostly an attack on phone systems manipulation, computer enabled form can be applied as data manipulation by hackers.

Defensive Information Warfare refers all actions taken to defend against information attacks (Alberts, 1996). The strategy that should be followed by countries in order to protect themselves from these attacks begins with creating awareness on the problem. Subsequently, a vision should be put forward by the government and the target to be achieved should be explained. The next stage should be to ensure information security through laws and regulations. Additionally, the government should allocate the financial funds to the private sector to ensure information security. Organizations and disparate groups other than the private sector should be engaged in this process, so that the necessary cooperation will be provided to solve the problem. Moreover, the duties and responsibilities of the organizations and groups collaborating with the government should be defined (Liu & Jajodia, 2013).

2.2. Three Classes of Information Warfare

Information Warfare is defined comprehensively in Winn Schwartau's book Information Warfare, published in 1996, and he categorizes this concept into various classes. According to Winn Schwartau, Information Warfare is divided into three different classes: Personal, Corporate and Global.

2.2.1. Class I: Personal Information Warfare

Winn Schwartau stressed three points about Personal Information Warfare: First off there is no such thing as electronic privacy. Second, in cyberspace, you are presumed guilty unless proven innocent. Finally, information is a weapon. Class I information warfare refers to attacks targeting an individual's electronic privacy, encompassing digital records, files, and various elements of their digital identity (Schwartau, 1994). The easy accessibility of personal information brings along many risks. For instance, individuals with malicious intentions can easily obtain highly confidential information of individual, such as dates of marriage or divorce, financial transactions conducted at banking systems, criminal records, past lawsuits, and hospitalizations, for the purpose of wrongful use. Information of an individual could be used for nefarious purposes, to extort money from them, or to harm their reputation if it is obtained by malicious people.

2.2.2. Class II: Corporate Information Warfare

Class II's primary motto is related to information use rather than information acquisition. Information disseminated about a company can be used not only to generate profits from that company but also with the intention of damaging its reputation. For instance, gaining access to a company's commercial secrets can be used to attempt to foster a competitive environment. This situation is not limited solely to companies but may also cause competition between states. According to Schwartau (1997), after assisting America in information acquisition for Germany, Japan, South Korea, and France, he emphasized the possibility that this assistance could potentially be used against America in the future. Interstate political and economic competition can incentivize the use of information power as a weapon (Schwartau, 1997). Information weaponry is carefully selected by researching the weaknesses or strengths of the opponent. If well-planned, Class II Corporate Information Warfare can lead to destructive effects for both governments and companies.

2.2.3. Class III: Global Information Warfare

Class III Information Warfare is much more comprehensive than Class II Information Warfare. This is due to the fact that Class III envisions a genuine conflict against companies, countries, and the global financial system, invisibly. Another feature that distinguishes Class III from Class II is that Class III is much costlier because its area of effect is larger and wider. It is run by a group of people as the aim is to create a truly global impact. According to Schwartau (1994), this group of individuals or elites must meet certain criteria. For instance, Information warriors of elites

must have substantial financial backups and motivation to believe they will become richer than Bill Gates. Recognizing the limitations of individual efforts, they need people who will work towards the goal without any questioning. Adequate technical infrastructure is essential for effective usage of information, and patience is important to witness the outcome of these stages (Schwartau,1994, p. 140).

2.3. History of Warfare: Agrarian Wave, Industrial Wave, Information Wave

The definition of Information Warfare in its historical context was formulated in 1997 by Reto E., who drew on concepts from Alvin and Heidi Toffler's book *War and Anti-War.* According to this seminal study, the evolution of Warfare across history can be separated into three waves: agrarian, industrial, and information.

Figure 2: Three waves of warfare

Source: (Toffler & Toffler, 1995).

2.3.1. First Wave: Agrarian Wave

The Agricultural Revolution played a significant role in precipitating conflicts over "soil" This phenomenon was caused by two major factors. Firstly, fighting for land from which economic gains can be made, and

secondly, helping accelerate the development of the state.

The connection between war and soil is summarized in ancient Chinese writings by "The Great Lord Shang" as follows: The nation's peace is depending on agriculture and war (Toffler & Toffler, 1995).

In the initial period of the warfare wave, everything is connected to agriculture. The greatest damage that can be inflicted on a country is to destruction of its agricultural resources after defeating enemy forces on the battlefield. During this initial period, military structure can be diversified in terms of training, leadership quality, morale, and capabilities. Additionally, the communication systems were also primitive. Soldiers' salaries were paid with the economic returns obtained from agriculture. The war tools of the time commonly included pikes, swords, axes, and lances.

2.3.2. Second Wave: Industrial Wave

The formation of this period occurred after the Industrial Revolution. The most significant word defining this period is "mass production". Mass production has occurred not only in the military field but also in the fields of education, communication, consumption and entertainment. World War I and Second World War were two major wars that occurred during the industrial wave period. These wars brought about unprecedented levels of destruction never before witnessed in human history. During the Cold War, intense competition between the two superpowers emerged over the large-scale production of armaments (Haeni, 1997).

2.3.3. Third Wave: Information Wave

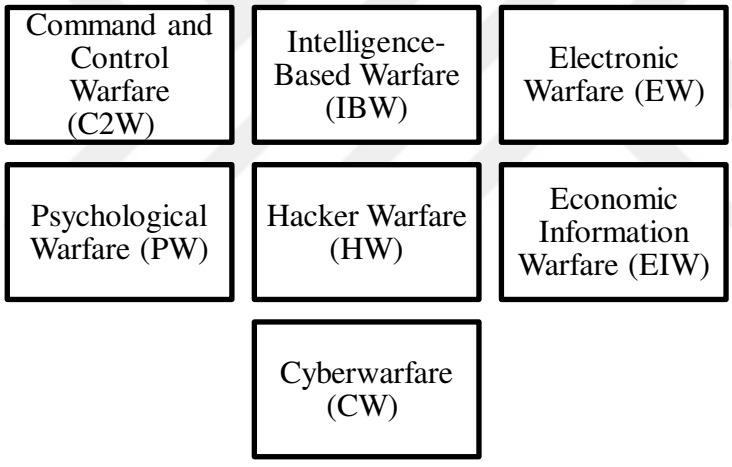
The word that can briefly describe the Third Wave is “knowledge”. In order to be powerful in the third wave, one must have access to information strategically and operationally and be able to use this information correctly. According to Toffler & Toffler (1995), the first example of the transition from the Second Wave to the Third Wave is the Gulf War. Although Haeni opposes this view, the controlled dissemination of information by the US and its partners was also critical in this conflict.

Toffler & Toffler (1995) stated that the Gulf War is a war that also displays Second Wave and Third Wave characteristics (Toffler & Toffler, 1995). First of all, the most concrete example of the transition from the destruction and long running unremunerative wars that occurred during the Industrial Wave period to experiencing quick victories and less casualties were the 1991 Gulf War (Eriksson, 1999). It is seen that casualties are less with this war compared to other wars. However, it seems that the Gulf War did not completely break away from the Second Wave methods. This means that the United States and its allies fought against Saddam Hussein with two different war methods. Secondly, it was the war against Iraq by dropping bombs from airplanes, one of the tools of the Second Wave period. Third, the technology, one of the Third Wave tools, has been widely used by the United States and its allies. For instance, one of the ways in which the perception of war changed from the Second Wave was the TV broadcasts showing the bombing of Baghdad (Haeni, 1997). Additionally, the main goal of these bombardments is to destroy Iraq’s communication bases and disrupt the flow of information.

2.4.Seven Forms of Information Warfare

Another scholar who has contributed to the definition of Information Warfare is Martin C. Libicki. Libicki explains the seven forms of Information Warfare one by one in his book What is Information Warfare, published in 1995.

Figure 3: Seven Forms of Information Warfare by Libicki



Source: (Libicki, 1995).

C2W based on physical manifestation through taking the commander's head in earlier versions of warfare, but today, it involves destroying the opponent's command centers (Libicki, 1995). An example of this was observed in the Gulf War. America especially targeted Iraq's command centers. The reason why command centers are important for Information Warfare is that these centers form the opponent's communication networks. If these centers are destroyed at the appropriate time, they can alter the course of the war without suffering too many casualties. Detecting the location of the opponent's control centers and

destroying the detected places can be done through iron bombs, cutting off the power of the control center or computer viruses. Destruction of command centers causes the communication organ to lose its function, which has been likened to the separation of the head from the body and the body remaining motionless.

Intelligence-Based Warfare (IBW) is generally about increasing awareness. This awareness is achieved by collecting information about the battlefield. It is possible to use the collected information for both offensive and defensive purposes. The use of intelligence in gathering information is the fundamental basis of IBW. Traditionally, intelligence is used to understand the intention and location of the enemy. The aim is to protect against surprise attacks from the enemy and to organize the battle plan. Today's intelligence allows the location of combat vehicles and their destruction without confronting the opponent. With the integration of technology and intelligence, the use of technologies that will provide intelligence such as seismic sensors, unmanned aerial vehicles or light detection will increase in the future (Libicki, 1995).

EW relies heavily on digital technologies. With digital technologies, it is possible to understand where the message sent comes from, who sent it, or what the purpose is to be achieved with the message. One of the Electronic Warfare tools is cryptography. It is an encryption used to make information unreadable by unwanted people. To understand the message, it is necessary to decode it. However, decoding is a job that requires time and money, and time and money are key for EW. Another important tool that concerns EW is radars. The signals emitted by radars can be targets. That's why the importance of jammers is increasing. Jammers detect signals and send signals back to minimize the strength of the signals (Damjanovic, 2017).

PW is the use of information against the way humans think. The example used by Libicki makes the PW form more understandable. Libicki (1995) wrote about how Somali leader Mohamed Aideed won the Information Warfare against America by correctly using critical information at the right time and place. According to this, Aideed sent photos to CNN depicting how Somalis were dragged through the streets of Mogadishu by U.S. soldiers, causing discomfort among the American public, which ultimately led to the withdrawal of U.S. forces from Somalia. Communication channels like TV broadcasts, newspapers, radios, social media, in short, any means that are used for communication today are important tools in shaping countries' threat perceptions (Bryczek-Wróbel & Moszczyński, 2022). Media can manipulate communities by filtering information through its own lens. This way, enemies can be turned into friends and friends into enemies, and this is entirely possible by shaping individuals' opinions through media manipulation. Furthermore, this manipulation is not limited to ordinary individuals. Manipulating the enemy commander to mislead the target is also an important part of Information Warfare. Another topic discussed by Libicki (1995) is whether there is such a thing as "cultural warfare." Cultural warfare is the exportation of a country's own cultural values to another country. One example of this is America's desire to expand its influence by exporting its fast-food culture, Hollywood movies, or its own style of clothing.

Hacker Warfare (HW) can be summarized as a form of Information Warfare that involves attacks on computer networks. These attacks aim to steal information, spread false messages, and gain access to data that can be used for blackmail (Damjanovic, 2017). These attacks generally target both military systems and individual systems. At this point, it's an

undeniable fact that military systems are more secure. The protection of individual systems is in the hands of governments. Hacker attacks can trigger conventional military operations. To prevent such outcomes, countries should enhance their security against hacker attacks.

The form of warfare in which the integration of the economy and information is explained is known as Economic Information Warfare (EIW). Economic Warfare is related to the products a country needs or is dependent on. For instance, Japan's need for raw materials or Iraq's ability to sustain itself by selling certain essential resources represents a national security concern for countries, making them economically vulnerable to attacks. In order to be protected from these attacks, the integration of economy and information must be ensured at this point. Without real-time access to commodity exchanges, Iraq may encounter difficulties in selling oil (Libicki, 1995). However, an economy that is so dependent on information makes the country vulnerable to threats. Apart from this, industries that are strong in accessing or controlling information are better than other industries. It is a fact that Silicon Valley is more advantageous in reaching customers, suppliers or highly skilled workers. It is likely that countries will compete with each other to have such advantages. A country does not want to be economically inferior to other countries, but today's technology makes countries more dependent on trade.

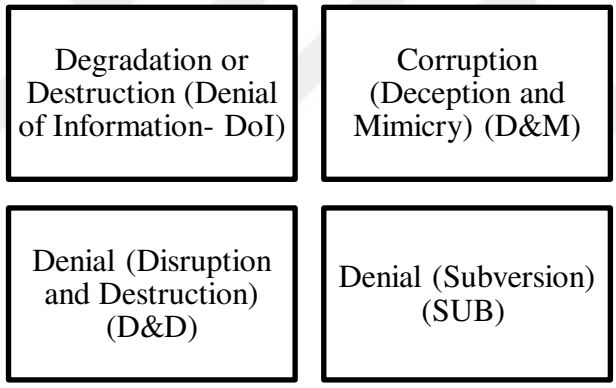
Cyber Warfare (CW) is associated with information terrorism that targets individuals by hacking computers or destroying systems. Information terrorism carries out attacks targeting individuals. Individuals' data such as education and health history can be captured and blackmailed. In addition, cyberwarfare is also shaped by developing technology. For instance, it can create a battlefield environment and create war strategies with simulation technology, which does not have the

dangerous, dirty and dull environment of real war (Sulaiman, 2000-2005).

2.5. Strategies of Information Warfare

In the year 2000, C. Kopp published an article in which he contributes to the definition of information warfare and outlines various Information Warfare strategies. C. Kopp describes four different Information Warfare strategies.

Figure 4: Information Warfare Strategies by C. Kopp



Source: (Kopp, 2005).

In general, Kopp (2005) tries to answer the question "what does opponent want me to think and why?" Therefore, before explaining the four strategies developed by Kopp, it is crucial to first grasp how Kopp defines information warfare, which will make the four strategies more understandable (Kopp, 2005).

According to Kopp, Information Warfare is the manipulation of information to gain an advantage over the opposite party. While talking about the taxonomy of IW, Kopp generally developed strategies on

Cyberwar and Electronic Warfare. Cyberwarfare is collecting information by entering people's systems and using this collected information as a propaganda tool. It is to confuse, mislead, distract or destabilize the opposing party's population or military forces through propaganda or other types such as Perception Management or Psychological Operations (Kopp & Mills, 2002). Electronic Warfare, on the other hand, is about disrupting the opposing party's radar systems.

By general definition, DoI is related to concealment, camouflage or stealth. D&M briefly defines as intentional misleading the information. D&D is more about destroying the opponent's system. Finally, SUB refers to information that cause the opponent to engage in self-destructive behavior (Kopp, 2003).

Kopp (2000) explained these strategies through cyberwarfare and electronic warfare. In Electronic Warfare, the primary Denial of Information (DoI) revolves arund protection from adversary radar sytem, with Deception and Mimicry (D&M) determine the hostility of radar signals. With the Disruption and Destruction (D&D) strategy include the using a jamming system to prevent possible radar attacks as well as countermeasures to prevent misleading signals. In Cyberwarfare, usage of encryption and concealing techniques to protect confidential information from unauthorized access, while Deception and Mimicry (D&M) apply various techniques to hide identity. Disruption and Destruction (D&D) strategies include fighting denial of service attacks, as well as retaliatory activities such as operating damaging programs such as viruses to disrupt adversary systems.

Kopp draws attention to the increasing importance of Information Warfare. While explaining this, he emphasizes the transition from the industrial age to the digitized information age. Kopp initially discusses

how knowledge is passed down from one generation to another, ultimately resulting in a wealth of wisdom for humanity. This knowledge has been utilized throughout generations to gain an economic and military edge over the opposing side. With the advancement of digital technology, knowledge has gradually reached a position where everyone can easily access it. However, the ease of accessing information, as Kopp puts it, has also brought along with it "information garbage." A heap of information, where it's unclear whether it's true or false, is often referred to as "information garbage." Lastly, Kopp (2000) argues that the world will be divided into two categories: developed countries with strong digital infrastructure and weaker countries with insufficient digital infrastructure, mainly reliant on agriculture for their economy.

2.6.Weapons of Information Warfare

In accordance with the model outlined above, the history of warfare divided into three periods, as explained in the book "War and Anti-War" by Toffler. These periods are referred to as Agrarian Wave, the Industrial Wave, and the Information Wave. The respective periods were carefully explained, providing information about the history of warfare. The reason for reemphasizing this topic is that, in addition to the previously explained changing nature of war, a separate section will be opened to examine how the tools used in warfare have also evolved. Upon conducting a comprehensive literature review, it becomes apparent that Haeni has provided a well-organized study on this subject. However, the following information has been obtained from the examination of information warfare weaponry in the literature.

In the realm of information warfare, various weaponry is employed to

disrupt or deceive adversary's communication system. Knowbots, demons, viruses, worms, Trojan horses, logic bombs, and trap doors are among the software system used to cause harm within targeted systems. Knowbots, for example, enter the enemy's computer system, replicating themselves to collect information and deleting themselves if discovered (Crawford, 1997). The primary goal of these tools is to enter computer systems with the intention of causing harm by destroying, changing or denying access to data. Furthermore, video morphing techniques are utilized to change videos for misinformation aim, while psychological operations are performed through social media (Instagram, X (Twitter), TikTok, Telegram, Youtube). The purpose of psychological operations is to influence information in the desired way on large populations.

In this section, the conceptual framework of information warfare is discussed in detail. Information warfare has been defined as a strategy that focuses on information control and emphasizes the interaction of information and communications systems rather than conventional military force. This concept has been discussed from a different perspective by various researchers, especially after the 1990s, and has been divided into various subheadings.

Definitions of information warfare at the political level were examined and an attempt was made to draw parallels with the information warfare policies implemented by Russia, especially in the context of the Ukrainian war. Offensive and Defensive types are explained, and Winn Schwartau's concepts of individual, corporate and global information warfare are discussed. Additionally, information is given that emphasizes Alvin and Heidi Toffler's transition to the information warfare era in the history of war.

The seven forms of warfare determined by Martin C. Libicki,

information warfare strategies by C. Kopp and the weapons used in information warfare are explained in detail. In this context, the evolution of information warfare and its areas of use in contemporary conflicts are discussed in a broad perspective.

As a result, information warfare occupies an important place in today's complex and technology-driven conflict environment. Understanding this war in all its dimensions and developing effective policies is of critical importance in terms of national security and strategic policies.

3. CHAPTER 3: RUSSIAN INFORMATION WARFARE POLICIES

All warfare is based on deception.
(Sun Tzu, 2005, p.161).

In this section, Russia's information warfare policies and the conceptual framework behind these policies will be examined in detail. In order to analyze Russia's information warfare policies, it is planned to first focus on how this concept is defined by Russia. In the first part of the study, the definition, purposes and methods used of information confrontation will be discussed in detail. After that, the evolution of Russia's information confrontation policies throughout history will be explained and how they are integrated into today's national security strategies will be explained in detail. Finally, Russia's information confrontation doctrines will be examined and their effects on Russia's domestic and foreign policies will be analyzed.

3.1.Russian Information Warfare Concepts

In order to analyze Russia's information warfare policies, it is essential to first examine how Russia defines its information warfare. Many English terms, such as information operations, cyberwar, psychological operations, information security, and command-and-control warfare, have a similar meaning in Russian. Based on this, care will be taken to avoid confusion when using information warfare terminologies in this thesis.

3.1.1. Information Confrontation instead of Information Warfare

If a common concept has not been used in defining information warfare or in terminology usage in world literature, the definition and terminology of the concept of "information warfare" has been a matter of debate in the Russian literature. For example, although terms like information influence and information war are used instead of information warfare, it has generally found its place in Russian sources as "information confrontation".

Information confrontation characterized by the Russian Federation's Ministry of Defense as a type of conflict in which competing parties- such as states, socio-political movements, or military forces strike the opponent using informational tactics inside the information domain.

This includes both the infrastructure and systems that manage information and social relations, while simultaneously defending against such effects on their own side (Grisé et al., 2022, p.7).

Russian sources emphasize that information confrontation aims to ensure information superiority in political, economic, military or other fields. However, this thesis will focus on the role of information confrontation in the military sphere. In Russian sources that have been studied, while explaining the purpose and scope of information confrontation, it is categorized into two different periods: peacetime and wartime. In this framework, peacetime focuses on capabilities such as espionage activities, reconnaissance or covert measures to achieve information superiority. During wartime, due to the nature of war, more aggressive actions are taken in order to gain superiority over the other side. These aggressive actions mainly involve disinformation, hacking, or discrediting leaders (Giles, 2016).

Apart from these, Russian military scholars divide information confrontation into two subcategories: information-psychological and information-technical (Mărășoiu, 2023).

Information-technical is to destroy the enemy's electronic and computer networks. However, the definition should not be limited to this (Giles, 2016). The use of information technical is crucial to achieve information superiority against the enemy. In order to achieve this superiority, it is necessary to seize the command-and-control systems of the opposing party. For this to be possible, physical precautions must be taken. For instance, the use of computer networks.

Information-psychology is the manipulation of information to influence societies in the desired way. Especially since the 20th century, with the development of technology, information psychology has emerged as "creating an atmosphere of fear among the population of the enemy", "ensuring the dissemination of information that will demoralize the enemy", and "misleading the enemy" (Goldstein & Findley, 1996). Before the 20th century, radios and newspapers were mostly used to achieve these purposes.

There are some components to ensure information psychological security. The first of these is the state of the mental health of the society affected by the information and psychological influence of the enemy. The second is to take measures against information manipulation of communities. The third is to support the country's global, regional and national interests, values and goals in the field of information. Finally, it is the observation of society's attitude towards issues such as national security, the mental state of population and military personnel.

3.1.2. Main Terminologies Related to Information Confrontation in the Literature

The definition of other terminologies used in Russian sources regarding information confrontation will give an idea about how the Russians perceive the subject. Although complementary terminologies related to information warfare do not vary significantly in Russian literature, there are some nuances. Explaining these terminologies will make the Russian literature on information warfare more comprehensible.

In Russian literature, the "information sphere" is equivalent to the "information environment" used in American literature. In American literature, the information environment is the sum of individuals, institutions and systems that collect, process and disseminate information. Information sphere, which is its equivalent in Russian literature, is the entire system that collects, organizes and disseminates information and social relations. On the other hand, there is no equivalent of this term "information space" in American-based literature. Since this term will be used in the thesis, it is beneficial to define it. Information space is the domain of activities related to the formation, transformation, transmission and use of information on individuals and public consciousness (Grisé et al., 2022, p.6).

Information war, according to the Ministry of Defense of Russian Federation (2011), is a type of conflict that emerges with the aim of achieving information superiority. The aim is to disrupt the normal functioning of information in order to destabilize the state. Additionally, it causes disruption of the order of society through large-scale psychological manipulation. Aside from the Ministry of Defense, researchers define information war as the struggle between opposing forces for dominance over the opponent in terms of timeliness, certainty,

completeness of information, and the speed and quality of its processing and distribution (Ministry of Defense of the Russian Federation [MoD], 2023).

Information operations are the most crucial activities of information warfare during wartime. Information operations aim to establish and maintain information superiority over the enemy during wartime, or to prevent the enemy from having information superiority. Information influence generally includes information warfare activities during peacetime and is performed before the onset of operation. Finally, information superiority is the goal of the conflict. It is to have command and control forces and equipment that possess more comprehensive, precisely verified, and accurate information than the enemy (Anderson, 2018).

3.1.3. Weapons of Information Confrontation

To approach the issue from the most basic point, Russian sources emphasize that information itself is considered as effective as missiles or bombs. According to the Russian understanding information weapons can be deployed in a wide range of realms outside cyber, including the human cognitive domain (Giles & Hagesta, 2013). By using cyber, one of the information weapons tools, it is aimed to stop the enemy's weakly defended technological devices such as computers and weapon control systems, thus preventing the flow of enemy information. What is meant by human cognitive is to ensure that information is turned to one's advantage.

According to the Russian perspective, information weapons are classified according to their domain. This domain is classified in three

categories: physical, informational, software-technical or radio-electronic (Thomas, 2020, p.133). The physical domain, as the name suggests, is to obtain a visible result in the destruction of the enemy's information system through the use of equipment. The tools used to destroy information systems can be listed as anti-radar missiles, graphite bombers, and rechargeable batteries. For instance, during the 1991 Gulf War, Iraq's ground-based radar systems were destroyed by the United States with the help of anti-radiation missiles (Late, 2023). In addition, graphite bombs used by the United States in the Kosovo and Gulf Wars caused electrical circuits to short circuit. Thus, a significant advantage was gained over the enemy. The informational domain, another domain of information weapons, involves its application in global information networks such as all types of media or the internet. It is to create an atmosphere of fear by influencing the consciousness of every member of society through information manipulation, disinformation and propaganda tools. As a result, it causes the spread of uncontrolled information within the country. For example, with the current technological developments, it is possible to intervene by providing deceptive commands to enemy units via radio networks through voice disinformation. The software-technical domain is implemented with tools that can destroy the enemy's information systems, such as computer viruses, logic bombs, and trojan horses. The main purpose of using these tools is to collect, modify and destroy the information in the database. The collection of information is possible with tools such as knowbot, demon, sniffers and trapdoor. For instance, knowbot enters the computer system, copies itself, and stays for a while, performing the task of collecting information (Zenarmor, 2024). The destruction of information is achieved through tools such as Trojan Horse or Worm. Trojan horses and worms secretly infiltrate computer system,

causing the destruction of information and slowing down the system (Harvard Cybersecurity, 2024). The aim is to gain superiority over the enemy by manipulating information as a result of infiltration into the information system with tools such as logic bombs. The activation of the logic bomb in the Gulf War, Iraq was unable to use France-based defense systems (U.S. Cyber Security Magazine, 2024). Lastly, radio-electronic domain, on the other hand, involves any of kinds of manipulation and disinformation that may negatively affect the enemy through electronic intelligence or radio-electronic suppression methods. This domain is activated through the use of media tools, aiming to diminish the enemy's combat capability (Harvard Cybersecurity, 2024).

3.1.4. Who use Information Confrontation in Russia?

Information confrontation in Russia involves two main primary groups: states and non-state actors. State actors include various entities such as military organizations like Main Intelligence Directorate (GRU), which conducts hacking activities to gain political influence. The 8th Directorate of the General Staff collaborates with the media to ensure the operational security of the Russian military, while the Electronic Warfare Troops (REB Troops) focus on maintaining Russia's superiority in the field of commons and control. Military universities are one of the essential elements of the state actors in the information confrontation. It aims to train the new generation for Russia's information defense. Federal agencies such as the Federal Security Service (FSB) and Foreign Intelligence Service (SVR) work towards achieving information superiority through Russia's hacking movements. State- run media utilizes propaganda and disinformation to shape public opinion, and state

elites use communication tools to influence public consciousness in alignment with their interest (Grisé et al., 2022, p.17)

On the other hand, non-state actors include universities collaborating with the Ministry of Defense to enhance Russia's information capabilities, private business and non-state media engaging in pro- Western propaganda and disinformation campaigns against Russian interests, terrorist organizations targeting Russia's domestic policies to destabilize the nation, and individual patriots participating in hacking activities to protect Russia's information security.

This section provides an overview of the diverse array of actors involved in information confrontation in Russia, illustrating their roles in shaping the country's information warfare strategies.

3.2. Historical Perspective of Russia in Information Confrontation

In this section, the focus will be on how the place of information confrontation in Russian military thought has evolved from early historical periods to the present day. The analysis is structured into four main sections: Before the Soviet Era, During the Soviet Era, Post- Soviet Era, and 21st Century Developments will be examined with a series of different case studies. The aim is to understand how Russia has implemented information confrontation throughout history. In the previous chapters, information confrontation was generally discussed within a theoretical framework, but in current chapter, the role of information confrontation in practice will be discussed.

3.2.1. Information Confrontation Before the Soviet Era

In ancient times, although it was difficult to manipulate large groups of people due to limited means of communication, various tactics were used to achieve psychological advantage by affecting the morale of soldiers in order to disrupt the functioning of enemy armies. Within the context of Russian historical practices, the desired psychological superiority over adversary forces was expressed with the term "spetsprop" and was used instead of information confrontation. The earliest example of Russia's spetsprop practices can be traced back to 1799. During this period, general Suvorov, one of Russia's leading heroes, spread messages to the Piedmontese soldiers, who were the soldiers of the opposing side, in an attempt to persuade them to surrender to the Russian-Austrian army (Kolbe, 2022).

During the Napoleonic Wars, the Russian military disguised itself as the enemy and entered enemy camps to spread propaganda messages in order to gain moral superiority over the opposing side's armies. By targeting German soldiers fighting aligned with Napoleon, the Russians strategically spread propaganda messages that would cause German soldiers to question why and for whom they were fighting. As a consequence, the surrender rate of German troops increased significantly compared to French troops (Grisé et al., 2022, p.23)

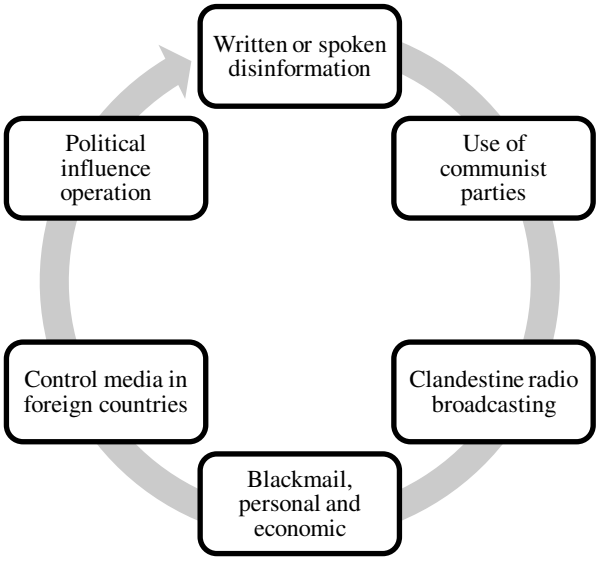
In the midst of the First World War, Russia tried to influence various communities through escalating nationalist propaganda. A focal point of this influence campaign was directed towards Slavic nations, accentuating the imperative of uniting these nations under one roof. Notably, propaganda messages were disseminated to Slavic soldiers fighting for Austria-Hungary in order to disrupt the order of the armies, emphasizing the necessity of not fighting for the Austro-Hungarian Empire. Additionally, a noteworthy feature of this period was the development of

the tools employed for propaganda. It is seen that Russia tried to spread its messages through newspapers and magazines after the First World War (Mullaney, 2020).

3.2.2. Information Confrontation During the Soviet Era

This section, which will cover the information confrontation policies of the Soviet era, will include the period starting with the October Revolution of 1917 until the dissolution of the Soviet Union in 1991. It seems that the Soviet Union basically adopted ideology as an information confrontation propaganda tool. The central focus of Soviet propaganda resided in the spread of communist ideology.

Figure 5: Methods used to spread communist ideology



Source: (Fedchenko, 2016.)

Until the 1930s, it was realized by using propaganda tools to strengthen the place of the Soviet Revolution in the national and

international arena. The objective was twofold: firstly, to solidify the presence of the Bolshevik Red Army in Russia by destroying the Tsarist Empire, and secondly, to increase the popularity of the Red Army (Pipes, 1990). However, another goal was to propagate against adversaries that the Soviets were a country with very advanced technologies, through brochures, leaflets and magazines, in order to restore the image damage resulting from the devastating effects of the First World War and the revolution (Kotkin, 2014).

Owing to the impact of Stalin and the Second World War, the rise in military propaganda became inevitable. Throughout this period, the Soviets applied their usual propaganda tactics against German soldiers. Initially, calls for German soldiers in order to surrender and the distribution of leaflets praising communism did not have the desired effect, as it was thought that Germany was winning the war (Figes, 1996). Nevertheless, the war turning in favor of the Russians and the development of the idea of why the working class was fighting for the bourgeoisie caused the soldiers of the opposing side to relinquish their weapons (Fitzpatrick, 2008).

Following the Second World War, in 1946, both Stalin's emphasis in his election speech that war with the West was inevitable and Winston Churchill's response to this, the Iron Curtain discourse between the Soviet-dominated East and the America-dominated West, drew an invisible wall with words, signifying the high level of information warfare from the very beginning of the war (Kalinovsky & Daigle, 2014). As a result of the propaganda environment created by the Cold War, information warfare became controversial between the parties. This contentious environment prompted the Soviets to develop a new theory called "reflexive control" towards the end of the 1950s.

Reflexive control theory began to be developed during the Soviet period and is still valid in today's Russia. Reflexive control expresses a meaning that overlaps with concepts such as disinformation, deception and perception management. It contains information designed to encourage the enemy or cooperating partner to act in the desired way. The Timothy L. Thomas was instrumental in introducing this theory to the Western world. He referenced the concept of "reflexive control", originally developed by Colonel S.A. Komov, a Russian military theorist, who outlined the fundamental intellectual approached to information warfare.

In military strategy, a variety of tactics can be employed to undermine and manipulate adversaries. Distraction forces adversaries, mid-preparation for conflict, to reconsider their strategies. Overload involves inundating foes with frequent, misleading information to provoke irritation. Paralysis creates an existential threat, immobilizing enemy responses. Exhaustion entails draining enemy resources through repetitive trivial tasks. Deception redirects enemy forces towards false threats. Division fosters dissent within enemy coalitions. Pacification diverts attention by misleading foes with the appearance of non-aggressive activities. Deterrence establishes an aura of overwhelming superiority. Provocation induces advantageous enemy actions. Suggestion influences adversaries through legal, moral, or ideological means. Pressure undermines government credibility through public information dissemination (Euromaidan Press, 2023).

Another crucial aspect of reflexive control is how to transfer information to gain control over the enemy. Major General M.D. Lonov, a prominent Russian military theorist, explained this control over the enemy with certain principles. Timothy summarized these principles by

citing Lonov. The first of the principles involves exerting pressure on the enemy by using elements such as psychological attacks, cutting off the enemy's communication with specific regions, issuing an official declaration of war, presenting ultimatums, threatening sanctions, displaying shows of force, and implementing brutal actions (Thomas, 2004).

The second principle covers the spreading of deceptive information intended to give the enemy with an advantage. This involves engaging in destructive provocation actions, forcing the enemy to take retaliatory actions that will waste their time and resources, practicing concealment, dropping information changing devices into electronic systems (such as logic bomb, Trojan horses, etc.), creation of mock installation (Healey, 2013).

The third principle is to publish doctrines containing deliberately false information in order to neutralize the enemy operationally, and to influence the enemy's decision-making algorithm by attacking the enemy's control systems. Finally, it is to change the enemy's decision-making system with unexpected actions in order to try to influence the enemy's decision-making actions. In short, these principles are important to ensure that the enemy is controlled in the desired way (Thomas, 1996).

Examining the reflexive control features of the Soviet Union reveals a combination of internal and external policies. Internal policies include defensive reflexive control policies. The purpose of this is to provide the Russian people with information that they consider correct, through communication tools such as televisions, radios or newspapers. External policies constitute the offensive side of reflexive control. It is the Soviets' application of disinformation to the international public in a more offensive sense. The Soviets dismiss, distort, distract and dismay the

perception threats coming from the Western world.

Due to the effective application of the aforementioned reflexive control principles and methods, the enemy is enabled to act in the desired way. Reflexive control methods applied during the Soviet era will leave a legacy of information confrontation policies for the future Russia in the 21st century.

In the later stages of the Cold War, specifically towards the end of the 1960s, Soviet Russia witnessed the emerge of another practice called "active measure", which, akin to the reflexive control theory, gained attention in KGB documents. This concept has been emphasized as an application used especially by intelligence services. Soviet intelligence active measures are defined as influencing the enemy in the interest of the Soviet Union and other socialist countries. Active measures have an aggressive scope and include key elements such as sabotage, disinformation, deception, espionage and destabilization. Within this framework, an aggressive attitude is adopted towards the intended targets, such as destabilizing political authoritarianism, diminishing public morale and disrupting the functioning of the military forces in unity (Kux, 1985).

Active measure has a more limited scope than reflexive control. The overarching scope of active measure is the ‘‘ideological sabotage of the enemy’’. This means that active measure generally advocates the spread of communist ideology propaganda by Soviet intelligence, countering the capitalist ideology promoted by the West adversaries. Oleg Gordievsky, a KGB defector, emphasized some of the points of Soviet intelligence, including preparing materials, such as false documents, primarily aimed at compromising US policy, organizing campaign groups to incite conflicts between NATO and EU allies, and supporting pacifist movements and the potential for protest in the West (Darczewska &

Żochowski,2017, p.21).

During the Cold War, in the 1980s, Afghanistan witnessed the effective deployment of active measures. In this era, as a result of the deterioration of relations with the West, active measures were implemented in a more offensive way. Notably, various campaigns have been carried out, such as kidnapping children from third world countries for organ trafficking and the dissemination of disinformation about America's HIV virus to harm African Americans (Selvage & Nehring, 2019). In short, active measure application found a place in the Soviets' information confrontation policy within an ideological framework (Thomas 2024).

Russia waged propaganda war against capitalism in the Cold War, aiming to criticize capitalism outside of the country, while its effort to prove to its domestic audience that it was the most technologically advanced nation. This narrative found expression in the mass media of that period. As can be seen in the posters below, Russia criticized structure of capitalism based on ambition to its people and non-socialist countries. Additionally, there was a consistent emphasis on their success in space.

Figure 6: *"If this is freedom, then what is prison"*

Source: (Views and Re-Views: Soviet Political Posters and Cartoons | Medium: Posters, n.d.)

Figure 7: *"Conquering Space" David Pollack 1960s.*

Source: (Hecimovic, 2022).

3.2.3. Information confrontation in the Post-Soviet Era

As a result of the dissolution of the Soviet Union in 1991, Russian policymakers were faced with an important dilemma and began to work on an information warfare policy that could combat the new West. The idea of uniting under a common ideological roof that kept the Soviet Union alive had collapsed during the revolutionary movements between 1989 and 1991. After 1991, Russia created a new identity and did not want its former Soviet satellites to succumb to Western propaganda and take a stand against Russia. Thus, Russia had to develop new methods suitable

for the world system, drawing from the Soviet tradition, including active measures, disinformation and reflexive control. These methods have been shaped by important historical developments.

The methods used in the Iraq war in 1991 demonstrated the significance of Russia's utilization of information in modern warfare. In the changing nature of war, the focus will be on the theories of Russian thinkers on information warfare in order to develop new policies suitable for modern warfare with Russia's information warfare capabilities inherited from the Soviet era.

The first theory developed within the scope of Russian information warfare after the 90s was "subversion-war (myatezhevonya)" developed by Eveny Messner (Fridman, 2017). Messner's theory was influenced by the ideological war between the two great powers in the Cold War. However, Messner emphasized that the physical wars that remained during the Cold War period were replaced by psychological wars, that is, subversion wars (Pomerantsev & Weiss, 2014). This new type of war is not about seizing the enemy's territory, but about bringing confusion and discomfiture of the enemy's soul to the enemy with the main value psychological flesh. He argued that it was possible as a propaganda tool to achieve this goal. He expressed his views that propaganda should not be limited only to the military field but should also be expanded to the economic, social and political fields (Fridman, 2017). Moreover, according to Messer, propaganda should be versatile, that is, it should have the power to not only affect the enemy audience but also your own audience (Pomerantsev & Weiss, 2014). As a result, Messer emphasized that the way to achieve victory in subversion war is to destroy the enemy's psychological power, not their human power (Thomas, 2015).

Another prominent Russian thinker, Aleksandr Dugin, introduced

post-Soviet net-centric war theory into Russian academia and political discourse. Dugin's concept of net-centric war predominantly touched on the points that distinguish Western values from Russian values and argued that the West engaged in offensive information warfare against Russia in the 20th and 21st centuries. According to Dugin, in the postmodern world, America wins the war by manipulating its own ideas and perspectives before the physical war even begins. Dugin contends that if Russia does not modernize its secret services and information and communication systems to keep up with this system, it will face inevitable defeat. Briefly, Dugin posits that information warfare is influencing a network of people, foundations, organizations, etc. to support or oppose certain ideas in order to achieve political goals (Darczewska, 2014).

The examination will delve into Igor Nikolaevich Panarin's treatment of the concept of information warfare, drawing attention to his noteworthy works in the post-Soviet era. According to Panarin, the definition of information conflict is to achieve the targeted goal between the parties by influencing the public opinion of the other party through political, economic, diplomatic, military and other means. Control over public opinion is achieved through tools such as information manipulation, misinformation, blackmail, lobbying, fabrication of information and extortion of desired information (Ibid.) Accordingly, Panarin posits the existence of an information war between the West (maritime-oriented; US and British Empire) and the East (continent-oriented; Germany and Russia). Panarin's Cold War interpretation of the information war between the West and East is based on the West winning against Russia with the collapse of the Soviets in 1991 (Göransson, 2022, p. 531). For this reason, Panarin emphasizes that the West's information war against Russia will continue after the Cold War, underscoring the imperative for

Russia to enhance its preparedness.

3.2.4. 21st Century Developments and Gibridnaya Voyna (Hybrid War)

After the collapse of the Soviets, at the outset of the 21st century, the world witnessed conflict processes among nations seeking for a position in a new order. The ideological gap that emerged following the dissolution of the Soviets in the early 2000s caused chaos and confusion in countries searching for their own identity. Despite the information superiority challenge faced by the Soviets, its endeavored to maintain influence. However, in this period when information superiority over the West was lost with the collapse of the Soviets, the USA tried to take advantage of the gap and spread its principles such as democracy in these countries' trough information warfare tools against Russia. The initial outcomes of these efforts materialized with the Rose Revolution in Georgia (2003), the Orange Revolution in Ukraine (2004) and the Tulip Revolution in Kyrgyzstan (2005).

These uprisings, also called Color Revolution, can generally be described as protests aimed at government changes after the Soviet Union. Russia's perspective on these uprising, according to Göransson (2022), can be summarized as follows: The West is accused of intentionally provoking these uprisings to propagate its values of liberalism and democracy to the former Soviet countries. Governments in these countries have been replaced with Western support as a result of the elections held after the Soviets withdrawal, fueling accusations of Western destabilization efforts. Additionally, Russia alleges that the Wes seeks to diminish its influence in post- Soviet regions by expanding its own presence. Western narrative framing these endeavors often revolves

around the narrative of ‘‘people’s desire to choose democracy against authoritarian regimes’’ against Russia (Nikitina, 2014).

In the late 2000s, the concept of “hybrid war” (Gibridnaya Voyna) became prominent in Russian information literature. Introduced by U.S. Military theorist Frank Hoffman in 2007, hybrid warfare refers to the blending of various odes of war, including conventional and irregular tactics, terrorist acts, and criminal activities. Hoffman describes it as complex form of conflict that can be waged by both states and non-state actors, characterized by the merging of different warfare techniques and technologies (Hoffman, 2007, p.14).

Hoffman states that conflicts no longer occur with the use of force, as in old conflicts, but rather manifest on a psychological and identity-based grounds. Additionally, groups are organized to provide command and control in the battlefield utilizing modern information technologies (Fridman et al., 2018).

Russian strategists, military thinkers, and scientists have reevaluated the Western concept of hybrid warfare and reconceptualized it as gibridnaya voyna to align with Russia’s political and military experiences. Russian hybrid warfare is explained by Ofer Fridman in his book Russian Hybrid Warfare. An in-depth exploration of the features of Gibridnaya Voyna step by step will make the features that distinguish the theory from hybrid warfare.

Gibridnaya voyna, Hoffman’s reconceptualization of hybrid warfare theory, integrates elements from Dugin’s net-centric warfare, Panarin’s information warfare, and Messer’s subversion warfare. Unlike, traditional military approaches, this strategy uses information technologies, psychological tactics and other methods to neutralize the opposing side. According to Fridman (2018) and other Russian thinkers emphasize that

the information war is the basis of Gibridnaya Voyna. The prevailing consensus on this issue is "the West's information war against Russia" (Fridman, 2018). In this respect, it is understood that the geopolitical conflict aspect of Gibridnaya Voyna. The overarching goal is to shift contemporary conflicts towards non-military measures in informational, economic, or political directions, and that the other side will deal with internal turmoil by damaging its military and economic potential through information and psychological pressure methods (Darczewska, 2014).

The initial reflections of this concept, which was discussed towards the end of the 2000s, became evident during the 2008 Georgian War. The characterization of the 2008 Georgian War as the first European war of the 21st century encompasses a broad scope of influence. Although Russia's swift victory in just five days, the Georgian government tenaciously resisted to win the information war against Russia. Thus, whether the policies implemented by Russia in the field of information confrontation in the Georgian War resulted in success or failure is a matter of debate among Russian thinkers.

Russia's military and non-military practices show the hybrid feature of the Georgian War (Nilsson, 2018). The non-military aspects of the Georgian war will be discussed in the field of "information conflict". Accordingly, it is possible to examine the information confrontation policies implemented by Russia in the Georgian War both in the information-technical field and in the information-psychological field (Iasiello, 2017).

In the information-technical field, Russia aimed to neutralize Georgia's command and control mechanisms. To achieve this, first of all, Georgian citizens' access to government websites was restricted and thus the Georgian government's communication with its own citizens and the

world was cut off. Moreover, Russian cyber operations extended to targeting Georgian banks, transportation companies, and private telecommunications providers (Connell & Vogler, 2017). In the field of information-psychology, the necessary messages were given through TVs, one of the media tools managed by the Russians, regarding the limitation of Georgian citizens' use of the internet in 2008 (Fraser, 2022). Russia employed several narratives: firstly, Russia has emphasized NATO's expansion efforts in the former Soviet areas and uses the discourse that the internal turmoil and unrest in these areas is caused by the West. Secondly, accusing Georgia of carrying out ethnic cleansing against native Ossetians and constructing a discourse of Russia protecting its citizens. Thirdly, Russia sends a message through the media to Georgian citizens that Georgia's traditions and values are endangered as a result of increasing relations with the EU and NATO.

Russian thinkers are divided into two in Russia's information warfare struggle with Georgia. While Panarin and analyst Anatoliy Tsyganok argued that Russia had lost information warfare, general Anatoliy Nogovitsyn and Clonel P. Koayesov made statements that Russia had won information warfare. Panarin and Anatoliy Tsyganok emphasized that Russia was ill-prepared for this form of warfare against Georgia, failing disable command-and-control systems, and inadequately imposing moral and cultural norms on the populations. Conversely, General Anatoliy Nogovitsyn and Clonel P. Koayesov approached the situation from a more optimistic side and said that Russia worked heroically and was successful in both the information technical and information psychological fields (Thomas, 2010).

In the 2010s, Russia's information confrontation policies were not limited to the former Soviet areas, but rather spread to wide areas. The

most significance development supporting this situation was Arab Spring. Russia aimed to reinforce its controlling role in world politics, especially vis-a-vis the USA, and sought to shape the region by actively participating in the upholding events. While Russia was positive about this initiative launched by the people struggling with social and economic problems at the beginning of the Arab Spring against the regimes that had been in power for a long time, it was concerned about the spread of the popular uprisings to post-Soviet regions (Nikitina, 2014). However, two factors mitigate this concern. The first is that while these popular uprisings that started in the Middle East were thanks to the propaganda spread through media manipulations such as Al Jazeera, similar tactics worked in favor of the regimes in post-Soviet areas like Central Asia. Secondly, it is not possible to see young people's unity in post-Soviet areas as in the Middle East (Center for Strategic & International Studies (CSIS) 2011). Consequently, Russia's narrative on the Arab Spring is the experience of chaos and confusion that emerged as a result of the West's effort to impose liberal norms.

One critical juncture where Russia and the USA faced each other during the Arab Spring occurred in Syria. Russia's argument for the information warfare carried out by both sides through the Assad regime is that the Western media manipulates the facts, and the realities on the ground are distorted trough false documents by international organizations affiliated with the West (Averre, 2019). Overall, with the Arab Spring process, it has become clearer how much influence Russia's information tools have and how a potential threat against Russia may emerge.

Another significant application area of Russia's information confrontation policies in the 2010s was the annexation of Crimea. It is the

second time that post-Soviet Russia has experienced information confrontation policies after the Orange Revolution in Ukraine in 2004. Russia realized the importance of using information tools with the Color revolutions, the Georgian War and the Arab Spring, and learned from its mistakes and approached the annexation of Crimea more cautiously. Accordingly, Russia has introduced new applications in the field of information confrontation by intertwining the reflexive control and active measures practices inherited from the Soviet period with the new type of conflict, hybrid warfare.

The following inferences have been made regarding the information-technical and information-psychological information confrontation policies implemented by Russia in the annexation of Crimea.

Information- technical:

Russia's information warfare policies reveal a calculated approach to increase its effectiveness by benefiting from past experiences, especially in the context of the Ukrainian conflict. It is planned to improve the policies implemented in Georgia and to optimize cyber operations by overcoming the technical problems Russia faces in Crimea. By organizing these cyber operations, it is aimed to keep critical communication infrastructures under control.

Russia intends to correct the failures and problems that arose in Crimea by learning from the information activities it implemented in Georgia. As a result, cyber-attacks were executed on the Ukrainian government's website, telecommunications and private sector information technologies infrastructure (Iasiello, 2017). Russia's primary objective is to seize the command-and-control system by severing communication

between the Ukrainian government and its population. Cyber-attacks, especially targeting the Ukrainian army, attempted to escalate tensions among allied partners by disrupting communication (Connell & Vogler, 2017).

Information- psychological:

Russia's information-psychological warfare policies in Ukraine provide a comprehensive framework that shapes both the country's domestic and foreign policies. These policies are carried out through various elements such as the threats of the West, the cultural sphere, the dream of the Soviet Union and the role of social media.

Western Threat: NATO's endeavors to pursue expansionist policies towards the former Soviet regions in order to eliminate Russia and ensure a unipolar world order, and thus to squeeze Russia into a single area. The Black Sea is under NATO threat, so the importance of Crimea's pivotal role and the developing relations between the European Union and the former Soviet countries are a cause for discomfort for Russia.

Cultural Domain: There is a belief that the common values and culture that Russia and Ukraine share with the Slavic Orthodox civilization should not be separated and, instead, should be unified under a single roof. Additionally, it is also argued that the concession of Crimea to Ukraine resulted in the infringement of the human rights of Russian-speaking populations.

Soviet Union Dream: The need to work to avoid the reoccurrence of the pride injury caused by the collapse of the Soviet Union, defined by Putin as the greatest disaster of the century, has been underscored. As emphasized in the cultural domain, the development of the understanding

of Ukraine and Russia as one nation, united under the Russian World was underlined in order to unite the Slavic races under a single roof (Lange-lonatamišvili, 2015).

Role of social media: The most effective tool for Russia to spread its messages has been social media. On social media platforms such as Twitter and Facebook, pro-Russian accounts have made efforts to spread messages against Ukraine. In addition, on television channels, pro-Russian propaganda consistently blamed the West for events in Crimea, emphasizing the alleged humanitarian crisis. These activities made references to the peace-loving nature of the Soviets and the fight against Neo-Nazis (Snegovaya, 2015).

In short, as a result of Russia's past experiences and its gains by keeping the information domain under control without any military intervention, a message has been conveyed to both Western countries and former Soviet nations, affirming Russia's continued significance as a key actor in the international system.

There have been allegations of Russian interference in the US elections in 2016 and 2020. There are some reasons and motivations for Russia to implement such an information confrontation against the US through elections (Nelson, 2022).

The collapse of the Soviet Union led to significant efforts to reshape Russia's image due to the loss of information warfare against the West. During the Soviet period, preventing Russia from competing with the USA as a global superpower was crucial, it became essential to prevent the USA from gaining a place in the system as a single power after the Soviet period. There was also a hope that the trauma caused by the collapse of the Soviet Union will make Russia a great and influential power again.

Geopolitically, Russia seeks to maintain influence over its near abroad countries (former Soviet countries), perceiving them to be under from the USA. The USA's role in promoting Color revolutions to spread western values against Russia. US support for the Color Revolutions and the uprisings of former Soviet countries against the Putin regime (Intelligence Community Assesment, 2017). Additionally, the expansionist policies of the EU and NATO in the former Soviet regions, Russia is isolated from the world system and causes social instability within Russia and in neighboring regions (Charap & Colton, 2017).

Politically, there are attempts to damage the image of Western values such as democracy in the world. Russia aims to ensure its political goals are achieved by supporting candidates aligned with its interests in foreign elections. For instance, it was believed that supporting Trump against Clinton in 2016 would have a positively impact on Russia's national interests in Syria and Ukraine (Oates, 2020).

The main goal of Russia's intervention in the elections is to use information systems to ensure that people vote for the candidate that suits Russia's interests. This involves employing various information confrontation tools. Firstly, propaganda strategies are employed, utilizing tactics such as damaging the reputation of the rival candidates to enhance the image of those supported by Russia (Rid, 2020). Secondly, it involves a situation where voter registration database, voting machines and voting tabulation equipment may be exposed to cyber-attacks during the election process (Wonjnowki, 2021, p.9). This may entail damaging hardware, software, hacking and decryption systems and communication infrastructure. Thirdly, the interference in elections aims to exacerbate social polarization among the society and fostering instability was achieved through the use of social media tools. For instance, propaganda

campaigns spread through troll accounts and misinformation messages as well as strategically placed high-value advertisements on platforms such as Facebook and Twitter (DiResta et al., 2018). Notably, the Internet Research Agency, Russian Today (RT), and Sputnik waged trolling campaigns that increased disagreement among African American, LGBT, Hispanic, and Muslim populations within America (Savage, 2017).

3.3. Russian Information Warfare Doctrine

Russia's information confrontation policies are best explained in the doctrinal documents of the country. These doctrinal documents can be listed as Russian foreign policy concepts, national strategies and military doctrines (Giles, 2016). In general, Russia's doctrinal documents have enabled the creation of some directives shaping both Russia's domestic and foreign policies as a result of evaluating the threats that Russia may face, the situations that may arise in future conflicts and other parameters. The common point of these doctrines is that information is a dangerous weapon. It should not be forgotten that Russia's doctrinal documents define information warfare not only as a defensive mechanism but also as an offensive tool and act accordingly. Therefore, Russia's information warfare strategies are not only limited to the use of military force, but are also effective in economic, political and social areas. These arguments will help us objectively look at the scope of Russia's information warfare policies.

3.3.1. 2011- Information Space Activities Concept

In 2011, the Russian Ministry of Defense released a document titled Information Space Activities Concept of the Russian Federation Armed Forces. This concept aims to address the emerging threats in the evolving

global information environment, which has been significantly influenced by technological advancements. The document emphasizes what these new threats are and what measures should be taken to address them (MoD, 2011).

Information Space Activities Concept refers to The Russian Federation Information Security Doctrine published in 2000. Accordingly, the Information Space Activities Concept begins with the following sentences explaining that the information confrontation poses a significant threat to the information security of Russia.

Thus, it is understood that the Information Space Activities Concept was published as a result of the increasing threats that The Russian Federation had to face with the developing technology until the year 2011. When the content of the Information Space Activities Concept is examined, it is understood that the activities of the armed forces of the Russian Federation in the information field are based on six principles: legitimacy, priority, complexity, interaction, cooperation and innovation.

The concept underscores the commitment of the Russian Federation Armed Forces to uphold state sovereignty by adhering to international law, avoiding interference in the international affairs of other nations, refraining from the use of force, and respecting the right of countries to self-defense (MoD, 2011; Thomas, 2015). The principle of *priority* involves the acquisition of timely and reliable information about threats, rapid processing and analyzing this information, and implementation of preventive measures. The principle of *complexity* entails the use of all resources of the Russian Federation in solving the problems encountered (MoD, 2011, Pomerantsev & Weiss, 2014). *Interaction*, as its name suggests, proposes to work in coordination with federal authorities (MoD, 2011; Draczewska, 2014). *Cooperation*, on the other hand, aims to elevate

the principle of interaction to the global level and establish an international legal regime against the threat posed by information space by working in a friendly manner with other states and organizations. Finally, the principle of *innovation* underscores the necessity of using the latest technology and having highly skilled employees them (MoD, 2011).

In the last section of the Information Space Activities Concept, the Russian Federation outlines some rules for armed forces, including the containment and prevention military conflict, conflict settlements and confidence building. The discourse that draws attention with these rules is generally a call to international organizations. In particular, the call to the United Nations emphasizes the necessity for an agreement that determines the limits regarding information security and is universally accepted by everyone. In addition, Russia has called upon the members of the Collective Security Treaty Organization, the Commonwealth of Independence States, and the Shanghai Cooperation and advocated the development of mutual cooperation by admitting new countries as members to ensure information security. Finally, the prevailing opinion suggests that sharing national security concepts among countries can contribute to confidence building between them.

In short, the Information Space Activities Concept is a doctrine that emphasizes the defensive capacity of the Russian Federation in ensuring information security. While, highlighting these defensive capacities, it does not mention the offensive measures taken to ensure the information security of the Russian army. At the 2012 conference of the Russian Academy of Military Science in Moscow, the offensive role of the Russian army as summarized in three main areas: disrupting the other party's information systems, defending Russia's own communications and control systems, and influencing internal and external public opinion

through media and the internet (Drazdovich & Uladzislau, 2023).

3.3.2. 2014- The Military Doctrine

The Military Doctrine of Russian federation, published in 2014, is part of a series of doctrines dating back to 1993, 2000 and 2010. These documents broadly address the military threats encountered by the nation and their evolving nature, along with defense and security measures. The Military Doctrine (2014) provides an in-depth analysis of Russia's security threats, with a notable focus on information security issues.

Emphasis on Information Security

Previous doctrines have highlighted the significance of information confrontation. In particular, the growing importance of information confrontation is mentioned. The role of information in the field of security is first mentioned in the general provisions of the military doctrine. It specifies that any military operation to be initiated to protect the country's interests will be used only after non-violent means such as information, political and diplomatic channels have been exhausted (Embassy of the Russian Federation in the Kingdom of Thailand [ERFKT], 2014, art. 5).

Main External Military Dangers

The military doctrine highlights various external military threats, with a specific focus on the misuse of information and communication technologies for military-political objectives that violate international law. These threats pose risks to sovereignty, political independence, territorial integrity, and international peace, security, as well as global and regional stability (ERFKT, 2014, art. 12/k).

Main Internal Military Dangers

Furthermore, the doctrine details key internal military threats, including efforts to influence the populations, particularly the youth, in ways that undermine the historical, spiritual, and patriotic traditions related to the defense of the nation (ERFKT, 2014, art.13/b).

Tools of Information Confrontation

The doctrines specify a range of information confrontation tools employed in contemporary conflicts. These encompass extensive use of advanced weapon systems and military technology, including precision and hypersonic weapons, electronic warfare capabilities, new physical principle- based weapons with effectiveness comparable to nuclear arms, management information systems, as well as unmanned aerial vehicles, and robotic- controlled military equipment (ERFKT, 2014, art.15/b).

Significance of Information Technologies

Additionally, the doctrine highlights the crucial role of information technologies in averting conflicts between nations. This involves assessing and forecasting the military- political landscape on both global and regional levels, as well as analyzing bilateral military-political relations using contemporary technical tools and information technology (ERFKT, 2014, art.21/a).

As a result, the military doctrine has a defensive nature, as in the Information Space Activities Concept published in 2011. Additionally, Russia must improve its technological capabilities in order to prepare for non-military measures to gain advantage against information threats.

3.3.3. 2015- 2021- Strategies of National Security

Unlike The Military Doctrine and Information Space Activities Concept, 2015 and 2021 National Security Strategies draw a broader perspective on Russia's national interest and strategic national priorities.

The scope of the 2015 National Security Strategy includes developments aimed at improving the quality of life of citizens, protecting the political order of society, ensuring the security of the country, as well as increasing the international prestige of the Russian Federation. Similar to the Military Doctrine and Information Space Activities Concept, in the 2015 National Security Strategy, the country's security is not limited to dynamics such as economic, public affairs and state matters, but is expanded to include information and the environment.

When the 2015 National Security Strategy is examined, it is understood that Russia primarily feels under informational pressure. Russia's perspective on information confrontation involves manipulating the society in order to achieve the countries' geopolitical goals, by transferring false historical realities. The realization of these objectives relies on the use of information and communication technologies.

The 2015 National Security Strategy outlines that national interests are achieved through the pursuit of strategic priorities, which encompass national defense, state and public security, economic development, advancements in science, technology, and education, improvements in healthcare, cultural growth, ecological sustainability, effective resource management, strategic stability, and the promotion of balanced strategic partnerships (Russian Federation, 2015).

One of the primary threats to state and public security involves activities related to the misuse of information. Prominent among these

activities is the use of communication technologies to disseminate ideologies such as extremism, terrorism and separatism. Measures to be taken against such threats are also outlined in the document. Accordingly, the document addresses how to identify and analyze threats in the information field and what kind of systems can be developed to counteract them. It is also emphasized that measures are being taken to protect citizens from the effects of destructive extremist propaganda movements.

In order to improve the quality of life of Russian citizens, the aim is to develop information infrastructures, to ensure that the society has easy access to information on all kinds of issues, and to provide equal access to all individuals within the territory of the Russian Federation.

In the cultural sphere, the 2015 document emphasizes the significance of information in ensuring national security. It highlights several key concerns, including the potential weakening of unity among Russia's multinational population. Additionally, the document addresses the spread of propaganda promoting permissiveness and violence, which is seen as a threat to societal cohesion. Another highlighted issue is the declining the role of the Russian language in the world, perceived as a challenge to Russia's cultural influence and identity. Furthermore, the document expresses concern about attempts to falsify Russian and world history, emphasizing the importance of accurate historical narratives in shaping national identity and international perception (Russian Federation, 2015).

It was emphasized that protective measures should be taken against divisive information and psychological effects in the cultural field, and that measures should be taken to prevent violence that may occur through propaganda among the ethnic, religious and racial groups of the Russian Federation.

Following the rising global instability and escalating geopolitical

tensions after 2015, President Vladimir Putin signed Russia's updated national security strategy, Strategy of National Security of Russian Federation, on July 2, 2021. This document notably distinguishes itself from the 2015 National Security strategy and other doctrines by placing a district emphasis on information security, which is addressed as a separate domain. Additionally, the scope of information and communication technologies has been significantly broadened.

The 2021 National Security Strategy of Russia enumerates several factors posing threats to information security and outlines strategies to address them.

Table 1: Information Security Threats and Mitigation Policies in the National Security Strategy of Russia

Threats to Information Security	Strategies to Mitigate Threats
1. Cyber Attacks	Strengthening information security across military and civilian sectors.
	Promote digitalization while protecting cultural sovereignty.
	Counter historical distortion and psychological sabotage.
	Safeguard Russian's position in global media and communication.
	Advocate for international cooperation to enhance global information security.
Most of these attacks originate from foreign states (Russian Federation, 2021, art. 50).	
2. Anonymity in information and communication technologies	
Facilitating crimes like money laundering, terrorist financing, and drugs distribution (Russian Federation, 2021, art. 54)	
3. Militarization of Information Conflicts	
Necessitating enhanced security of the Armed Forces and military equipment (Russian Federation, 2021, art. 9).	
4. Economic Risks	
Related to information and communication technologies production and challenges in digital economy (Russian Federation, 2021, art. 88).	
5. Psychological Impact	
Regarding traditional Russian values, culture, and historical heritage (Russian Federation, 2021, art. 88).	

Source: (Russian Federation, 2021).

The 2021 National Security Strategy, it is emphasized that Russia needs to maintain its position in the global information space in terms of media and communication. Additionally, there is a call for international cooperation enhance information security on international stage, addressing both international organizations and states.

The reason why Russia attaches so much importance to this issue is

that, as emphasized in the document, it is believed that enemies are trying to create a hostile image towards Russia through disinformation campaigns and that sanctions are being imposed on Russia's information sources. This significant threat perceived by Russia has prompted the expansion of the information security domain in the 2021 National Security Strategy. Russia has, effectively issued a manifesto addressing the perceived threats to its own security.

Finally, the comparison of national priorities in 2015 and 2021 above reveals significant changes in Russia's strategic focuses. The table below shows the changing spectrum.

Table 2: Russia's Strategic National Priorities (2015-2021)

Priorities in 2015	Priorities in 2021
Improving Quality of Life of Russian Citizens	Preservation of People of Russia and Development of Human Potential
National Defense	National Defense
State and Public Security	State and Public Security
-	**Information Security**
Economic Growth	Economic Security
Science, Technology and Education	Science and Technological Development
Culture	Protection of Traditional Russian Spiritual and Moral Values, Culture and Historical Memory
Economy of Living Systems and Rational Use of Natural Resources	Environment Safety and Management
Strategic Stability and Equal Strategic Partnership	Strategic Stability and Mutually Beneficial International Cooperation
Public Health	-

Source: (TASAM,2021).[5]

As a result, these changes between the 2015 and 2021 strategies show that Russia has comprehensively re-evaluated its strategic priorities in the field of national security and its approach to information security, and accordingly revised its strategic priorities in line with current threats.

3.3.4. 2016- Doctrine of Information Security

On December 5, President Vladimir Putin approved and published the Doctrine of Information Security of the Russian Federation, replacing the

[5] This table compares Russia's Strategic National Priorities from 2015/2021, based on data from the TASAM 2021 report. It highlights the changes in strategic priorities and their evolution over years.

previous doctrine issued in 2000. This doctrine is the official statement for ensuring Russia's national security in the field of information.

This doctrine addresses four fundamental concepts: national interest within the information sphere, major information threats and the current state of information security, strategic goals and key areas for ensuring information security, and the institutional framework for information security.

In this doctrine, as presented by the Ministry of Foreign Affairs of the Russian Federation in 2016, reflects concerns similar to those found in other published doctrines. It highlights several key issues pertinent to its own security.

Firstly, the doctrine addresses concerns about threats to Russia's territorial integrity, arising from both internal and external actors. The doctrine addresses the growing information pressure the Russian population and underscores the need to safeguard societal stability and resilience against external influences.

Secondly, the document points out the rise in computer crimes, particularly those affecting the credit and financial sectors, underscoring the need for robust cybersecurity measures. Moreover, the document condemns the exploitation of information technologies for military and political objectives that breach international law, emphasizing of adhering norms and regulations.

It raises concerns about heightened intelligence activities conducted by foreign states against Russia, emphasizing the need for enhanced count intelligence measures. Additionally, the doctrine discusses the use of information tools to manipulate individual, group, and public consciousness, which could potentially exacerbate interethnic and social tensions within Russia.

At this point, the features that distinguish the doctrine of information security from other doctrines will be emphasized. The areas that are examined one by one in other doctrines are emphasized in this document, placing information security as the main axis and how information security is characterized in terms of national defense, economics, science, technology and strategic partnership.

The first point that distinguishes The Doctrine of Information Security from other documents is the statement that intelligence services activities pose a threat to Russia's information security. While other documents focus on countries' use of information tools against Russia, the Doctrine of Information Security explains the information operations conducted by of intelligence services against Russia.

The second point elaborates on the government agencies of the Russians Federation involved in the information security system, including entities such as Central Bank of the Russian Federation or judicial bodies.

This doctrine bases the information security activities of state actors affiliated with the government of Russia on certain duties and objectives. Several of these principles include collaboration among actors to ensure information security and acting in accordance with the legal norms of the Russian Federation and international law. The main objectives of these actors are to strengthen the vertical management system and improve the functioning of the information security system.

3.3.5. Foreign Policy Concepts

The Russian Federation released five Foreign Policy Concepts in the years 2000, 2008, 2013, 2016, and 2023. Russian Federation's The

Foreign Policy Concept is referred just as “The Concept”. The general objective is to convey the principles, priorities, goals and objectives of the Russian Federation’s foreign policy

These five concepts analyze how information security has been shaped over time in the changing and developing world. In these documents, examinations were made in many areas other than information security while defining the general scope of Russian foreign policy. However, in this thesis, these five documents will be examined in terms of how Russian foreign policy to information confrontation. The concept of information confrontation, which was published from 2000 to 2023, is mentioned under the title of information support for foreign policy activities.

Russia aims to sphere its global perception, develop effective methods for influencing public opinion abroad, enhance the role of Russian mass organizations through substantial state support, engage actively in international information cooperation and take necessary measures to protect its sovereignty and public diplomacy from information threats (The Ministry of Foreign Affairs of the Russian Federation [MFA], 2008).

In the Concepts published in 2013 and 2016, another point regarding information confrontation was evaluated in the context of soft power. Alongside traditional diplomatic methods, “soft power” has become essential for achieving foreign policy goals. This approach covers tools provided by civil society and numerous technologies, such information, communication, humanitarian and other related activities (MFA, 2016, art. 9).

However, the foreign policy concept of the Russian Federation, approved by Vladimir Putin and published on March 31, 2023, places a significantly greater emphasis on information security compared to previous concepts. In the 2013 and 2016 The Concepts, information

associated with soft power, by 2023, has witnessed an increased perception of threats emerging from the information and communication domain. The concept of militarization of information with increasing threat perception is briefly summarized in 2023 as “information space as new spheres of military action” (MFA, 2023).

The Foreign Policy Concept of 2023 emphasizes information security across various domains. For example, Article 5 of the third section outlines national interests and strategic goals, including creating a secure information environment and shielding Russian society from harmful psychological influences (MFA, 2023, art. 5).

Further in the document, it is emphasized that Russia can legally take symmetrical and asymmetrical measures as a state policy to suppress the unfriendly technologies by other states. In this case, it can be concluded that Russia expressed bolder statements than other documents.

In addition, another information-based threat to Russia is increasing hatred towards Russia by manipulation of Russian historical narratives. In this regard, the foreign policy concept emphasizes the dissemination of misinformation aimed at diminishing the significance of Russia’s victory over Soviet Russia against Nazi Germany, its founding role in the United Nations, and its contributions to decolonization movements in Africa, Asia and Latin America.

Finally, in the information support for the foreign policy of the Russian Federation section of the document, it touches upon some issues that Russia prioritizes in order to obtain accurate information. In general, The Concept addresses topics such as the provision of accurate information to foreigners against disinformation campaigns against Russia’s historical achievements, the dissemination of information that will enable the development of peace and friendly relations between

countries, the prevention of movements excluding Russia in the global information space and creating a common information space between the Commonwealth of Independent States and the Russian Federation.

The publication of these doctrines is inherently related to the evolving global events and Russia's involvement in these unfolding events. Moreover, the timing of the publication of these doctrines is not coincidental. However, in this section of the thesis, examinations have been conducted to explore how information confrontation, information security and information space find a place in doctrines, and a comprehensive framework has been drawn on Russia's policies on information confrontation.

Russia's national doctrines lay out various structures, including information warfare policies. The focus of these doctrines' points to the effective use of information technologies. Russia's information warfare policies have evolved throughout the historical process and found a place in today's strategic doctrines. As a result, Russia aims to achieve information superiority with effective policies.

Throughout this section, it is clear that Russia's information warfare policies are based on a comprehensive and multifaceted strategy. Russia has tried to achieve information superiority by applying information confrontation strategies in both peacetime and wartime. These strategies are generally divided into two main categories, "information-technical" and "information-psychological", each of which includes different tactics. While information technique targets the enemy's electronic networks, information psychology involves manipulation of information to demoralize the enemy by influencing societies.

4. CHAPTER 4: RUSSIAN INFORMATION WARFARE POLICIES IN UKRAINE CONFLICT

Information warfare is about achieving goals that used to require serious military force and a lot of bloodshed, e.g. annexing a part of another country by other means

(Franke, 2015).

In this section, Russia's information warfare policies in the Ukraine conflict will be examined in detail. First, the nature of the Russia-Ukraine conflict will be analyzed, and the historical and political background of this conflict will be emphasized. Later, Russia's information warfare policies against Ukraine will be examined under two main headings: information-technical and information-psychological. In the information-psychological field, the Kremlin's rhetoric and use of social media will be emphasized, and in the information-technical field, Russia's cyber-attacks and other technical information warfare methods will be evaluated.

4.1. The Nature of the Conflict

The Ukraine-Russia conflict is a complex issue that is examined in different areas. The geopolitical reasons, consequences, military aspects and effects of this conflict on the global economy have been discussed by various scholars and academics with different currents of thought. Nevertheless, this thesis argues that the main focus of the Ukraine-Russia conflict lies within the realm of information warfare. Prior to delving into the field of information warfare, a comprehensive analysis of the nature of the Ukraine-Russia conflict will be undertaken.

The escalation of tensions between Russia and Ukraine did not arise

suddenly but rather evolved through a sequence of events. Events such as the 2004 Orange Revolution and the 2014 annexation of Crimea caused a series of developments culminating the 2022 Ukraine-Russia conflict. In particular, the "Euromaidan" protests, which started in November 2013 after Pro-Russian President Victor Yanukovch refused to sign the Association Agreement with the EU, caused the tension in the region to constantly increase. With Russia's support for separatism in Crimea in February 2014 and the referendum held in March 2014, Russia strengthened its control in Crimea. Despite the increasing conflicts in the eastern "Donbas" region of Ukraine after Crimea, the conflict was aimed to end with the Minsk I and Minsk II agreements in 2014/2015; however, the tension in the region has not decreased. The development of relations with NATO and the EU in 2016/2017/2018 led to the acceleration of rapprochement with the West with the election of Volodymyr Zelenskyy in 2019.

The unfolding sequence of events collectively precipitated the emerge of the 2022 Ukraine-Russia conflict. In March 2021, Russia began to accumulate military equipment along the Ukrainian border. During this process, Russia has put forward some demands, and the prominent ones among these demands are the call for Western states to re-join the Minsk II negotiations in order to prevent a possible conflict between Russia and Ukraine, the reconsideration of the relations that Ukraine wants to develop with Western countries, and finally, the necessity for a rapid military intervention in case of invasion (Zabrodskyi et al., 2022). The rejection of these demands by Ukraine and its international partners prompted Russia to deploy almost 100,000 Russian soldiers to the Ukrainian border in the autumn of 2021. NATO's decision to deploy 8,500 soldiers to Europe on January 24, 2022, increased the security concern in Russia, and

on February 10, 2022, Russia conducted its largest army exercise since the Cold War. When negotiations with Western countries failed, on February 21, 2022, Putin recognized the independence of Donetsk and Luhansk and allowed peacekeepers to enter Ukrainian territory, and Russia's military position in Donbas, which has been ongoing since 2014, became obvious (Walker, 2023). Thus, the commencement of the Ukraine-Russia conflict signals a protracted and intricate trajectory.

4.2. Information Confrontation Policies of Russia in Ukraine

In this section, Russia's information confrontation policies towards Ukraine will be examined under two main headings. Initially, the subject will be discussed in the information psychological field and then in the information technical field. The main argument to be discussed in the information-psychology section is to reveal Putin's narrative on information warfare policies shaped on both historical and ideological foundations. Using elements such as the threat of NATO expansion, the rise of Neo-Nazis in Ukraine, and allegations of Western-backed corruption, Russia's actions are portrayed as a necessary step to defend Russian identity, security, and historical heritage. This narrative has been carefully constructed to appeal to both local and international public opinion. It portrays Russia not as an aggressive power, but as a guardian of our common Slavic heritage and a defender against Western interventions. In particular, historical references to the Second World War position Russia as the rightful heir of the Soviet Union's anti-fascist struggle and reinforce this image by referring to religious values. Putin's discourse of preserving Orthodox Christian-Slavic unity portrays Ukraine's integration into Western civilization as a threat to Russia's

historical and religious identity. The complex interaction of these historical, cultural, religious and geopolitical elements reveals how effectively Russia conducts information warfare by manipulating perceptions of legitimacy, victimization and moral superiority in the ongoing conflict with Ukraine. The argument in the field of information technology is that Russian cyber-attacks not only targeted Ukraine's infrastructure and communication systems, but also aimed to create a wide-ranging impact by spreading these attacks to Europe. These attacks show that Russia aims not only to achieve short-term tactical gains, but also to destabilize the Ukrainian state and shake the people's trust in the long term.

4.2.1. Information- Psychological Field: Kremlin Rhetoric

The decoding analysis of Vladimir Putin's address to the public, published on the President of Russia website on both February 21, 2022, at 22:35, and February 24, 2022, at 06:00, by unraveling the propaganda elements in the information-psychological field, will facilitate a better understanding of Russia's information confrontation policy on Ukraine. This analysis, obtained from the message intended for both the global audience and the Russian public, aims to provide insights into the conveyed implications.

In academic studies conducted outside Putin's discourses, scholars emphasized that historical and cultural domain propaganda is used as a tool in the Kremlin's information confrontation policies towards Ukraine. There are parallels between the Kremlin's discourse on the annexation of Crimea in 2014 and its discourse on the Ukraine-Russia conflict in 2022. The analysis of both instances indicates that a key aspect of the Kremlin's information confrontation policies towards Ukraine is to emphasize

shared historical and cultural ties with the country.

4.2.1.1. Historical and Cultural Domain

The point emphasized by Putin in the video is that in the historical and cultural domain, Ukraine is literally a part of Russia in terms of religion, language, race, ideology and geopolitics.

In his statement, Putin highlighted that Ukraine is not just a neighboring state, but an integral element of Russia's historical, cultural and spiritual heritage (Kremlin.ru.,2022, February 21).[6] This statement underscores the deep- rooted connections Russia attributed to Ukraine in its historical and cultural narrative.

It is claimed that Ukraine is an indivisible part of Russia, emphasizing common cultural and historical ties dating back to The Great Russian Empire, World War II and the USSR. Putin consistently describes the collapse of the Soviet Union as a calamity and underscores the pivotal role of Ukraine for Russia to return to its former glory days. Within the framework of the idea of Great Russia, Ukraine is acknowledged to possess a unique status.

In his remarks, Putin noted that the Ukrainian authorities have based their statehood on rejecting the shared history that once united the nations. He criticized these efforts as attempts to alter the collective mentality and historical memory of millions of people and multiple generations residing in Ukraine (Kremlin.ru.,2022, February 21).[7] This statement highlights

[6]Original Text: "Еще раз подчеркну, что Украина для нас не просто соседняя страна. Это неотъемлемая часть нашей собственной истории, культуры и духовного пространства." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

[7]Original Text: "При этом украинские власти изначально, хочу это подчеркнуть, с первых же шагов начали строить свою государственность на отрицании всего, что нас объединяет, стремились исказить сознание и историческую память миллионов

the critical need to explore the implications of historical and cultural narratives in the context of Russian foreign policy. However, it is claimed that the glorious Russian history, including Ukraine, has been corrupted by Ukrainian officials and that there are efforts to make common memories forgotten.

Putin's remarks on historical and religious connections, he expressed that the individuals living in the southern-western regions, historically part of Russian lands, have long considered themselves both Russian and Orthodox Christian.[8]

Additionally, Putin stated on Kiev's ongoing efforts to undermine the Ukrainian Orthodox Church of the Moscow Patriarchate (Kremlin.ru.,2022, February 21).[9] This reflects the ongoing religious tensions and conflicts in the region.

The underlying reason for Putin's statements is to unite the Orthodox Christian Slavic world under the leadership of Russia through concepts such as kin-state nationalism, Pan-Slavism, and Russkiy Mir (Russian World or Russian Peace), which gained momentum following the dissolution of the Soviet Union (Goudimiak, 2016). With these efforts, an attempt was made to create a Russian civilization identity, and Ukraine holding a significant position within this emerging Russian identity. All these emphases mobilize people with religious similarities, place them at the center of national identity and cultural heritage, and present them as a mission to protect and spread this heritage.

людей, целые поколения, живущие в Украине." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

[8]Original Text: "Издавна жители юго-западных исторических древнерусских земель называли себя русскими и православными." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

[9]Original Text: "В Киеве продолжают готовить расправу и над Украинской православной церковью Московского патриархата." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

The concepts of Kin-state nationalism, Pan-Slavism and Russkiy Mir share a similar perspective. The concepts of Kin-state nationalism and Pan-Slavism date back to the era of Peter the Great. Both these concepts argue that Russia and Ukraine share identical attributes in terms of ethnicity, religion, historical affiliations and linguistic ties (Goudimiak, 2016). According to Putin's claim, these two-nation emanating from the same Slavic origin, sharing a common religious understanding and language, are inseparable entities.

The primary feature that distinguishes Russkiy Mir from other concepts is that, unlike other concepts, it is a 21st century concept. The Russkiy Mir Foundation, established under Putin's auspices in 2007, aimed to popularize the Russian language. However, this organization has a broader goal than just popularizing the Russian language: building a new Russian identity after the collapse of the Soviets. The Russkiy Mir concept consists of five main dimensions: geopolitical, nationality, religious, cultural and psychological (Kozdra, 2018). Among these dimensions, the religious emphasis is of great importance, and the unifying power of the Russian Orthodox Church constitutes the primary focal point in the Russkiy Mir concept. Thus, it aims to create a Holy Russia civilization wherein the Russian Orthodox Church assumes the role of common church, the Patriarch of Moscow as the common patriarch, Russian as the shared common language, Moscow as the political center, Kiev as the spiritual center, and Putin as the leader. This envisioned civilization includes Russia, Ukraine, Belarus. and sometimes extends to encompass Moldova and Kazakhstan (Gallaher & Kalaitzidis, 2022). Putin's emphasis on the Russian Orthodox Church reflects his attempt to expand Russia's cultural and religious hegemony. Putin's effort to gather the Orthodox Christian Slavic world under Russian leadership is an important

rhetorical policy that could threaten Ukraine's independent identity and national sovereignty. These statements of Putin are an important example of the role of religion on national identity and political strategy. At the same time, the Orthodox Christian identity is highlighted, and the position of religious leader is emphasized. This situation shows Russia's efforts to expand by using its religious identity, and depending on the outcome of the Ukrainian conflict, it seems inevitable that this expansion will be reflected in other countries.

In the context of geopolitics, Putin discussed historical territorial changes, noting that Stalin incorporated lands from Poland, Romania, and Hungary into USSR and transferred them to Ukraine both before and after WW II. He also mentioned that part of traditionally German territory was given to Poland as compensation, and in Khrushchev transferred Crimea from Russia to Ukraine. This series of actions significantly influenced the territorial boundaries of modern Ukraine (Kremlin.ru.,2022, February 21).[10]

The fundamental idea underlying Putin's words is that, geopolitically, Ukraine is part of an inseparable entity with Russia. In this context, Putin's vision reflects a perspective that seek to create a Eurasian Union instead of the Commonwealth of Independent States, which includes Ukraine (Lange-lonatamišvili, 2015, p. 7). This narrative derives from theoretical foundations of the Heartland and Rimland theories.

The Eurasian Union envisioned by Putin finds its conceptual

[10] Original Text: "Затем, накануне и после Великой Отечественной войны, Сталин аннексировал СССР и передал Украине часть земель, ранее принадлежавших Польше, Румынии и Венгрии. При этом в качестве компенсации Сталин отдал Польше часть исконных немецких территорий, а в 1954 году Хрущев почему-то отобрал у России Крым и также передал его Украине. Собственно, так и образовалась территория Советской Украины." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

foundations in Alexander Dugin's neo-Eurasianist theory, taking its essence from H. Mackinder's Heartland theory. In 1904, H. Mackinder put forward The Heartland theory with his work "The Geographical Pivot of History" and defined this Eurasian region extending from the Volga to the Aral as the most advantageous location in the world (Kumar, & Kafi, 2015). This region mentioned by Mackinder covers the area of influence of the former USSR. With H. Mackinder's famous expression "whoever controlled East Europe would command the heartland, whoever controlled the heartland would command the world island, and whoever controlled the world island would command the world," Russia has adopted a vision positioning itself as a strategic power right in the middle of this region, aiming to govern the world. Nicholas Spykman also developed the Rimland theory by modifying Mackinder's Heartland theory. With the phrase "who rules Eurasia controls the world," Spykman defends the theory that since Eurasia has rich resources and critical sea routes, whoever controls this continent will have world maritime hegemony (Rahim, 2020). The region of East Europe or Eurasia, emphasized by both Mackinder and Spykman, encompasses Ukrainian territories. Nevertheless, these two thinkers are of Western origin and there is apprehension regarding Russian's control over the territories they idealize. In this case, Russia formulated its own Heartland theory, which Dugin characterized as Neo-Eurasinism.

After the collapse of the Soviets, new theories were developed to restore the integrity of Russian lands, and the Neo-Eurasinism theory developed by Dugin is suitable for the Greater Eurasia in line with Putin's vision. Both the Heartland theory, the Rimland theory, and ultimately the Neo-Eurasinism theory show that Ukraine is in a critical position. As such, Ukraine's geopolitical position is of key importance for Russia. This

includes Ukraine creating a buffer zone between western countries, Crimea having a strategic commercial and military location in the Black Sea, Russia transporting energy through Ukraine, and Russia exerting political influence in the Soviet regions through Ukraine. The geopolitical importance that Russia attaches to Ukraine is supported by these theories and creates a narrative for the Ukraine-Russia conflict.

Regarding the language factor, Putin remarked that individuals identifying as Russians and wishing to maintain their identity, language, and culture receive a clear massage of exclusion in Ukraine. He highlighted that, under Ukraine laws on education and the use of the Ukraine language, Russian has been effectively excluded from schools, public spaces and even everyday commercial settings (Kremlin.ru.,2022, February 21).[11]

Language is a factor that brings together multi-state countries and strengthens ties. Language brings together even nations that do not have a common past or interest. In addition, language plays an important role in the construction of cultural identity among states. For Russia, language is a tool used as a propaganda tool to spread ideology and promote Russian nationalism in former Soviet regions with a multi-ethnic structure (Aronova, 2017). The widespread use of Russian in the former Soviet regions strengthens Russia's claim in these regions. For example, an attempt was made to legitimize Russia's annexation by emphasizing the human rights violations committed against the Russian-speaking people in Crimea. Likewise, Putin points out that Russia is disturbed by the

[11] Original Text: "Людям, считающим себя русскими и желающим сохранить свою идентичность, язык и культуру, прямо дали понять, что они чужие в Украине. В соответствии с законами об образовании и о функционировании украинского языка как государственного, русский язык исключен из школ, из всех общественных сфер, даже из обычных магазинов." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

efforts of the Ukrainian authorities to erase the Russian language from daily life.

4.2.1.2. Anti- Westernism Domain

In the Anti-Westernism domain, the first focus is on NATO opposition. In this context, Putin's views on NATO's presence in Ukraine and its eastward expansion are detailed. His discourse on NATO's presence in Ukraine noting that nato training missions effectively function as foreign military bases under a different name. he pointed out that ukraine has long pursued a strategic goal of joining NATO, which Russia perceives as a direct threat to its security. Putin criticized the West for failing to honor promises made regarding NATO's expansion, highlighting that despite assurances to the contrary, there have been multiple waves of NATO enlargement, including Poland to North Macedonia. Consequently, NATO's military infrastructure has moved close to Russia's borders (Kremlin.ru.,2022, February 21).[12]

Putin mentioned "NATO" fifty times in both of his speeches. Russia's perception of NATO as a threat and its connection of the conflict with

[12] Original Text: "На Украине развёрнуты учебно-тренировочные миссии стран НАТО. Это, по сути, уже и есть иностранные военные базы. Просто назвали базу миссией – и дело в шляпе." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].
"Иными словами, выбор методов обеспечения безопасности не должен создавать угрозу другим государствам, а вступление Украины в НАТО является прямой угрозой безопасности России." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].
"Сегодня достаточно лишь одного взгляда на карту, чтобы увидеть, как западные страны «сдержали» свое обещание не допустить продвижения НАТО на восток. Просто обманули. Мы получили одну за другой пять волн расширения НАТО. В 1999 году в Альянс были приняты Польша, Чехия и Венгрия, в 2004 году – Болгария, Эстония, Латвия, Литва, Румыния, Словакия и Словения, в 2009 году – Албания и Хорватия, в 2017 году – Черногория, в 2020 году – Северная Македония." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

Ukraine to this narrative are based on a historical process.

The purpose of establishing NATO was to ensure the security of member countries by forming alliances against the Soviet threat. However, after the collapse of the Soviet Union, its mission was expanded and evolved to ensure stability and security against regional and global threats. NATO's expansion policies became prominent with the reunification of Germany and the collapse of the Warsaw Pact agreement on February 26, 1992 (Cuiriak, 2023). Thus, the expansion policies aimed at incorporating former Warsaw Pact members into NATO have garnered significant attention.

In the early 1990s, United States' intention to include Poland, the Czech Republic and Hungary in NATO materialized at the Madrid Summit in 1996, and the accession of these countries to NATO took place in 1999. Although Gorbachev and Yeltsin, the Russian leaders of that period, viewed this expansion with hesitation, they did not strongly object. This is due to the fact that the NATO-Russia Establishing Act, signed in 1997, left the door open for Russia regarding new NATO members. Apart from this, Russia considered the Baltic countries and the borders of the former Soviet Union as red lines in NATO expansion (Chesnut, 2023).

In 2004, the second phase of NATO expansion, a large number of members were enlisted from both the Baltic states and the former Soviet Union countries. Global events following the first phase, such as the Kosovo War, the Second Chechen War, the September 11 Attacks and the Iraq Invasion, heightened security threats for both Western countries and Russia (Cuiriak, 2023). Russia opposed NATO intervention in response to these events and claimed that these interventions violated the UN Charter. Throughout this period, Russia maintained a neutral position against the expansion of NATO, framing it as a fair accompli.

However, with the inclusion of Ukraine and Georgia in NATO's expansion policies, Russia's perspective on NATO turned from neutral to negative. In this last phase, the developments in Georgia in 2003 and Ukraine in 2004 strengthened the perception that NATO's military aims were evolving into political aims, attempting to spread Western values, thereby increasing Russia's threat perception. It was understood that a new era would begin with Putin's speech at the Munich Conference in 2007, where he emphasized that the expansion of NATO would not only undermine the security of Europe but also erode common trust and lead to conflict (Maitra, 2021). Another crucial point emphasized by Putin at this conference is the dysfunctionality of the unipolar model and its unacceptable nature. For Russia, NATO's expansion policies targeting Ukraine and Georgia have been completely unacceptable and have heightened tensions in the region. Thus, Russia views NATO expansion as one of the most significant threats in its military doctrines. The argument is made that the tension in the region has escalated due to the expansion policies of NATO, evident in the 2014 annexation of Crimea and the 2022 Russia-Ukraine Conflict, creating a domino effect in the region after the events in Georgia.

Putin highlights the differences between Russia and Western civilization by statin that despite Russia's unprecedented openness and sincere engagement with the U.S. and Western partners following the USSR's collapse, along with its substantial disarmament, there were attempts to undermine and completely dismantle the country (Kremlin.ru.,2022, February 24).[13]

[13] Original Text: "Что касается нашей страны, то после распада СССР, при всей беспрецедентной открытости новой современной России, готовности честно работать с США и другими западными партнёрами, и в условиях практически одностороннего разоружения, они тут же попытались надавить на нас, добить и

Putin also critiqued the disparity between the proclaimed values of democracy and economic progress versus the reality of widespread poverty and shortages. He argued that amidst this rhetoric, there was lack of concern from the ruling powers about the severe consequences facing the country (Kremlin.ru.,2022, February 21).[14]

As can be understood from this part of Putin's speech, he uses the narrative "clash of civilizations". Accordingly, Ukraine plays a key role in the conflict between Western civilization and Slavic-Orthodox civilization. However, before delving into Ukraine's role, it is imperative to comprehend Russia's place in the Clash of Civilization theory.

Samuel P. Huntington's thesis "The Clash of Civilizations" is based on the fact that people's cultural and religious identities will be the main source of conflict in the new era. Huntington argued that while ideologies were the source of conflict during the Cold War, this situation would be replaced by conflicts arising from cultural division after the Cold War. Moreover, Huntington mentions that the importance of civilizational identities will increase in the future and the interactions among seven or eight main civilizations will shape forthcoming conflicts. These civilizations are categorized as Western, Confucian, Japanese, Islamic, Hindu, Slavic-Orthodox, Latin American and African (Huntington, 1993).

In Russia, the process of integration with the West was supported during the Gorbachev and Yeltsin periods, and there was a belief in being an integral part of the same civilization (Šulc, 2023). However, with

---

полностью уничтожить." (Kremlin.ru., 2022, February 24). Retrieved from http://en.kremlin.ru/events/president/news/67843 [12 August 2024].

[14] Original Text: "На фоне поверхностной и популистской болтовни о демократии и светлом будущем, построенном на основе то ли рыночной, то ли плановой экономики, но в условиях реального обнищания народа и тотального дефицита, никто из власть имущих даже не задумывался о неизбежных трагических последствиях для страны." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

Putin's election as president, the emphasis on Russian patriotism, the role of the church and the importance of armed forces for maintaining Russia's major power status in world politics have strengthened the narrative asserting that Russia has a unique structure distinct from Western civilization (Oldberg, 2014). Thus, Russia positioned itself within the Slavic-Orthodox civilization and claimed as the main actor.

In this context, as Russia positioned itself within the Slavic-Orthodox civilization, Neo-Eurasianism, which took its origin from Samuel Huntington's theory, was shaped by Alexander Dugin. Beyond being just a geopolitical theory, Neo-Eurasianism has provided Russia a new identity after the collapse of the Soviet Union. The theory of Neo-Eurasianism, which forms the basic narrative of the Ukraine-Russia conflict, includes some basic principles it defends. It asserts the inevitability of conflict between the West and Russia (Melin, 2017), emphasizes the importance of developing close relations with near abroad countries and new nations established after the dissolution of the Soviet Union, and seeks to strengthen Russia's political and economic ties with Slavic brothers. Furthermore, it rejects Western values as incompatible with the rest of the world- arguing that the latter leads to expansionist imperialism- and supports regional integration rather than global integration is more suitable for cultural diversity (Hudson et al., 1994).

Based on the ideals of Huntington and Dugin, Ukraine is observed to be entangled in the middle of the conflict between the West and Russia. The fundamental question at hand is the contradiction of whether Ukraine belongs to Western civilization or Russian civilization. Putin's narrative throughout his speech is that the West cannot bring any benefits to Ukraine and that Ukraine's political, historical and traditional loyalty lies exclusively with Russian civilization.

There are some features in Putin's narrative that make Ukraine a central element of Huntington's Slavic-Orthodox or Dugin's Neo-Eurasianism theories. These features include Kiev serving as the spiritual cradle of modern Russia, Crimea being considered as the main center of the Russian Orthodox belief, the conceptual positioning of Kievan Russians as "older brothers" and Ukrainians are the "younger brothers", and the assertion that both Kievan Russians and Moscow Russians share common roots (Kowalski, 2022).

In the context of Russia's security concern, putin underscores Russia's significant role in maintaining regional and global stability by recalling 2008 initiative fro European Security Treaty. This proposal aimed to prevent ant Euro-Atlantic state or international organization from enhancing their security at the expense of others. However, it was dismissed, ostensibly because it was unacceptable for Russia to impose restrictions on NATO's activities (Kremlin.ru.,2022, February 21).[15]

Additionally, Putin notes that despite these efforts, Russia made another attempt in December 2021 to negotiate with the US and its allies on European security principles and NATO's expansion. These attempts, however proved unsuccessful (Kremlin.ru.,2022, February 24).[16]

In his speech, Putin asserted that he did his best to prevent this conflict,

[15]Original Text: "Мы хорошо осознаем свою колоссальную ответственность за региональную и глобальную стабильность. Еще в 2008 году Россия выдвинула инициативу о заключении Договора о европейской безопасности. Смысл его заключался в том, что ни одно государство и ни одна международная организация Евроатлантики не могла укрепить свою безопасность за счет безопасности других. Однако наше предложение было сразу отвергнуто: России, дескать, нельзя позволить ограничивать деятельность НАТО." (Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

[16]Original Text: "Несмотря ни на что, в декабре 2021 года мы в очередной раз предприняли попытку договориться с США и их союзниками о принципах обеспечения безопасности в Европе и о нерасширении НАТО. Все напрасно." Kremlin.ru., 2022, February 24). Retrieved from http://en.kremlin.ru/events/president/news/67843 [12 August 2024].

but NATO ignored these efforts and facilitated all kinds of opportunities that could threaten Russia's security for its enemies. One of the most prominent thinkers supporting this narrative is John J. Mearsheimer.

According to Mearsheimer, the primary responsible of the Ukrainian crisis is the West's policy of framing Russia. He determined that the process of making Ukraine a member of NATO has accelerated, even though there is awareness that Ukraine's integration with the West poses an existential threat to Russia. The main reason why Ukraine's integration into NATO is the main threat for Russia lies in the direct confrontation anticipated between NATO forces and Russia, with no borders acting as a buffer (Mearsheimer, 2022). To support this perspective, Mearsheimer quoted an interview given by the American diplomat George Kennan in 1998 and explained that NATO expansion could provoke the Russians by saying, "We have always said that the Russians are like this." (Mearsheimer, 2014). In general, Mearsheimer believes that NATO's initiative during the 2008 Bucharest Summit for Ukraine and Georgia to join the alliance created a security dilemma for Russia. He claims that this security dilemma caused the United States to cross the red line, particularly with the acceleration of Ukraine's accession to NATO in 2021, ultimately precipitating the commencement of the war in 2022.

4.2.1.3. Other Domains: Examining the Dynamics of Ukraine Authorities

Under the other domain, neo-Nazi influence, Putin claims the operation seeks to protect those facing years of alleged genocide by the Kiev regime, aiming to demilitarize and de-Nazify Ukraine and bring

perpetrators to justice (Kremlin.ru.,2022, February 24).[17]

Various rhetorical elements employed by the Kremlin against the authorities in Ukraine include “fascism”, “Neo-Nazi” and “banderovtsi”. These rhetorical elements take their origin from the Second World War, referred to as the Great Fatherland War by Russia. During this war, the Soviet Union suffered greatly against the Nazi occupation; however, they also fought together against the destruction of fascism. The substantial contribution in this great struggle played a pivotal role in the exemption of communists from prosecution in the Nuremberg trials (Prys, 2021).

In the Great Fatherland War, the member states of the Soviet Union were directly part of the anti-hitler coalition. Putin describes the Soviet Union countries’ resistance against Hitler as heroism in every field and emphasizes the important contributions of these countries to Russia’s victory in the war. During the Cold War, after the Great Father Land War, countries that refused to join the Soviet Union were positioned as supporters of genocide or fascism. This situation gave rise to the rhetoric of “other and us.” Following the collapse of the Soviet Union, a discourse was developed, designating countries supporting Russia as “one of us”, while categorizing every opposing country as supporters of fascism, who were categorized as “others”. This dichotomy has been shaped by Russia against Ukraine as “other vs. brother.” (Khaldarova, 2019). It is argued that Ukraine’s transition from brother to other category is due to the rising nationalism movement in Ukraine. A narrative has been developed in

[17]Original Text: “Его цель — защитить людей, которые на протяжении восьми лет подвергались издевательствам и геноциду со стороны киевского режима. А для этого мы будем добиваться демилитаризации и денацификации Украины, а также привлечения к ответственности тех, кто совершил многочисленные кровавые преступления против мирного населения, в том числе граждан Российской Федерации.” Kremlin.ru., 2022, February 21). Retrieved from http://kremlin.ru/events/president/news/67828 [12 August 2024].

which supporters of the rising nationalism in Ukraine are associated with ultra-radicalist groups that support Nazi ideologies (Waller, 2023).

Putin advocates that the denazification process will be initiated in Ukraine within the framework of the Ukraine-Russia conflict and will thus help the Ukrainian people be purified from their fascist and pro-Hitler rulers. As can be understood from Putin's statements, there is an indication that far-right nationalism has increased in Ukraine, particularly evident during the Maidan protests, with additional emphasis on the fact that Volodymyr Zelensky is also a supporter of this trend.

Finally, Putin emphasized this situation in his speech, articulating allegations of corruption and the exercise of puppet governance against the leadership of Ukraine. Putin posited that, following the events of 2014, a Western-backed coup administration began to rule Ukraine, and this administration, instead of providing all kinds of support that could serve the interests of the country, is enriching a certain segment and impoverishing the people through corruption. Putin claims that this administration not only oppresses the people in the Donbas region but also the entire Ukrainian people.

Putin refers to the Maidan events of 2014 by calling the Ukrainian administration a "coup" and a "puppet." The removal of pro-Russian Viktor Yanukovych after his refusal to sign the proposed association and free trade agreement with the EU is considered a Western-backed coup. Each successive Ukrainian government, from the administration led by Petro Poroshenko to that of Zelenski, is viewed as a direct threat to Ukraine's future.

Throughout its historical trajectory, Ukraine has struggled with the issue of corruption, drawing criticism even from NATO. Research has found that the main causes of corruptions in Ukraine are business and

political ties, weak judicial systems and an over-controlling transparent government (The Bleyzer Foundation, 2016). Putin draws attention to the issue by attributing corruption in Ukraine to pro-Western governments.

Table 3: *Main Narratives of Putin's Speech*

Main Narratives of Putin's Speech
Historical and Cultural Domain
Ensuring Orthodox Christian-Slav unity under the Russian Protectorate
Ukraine does not want to transfer the common history it shares with Russia (Great Russian Empire, World War II, USSR) to future generations.
Ukraine's geopolitical location emphasizes its importance as a buffer zone between Russia and the West, which includes efforts by western countries to gain strategic advantage against Russia.
The persecution of Russian-speaking people in Ukraine constitutes a noteworthy human rights issue that warrants careful examination.
Anti- Westernism Domain
NATO's expansionist policies towards Ukraine and Georgia pose a security threat to Russia.
Russia and Ukraine are historically and traditionally part of the same civilization. For this reason, there is a prediction that Ukraine will not be able to integrate into Western civilization.
Russia has endeavored to avoid conflict with Ukraine, yet Western countries have been instrumental in causing conflict.
The West is aware of Russia's increasing power and aims to diminish this influence.
Other Domains
The Ukrainian administration is described as a puppet regime under the influence of the West.
The Ukrainian administration is observed to grapple with corruption allegations.
There is a perception that the Ukrainian people are ruled by Neo-Nazi supporters.
Ukraine is characterized as a non-existent and failed state.

Source: Kremlin.ru.,2022 (Created by Author).

4.2.2. Information- Psychological Field: Social Media

The development of Internet technology has significantly facilitated access to and dissemination of information. Social media platforms, which emerged after the 2000s, have evolved over time and become an indispensable part of our lives, strengthening interpersonal communication by crossing information boundaries. Widely utilized contemporary social media tools include Twitter, Instagram, TikTok, Telegram, YouTube, and Facebook. With the spread of these platforms, the influence of traditional media tools such as television and newspapers has decreased, consequently propelling information access to unprecedented levels.

The role and significance of social media in conflicts constitute a pivotal element of information warfare. This stems from the capacity of social media tools to confer influence on individuals across many issues, spanning decision-making mechanisms to choices. Unreliable information, propaganda, and misinformation are frequently encountered problems on these platforms, where every individual can easily become a member and share content freely.

With the development of communication technologies, notably social media platforms, the importance of conventional weapons in conflicts has become secondary, and social media has become the main center of new-generation conflicts. The use of social media in conflicts has a more indirect effect than a direct one, surpassing the efficacy and convenience of conventional weaponry. Social media utilization affects conflict on various issues. Firstly, it can lead to regime changes, leadership transitions, and alterations in governance. The instrumental mechanism facilitating this phenomenon lies in the mobilization of individuals

through social media manipulation, causing uprisings and fomenting the outbreak of conflicts. In the case of the Arab Spring, the resistance that people started against the Ben Ali regime in Tunisia in 2010 by mobilizing through Facebook and Twitter is an example of this issue (Zeitzoff, 2017). Secondly, another situation where social media affects conflicts is when radical terrorist groups use communication technologies. Notably, the images and statements spread by ISIS on social media have created a situation that makes it easier for people to join the organization (Prier, 2017).

The wide influence of social media makes the dissemination of information in the field of information psychology inevitable. Particularly through social media, individuals are manipulated to achieve political goals. Leaders and governments are trying to influence the masses, establish their ideological order, and attain electoral success through the strategic deployment of social media. As a result, social media is becoming a battleground for both individuals and governmental and military entities.

Russia has been known for its awareness of the power of social media since its inception. As social media platforms have evolved and become weaponized, these platforms have moved beyond the areas where people share their daily lives or communicate with each other. Russia has effectively employed these platforms not only in the 2022 conflict but also during the periods of the 2014 Maidan and the 2004 Orange Revolution. The main reason why Russia uses social media in these conflicts is to shape the public perception and opinion of the Ukrainian populace, the international community, and the Russian citizenry through the deployment of propaganda methods (Hou, Fu, & Lai, 2023).

This ongoing Russia- Ukraine conflict is often described as the first

social media war. To make this definition more understandable, The Spanish-American War is classified as the first media war, the Vietnam War as the first television war, and the civil war in Yugoslavia as the first internet war (Bojor & Cîrdei, 2022). Thus, scholars assert that the present conflict has been recorded in the literature as the first social media war, with Russia strategically aims to be the winner of the war by using information confrontation policies against Ukraine through various social media platforms. For this reason, Russia's information confrontation policies will be examined first through Russian-based media tools and then through international social media platforms.

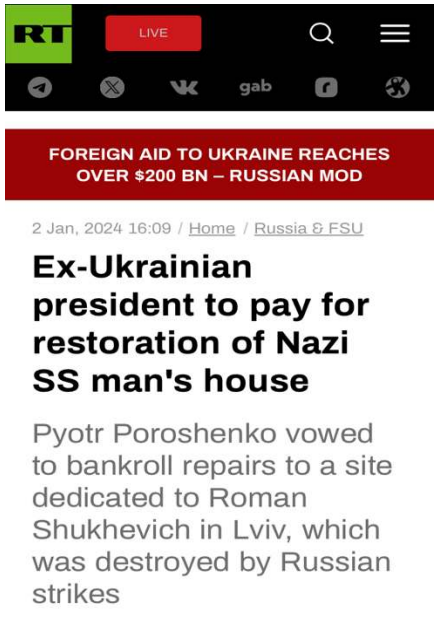
4.2.2.1. Russian Based Media Tools

Online news sources such as Komsomolskaya Pravda, TV Zvezda, Sputnik, and RT (Russian Today) describe Russia's information confrontation policies on Ukraine from Russia's perspective. While not exhaustive in encompassing the entirety of Russia's perspective, these sources provide a general framework. Each source offers a unique genre, and the disparities between these sources arise from Russia's efforts to reach various target audiences.

RT and Sputnik serve as gateways to the world to convey Russia's narrative to international audiences, facilitated by their multilingual broadcasts, including English. In the direct aftermath of the Russia-Ukraine conflict's onset, sanctions were imposed on these two media outlets that also extend their reach into European broadcasts. RT and Sputnik assume a pivotal role in conveying Russia's information confrontation policies to people in Europe and many other countries. They assert diverse claims on a range of issues, from genocide allegations

against Ukraine and NATO to anti-Neo-Nazi propaganda. Russia uses these media tools not only to spread anti-NATO and anti-Ukraine propaganda but also to prove that Russia is one of the world's leading powers.

Figure 8: *RT News*



Source: (Sputnik International, 2023)

Figure 9*: Sputnik Global News*

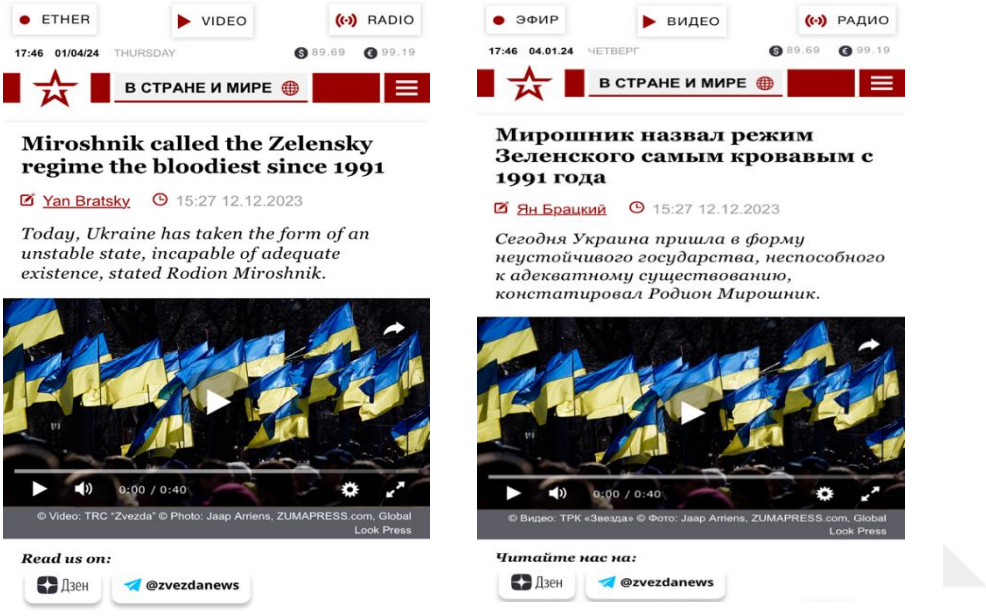
Source: (RT International, 2024)

Russian-backed media sources, namely RT and Sputnik, were established to create an alternative narrative to Western media sources. Russian-language media sources such as Komsomolskaya Pravda and TV Zvezda do not limit their target audience only to the Russian populace but also include those living in former Soviet countries. Komsomolskaya Pravda continues its activities in countries such as Russia, Belarus,

Kazakhstan, Kyrgyzstan, and Moldavia and assumes a crucial role as a means of disseminating Russia's state propaganda. Founded in 1925 during the Soviet period, Komsomolskaya Pravda stands as the oldest newspaper in Russia and still maintains its reputation. Based on the Kremlin's rhetoric, this publication makes propagandist claims such as accusing the Ukrainian government of corruption and accusing the Ukrainian army of terrorism and Nazi affiliation.

TV Zvezda, a significant broadcasting organ, constitutes a media tool owned by the Russian Ministry of Defense. Although TV Zvezda tries to spread propaganda akin to Komsomolskaya Pravda, it highlights criticisms centered on the West. For instance, topics such as Ukraine being ruled by a Western-backed government or the portrayal of the West as an evil enemy against the Russian people are covered on TV Zvezda (Sazonov & Müür, 2017, pp. 91).

Figure 10*: TV Zvezda*



Source: (Брацкий, 2023).

These media, especially Russian-backed sources such as RT, Sputnik, Komsomolskaya Pravda and TV Zvezda, aim to reach international audiences and the public in former Soviet countries from the Russian perspective. These sources are used to spread the policies and propaganda of the Russian state by offering an alternative perspective to the news presented by the Western media. For example, it deals with issues such as allegations that Ukraine is ruled by a Western-backed government or the portrait of the West as hostile to the Russian people. These media outlets play an important role in increasing Russia's international awareness and strengthening its anti-Western narratives.

4.2.2.2. International Social Media Tools used by Russia

Russia has placed special attention to using international social media platforms such as Instagram, Twitter, YouTube, Facebook, Telegram and TikTok effectively and accurately in the information confrontation against Ukraine. Efforts have been undertaken to make the conflict against Ukraine visible through these platforms. The Russian state's rhetoric spreads to the global audience and emphasizes the injustice of Ukraine. For instance, Russia has used YouTube to upload videos depicting Ukrainian forces as aggressors, gaining millions of views and sparking debates in the comment sections (Lin, 2022).

Ukraine is aware that its relative lack of strength compared to Russia in terms of political, military, economic and demographic aspects. Therefore, Ukraine seeks to prevail in the conflict against Russia by influencing the masses through social media. Ukraine aims to use its social media power to develop various arguments against Russia's rhetoric and end the conflict in its favor. Especially at the beginning of the conflict, Zelensky's clothing symbolism effectively uses information confrontation tools such as life in the shelter videos shared on TikTok or the location information of the Russian soldiers spread on Telegram (Chayka, 2022). In response, Russia has developed various policies to eliminate Ukraine's rhetoric. The first of these is to adopt a discourse that focuses on Zelensky's ignorance of state administration. To support this discourse, quotes from Zelensky's past shows are shared, and Zelensky's legitimacy is questioned by the public. For instance, clips from Zelensky's comedy shows have been edited and spread on social media to portray him as an inexperienced leader, undermining his credibility (Dugin & Pavlova,

2023).

Secondly, by sharing posts on social media about the inadequacy of the Ukrainian army, attempts are made to diminish the prestige of the Ukrainian army, thus directly demotivating the Ukrainian people and international public opinion. An illustrative example is a video spread on Twitter and TikTok, images of children on the autism spectrum being recruited to the Ukrainian army, claiming that they could not find soldiers into an army (Intelligence Community Assessment, 2017). This portrayal emphasizes the challenging circumstances Ukraine purportedly faces.

Thirdly, Russia has strategically made sure to spread all kinds of discourse on social media platforms to depict itself as the genuine victims in the ongoing narrative. Russia tried to announce its grievances to the international public through social media platforms, claiming that NATO was deceiving them by continuing its expansionist policies and that this situation created a security dilemma for Russia (Ciuriak, 2022). Furthermore, by framing the genocide that took place in Donbas as a justification for Russia's intervention, it has introduced a new dimension to the discourse of victimization that they had to ensure the security of the people in this region.

Finally, Russia endorses campaigns on social media aimed at damaging Ukraine's reputation. One such endorsement is the claim that Ukraine lacks a distinct historical identity within the context of Russia and therefore the current Ukrainian state lacks distinctive characteristics. Additionally, among the main discourses spread by Russia is that Ukraine is associated with Nazi ideology and is not a genuine nation-state. Propaganda images and videos on platforms like Instagram and Telegram depict Ukrainian symbols alongside Nazi iconography, aiming to discredit Ukraine internationally (Mihanski, 2024).

Russia's discourses necessitate constant dynamism, requiring substantial number of social media users for effective dissemination. Some mechanisms have been developed to meet this need and support Russia's information conflict operations: Trolls and Bots (Ibid.). Nevertheless, the propaganda messages spread from these troll and bot accounts will be examined in detail in the cyber field.

4.2.3. Information- Technical Field: Cyberwarfare

Russian information confrontation policies are examined within two main domains: information-psychological and information technical. The realm of Information technical includes technical tools and systems for creating, transforming, transmitting, utilizing, and storing information. However, it is essential to note that information technical and information psychological are mutually supportive domains. As a result, both areas serve the same purpose, and efforts are made to spread Russia's propaganda and disinformation rhetoric.

Cyberweapons employed in the informational technical field are designed specifically to damage the enemy's infrastructure systems, data collection systems, smart phone systems, psychological structures, and military systems. Russia's deployment of these cyber weapons during the Ukrainian conflict not only neutralizes the adversary's control infrastructure but also causes the state and the army to completely demoralize and create an atmosphere of panic. The physical and psychological impact created by such low-cost weapons makes them a more favorable option compared to conventional weaponry (Lilly & Cheravitch, 2020).

Russia's information technology policies are shaped directly through

the conduits of cyber warfare. Leveraging computer technology, such attacks are carried out in order to gain superiority in information confrontation. This involves obtaining strategically significant military, economic, and political information, destroying military systems, transportation systems, and water supplies, and accessing pivotal documents such as denial of service (Rashid et al., 2021).

CERT-UA recorded 1,123 cyber-attacks attributed to Russia during the first six months of the conflict (Schulze & Kerttunen, 2023). The analysis of Russia's cyberattacks against Ukraine within the framework of four main objectives. Firstly, these aim to cause irreversible damage to Ukraine's data and systems, with long-lasting effects (Duguin & Pavlova, 2023). The aim is to spread this malware to European countries via Ukraine by deleting user data, programs, and hard drives through malicious software programs (Lin, 2022). Secondly, the attacks intend to disrupt Ukraine's services and operations. For instance, denial of service attacks targeting various Ukrainian websites, including the attack on the Ukrainian Ministry of Defense, can be evaluated in this context. Additionally, Russia's attacks against Starlink terminals are also prominent attacks in this field. Thirdly, these cyberattacks are encouraged for the purposes of data theft, exfiltration, surveillance, and intelligence gathering. Lastly, cyberattacks directed at shaping Ukraine's information space include social media campaigns. Propaganda messages disseminated through bots and troll accounts stand out as pivotal policy tools in Russia's approach.

Russia has been developing cyberattack policies in both defensive and offensive strategies for a long time. It is possible to examine Russia's attack cyber policies in the information technical field towards Ukraine in different categories. These categories can be divided into areas such as

communications, military, administration, energy, and social media. However, Russia's cyberattack experiences in cases such as Georgia, Estonia, and Crimea should be taken into consideration. These experiences indicate a concerted effort by Russia to adopt a more organized policy for cyberattacks against Ukraine.

Cyber Activity against Ukraine Military Systems

Russia's main goal is to neutralize Ukraine's combat power. Although there is no indication of direct cyberattacks on the Ukrainian military systems, Russia allegedly uses information warfare tools such as jamming to damage Ukraine's drone capabilities (Bateman, 2022). Forbes (2023) reports that Russia has developed the RP-377 jammer system and uses it against Ukraine's radio-controlled drones (Axe, 2023).

Cyber Activity against Ukraine Communication Systems

Russia has carried out various cyberattacks against the communication systems utilized by the Ukrainian army, government, and civilian population. The most prominent of these attacks is the Viasat Hack, which is claimed to have been conducted by GRU (Bateman, 2022). Viasat, an American company based in Italy, owns the KA-SAT communications satellite. Any attack on this satellite not only jeopardizes Ukraine but also poses a threat to the communication systems of all of Europe. Following the Viasat hacking incident, Starlink satellites were sent to Ukraine.

Another attempt was made to damage the country's communication networks by targeting the internet service provider Triolan, which plays a key entity in Ukraine's communication infrastructure, and the state-owned

telecommunications system Ukrtelecom (Security, 2022). These attacks were strategically designed to cause disruptions in the communication channels between the military and the administration, impeding regular operational processes.

Cyber Activity against Ukraine Administration Systems

Certain cyberattacks against Ukraine include allegations of cyberattacks aimed at disrupting the functioning of the state, disrupting the functioning of Ukraine's government websites and creating panic among the public. Noteworthy systems employed for such purposes encompass WhisperGate, HermeticWiper, and IsaacWiper. Although this wiper software seems to be well-intentioned systems that can encrypt free data, it is known that they are actually malicious software and aim to delete the system (Fendorf & Miller, 2024). According to Lewis (2022), Russia had employed these systems to target Ukrainian government websites prior to the commencement of the conflict. For instance, in January 2022, Russia was targeting Ukrainian government websites with malware such as WhisperGate (Lewis, 2022).

Cyber Activity against Energy Sector

As reported by Reuters (2023), Russia hacked Ukraine's power grid towards the end of 2022, causing electricity outages across various regions of Ukraine (Pearson, 2023). These attacks turn into physical interventions carried out by Russia and damage Ukraine's infrastructure. The main target of these attacks is to cause unrest within Ukraine and erode Ukrainian citizens' trust in the government (Microsoft's Digital Security

Unit, 2022).

Cyber Activity against Social Media

Social media has found its place as an important information confrontation tool in both information physiological and technical policies. In information psychology, social media is employed to disseminate propaganda. The systematic dissemination of propaganda is achieved by utilizing of troll and bot social media accounts by Russia. These accounts are typically anonymous and there is no information about who shared the content (Helmus et al., 2018). Assertions from Western media and literature claim that these troll and bot accounts are often organized by the St. Petersburg-based Internet Research Agency.

Actors of Cyber Attacks

One of the key players in these attacks conducted by Russia is GRU. The GRU has been organizing digital information operations against Ukraine since 2014. While the GRU generally leverages information for sabotage purposes, SVR uses the traditional method of stealing information to help the Kremlin understand Ukraine's strategies against Russia. Lastly, FSB, the successor of the KGB, possesses the authority to monitor data traffic in Russia and has significant authority in the field of information technology (Hakala & Melnychuk, 2021). In addition to these government services, several hacker groups, such as APT28, CyberBerkut, CyberCaliphate, Sandworm, APT29, and Turla APT, also carry out information operations in many different areas, such as Ukraine's infrastructure and computer network.

Russia has to protect itself from cyberattacks and improve its defense systems because it is in an environment where such attacks may cause possible security problems. Especially during the period of destabilization marked by the color revolution, Western efforts and uprisings posed a risk to the stability of the regime in Russia. To prevent a recurrence of such an experience, it has taken precautions to protect itself against cyberattacks. These measures were made possible by specific legal regulations, such as the Yarovaya Law adopted in 2016, which mandates that every data flow within Russia's territory must be within the knowledge of the Russian special service. For instance, Russian special services will have unlimited access to the data and activities of individuals using Facebook and Google in Russian territory (Topor & Tabachnik, 2021).

As a result, in this section, the background of the Ukraine-Russia conflict and Russia's information warfare policies are examined. The historical and political roots of the conflict, Russia's strategic moves towards Ukraine and information warfare methods are comprehensively discussed. As a result, Russia implemented policies in many areas during the information war against Ukraine and the complex structure of these policies was revealed. These policies, in the Ukraine-Russia situation, will increase Russia's ability to gain legitimacy as a result of influencing international public opinion and turning it in its favor.

5. CHAPTER 5: CONCLUSION

The thesis was examined in three main chapters to answer the research question "*What are the key elements of Russian information warfare policies in the context of Ukrainian Conflict*?" In the second chapter, "Conceptual Framework of Information Warfare", the theory of information warfare is discussed with a comprehensive definition, taking into account the works of different researchers. In this direction, Information Warfare theory has been tried to be explained with definitions made by various scholars. The aim of this is that the information warfare theory should not be evaluated from only one perspective. This new discipline is broad, dynamic and complex. Although information warfare has found a field of study in many different fields due to its multidisciplinary nature, it has not had a common definition accepted by everyone. The aim of the second chapter of this study, the conceptual objective of the information warfare, is to deepen the understanding of information warfare by including its different definitions. Hence, the definition formulated by DoD was undertaken in the study, and explaining the two types of information warfare, offensive and defensive. Subsequently, Winn Schwartau's Information Warfare theory, which examined it into three different classes, was delineated. Schwartau's theory of Information Warfare Class I: Personal, Class II: Corporate and Class III: Global, is explained. Furthermore, it is noteworthy to emphasize that Toffler & Toffler divided the history of warfare into three and called the new era together with the information revolution as information wave. Martin C. Libicki introduced seven forms of information warfare, namely Command and Control Warfare (C2W), Intelligence-Based Warfare (IBW), Electronic Warfare (EW), Psychological Warfare (PW), Hacker

Warfare (HW), Economic Information Warfare (EIW), Cyberwarfare (CW). The study also highlighted the four information warfare strategies developed by C. Kopp: Degradation or Destruction (Denial of Information) (DoI), Corruption (Deception and Mimicry) (D&M), Denial (Disruption and Destruction) (D&D), Denial (Subversion) (SUB). This chapter emphasizes that information warfare should not be limited only as a concept but should also be considered in the context of various strategies and applications. Information warfare, unlike traditional warfare methods, is a new era warfare style that can be effective at both individual and global levels by levering technological advancement. The contributions of many scholars' thinkers mentioned above offer an important perspective to the understanding of this new form of warfare.

The war tools that have changed with the development of technology and the weapons used in information warfare have been described. The use of these weapons has created a new debate in the international arena about the legal status of information warfare. For this reason, it has become necessary to determine the legal status of information warfare, to update international legal norms and to take into account the effects of technology on the battlefield. The current international law framework focuses on the concept of conventional warfare and cannot fully cover the effects of information warfare, and the methods used in this warfare. This situation reflects the need for an international legal regulation.

In summary, the conclusion reached in the definition of information warfare is "*Information warfare is the struggle to ensure information superiority over the opposing party. The weapons and strategies used in this struggle are as diverse, and therefore, it is not possible to examine information warfare with a single dynamic*."

The second part of the thesis, titled "Russian Information Warfare

Policies," comprises a study to understand Russia's information warfare policies under three main headings. Russia's information warfare policies have become an important tool that has begun to find its place in international relations. Information warfare has become not only a military strategy for Russia but also an important tool to spread its own discourse. Thus, examining Russian information warfare policies both in historical context and in the light of today's developments is important to understand their impact on dynamics in the international order of Russia. This study investigates Russia's conceptualization of information warfare within its own literature. Within this context, the utilization of the term "information confrontation" instead of "information warfare" has garnered attention. Although information confrontation is the same as the definition of information warfare, it is discussed from two distinct perspectives in Russian literature. The first perspective, termed "information-technical," encompasses attacks directed at disrupting destroy electronic networks. The second perspective, termed "Information- Psychological," aims to influence the adversary's behavior through manipulation of information. Furthermore, Russian information warfare terminology bears resemblances to American terminology, but exhibits certain nuances. For instance, the term "information environment" is used as the equivalent of "information sphere" in Russian terminology.

The tools used by Russia in the field of informational warfare have been examined across four different domains: physical, informational, software-technical and radio-electronic. In the physical domain, the aim in to disturb the adversary's communication networks. Within the informational domain, the objective is to influence public opinion through media manipulation. The software-technical domain involves the

interception of enemy communications using computer systems. Lastly, in the domain of radio-electronics, the aim is to transmit information to people who will be manipulated by methods such as radio. Information warfare in Russia is employed by both state and non-state entities.

When Russia's information warfare policies are examined from historical antecedents and evaluated through events such as the Ukrainian conflict, it becomes more understandable how these policies are shaped and implemented. The aforementioned conflict serves as a pivotal case study, underscoring the impact of Russia's information warfare policies and providing valuable perspectives into their efficacy.

The examination of Russian policies spans distinct historical epochs including pre-Soviet, Soviet period, post-Soviet and 21st Century period. Prior to the Soviet Union, Russian information warfare policies carried out under the name of "spetsprop". During this period, the strategic manipulation of information emerged as a cornerstone tactic to achieve defined objectives. Notably, in the Napoleonic wars, a policy of manipulation was followed by targeting German groups, claiming that it was unnecessary for them to fight for France, and positive results were achieved. This epoch not only witnessed policy formulation but also underscored the strategic use of information as a pivotal aspect of Russian statecraft. However, information warfare became more organized during the Soviet period. The reason for this situation is that America tried to break the Soviets' sphere of influence by using propaganda tools on Communist countries. Thereupon, policies such as "reflexive control" in the 1950s and "active measure" in the 1960s were developed and the aim was to sabotage the ideological integrity of adversaries. Throughout the Soviet era, the primary focus of information manipulation centered on countering perceived pro- American ideological adversaries. Policies

were strategically crafted and executed to undermine the influence of these targets through deliberate information manipulation. After the disintegration of the Soviet Union and the perception of the West prevailing in the propaganda war, some intellectuals embarked on theorizing the trajectory that post- Soviet Russia should pursue. The most famous of these are Eveny Messner's theory "subversion-war", Aleksandr Dugin's "concept of net-centric war" and Igor Nikolaevich Panarin's "concept of information warfare". These three intellectuals share the common prediction that the anti- Western information warfare would persist beyond the dissolution of the Soviet Union. Moreover, they underscored the necessity for Russia to anticipate and ready itself for such ongoing ideological conflicts.

As a result of the developments in the 21st century, Russia has introduced a new theory, "gibridnaya voyna", which it developed in parallel with America's "hybrid warfare". Events such as Color Revolutions, Georgia War, Arab Spring and Annexation of Crimea, American elections, and the global pandemic have pushed Russia to more security-oriented policies. In particular, Russia has developed some discourses as an outcome of the West's aggressive policies towards the former Soviet areas through NATO and the EU.

In addition to historical developments, these policies developed by Russia are revealed concretely through the doctrines it publishes. Throughout Russia's history, numerous doctrines have been published, elucidating its policies. Foremost among these is the "Information Space Activities Concept," which comprehensively addresses information security. This Concept draws attention to external threats to Russia and emphasizes the imperative of safeguarding its information security to thwart attempts by adversaries to manipulate the Russian populace

through disruptions in the normal flow of information. Another significant doctrine regarding information security is Russia's Military Doctrine. This doctrine is comprehensive and explains threats to Russia's security on many different issues. Information security is discussed under different headings in the doctrine. For instance, it highlights that the manipulation of information by foreign powers contravenes international law and undermines the sovereignty of nations.

Strategies of national security of Russia offers a comprehensive overview on Russia's overarching national strategies. One of the most significant points of the published strategies is the evolving perspective on information security, evident in two different documents released in 2015 and 2021. While information security was briefly discussed in 2015 document, it is delineated as a separate and prominent topic in the 2021 document. This evolution underscores the increasing significance accorded to information security within Russia's strategic framework over time. Notably, unlike previous doctrines, the 2021 document explicitly identifies westernization as a perceived threat.

The Doctrine of Information Security, another pivotal document, addresses four primary issues: the nation's interests in the information domain, significant information- related threats alongside the current status of information security, overarching goals and fundamental approaches to safeguarding information security, and the institutional structures that support information security. In this doctrine, Russian institutions dealing with information security are explained in detail and the limits of information security are determined. The main threats identified include compromising Russia's territorial integrity, the unlawful use of information against the Russian people, and the proliferation of cybercrimes. Finally, some evaluations are made on

information security in the Foreign Policy Concepts published by Russia. It can be seen that this issue is addressed more sensitively in the last foreign policy concept published in 2023. While Russia initially interpreted information warfare through the lens of soft power, there has been a shift towards a more assertive stance, particularly characterized by the acknowledgment of "information space as new spheres of military action" in 2023.

These discourses can be briefly summarized as follows: Russia is trying to restore its destroyed strong image by expanding its sphere of influence lost in the aftermath of the Soviet collapse. For this reason, it aims to achieve this goal by developing common discourses such as "common religion, language, race" particularly within the Soviet regions. By completely rejecting Western values and demonizing them, Russia seeks to ensure the status of Russian values in the former Soviet regions, thus ensuring their resurgence in prominence. It can be said that both Russia's historical process and the policies put forward through doctrine and strategic documents are a reflection of Russia's efforts to protect its national security and sovereignty.

The final chapter of the thesis, titled "Russian Information Warfare Policies in Ukraine Conflict", provides a summary of the topics discussed in the previous two chapters. The Russia-Ukraine conflict is regarded as being one of the largest and most significant examples of efficient information warfare policies. In this regard, the last part, a detailed examination of Russia's information confrontation policies against Ukraine was made, divided into two as info-psychological and info-technical.

In the field of info-psychological, Russia's information warfare policies in Ukraine focus on psychological impact and perception

management. It has been observed that Russia is attempting to have an impact the perception of the public and the international community in Ukraine by using methods such as propaganda, manipulation and provocation. Within this field, it has been examined as Kremlin Rhetoric and social media. The Kremlin's rhetoric, as conveyed by Putin in his addresses to the nation on February 22nd and 24th, entails the announcement of the underlying reasons for the forthcoming conflict with Ukraine to both the Russian domestic audience and the international community. The points emphasized in these speeches are summarized in table 3. Another information-psychological area has been identified as social media. This is because information spreads very quickly through social media. Russia has taken care to spread its discourse through both Russian-based media outlets and international-based platforms, leveraging social media channels to serve its own interests.

In the field of information technical, Russia's information warfare strategies against Ukraine tried to gain superiority by damaging Ukraine's communication networks through cyber operations. Russia's cyber-attacks on Ukraine's systems have been examined in different areas. These include Ukraine Military Systems, social media, Energy Sector, Ukraine Administration Systems and Ukraine Communication System. These cyber-attacks were carried out with the aim of weakening Ukraine's defense capabilities, blocking communication networks and creating chaos in society. With these attacks, Russia tried to neutralize Ukraine's military operations, increased propaganda on social media, created disruptions in the energy sector and intervened in Ukraine's management systems. These attacks represent the technical side of Russia's information warfare strategies and are aimed at destabilizing Ukraine.

Based on these investigations, Russia's information warfare policies

concerning Ukraine characterized by a comprehensive and assertive approach. Russia constantly ignores Ukraine's sovereignty and tends to reject its status as an independent state, instead seeking to portray it as an integral part of Russia. While the West is trying to create a natural border with Russia by using Ukraine as a buffer zone against Russia, Russia opposes this situation. This stance reflects Russia's perception of NATO and the EU's particularly involvement in Ukraine as expansionist threats aimed at undermining its regional power. Consequently, Russia seeks to counteract and thwart these efforts to safeguard its geopolitical interest.

Russia emphasizes shared elements such as common religion, language and ethnicity to counter Western propaganda in Ukraine. It disseminates claims that Ukrainian leaders are e pro-Western and sympathetic to neo-Nazi ideologies, while also leveling accusations of corruption within the country's governance structure. Russia is trying to spread the image that a pro-Western government governs Ukraine by using the power of social media to its advantage. This includes narratives depicting Ukraine as under the influence of Western-backed forces, as well as portraying the West as evil enemy against the Russian people.

To protect Russia's reputation, publications are being made in English on international platforms stating that Russia is right in the Ukraine-Russia conflict. Additionally, Russia organizes cyber-attacks to intimidate Ukraine, blocks the flow of information by targeting communication systems, prevents access to accurate information by hacking state websites, and personal information of Ukrainians is seized.

In conclusion, there are changes in the current and future geopolitical structure of the world. These changes occur together with factors such as increasing economic difficulties and immigrant crises, which are exerting significant pressure on the established status quo in Europe and America.

For this reason, the people of America and Europe are apprehensive about the necessity of becoming a party to the conflict, and this can be considered a positive development for Russia's interests. The presence of signals suggesting a prolonged conflict implies that sustaining economic and military support for Ukraine will pose challenges for external backers. This situation may create a sense of despair among the people of Europe and America. The prolongation of the conflict can be construed as an advantageous situation for Russia's interests. In the Russia-Ukraine information warfare war, the discourse spread by Russia that Ukraine is weak and isolated, relying on the support of Europe and America, finds a response within the international arena over time. Issues such as Zelensky's loneliness on social media and the recruitment of disabled individuals due to the lack of soldiers are also supporting these discourses and serving Russia's interests. The high tension between Palestine and Israel diverts attention from Ukraine, which is positive development for Russia. Additionally, Putin and Russia's persistent resistance against America and European states contributes to Russia's prestige in the region, representing another favorable outcome. Accordingly, without specifying any side, it can be asserted that Russia has effectively employed information warfare policies in this conflict in its own favor and in accordance with its interests.

BIBLIOGRAPHY

Alberts, D. S. (1996, January 1). *Defensive Information Warfare*. National Defense University Press.

Aldrich, R. W. (1996). *INSS Occasional Paper 9 Information Warfare Series: The International Legal Implications of Information Warfare* (p. 3). USAF Institute for National Security Studies, US Air Force Academy, Colorado.

Anderson, A.D. (2018). *The Sources of Russian Information Warfare*. (Master's thesis). School of Advanced Air University, Maxwell Air Force Base, Alabama.

Anthony, K. D. (1997). Information Warfare: Good News and Bad News. *Military Intelligence Professional Bulletin*. https://irp.fas.org/agency/army/mipb/1997-1/anthony.htm

Army Cyber Institute at West Point. (2020). *Invisible Force: Information Warfare and the Future of Conflict* (Introduction by P.W. Singer & August Cole, p. 39).

Aronova, E. (2017, September 1). Russian and the Making of World Languages during the Cold War. *Isis, 108*(3), 643–650. https://doi.org/10.1086/694163

Averre, D. (2019, September 25). Russia's 'Strategic Narratives': The Case of Syria and the 'Arab Spring.' *Вестник Удмуртского*

Университета. Социология. Политология. Международные Отношения, 3(3), 317–325. https://doi.org/10.35634/2587-9030-2019-3-3-317-325

Axe, D. (2023, December 22). *More And More Russian Vehicles Have Drone-Jammers. Ukrainian Drones Blow Them Up Anyway.* Forbes. https://www.forbes.com/sites/davidaxe/2023/12/22/more-and-more-russian-vehicles-have-drone-jammers-ukrainian-drones-blow-them-up-anyway/?sh=1b2baff776d7

Barkham, J. (2001). *Information Warfare and International Law on the Use of Force. Vol. 34*, 57, 108.

Bateman, J. (2022). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influence, and Implications.* Carnegie Endowment for International Peace. Working Paper.

Bojor, L., & Cîrdei, A. (2022, December 1). The Challenges of Social Media Platforms. Aspects of the Social Media War in Ukraine 2014-2022. *Land Forces Academy Review, 27*(4), 296–301. https://doi.org/10.2478/raft-2022-0037

Bryczek-Wróbel, P., & Moszczyński, M. (2022). The Evolution of the Concept of Information Warfare in the Modern Information Society of the Post-Truth Era. *Defence Science Review*, No. 13, p.50.

Center for Strategic & International Studies (CSIS). (2011). *What does the Arab Spring mean for Russia, Central Asia, and the Caucasus?* (A.

Zikibayeva, Ed., S. Korepin & S. Shara, Rapporteurs).

Charap, S., & Colton, T. J. (2017). *Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post- Soviet Eurasia.* Routledge.

Chayka, K. (2022, March 3). *Ukraine Becomes the World's "First TikTok War."* The New Yorker. https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war

Chesnut, M. (2023). *US/NATO- Russian Strategic Stability and the War in Ukraine* (Occasional Paper). CNA Corporation.

Church, W. (2000). *Information Warfare. IRRC March*, Vol. 82, No. 837, p. 213.

Connell, M., & Vogler, S. (2017, March). *Russia's Approach to Cyber Warfare.* CNA Analysis & Solutions

Crawford, G. (1997, December 3). *Information Warfare: New Roles for Information Systems in Military Operations,* DTIC. https://apps.dtic.mil/sti/citations/ADA332446

Ciuriak, D. (2022, April 8). *The Role of Social Media in Russia's War on Ukraine.* Commentary. Ciuriak Consulting Inc.

Ciuriak, D. (2022). NATO's Role in the Russia- Ukraine Conflict: An Analysis. *International Security, 46*(1), 97-119.

Cuiriak, D. (2023, October 25). *NATO's Enlargement and Russia's Interest: Existential Threat or Invaluable External Dicipline?* [Policy Commentary]. Cuiriak Consulting INC. https://ssrn.com/abstract=4202776

Damjanovic, D. (2017). Types of information warfare and examples of malicious programs of information warfare. *Vojnotehnicki Glasnik, 65*(4), 1044–1059. https://doi.org/10.5937/vojtehg65-13590

Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* Warsaw: Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study

Darczewska, J., & Żochowski, P. (2017). *Active Measure: Russia's Key Export* (p.21). Point of Wiew, 64, Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia

DeCaro, C. (1994). *Sats, Lies, and Video-Rape: The Soft War Handbook*. AEROBUREAU Corporation.

DeVries, A. D. (1997). *Information Warfare and Its Impact on National Security*, 1-17.

DiResta, R., Shaffer, E., Ruppel, B., & Sullivan, D. (2018). *The Tactics and Tropes of the Internet Research Agency.* New Knowledge.

Douai, A. (2019). Global and Arab Media in the Post-truth Era:

Globalization, Authoritarianism, and Fake News. In *Mediterranean Yearbook 2019* (Chapter Title: Dossier: Social Movements, Digital Transformations and Changes in the Mediterranean Region).

Dugin, A., & Pavlova, I. (2023). Hybrid Warfare and Information Confrontation: The Russian Perspective. *Military Review, 103* (1), 112-128.

Dugin, S., & Pavlova, P. (2023, September). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict.* Workshop requested by the SEDE Subcommittee.

Elam, D. E. (1996). *Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare* (master's thesis). Naval Postgraduate School, Monterey, California.

Embassy of the Russian Federation in the Kingdom of Thailand. (2014). Military Doctrine of the Russian Federation (Unofficial Translation). Approved by the President of the Russian Federation. https://thailand.mid.ru/en/o_rossii/vneshnyaya_politika/voennaya_doktrina_rf/

Eriksson, E. A. (1999). Information Warfare: Hype or Reality? *Nonproliferation Review, VIEWPOINT.*

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International*

Political Science Review, 27, 221. doi:10.1177/0192512106064462

Euromaidan Press. (2020). *A guide to Russia propaganda. Part 5: Reflexive Control.* https://euromaidanpress.com/2020/03/26/a-guide-to-russian-propaganda-part-5-reflexive-control/

RT International. (2024). *Ex-Ukrainian president to pay for restoration of Nazi SS man's house*. https://www.rt.com/russia/590039-poroshenko-nazi-museum-restoration/

Fedchenko, Y. (2016). Kremlin Propaganda: Soviet Active Measures by Other Means. *Sõjateadlane (Estonian Journal of Military Studies)*, 2, 141-170.

Fendorf, K & Miller, J. (2022, March 24). *Tracking Cyber Operations and Actors in the Russia-Ukraine War.* Council on Foreign Relations. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

Floridi, L., & Taddeo, M. (2014, March 25). *The Ethics of Information Warfare*. Springer Science & Business Media.

Sputnik International. (2023, December 27). *Former US Marine: West Can't Grasp Russia's Technological Supremacy on Battlefield.* https://sputnikglobe.com/20231227/former-us-marine-west-cant-grasp-russias-technological-supremacy-on-battlefield-1115842989.html

Fitzpatrick, S. (2008). *The Russian Revolution.* Oxford University Press.

Figes, O. (1996). *A people's Tragedy: The Russian Revolution 1891-1924*. Viking.

Franke, U. (2015, March). *War by non-military means: Understanding Russian Information Warfare.* Totalförsvarets Forskningsinstitut (FOI). Stockholm, Sweden. http://arks.princeton.edu/ark:/88435/dsp019c67wq22q

Fraser, C. (2022, November 3). *How Russian Disinformation Tactics* Institute for Development of Freedom of Information (IDFI). (N.d.). *Were Utilised in the Context of the 2008 5-day War.* https://idfi.ge/en/how_russian_disinformation_tactics_were_utilised_in_the_context_of_the_2008_5_day_war

Fridman, O. (2017, August 3). The Russian perspective on information warfare: conceptual roots and politicisation in russian academic, political, and public discourse. *Defence Strategic Communications, 2*(1), 61–86. https://doi.org/10.30966/2018.riga.2.3

Fridman, O. (2018, August 1). *Russian "Hybrid Warfare."* Oxford University Press.

Fridman, O., Kabernik, V., & Pearce, J. C. (2018, October 31). *Hybrid Conflicts and Information Warfare*. Lynne Rienner Publishers.

Gallaher, B., & Kalaitzidis, P. (2022, June 7). A Declaration on the "Russian World" (Russkii Mir) Teaching. *Mission Studies, 39(*2), 269–

276. https://doi.org/10.1163/15733831-12341850

Giles, J., & Hagestad, W. (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins et al (Eds.), *5th International Conference on Cyber Conflict.* CCDCOE, Tallinn. https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

Giles, K. (2016). *"Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power."* Chatham House.

Giles, K. (2016, January 1). *Handbook of Russian Information Warfare.* NATO Defense College "NDC Fellowship Monograph Series." http://books.google.ie/books?id=sSddtAEACAAJ&dq=HANDBOOK+OF+RUSSIAN+INFORMATION+WARFARE&hl=&cd=1&source=gbs_api

Goldstein, F. L., & Findley, B. F. (1996, January 1). Psychological Operations. http://books.google.ie/books?id=AlyLDAEACAAJ&dq=Psychological+Operations+Principles+and+Case+Studies&hl=&cd=2&source=gbs_api

Goudimiak, I. (2016). *Justifying War in Ukraine: An Analysis of Speeches, Excerpts and Interviews by Vladimir Putin* (Master's Thesis). McAnulty Graduate School of Liberal Arts, Duquesne University.

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). *Information Warfare and International Law.* National Defense University Press. p. 19.

Grisé, M., Demus, A., Shokh, Y., Kepe, M., & Welburn, J. W. (2022, August 18). *Rivalry in the Information Sphere.* RAND Corporation. http://books.google.ie/books?id=vgxXzwEACAAJ&dq=HOLYNSKA+Rivalry+in+the+Information+Sphere&hl=&cd=1&source=gbs_api

Grisé, M., Shokh, Y., Holynska, K., & Demus, A. (2022, August 18). *Russian and Ukrainian Perspectives on the Concept of Information Confrontation.* RAND Corporation.

Guttman, B., & Roback, E. A. (1995, April 1). *An Introduction to Computer Security.* DIANE Publishing.

Göransson, M. B. (2022, October 20). Russian scholarly discussions of nonmilitary warfare as securitizing acts. *Comparative Strategy, 41*(6), 526–542. https://doi.org/10.1080/01495933.2022.2130675

Haeni, R. E. (1997). *Information Warfare: An Introduction* (pp. 3-15). Washington, DC.

Hakala, J., & Melnychuk, J. (2021). *Russia's Strategy in Cyberspace.* Riga: NATO Cooperative Cyber Defence COE. ISBN: 978-9934-564-90-1.

Harvard Cybersecuriy. (2024). *Cybercrime.* Retrieved from https://cyber.harvard.edu/

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to*

2012. Cyber Conflict Studies Association.

Hecimovic, A. (2022, October 19). *Seven Decades of Soviet Propaganda – in Pictures.* the Guardian. https://www.theguardian.com/world/gallery/2014/jun/09/soviet-propaganda-art-posters-in-pictures

Helmus, T. C., Bodine- Baron, E., Radin, A., Magnus, M., Mendelson, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe.* RAND Corporation. ISBN: 978-0-8330-9957-0.

Hoffman, F. G. (2007, December). *Conflict in the 21st Century* (p. 14). Potomac Institute for Policy Studies. http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf

Hopkins, M. (2020, October 29). *Disinformation That Kills: The offExpanding Battlefield of Digital Warfare.* CB Insights Research. https://www.cbinsights.com/research/future-of-information-warfare/

Hou, S. M., Fu, W. C., & Lai, S. Y. (2023). Exploring Information Warfare Strategies during the Russia–Ukraine War on Twitter. *The Korean Journal of Defense Analysis, 35(*1), 19-44. https://doi.org/10.22883/kjda.2023.35.1.002

Hudson, G. E., Mitropol'skii, A. B., Smirnov, P. E., Zagorskii, A., & Lucas, M. (1994, October). Russia's Search for Identity in the Post-Cold War World. *Mershon International Studies Review, 38*(2), 235.

https://doi.org/10.2307/222716

Huntington, S. P. (1993). The Clash of Civilizations? *Foreign Affairs, 72*(3), 22-49. https://doi.org/10.2307/20045621

Iasiello, E. J. (2017, June 1). Russia's Improved Information Operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters, 47*(2). https://doi.org/10.55540/0031-1723.2931

Intelligence Community Assesment. (2017, January 6). *Assessing Russian Activities and Intentions in Recent US Elections* (ICA 2017- 01D).

Kalinovsky, A. M., & Daigle, C. (2014, June 5). *The Routledge Handbook of the Cold War.* Routledge.

Khaldarova, I. (2019, May 29). Brother or 'Other'? Transformation of strategic narratives in Russian television news during the Ukrainian crisis. *Media, War & Conflict, 14*(1), 3–20. https://doi.org/10.1177/1750635219846016

Kolbe, P. (2022). How Russian history- and human psychology- can explain the crisis in Ukraine. In S. A. Hughes (Ed.), *Harvard Kennedy School's Belfer Center for Science and International Affairs*. Retrieved from https://www.hks.harvard.edu/faculty-research/policy-topics/international-relations-security/how-russian-history-and-human

Kopp, C. (2000). Information Warfare: A Fundamental Paradigm of Infowar. *Systems: Enterprise Computing Monthly,* Auscom Publishing

Pty Ltd, Sydney, Australia, 46-55.

Kopp, C., & Mills, B.I. (2002). Information Warfare and Evolution. In *Proceedings of the 3rd Australian Information Warfare & Security Conference*, ECU, Perth, pp. 352-360.

Kopp, C. (2003). Shannon, Hypergames and Information Warfare. *Journal of Information Warfare, 2*(2), 108-118.

Kopp, C. (2005). *The Analysis of Compound Information Warfare Strategies.*

Kotkin, S. (2014). *Stalin: Volume I: Paradoxes of Power, 1878-1928.* Penguin Press.

Kowalski, M. (2022, November 8). Determinants of Ukraine's geopolitical orientation. *Czasopismo Geograficzne, 93*(3), 435–450. https://doi.org/10.12657/czageo-93-17

Kozdra, M. (2018, February 28). The Boundaries of Russian Identity Analysis of the Concept of Russkiy Mir in Contemporary Russian Online Media. *Lingua Cultura, 12*(1), 61. https://doi.org/10.21512/lc.v12i1.2004

Kremlin.ru. (2022, February 21). *Address by the President of Russian Federation* [Web page]. Kremlin.ru. http://en.kremlin.ru/events/president/news/67828

Kremlin.ru. (2022, February 24). *Address by the President of Russian Federation* [Web page]. Kremlin.ru.

http://en.kremlin.ru/events/president/news/67843

Kumar, S., & Kafi, A. H. (2015). The Heartland Theory of Sir Halford John Mackinder: Justification of Foreign Policy of the United States and Russia in Central Asia. *Journal of Liberty and International Affairs, 1*(2).

Kux, D. (1985, July 4). Soviet Active Measures and Disinformation: Overview and Assessment. *The US Army War College Quarterly: Parameters, 15*(1). https://doi.org/10.55540/0031-1723.1388

Johnson, B. D., Draudt, A., Brown, J. C., Ross, L. C., & Coon, C. (2019). *Information Warfare and the Future of Conflict* (Technical Report, pp. 51-55). Retrieved from Arizona State University website.

Johnson, P. A. (2002). *Is It Time for a Treaty on Information Warfare?* In M. N. Schmitt & B. T. O'Donnell, (Eds.), *International Law Studies, 76*, 442.

Late, J. (2023, February 4). Desert Storm 30: SEPECAT Jaguars in the 1991 Gulf War. Key. Aero. Retrieved from https://www.key.aero/article/desert-storm-30-jaguars-over-gulf

Lange-lonatamišvili, E. (2015). *Analysis of Russia's Information Campaign Against Ukraine.* NATO StratCom Centre of Excellence (COE), Riga)

Lewis, J. A. (2022, October 13). *Cyber War and Ukraine*. https://www.csis.org/analysis/cyber-war-and-ukraine

Libicki, M. C. (1995, January 1). *What is information warfare?* National Defense University.

Lilly, B., & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. In T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.), *20/20 Vision: The Next Decade* (pp. 129-155). NATO CCDCOE Publications, Talinn.

Lin, C. (2022). Cyber Warfare in the Digital Age: The Case of Russia and Ukraine. *Journal of Information Security, 10*(2), 45-67.

Lin, H. (2022). Russian Cyber Operations in the Invasion of Ukraine. *The Cyber Defense Review, 7*(4), 31-46. Army Cyber Institute. https://www.jstor.org/stable/10.2307/48703290.

Liu, P., & Jajodia, S. (2013, March 14). *Trusted Recovery and Defensive Information Warfare.* Springer Science & Business Media.

Łukasik, P. (2020). *Between Digital Elections and the Information War: Post-truth, New Media and Politics in the 21st Century*. Historia i Polityka, *34*(42), 75-92. doi:10.12775/HiP.2020.037

Maitra, S. (2021). NATO Enlargement, Russia, and Balance of Threat. *Canadian Military Journal, 21(*3), Summer. https://doi.org/10.2139/ssrn.3887828

Mărășoiu, E. (2023, April 11). Considerations on the role of information

(-psychological) operations in Russian military thinking. *Bulletin Of "Carol I" National Defence University, 12*(1), 7–18. https://doi.org/10.53477/2284-9378-23-01

Mearsheimer, J. J. (2014). Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin. *Foreign Affairs, 93*(5), 77-84. https://www.foreignaffairs.com/articles/russia-fsu/2014-08-18/why-ukraine-crisis-west-s-fault

Mearsheimer, J. J. (2022). The Causes and Consequences of the Ukraine War. *Horizons, (21).* https://www.cirsd.org/en/horizons/horizons-summer-2022-issue-no.21/the-causes-and-consequences-of-the-ukraine-war

Melin, K. (2017). *A New Russian Idea? : Neo-Eurasianist Ideas in the Russian Presidential Addressesto the Federal Assembly 2014 – 2016*. DIVA. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1084876&dswid=-2091

Microsoft's Digital Security Unit. (2022, April 27). *Special Report: Ukraine- An overview of Russian's cyberattack activity in Ukraine.* Microsoft.

Mishankin, N. (2024, January 7). *Identification of Russian propaganda through social media.* URSS Showcase. https://urss.warwick.ac.uk/items/show/549

Mihanski, S. (2024). The Use of Trolls and Bots in Modern Information Warfare: A Russian Case Study. Cyber Defense Review, 12(1), 33-50.

Mullaney, S. (2022). Everything flows: Russian information warfare forms and tactics in Ukraine and the US between 2014 and 2020. *The Cyber Defense Review, 7*(4), 193-212. https://www.jstor.org/stable/48703300

Nelson, G. J. (2022, March). *Russian Influence in 2016 and 2020 U.S. Presidential Elections: A Cost-Benefit Analysis* [Master's thesis, Naval Postgraduate School- Monterey].

Nikitina, Y. (2014). The "Color Revolutions" and "Arab Spring" in Russian Official Discourse. *Connections: The Quarterly Journal, 14*(1), 87–104. https://doi.org/10.11610/connections.14.1.04

Nilsson, N. (2018). *Russian Hybrid Tactics in Georgia.* Silk Road Paper. Central Asia- Caucasus Institute and Silk Road Studies Program. ISBN: 078-91-88551-04-7.

Oates, S. (2020). *Revolution Stalled: The Political Limits of the Internet in the Post- Soviet Sphere*. Oxford University Press.

Oldberg, I. (2014). *Huntington's "Clash of civilizations" and Russia* (UI Brief #1). The Swedish Institute of International Affairs.

Oxford Dictionaries. (2016). *Word of the Year 2016.* https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-

2016

Qureshi, W. A. (2020). Information Warfare, International Law, and the Changing Battlefield. *Fordham International Law Journal, 43*(4), 901-938.

Pearson, J. (2023, November 9). *Russian spies behind cyber attack on Ukraine power grid in 2022. Reuters.* https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/

Pipes, R. (1990). *The Russian Revolution*. Vintage.

Pomerantsev, P., & Weiss, M. (2014). *The Menace of Unreality: How he Kremlin Weponizes Information, Culture and Money.* New York: Institute of Modern Russia. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly, 11*(4), 50-85. https://www.jstor.org/stable/10.2307/26271634

Prys, E. (2021). Soviet antifascism as main narrative of the Russian propaganda in hybrid warfare. *Polish Journal of Political Science, 7*(4), 52-71.

Rahim, S. (2020, June). Russian Geopolitics and Eurasia an Analytical

Study of Russia's Role in Eurasian Integration. *World Affairs, 24*(2), 90-104.

Rashid, A., Khan, A. Y., & Azim, S. W. (2021, June 30). Cyber hegemony and information warfare: A case of Russia. Liberal Arts and Social Sciences *International Journal (LASSIJ), 5*(1), 648–666. https://doi.org/10.47264/idea.lassij/5.1.42

Rid, T. (2020). *Active Measures: The secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux.

Robinson, P. A. (1992). Sneakers [Film]. Universal Pictures.

Russian Federation. (2015). *National Security Strategy* (Presidential Edict No. 683, December 31, 2015). Retrieved from https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Russian Federation. (2021). *Strategy of National Security of the Russian Federation* (Decree No. 400 of July 2, 2021) [Указ Президента Российской Федерации от 02.07.2021 г. № 400]. http://kremlin.ru/acts/bank/47046

Savage, P. (2017). *Russian Social Media Information Operations How Russia Has Used Social Media to Influence US Politics.* JSTOR. http://www.jstor.com/stable/resrep06042

Sazonov. V., & Müür, K. (2017). Russian Information Warfare Against

Ukraine I: Online News and Social Media Analysis. EMA Occasional Paper, (Issue No. 7), 69-101.

Security, C. C. F. C. (2022, July 14). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine - Canadian Centre for Cyber Security. Canadian Centre for Cyber Security.* https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine

Selvage, D., & Nehring, C. (2019, July 22). *Operation "Denver": KGB and Stasi disinformation regarding AIDS.* Wilson Center. https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids

Schulze, M., & Kerttunen, M. (2023, April). *Cyber Operations in Russia's War against Ukraine: Uses, limitations, and lessons learned so far* (SWP Comment No. 23). Stiftung Wissenschaft und Politik.

Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway* (1st ed.). Thunder's Mouth Press.

Schwartau, W. (1997). What Exactly Is Information Warfare? *Network Security*.

Snegovaya, M. (2015, September). *Putin's Information War in Ukraine* (Russia Report 1). Institute for the Study of War.

Sulaiman, R. (2000-2005). *Information Warfare* (Global Information

Assurance Certification Paper, pp. 1-11). SANS Institute.

Sun Tzu. (2005). *The Illustrated Art of War* (S. B. Griffith, Trans.). Oxford University Press, p.161.

TASAM. (2021). The Russian Federations's National Security Strategy of 2021: The increasing importance of Internal Security [Table]. https://tasam.org/en/Icerik/70118/the_russian_federations_national_security_strategy_of_2021_the_increasing_importance_of_internal_security

The Bleyzer Foundation. (2016). *Corruption in Ukraine and Recommendations* (TBF Report). https://bleyzerfoundation.org/tbf-reports

The Ministry of Defense of the Russian Federation. (2011). *Russian Federation Armed Forces's Information Space Activities.* https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

The Ministry of Defense of the Russian Federation. (2016). *Russian Federation Armed Forces' Information Space Activities Concept.* https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

The Ministry of Foreign Affairs of the Russian Federation. (2000, June 28). *Foreign Policy Concept of the Russian Federation.* https://www.bits.de/EURA/russia052800.pdf

The Ministry of Foreign Affairs of the Russian Federation. (2016, December 5). *Doctrine of Information Security of the Russian Federation.* http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2563163

The Ministry of Foreign Affairs of the Russian Federation. (2016, November 30). *Foreign Policy Concept of the Russian Federation.* https://interkomitet.com/foreign-policy/basic-documents/foreign-policy-concept-of-the-russian-federation-approved-by-president-of-the-russian-federation-vladimir-putin-on-november-30-2016/

The Ministry of Foreign Affairs of the Russian Federation. (2013, February 12). *Foreign Policy Concept of the Russian Federation.* https://www.voltairenet.org/article202037.html

The Ministry of Foreign Affairs of the Russian Federation. (2023, March 31). *Foreign Policy Concept of the Russian Federation.* https://mid.ru/en/foreign_policy/fundamental_documents/1860586/?TSPD_101_R0=08765fb817ab200013b0c2137837d9f21a2dacdb

The President of the Russian Federation. (2008, July 12). *Foreign Policy Concept of the Russian Federation.* https://russiaeu.ru/userfiles/file/foreign_policy_concept_english.pdf

The Russian Federation. (2000, September 9). *The Russian Federation Information Security Doctrine.*

Thomas, T.L. (1996). Russian Views on Information- Based Warfare.

Airpower Journal Special Edition.

Thomas, T. L. (2004, June). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies, 17*(2), 237–256. https://doi.org/10.1080/13518040490450529

Thomas, T.L. (2010). Russian Information Warfare Theory: The Consequences of August 2008. In S.J. Blank& R. Weitz (Eds.), *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald.* Strategic Studies Institute, US Army War College. https://www.jstor.org/stable/resrep12110.8

Thomas, T. (2015). Russia's Military Strategy and Doctrine. *The Journal of Slavic Military Studies, 28*(4), 445-459.

Thomas, T. (2015). Russia's 21st Century Information War: Working to undermine and Destabilize Populations. *Defense Strategic Communications, 1*(1), 11-26.

Thomas, T. L. (2020). Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice. *The Cyber Defense Review, 5*(2), 125-44. https://www.jstor.org/stable/26923527

Toffler, A., & Toffler, H. A. (1995). *War and Anti-War: Making Sense of Today's Global Chaos.* Grand Central Publishing.

Topor, L., & Tabachnik, A. (2021, April 30). Russian Cyber Information Warfare: International Distribution and Domestic Control. *Journal of*

Advanced Military Studies, 12(1), 112–127. https://doi.org/10.21140/mcuj.20211201005

Trifonov, R., Nakov, O., & Mladenov, V. (2018). *Artificial Intelligence in Cyber Threats Intelligence.* In *2018 International Conference on Intelligent and Innovative Computing Applications,* Plaine Magnien, Mauritius. URL: https://ieeexplore.ieee.org/document/8601235

U.S. Cyber Security Magazine. (2024). *Logic Bombs: How to Prevent Them.* Retrieved from https://www.uscybersecurity.net/logic-bombs/

Van Oorschot, P. C. (2021, October 13). *Computer Security and the Internet*. Springer Nature

Views and Re-Views: Soviet Political Posters and Cartoons | Medium: Posters. (n.d.). Retrieved November 18, 2023, from https://library.brown.edu/cds/Views_and_Reviews/medium_lists/posters.html

Waller, C. (2023). *The Global Far Right and the War in Ukraine Initial Reactions and Enduring Narratives* (Policy Brief). Global Center on Cooperative Security. https://www.jstor.org/stable/resrep48741

Walker, N. (2023, August 22). *Conflict in Ukraine: A timeline (2014 - eve of 2022 invasion)* [Research Briefing]. Commons Library. (CBP 9476)

Williams, L. (2018, December 1). Artificial intelligence - real war. *Engineering & Technology, 13(11), 66–69.* https://doi.org/10.1049/et.2018.1109

Wonjnowki, M. (2021, July, 4). *U.S. Democracy as the Target of Russian Secret Services* (Special Report, p.9). Warsaw Institute.

Wright, A. (2020, August 5). *The Future of Cyber Conflict | the Cove*. The Cove. https://cove.army.gov.au/article/future-cyber-conflict

Zabrodskyi, M., Watling, J., Danylyuk, O. V., & Reynolds, N. (2022, November 30). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February- July 2022*. Royal United Services Institute for Defence and Security Studies RUSI Special Report.

Zeitzoff, T. (2017, August 4). How Social Media Is Changing Conflict. *Journal of Conflict Resolution, 61*(9), 1970–1991. https://doi.org/10.1177/0022002717721392

Zenarmor. (2024). *What is Logic Bomb? Definition, Examples, and Prevention.* Retrieved from https://www.zenarmor.com/docs/network-security-tutorials/what-is-logic-bomb#what-is-a-logic-bomb

Šulc, V. (2023). *Vladimir Putin's Framing of the Russo- Ukrainian War: Exploration of the "Clash of Civilizations" Concept in Putin's Annexation Speech.* Thesis, Malmö University.

Информационная Война. (2023): In *Encyclopedia* of the Ministry Defense of the Russian Federation. https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5211