THE REPUBLIC OF TÜRKİYE

SOCIAL SCIENCES UNIVERSITY OF ANKARA

THE GRADUATE SCHOOL OF SOCIAL SCIENCES

CYBERWAR IN THE CONTEXT OF THE CHANGING CHARACTER OF WAR

Master's Thesis

HİLAL POLAT

INTERNATIONAL RELATIONS

DECEMBER 2023

THE REPUBLIC OF TÜRKİYE

SOCIAL SCIENCES UNIVERSITY OF ANKARA

THE GRADUATE SCHOOL OF SOCIAL SCIENCES

CYBERWAR IN THE CONTEXT OF THE CHANGING CHARACTER OF WAR

Master's Thesis

HİLAL POLAT

Prof. Dr. Murat YEŞİLTAŞ

INTERNATIONAL RELATIONS

DECEMBER 2023

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

UN	The United Nations
WMD	Weapons of Mass Destruction
UNDP	The Nations Development Programme
MPRI	Military Professional Resources Corporation
NGOs	Non-Governmental Organizations
DDoS	Distributed Denial of Service
PMSCs	Private Military and Security Companies
CNA	Computer Network Attack

ACKNOWLEDGEMENTS

First of all, I would like to offer my sincere thanks to my respected supervisor Prof. Dr. Murat Yeşiltaş, whose student I am happy to be, for his supervision and patience. His guidance and expertise helped me through all the stages while writing my thesis. I would like to express my gratitude to Prof. Dr. Nezir Akyeşilmen, who inspired my interest in the field of cyber security, for presenting new perspectives throughout my research and I owe speacial thanks to Prof. Dr. Gürol Baba, who helped me successfully complete my thesis with his construtive critism and his seminal feedback, and to all my other esteemed professors with whom I crossed paths throughout my education life and who have carried me to this day.

I am highly grateful to my beloved family as a whole for their unconditional support and love, particularly to my precious mother and father, who have supported me in every sense throughout my life. I would also like to sincerely thank my beloved husband who deserves the lion's share of my appreciation for his unwavering patience and loving support. Without his continuous understanding and encouragement, this thesis would not exist. I would like to express my gratitude towards my parents-in-law for their support in this process and finally, my little daughter Maria Hafsa, in whose eyes I see the endless sky, for giving me a ray of hope and strength to keep going even when things seem impossible.

''Do not fear failure but rather fear not trying.'' – Roy T. Bennett

Ankara, 2023

Hilal POLAT

ABSTRACT

Cyberwar in the Context of the Changing Character of the War

As a phenomenon that has existed for centuries, war has a variable character as well as structural and fixed features. With the end of the Cold War, the idea that the end of history had come, that the capitalist order would spread across the globe, wars would end and eternal peace would prevail was a great misconception, and while it was the old wars between states that ended, war itself relapsed in different manifestations (Münkler, 2010:190). In these emerging conflicts, the need for a new conceptualization arose with the realization that the structure of war, its means, its parties, in short, the character of war has undergone a serious transformation. 'New wars', 'Fourth Generation Wars' and other concepts with similar qualities have been introduced to the literature. The emergence of cyberspace with the developing technology after the Cold War is another phenomenon that has changed the character of war. Accordingly, the aim of this study is to understand the changes in the character of war and how cyber warfare has changed the character of war. Finally, the study also addresses the debate on the possibility that cyber warfare is changing the character of wars and that cyber warfare will replace conventional warfare in the future.

Keywords: Cyberwar, Cyber Warfare, Stuxnet, War, Character

ÖZET

Tarih boyunca savaş, hem dinamik bir karakter hem de sabit özellikler sergileyen, sürekli bir varlık olmuştur. Soğuk Savaş'ın sona ermesi, insanlığın ilerlemenin zirvesine ulaştığı, kapitalizmin dünya çapında hakimiyete kavuşacağı yönünde yanlış bir düşünceyi ateşlemiştir. Sonuç olarak savaşların sona ereceğine ve kalıcı barışın hakim olacağına inanılıyordu. Ancak bu inancın büyük ölçüde yanlış olduğu kanıtlandı; zira devletler arasındaki geleneksel savaşlar azalırken savaşın kendisi gelişip çeşitli biçim ve kisvelerde yeniden ortaya çıkmıştır (Münkler,2010:190). Bu farkındalık, önemli dönüşümlerden geçen savaşın yapısının, taktiklerinin, tarafların ve savaşın genel özünün yeniden anlaşılmasını gerektirmiştir. Sonuç olarak, bilimsel literatürde bu derin değişimleri kapsayacak ve aydınlatacak 'Yeni Savaşlar', 'Dördüncü Nesil Savaşlar' gibi terimler ve benzeri kavramlar ortaya çıkmıştır. Soğuk Savaş sonrası gelişen teknoloji ile beraber siber uzayın ortaya çıkışı savaşın karakterini değiştiren bir başka olgu olarak karşımıza çıkmaktadır. Bu doğrultuda savaşın karakterinde meydana gelen değişimleri ve siber savaşın savaşın karakterini nasıl değiştirdiğini anlamak, çalışmanın amacını oluşturmaktadır. Son olarak, siber savaşın, savaşların karakterini değiştirdiği ve gelecekte siber savaşın konvansiyonel savaşların yerini tutacağı ihtimaline dair olan tartışmalara da değinilmiştir.

Anahtar Kelimeler: Siber Savaş, Siber Harp, Stuxnet, Savaş, Karakter

CHAPTER I

1. INTRODUCTION

The concept of warfare, which has existed for as long as the history of mankind, has undergone transformations over time under the influence of political, economic, social and technological developments. However, it is in the aftermath of the Cold War and the Industrial, the Digital and the Information Revolutions that this evolution has become most pronounced, as the global order has experienced significant shifts and transformations and rapid changes have occurred in various fields, including warfare. When analyzing the wars that have taken place in the 21st century, it becomes evident that this new era, influenced by advancements in communication and transportation technology as well as globalization, possesses its own unique characteristics in comparison to previous periods. Researchers have used concepts such as 'new war', 'hybrid war', 'surrogate war', 'fourth generation war' and similar concepts to conceptualize these 21st century wars. Regardless of the term, it is evident that the character of war have been transformed in terms of its purpose, actors, target group, area/facade, method, economy, weapons used, beginning and end and symmetry.

The traditional security landscape, where it was clear who was a friend and who was an enemy, threats were concrete and visible, and strategies for combat were straightforward, has been replaced by an intricate security environment where uncertainty surrounds adversaries, threats are multifaceted and unpredictable, and new entities at both sub-national and international levels play a role. The distinction between war and peace, military and civilian, has become blurred, and concepts such as the front line, battlefield, conventional weaponry, and similar notions have undergone change and transformation. As a result of this transformation, the realm of conflict has expanded to encompass the entire world. Within this environment, non-state actors, including guerrilla fighters, special forces, terrorist organizations, private military companies, cyber criminals, and organized crime syndicates, have emerged as significant threats due to their enhanced capacity to employ force and access technologies that amplify their destructive capabilities. In this security landscape, the advancement of technology in the past century, along with the emergence of the internet and various communication tools, has made cyber space an essential aspect of everyday life. Consequently, this vast digital space has revolutionized nearly every sector in our society, such as banking, communications, security, energy and critical infrastructure etc., all of which now rely heavily on technology. The interconnectedness and interdependence of our modern world have heightened the capacity for cyber-related activities to exert a more prominent influence in achieving significant results with reduced risk and less traceability.

Especially after the Stuxnet attack, the possibility that cyber tools could be used to cause physical damage has initiated discussions that cyber wars have changed the character of war and cyber wars will replace conventional wars in the near future. Critics, often characterised as alarmists, have expressed

concern that the greatest threat of the future may come from cyberspace. This group has argued that cyber war has already begun and is already underway. In a study conducted by Benjamin B. Hatch (2018), an additional dimension is added to the understanding of cyber weapons. Hatch goes beyond the conventional understanding and categorizes a specific class of offensive cyber weapons that are specifically designed for destructive purposes as weapons of mass destruction (WMD). This classification raises concerns about the escalating threat posed by such destructive cyber weapons in the future joint operating environment and the potential consequences of these weapons in the physical realm.

Cyberspace's range, cost, accessibility, and range of effects undoubtedly have changed the character of war. The introduction of cyberwarfare as a military capability has been seen as a viable alternative to traditional physical warfare, primarily due to its low entry barriers, ability to transcend geographical boundaries, reduced risk to human life, covert maneuverability, and plausible deniability. These attributes have made cyberwarfare an attractive option for governments and militaries seeking to achieve their objectives without the high costs and risks associated with conventional warfare. However, it is important to recognize that cyber warfare cannot fully replace physical warfare, at least in the current security environment. There are multiple factors that need to align simultaneously for successful cyberwarfare to occur, making it a complex and challenging endeavor. Furthermore, the fact that adversaries can easily revert to conventional means of warfare at any given moment undermines the notion of cyberwar as a standalone concept. Recent instances of limited cyberwarfare have demonstrated that cyberattacks are always used in conjunction with other forms of warfare. However, it is crucial to note that due to the unique nature of cyberspace, it is impossible to accurately assess the cyber attack and defense capabilities of countries. As this field is relatively new, countries are still in the process of discovering their own capacities for cyber attacks and defense. Therefore, it remains uncertain what consequences cyber attack tools may bring and whether they have the potential to replace conventional wars in the future. With the continuous advancements in technology and the increasing reliance on digital systems, the question of the future role of cyber attacks and their impact on warfare continues to be perplexing, but it is certain that cyber warfare will continue to exist on the battlefield.

1.1. Problem Statement

During the post-Cold War era in academic studies, it was proposed that the conflict would persist in a different form following the end of the ideological struggle. This new dimension was referred to as the "clash of civilizations," and it was believed that the rival in this struggle would possess a structure that challenges traditional norms within the globalized system. Scholars argued that this shift in the character of the struggle would alter the way states engage in warfare, prompting authors to delve into a new phenomenon of war characterized by various terms.

Researchers, who have revealed that new generation wars differ from old generation wars in terms of purpose, actors, target group, area/facade, method, economy, weapons used, beginning and end and symmetry, have used concepts such as 'new war', 'hybrid war', 'surrogate war', 'fourth generation war' and similar concepts to conceptualize these wars. In the post-Cold War period, as a result of the rapid development of technology and the widespread use of information and communication tools and internet-based systems, cyber space has also been included in the battlefields. Especially after the Stuxnet attack, the possibility that cyber tools could be used to cause physical damage has initiated discussions that cyber wars have changed the character of warfare and will replace conventional wars in the near future. Accordingly, this study examines the transformations occuring in the character of war, with a particular focus on the impact of cyber warfare. It delves into the ways in which cyber warfare has transformed the traditional character of war. Additionally, the study delves into the ongoing discussion surroding the potentional for a singular cyber warfare to completely supplant conventional warfare in the future as the emergence of cyberspace has altered the character of traditional warfare.

1.2. Research Question

In order to make sense of these events, the study will try to answer five research questions.

1. What factors are changing the character of new wars?
2. What are the characteristics of new wars? In order to answer this question in more detail, 9 sub-questions were asked about how the aim, actors, target audience, field/aspect, method, economy, weapons used, start and end processes and symmetry of the war have changed.
3. How has the character of war changed over the generations?
4. What’s the place of cyber-warfare in the debate on the changing character of war? How does cyber-warfare change the character of war?
5. What do the discussions about the possibility of cyber war say in the context that cyber warfare changes the character of war?

1.3. Aim of the Study

At the point of deciding on the topic of this thesis, the effort to make sense of some events that occurred in international relations and were seen as extraordinary played an important role. Because in this process, we have witnessed attacks that were carried out not by bombs or missiles, but by means of a command screen on a computer, which no one can clearly attribute to these countries, and which, although virtual, can cause physical damage. Again, in this process, we have witnessed the processes of overthrowing their own governments by making their voices heard by wider masses with the help of the internet and social media, and how this has dragged a certain geography into civil wars with a domino effect.

It is crucial to comprehend the shifts occurring in the character of warfare and to thoroughly investigate this modern era of warfare, which deviates significantly from traditional methods, regardless of the terminology used. Such an understanding is essential to anticipate the types of threats that nations and societies may encounter and to reassess the organizational structure of military forces.

1.4. Stucture of the Thesis

In order to answer these questions, the first chapter focuses on the reasons for the emergence of the characteristics of today's wars. The second chapter focuses on the characteristics of new generation wars and how they differ from traditional wars. In order to answer this question in more detail, 9 sub-questions were asked about how the purpose, actors, target audience, area/aspect, method, economy, weapons used, start and end processes and symmetry of the war have changed, and tried to be answered in line with the arguments of academics and authors contributing to new generation war studies in the literature. Additionally, there is a section where the evolution of the character of warfare over the generations is analysed based on the significant work of Lind et al. called the 'The Changing Face of War: Into the Fourth Generationation'. The third chapter focuses on how cyber warfare has changed the character of war and the place and importance of cyber warfare in the debate on the changing character of war is analyzed. The 9 questions asked about the changing character of war were also asked for cyber wars and an attempt was made to find answers. Finally, the arguments arguing that cyber wars have changed the character of warfare and that cyber wars will replace conventional wars in the near future are analyzed. As a result, it is concluded that cyber warfare can be used as a force multiplier in conventional wars.

1.5. Methodology

The study was conducted using the qualitative research approach, as it was deemed appropriate and relevant for achieving its objectives. Extensive review of national and international literature, including books, articles, publications, and documents, was conducted to gather relevant information on the topic. The data gathered during the study were meticulously examined and interpreted in order to extract valuable insights. In order to reveal the data on the change in the character of war, 9 criteria were identified and a comparative analysis of old wars and new wars was conducted based on these criteria. For the question of how cyber wars have changed the character of war, a comparative analysis was carried out using the same 9 criteria and for this purpose, relevant cyber attack cases were included in the analysis.

CHAPTER II
What Changes the Character of War?

2. Reasons for the Change

Following the conclusion of the First World War, the disintegration of empires and the subsequent establishment of numerous nation states marked a significant shift in the global landscape. Similarly, in the aftermath of the Second World War, various countries seized the opportunity to assert their independence through the exercise of self-determination, as facilitated by the United Nations. Subsequently, the end of the Cold War brought about further changes, leading to a substantial increase in the number of states within the international system. However, this proliferation of states has not come without its challenges, as many of these newly formed entities have encountered difficulties in effectively fulfilling their fundamental functions. Consequently, the concept of a 'failed state' has emerged within the international community. Although these failed states may not pose a direct regional or global threat due to their internal shortcomings, they inadvertently create an environment conducive to the emergence of various threats, including terrorism, civil strife, poverty, and migration. These threats initially impact neighboring states, gradually extending their reach to the larger international system.The advent of globalization has given rise to an intricate web of interconnectedness, whereby any alteration or advancement within a single state can reverberate throughout the entire international system. Consequently, countries and international actors of today find themselves embroiled in the challenges faced by other nations. Specifically, regions plagued by internal instability and the inability to fulfill their core responsibilities have become hotspots for human rights abuses and numerous other issues, leading to an escalation of external interventions.

After the 1960s, when new states were established in Africa following the end of colonial rule, there was an initial sense of contentment among the local population. However, it soon became apparent that these newly formed states were merely extensions of the colonial period, which ultimately led to conflicts and civil wars. In an attempt to safeguard the territorial integrity of these states during the Cold War, both the Eastern and Western blocs provided military and economic assistance, driven by their respective ideological motivations (Batır,2017). Nevertheless, when the USSR disintegrated and stopped providing financial assistance to these nations, it became evident that their capabilities were severely limited. As a result of the state's disintegration, the separation between the control of violence and the state's authority created a conducive atmosphere for the emergence of various issues such as terrorism, organized crime, and civil strife. Consequently, the occurrence of conflicts between nations diminished, giving rise to internal disputes, and traditional armies were gradually substituted by non-state actors like paramilitary organizations, warlords, criminal factions, underage combatants, terrorists, and mercenaries.

Once again, it is important to highlight that in the era following the Cold War, there has been a noticeable surge in ethnic conflicts across various regions. These conflicts have particularly escalated within the former Soviet Republics, the countries of Central and Eastern Europe that were once affiliated with the communist bloc, as well as the African nations that secured their independence through the principle of self-determination. However, it is worth noting that the borders of these African states were established without duly considering the ethnic identities within their territories. As a consequence of this historical backdrop, the character of warfare itself has undergone a significant transformation. Traditional state-to-state conflicts, where conventional armies engaged in battles, have gradually given way to a new type of warfare commonly referred to as "new wars." Furthermore, the international system that emerged after the end of the Cold War, the process of economic and commercial globalization, the rapid advancements in defense, transportation, and communication technologies have had a profound impact on the character of war. Moreover, the influence of the media has grown exponentially, shaping public perception and influencing the conduct of war. The advent of cyberspace has further added a new dimension to warfare, while the securitization and privatization of war have introduced new actors and dynamics into the equation, fundamentally transforming the way wars are fought.

2.1. 'Failed States'

Following the end of the Second World War, there arose a notable surge in independence movements across Asia, Europe, and Africa, and conflicts intensified due to the newfound emphasis on the right to self-determination. Throughout the duration of the Cold War era, conflicts rooted in ethnic and ideological divisions were commonly referred to as "Lebanonization," resulting in a significant rise in wars and confrontations, particularly within so-called third world nations. However, as the international system shifted following the conclusion of the Cold War, the term "Lebanonization" was eventually replaced with the concept of a "failed state." This term, initially coined by Gerald B. Helman and Steven R. Ratner, characterizes a state that lacks the ability to function autonomously within the global community (Helman & Ratner,1992:3). Failed states are typically characterized by incomplete economic and political development, as well as a lack of stability and effectiveness within their administrative and bureaucratic systems. In such states, conflicts have become an inherent and commonplace aspect of daily life. The advent of globalization has further exacerbated this issue, with the proliferation of illegal arms trade enabling conflicting factions within these states to readily access weapons and military equipment through the black market. Consequently, the intensity of conflicts within failed states has experienced a marked increase (Helman & Ratner,1992:5-6).

Following their independence, newly formed states were in need of economic assistance. In response, the United Nations (U.N.) encouraged organizations like the World Bank and the United Nations Development Programme (UNDP) to provide aid. However, during this process, more emphasis was placed on the concept of self-determination rather than ensuring long-term sustainability. This was

due to the underlying principle of decolonization, which suggested that people could govern themselves best when they were free from the influence and control of foreign powers. As a result, the financial support from these institutions was overlooked. It was believed that although these new states might be impoverished, they would uphold their virtue of independence by rejecting aid from foreign entities, as accepting such assistance could be seen as a violation of the principle of self-determination. During the Cold War, several newly independent and developing countries with weak economies and governments were provided assistance by the United States and the Soviet Union. However, as the support from these superpowers gradually diminished, the societies of these nations suffered a decline and their governing bodies faced instability. Consequently, these states encountered numerous structural challenges when transitioning into the post-Cold War era (Helman & Ratner, 1992:3-4).

Helman argues that after the breakup of the USSR and Yugoslavia, a total of twenty states emerged, many of which had no previous history of being independent or governing themselves. These countries lacked experience in governance, had weak civic institutions, limited economic opportunities, and were plagued by ethnic conflicts. As a result, Helman predicts that these states are likely to fail. However, he also acknowledges that there are some states that are not on the brink of collapse but could potentially face failure within the next few years. Additionally, there are newly formed independent states in the former territories of Yugoslavia and the Soviet Union, whose long-term viability is uncertain and difficult to assess. (Helman & Ratner, 1992:5).

Political problems play a crucial role in determining the status of a failed state, as they are a necessary prerequisite for such a classification. Conversely, economic issues contribute to the state's instability and hinder its ability to achieve prosperity. Nevertheless, it is important to acknowledge that although economic problems significantly contribute to state failure, they should not be regarded as the sole determining factor in the demise of a state (Snow, 1996:98-99).

According to Robert I. Rotberg, failed states exhibit a myriad of problems that encompass various aspects of their functioning. These issues encompass a high occurrence of criminal activities and the presence of political violence, highlighting the inability of these nations to effectively safeguard their borders. Moreover, these countries are marred by widespread factionalization, often under the control of authoritarian leaders. As a consequence, the institutions of the state within these failed states are feeble, resulting in subpar educational and healthcare facilities for their citizens. Additionally, the inadequate national income further exacerbates the situation, fostering a culture of rampant bribery and fostering an environment prone to local anarchy. It is within these failed states that the central government lacks the necessary power and authority to maintain effective control over the entire nation, thereby giving rise to a power vacuum. This void is frequently occupied by terrorist groups, criminal networks, or individuals involved in subversive acts on behalf of foreign nations. Consequently, the prevailing atmosphere mirrors a state of inherent disorder, reminiscent of ancient societies before the

establishment of centralized authority. In such circumstances, the likelihood of conflicts and wars becomes highly probable, almost reaching an unavoidable state (Rotberg, 2002).

In the field of literature, the terms 'fragile states' (Brock et al, 2012) or 'weak states' (Freedman, 1994) are also utilized interchangeably with the term 'failed states'. These weak states are characterized by their vulnerability and are often weakened as a result of various political and economic challenges stemming from a deficient social structure and underdeveloped institutional systems. Consequently, insurgent movements tend to be more prevalent within these states. It is important to note that these failed states emerged either from the dissolution of empires or as a consequence of decolonization processes, wherein political entities were ill-prepared and lacked the necessary framework to establish a strong and stable structure (Freedman, 1994). The conflicts and instability experienced within failed states have sparked significant debates surrounding the concept of state and nation-building. The establishment of a functional and stable state authority within these failed states through various state-building initiatives, economic aid, or alternative means would undoubtedly contribute greatly to fostering international peace and security.

2.2. Identity Politics

One significant factor that has contributed to the transformation of the character of warfare is the rise of ethnic nationalism. This phenomenon has been fueled by the forces of globalization, leading to a decline in traditional wars and a surge in civil conflicts. In the post-Cold War era, the international security landscape has witnessed a notable increase in ethnic issues and civil wars driven by ethnic nationalism. This trend can be attributed, in part, to the dissolution of multinational states like Yugoslavia and Czechoslovakia, which further exacerbated tensions along ethnic lines. The Balkans and former Soviet Republics have particularly experienced the evolution of ethnic-based problems into full-blown conflicts and civil wars. According to the analysis of scholar Mary Kaldor, the motivations behind these new wars are not rooted in geopolitical or ideological aims. Instead, identity politics, specifically ethnic, religious, or tribal identities, serve as the driving force behind these conflicts. People now fight to defend and assert their identities, which have been reinvigorated by the process of globalization. The effects of globalization have made societies within states more conscious of their own identities, leading them to believe that they are entitled to establish their own independent states (Kaldor,2013b:2). The phenomenon of globalization has had a profound impact on various aspects of society, particularly in terms of travel and communication. With the advancements in these areas, diaspora communities have been able to exert a greater influence on global affairs. Additionally, the advent of electronic media has significantly accelerated the pace of political mobilization. The widespread use of mobile phones, the Internet, and social media platforms have played a major role in establishing and strengthening political networks (Kaldor, 2012:8).

Ethnic conflicts have had a significant impact on various regions around the world after the Cold War, including the Balkans, former Soviet Republics, and Africa. In Africa specifically, internal conflicts fueled by ethnic divisions have plagued the continent, leaving a lasting mark on its recent history. The root of these conflicts can be traced back to the fact that the borders of newly independent states were not established based on the ethnic composition of their populations. Consequently, civil wars driven by ethnic tensions have become prevalent. This is evident in notable cases such as Somalia and Rwanda, where ethnic conflicts have unfolded and left a devastating impact (Yılmaz,2020:134).

2.3. Changed Actors of War

Another significant factor that has fundamentally changed the character of warfare in the post-Cold War era is the diminishing ability of states to solely engage in conflict. Snow contends that civil wars in this period lack clear political objectives, distinguishing them from earlier conflicts. Furthermore, these conflicts are marked by an absence of a clear political will to legitimize the warfare. Snow also highlights the challenge of identifying the focal points of power between the government and rebel forces due to the absence of defined political goals and ideologies. Moreover, the warring parties' disregard for winning the support of any particular population group has led to the emergence of a new kind of war characterized by acts of genocide, forced displacements, and heightened levels of brutality and violence (1996:105-107).

In the present era of warfare, the level of violence has escalated dramatically and the unfortunate consequence has been a rise in the number of civilian casualties. This shift in warfare dynamics is characterized by the involvement of a wide array of factions. Mary Kaldor, an expert in the field, highlights that the new wars are waged by intricate amalgamations of both state and non-state entities. These include, but are not limited to, conventional military forces, paramilitary factions, foreign mercenaries, private contractors, and even influential warlords (Kaldor,20013b:2).

2.4. Increasing Role of the Air-Force

One of the most significant factors in the transformation of the character of warfare has been the introduction of airborne vehicles, which have effectively expanded the battlefield into a three-dimensional space. These air forces possess unparalleled advantages in terms of speed, altitude, range, and duration, thereby earning a prominent position in the strategic planning of nations involved in contemporary conflicts (Yalçınkaya,2004:212).

2.5. The Privatization of War

The phenomenon of globalization has had a significant impact on the traditional nation-state structures, causing them to erode. As a result, the institution of mercenary service has undergone

transformation and has now become an integral part of military structures. Following the conclusion of the Cold War, there was a reduction in the size of military organizations, coupled with a reluctance to intervene militarily in unstable regions. Additionally, the privatization trend that emerged during the 1990s played a crucial role in the development of the private military sector (Shearer, 1998). During the 1980s, the commercialization of security, specifically the privatization of security, has spearheaded by leaders such as Ronald Reagan and Margaret Thatcher in the United States and the United Kingdom respectively, when the commercial enterprises were granted the opportunity to create a market focused on violence, albeit limited to the production and procurement of military goods to improve the effectiveness and efficiency. These activities were categorized as noncore military functions, meaning they were not directly involved in the actual execution of armed force on the battlefield. Nevertheless, over time, this particular sector dedicated to military and security has expanded exponentially. It has evolved into a diverse and widespread entity, lacking appropriate oversight. Astonishingly, it now offers a wide array of services, valued at hundreds of millions of dollars. These services span from basic logistical support to the provision of armed forces, all within intricate and challenging operational landscapes (Krieg & Rickli,2019:44-45).

Due to the prevalence of conflicts in failed states with various social, economic, and political issues after the end of the Cold War, the responsibility of engaging in warfare fell upon private military contractors. With Western states losing interest in failed states, they were reluctant to get involved in conflicts using their own armies. Consequently, this created a demand for the establishment of private companies specializing in warfare. Additionally, the negative consequences of traditional armies intervening in intra-state conflicts within failed states, combined with the widespread media coverage of these atrocities, sparked a significant public outcry within Western nations. This outcry ultimately paved the way for the growth and expansion of war contracting (Shearer, 1998).

Morever, in the era of globalization, it has become increasingly difficult for the state alone to ensure public security and address the public's concerns about safety in a system without clear polarities, where threats are not confined within national borders and are often intangible, unpredictable, and socially constructed based on perceived risks. In this new era, the state's role in maintaining security has evolved into that of a dispatcher, delegating the responsibility of securing the public to various executive agents. This means that the traditional bonds between those who provide security and those who rely on it have become more diffuse, as the state grapples with the challenges presented by this new threat environment (Krieg & Rickli,2019:45).

Private military companies have a wide array of capabilities, with their primary function being to actively engage in combat on the front lines and in crucial regions during times of war. In addition to this pivotal role, they are also entrusted with various other tasks that are essential for the smooth functioning of military operations. These tasks encompass safeguarding convoys, countering surprise

attacks, ensuring the protection of esteemed individuals, as well as securing strategic facilities and vital sites. Apart from direct involvement in combat, private military companies also offer valuable expertise through military consulting services. For instance, renowned entities like the Military Professional Resources Corporation (MPRI) specialize in aiding armed forces in numerous aspects, including the development of effective military strategies, the structuring of defense ministries and overall military organization, conducting simulated war games, as well as providing guidance on advanced weaponry systems, among other areas. Furthermore, there exists another category of private military companies known as military support companies. These particular entities focus on delivering essential support services to military forces. Their contributions encompass various vital functions, such as provisioning of sustenance to troops, managing laundry services to ensure cleanliness and hygiene, and even engaging in minor construction projects as required. These support services play a crucial role in ensuring the overall well-being and operational efficiency of armed forces in the field (Yılmaz,2020:136-137).

2.6. The Emergence of Cyberspace

The act of war is a multifaceted phenomenon that is influenced by various interrelated factors such as politics, culture, economy, and technology. Throughout history, the methods of conducting warfare have undergone significant transformations, progressing from relying solely on foot soldiers and naval vessels to incorporating cutting-edge advancements like stealth aircraft and unmanned drones. This trend of evolution in warfare has persisted into the modern era, particularly in the latter half of the 20th century, as new technologies emerged from the rise of the Internet and interconnected information systems. As a result, contemporary militaries now harness the power of the virtual realm, known as cyberspace, to enhance the speed, flexibility, and destructive capabilities of warfare. The militarization of cyberspace was accompanied by an equally significant development in the civilian sector. Modern societies rapidly became reliant on networked technology to manage crucial infrastructure such as the national power grid, air traffic control, railroads, and marine navigation. Additionally, global financial markets, news media distribution, communications infrastructure, global supply chains, and essential human services also became heavily dependent on these networked systems. As a consequence, ensuring the security and reliability of this interconnected cyber infrastructure became crucial for the security of developed nations. However, with the increased reliance on networked systems, the number of vulnerabilities also grew. These systems not only face the possibility of being exploited by cyber-criminals and cyber-spies, but they are also susceptible to being targeted as military objectives in both the physical and digital realms. Nowadays, countries have the capability to launch cyber attacks on an enemy's networked technologies, such as vital infrastructure, without being limited by distance, the proximity of military forces, or logistical constraints.

The realm of cyberspace offers a unique platform for activities to occur rapidly and without geographical limitations. This is made possible through the utilization of electromagnetic forces, which

serve as a means of transportation within this virtual realm. As a result, any action taken within cyberspace has the ability to transcend national boundaries instantaneously, a concept that would be unimaginable in the physical world. In the context of warfare, the speed at which operations are conducted plays a significant role in determining their effectiveness. This principle applies equally to the realm of cyberspace, where the ability to swiftly execute actions provides commanders with a distinct advantage. This advantage allows them to make timely decisions, carry out strategic maneuvers, and achieve desired outcomes at an accelerated pace. It is this unparalleled capability that sets cyberspace apart from other domains of warfare (Department of Defense, 2006:4).

Not only can nation-states, but also non-state actors, access cyberspace, giving them the ability to carry out harmful cyber operations regardless of their location. The accessibility and affordability of cyberspace contribute to power imbalances, allowing smaller non-state actors to challenge the dominance of nation-states (Rosenzweig, 2013). This is a way for these actors to compensate for any weaknesses they may have in terms of weaponry and other traditional power capabilities. It is more practical and cost-effective for a group of hackers to launch a cyber attack on a specific power plant, for example, than to train soldiers and acquire and operate armored vehicles to physically destabilize the plant using traditional means.

The realm of cyberspace provides governments with the ability to manipulate or influence the decisions of another nation without the need for a substantial presence or the financial burden of traditional military forces. In conventional arenas, it is relatively easy to determine the responsible party behind an act of aggression or establish links between individuals and their actions. This is due to the availability of direct observation or the examination of tangible evidence, which often yields valuable insights. Nevertheless, the task becomes considerably more challenging when dealing with the expansive and intricate world of cyberspace. The internet's complex structure and the ability to create fake identities pose significant difficulties in accurately identifying and attributing cyber attacks. Unlike other areas where direct observation or physical evidence can aid in determining responsibility, the anonymity of the online world allows attackers to hide their digital tracks effectively. As a result, it becomes even more challenging to identify and hold cyber criminals accountable for their actions (Keely, 2011).

In the event that a cyberattack is detected and traced back to an IP address originating from a particular state, that state has the ability to argue that it is not responsible for the attack, but rather a hacker had utilized its digital infrastructure as a hiding place. Alternatively, they may claim that one of their own citizens is the culprit, although their accountability may be limited. The US Department of Defense recognizes the validity of this concern, as they highlight that the accessibility of cyber warfare tools allows even individuals or small groups of highly motivated cyber actors to potentially inflict substantial harm (DoD, 2011). For example, regarding Stuxnet, the virus was transmitting data back to

various servers spanning across different geographical locations worldwide (Zetter, 2014). The concept of attribution holds utmost significance in international law, as it serves as a fundamental principle in determining whether an act can be classified as internationally wrongful. In order for an act to be considered as such, it must be clearly and irrefutably attributable to a state (International Law Commission,2001).

The phenomenon of cyber warfare offers a unique opportunity for various actors, regardless of their significance in the global arena, to engage in this type of conflict. One of the key advantages of cyber warfare is the ability to maintain anonymity, thereby allowing perpetrators to evade attribution and avoid being held accountable for their actions. This plausible deniability creates a gray area where wrongdoings can be committed without facing direct consequences. Moreover, cyber warfare provides states with an alternative avenue to pursue their objectives, offering a more convenient and cost-effective option compared to traditional forms of warfare. By exploiting the realm of cyberspace, states can bypass ethical violations and legal obligations that are typically associated with conventional warfare. This ultimately challenges the established norms and principles of conflict, as states can now maneuver and strategize without fear of retribution under the traditional rules of engagement.

In the compemporary security landscape, states engage in warfare while minimizing their own direct involvement and avoiding the burden of warfare and negative public attention often assosicated with the use of violence. More recently, states have externalized the burden of warfare to cyber weapons because these tools grant the patron state with plausible deniability, as it becomes challenging to attribute the source of cyber-attacks with absolute certainty. This ambiguity surrounding the origin of attacks allows the patron state to distance itself from any potential consequences and military and financial burden of warfare (Krieg & Rickli,2019:93).

In addition to that, the vast expanse of cyberspace and the advent of the internet have opened up new avenues for interactive communication among individuals, transcending geographical boundaries, time limitations, and restrictions on personal freedom. This revolutionary development has also facilitated the transfer of various forms of content, be it visual, auditory, or written, thus enhancing the scope and effectiveness of communication. Moreover, the proliferation of smartphones and advancements in mobile technology during the late 2000s have further amplified the impact of social media, making it accessible to a wider audience. As a result, the network societies formed through social media within the virtual realm of cyberspace have harnessed an incredible transformative power, capable of reaching and mobilizing potentially millions of individuals across national borders, thereby creating a truly global public sphere (Krieg & Rickli,2019:94).

Cyberspace serves as a platform that offers immediate access to information for people all around the world. Consequently, when social media is manipulated, it can have a disruptive effect, especially when it is utilized to sway and rally individuals and communities. The current era has witnessed a

transformation in the methods of warfare, meaning that the way in which new conflicts are fought has evolved. While traditional warfare aimed to seize land by employing military strategies, in the 21st century, the objective is to gain control over the population through political means, rendering military advancements less significant and prioritizing the avoidance of battles whenever feasible (Kaldor, 2012:9). In the modern era, the battleground for conflicts has shifted to the digital realm, where the focus is on shaping narratives. Various actors, including both state and non-state entities, employ tactics such as information operations and propaganda to gain control over the minds of the population. Thanks to the advent of social media, these actors now have a highly efficient tool at their disposal, enabling them to instantly and extensively reach a much larger audience than ever before, and at a fraction of the cost. This has proven to be particularly advantageous for insurgent groups, as they can now easily target and influence a widely dispersed pool of potential recruits, supporters, and allies, all while minimizing the risk of being discovered. (Krieg & Rickli, 2019:95).

In cases of insurgency, the recruitment process has undergone a significant transformation due to the emergence of social media. Not only does social media transcend geographical boundaries, but it also serves as a platform for insurgent groups to broaden their support base. By tapping into the collective anger, frustration, and resentment that exist in various societies, these groups can now consolidate local grievances on a global scale through the use of social media. This provides them with an easy, affordable, and secure way to connect with a large audience of dissatisfied individuals. Global insurgency, in contrast to conventional insurgencies, possesses unique qualities that make it stand out. One noteworthy aspect is its transboundary essence, indicating that it functions beyond the confines of a solitary country and can be affected by diverse ideologies. Unlike conventional insurgencies that mainly focus on a particular community, global insurgencies cater to a wider range of individuals. Consequently, they no longer rely on a local safe haven to carry out their operations efficiently. Rather, they seek shelter in the vast and anonymous realm of the internet, which grants them abundant chances to plan and synchronize their endeavors.

In today's world, global insurgencies have undergone significant changes in order to adapt and thrive. They have embraced the advancements in technology and the borderless nature of cyberspace, using these tools to their advantage. This evolution has allowed them to break free from traditional boundaries and expand their reach to a much larger audience. Additionally, they have become more nimble and efficient in their operations. Contrary to the hierarchical structures typically seen in conventional insurgencies, global insurgent groups have adopted a different approach. They have embraced a nonhierarchical network model, which provides them with the flexibility to collaborate with other like-minded individuals or groups. This collaboration allows them to work together towards shared objectives. They can engage in various activities, such as exchanging valuable information, acquiring weapons and knowledge, gathering intelligence, and developing strategies that were previously unattainable. The global insurgent relies on influential individuals on social media, known as "super

influencers," to bear the burden of spreading their message. These super influencers, who have a significant number of followers on a specific social media platform, possess the authority and credibility to effectively communicate the insurgent's narrative. Through the power of social media, these super influencers consciously or unconsciously promote the global insurgent's message, allowing it to reach a wider audience and gain potential legitimacy. The impact of emotions in shaping narratives and values in our interconnected world is more influential than the mere dissemination of factual information. As stated by former British primeminister Tony Blair, the globalization of our society has led to interdependence, which in turn necessitates the establishment of a shared value system. In today's globalized world, the battle for global values and specific worldviews has become a defining feature of the character of war (Krieg & Rickli, 2019:96).

In regards to cyberweapons, in contrast to traditional weapons, cyberweapons possess a distinct characteristic of being widely dispersed and demanding considerably fewer resources for acquisition. The development of conventional weapons, such as weaponized drones, ballistic missiles, or even nuclear bombs, necessitates substantial investments in terms of human capital, financial backing, and physical infrastructure. Conversely, cyberweapons solely require a computer, access to the Internet, and proficient computer engineering expertise. This fundamental disparity has resulted in a paradigm shift, as it has enabled not only nation-states but also substate factions and even individuals to emerge as significant contenders in the cyber domain. In contrast to the limited accessibility of nuclear weapon or aircraft carrier development, the internet has enabled a unique phenomenon where individuals can collaborate remotely and instantly connect with a vast number of people. This interconnectedness has led to the sharing of valuable insights on online forums, where individuals can learn how to create complex malware. This form of crowd-sourcing has leveled the playing field, as it now only requires dedication and time for anyone to acquire the expertise needed to develop or deploy a powerful cyberweapon. This remarkable scalability has effectively erased the distinction between the capabilities of governmental bodies and non-state entities in the realm of cyber warfare (Thomas,2018).

Therefore, cyberweapons are intangible and reside within various levels of cyberspace. They possess the ability to be bought, replicated, modified, and shared with individuals who have a vested interest in them. For example, in the case of Georgian cyber attacks which took place in 2008, StopGeorgia.ru provided easy-to-use tools and instructions to launch DDoS from private machines. It even featured a user-friendly button called "FLOOD" which, when clicked, deployed multiple DDoS on Georgian targets. One hacktivist notes that the instructions provided were very accessible, even for a novice user (Shakarian,2011).

2.7. The Impact of the post-Cold War International System

The bipolar nature of the Cold War, characterized by the rivalry between the United States and the Soviet Union, along with the concurrent nuclear arms race, gave rise to an international system that, while seemingly peaceful, remained highly fragile and prone to volatility. In this era, the major powers were averse to engaging in armed conflicts, primarily due to the harrowing devastation wrought by the Second World War. Nevertheless, some argue that the absence of war during this period can also be attributed to the prevalence of democratic governance systems within many nations. Generally speaking, democratic states tend to exhibit a lower propensity for engaging in armed conflicts against one another (Bueno de Mesquita & Lalman,1992:146). Ever since President Wilson, the notion of democracy has become deeply intertwined with the concept of peace among Americans. Despite the fact that democratic nations often display high levels of aggression and allocate significant resources towards their military forces, they appear to exhibit a certain hesitance when it comes to engaging in conflicts with one another. Nevertheless, it is worth acknowledging that there are arguments which posit that democracies are unlikely to wage war against each other, yet it is not entirely uncommon for such nations to find themselves embroiled in disputes and armed conflicts with their democratic counterparts. A prime example of this can be seen in the American-British War of 1812, which unfolded between the only two democratic states in existence at that time, with tensions lingering between them for decades and even extending beyond the confines of the nineteenth century (Waltz,1993:78).

The end of the Cold War brought about significant shifts in the global system, which in turn had a profound impact on the character of war. Following the downfall of the Eastern Bloc and the disintegration of the Soviet Union, the United States assumed a dominant position in the international arena, ushering in a new world order. This unipolar structure of power, coupled with the rapid expansion of economic and commercial globalization, as well as advancements in defense, transportation, and communication technologies, has fundamentally transformed the concept of war. Additionally, there has been a notable increase in the influence of international organizations and the strengthening of international regulations, further complicating the ability of states to engage in armed conflict with one another. The advent of globalisation has not only expanded worldwide connectivity and trade, but it has also facilitated the globalisation of organized crime, terrorism, and other forms of asymmetric threats. Consequently, non-state actors have emerged as influential players in contemporary warfare. In today's era, conflicts predominantly occur within failed states, which can be identified as states characterized by limited economic prosperity and governed by illegitimate regimes. In response to humanitarian concerns and the violation of human rights, other nations often intervene in civil wars and conflicts taking place within these failed states.

2.8. Globalization

Throughout history, the outcome of wars was determined by armies that were under the direct leadership of their commanders, engaging in face-to-face combat. These battles would take place on

specific battlefields that were only accessible after days of travel. It was during these conflicts between different nations that the sacred authority and independence of a state were put at risk. However, in recent centuries there have been many events such as the Industrial Revolution, the Digital and Information Revolution, which have brought about fundemental and rapid changes and transformations in sociopolitical, socio-economic and other fields, and these changes have naturally affected the character of warfare (Krieg & Rickli,2019:40).

These changes were named 'globalisation' by James N. Rosenau in the twenty-first century. Since the changes experienced with globalisation are very different from the conditions and circumstances of the previous periods, changes in the definition of war are also considered possible. Changes in sociopolitical, sociocultural, socioeconomic and similar fields have become transnational and anarchic, which are difficult to be controlled only by states or state authorities. Even if states have full authority to regulate and manage global affairs, this authority and monopoly remain on paper, and in practice they are challenged by the presence of non-state actors, creating an apolar system. What is meant by the apolar anarchic system mentioned here is that it has become a transnational system in which states and non-state actors interact. The twentieth century was a period characterized by rapid globalization and a series of transformative revolutions. During this era, the transportation revolution played a crucial role in enhancing the movement of individuals across international borders, while the microelectronic revolution facilitated the speedy and efficient transmission of vital information and ideas on a global scale. Furthermore, the economic revolution enabled the seamless exchange of goods and services across borders, along with the flow of capital and ownership on a worldwide level. Additionally, the organizational revolution reshaped the way authority, influence, and power were distributed in an increasingly internationalized context (Krieg & Rickli,2019:40-41).

Globalisation, has had a profound impact on various aspects of society, including the sociopolitical, sociocultural, and socioeconomic realms. This transformation has resulted in the emergence of transnational flows, which have challenged and weakened established institutions, organizations, authorities, and values that were once dominant. Nation states and state authorities have found it increasingly difficult to exert control over these supranational flows, as they require a certain level of cooperation with international organizations. In the current world order, transnationality has taken precedence over national and international boundaries as the primary unit of analysis. This shift has resulted in non-state actors playing a significant role in the regulation and management of global affairs, often undermining the authority of nation-states. Despite the formal sovereignty of states, the increasing process of globalization has led to a reconfiguration of power dynamics, as the influence of non-state actors grows (Krieg & Rickli,2019:40).

This implies that due to the presence of other actors in international relations, such as non-state entities, the traditional concept of the nation-state holding power in all aspects has diminished. Instead,

a new system has emerged where power dynamics are constantly shifting between state and non-state authorities, disregarding the traditional notions of state sovereignty and territorial integrity. This transition has greatly impacted how we perceive and approach sociopolitical matters and even the concept of warfare (Krieg & Rickli,2019:41-42).

Communities are now questioning the traditional perspective of the state-controlled security and the perpetuation of violence. Instead, these communities perceive themselves as transnational entities, emphasizing their existence beyond the boundaries of a single nation-state and asserting their identity as societies that transcend national affiliations. With the progression of globalization, the concepts of state sovereignty and territoriality become more flexible, resulting in the inability of individual nations to effectively oversee and control the actions of their citizens and foreigners residing within their jurisdiction. The ideas surrounding state sovereignty and territoriality have experienced a shift towards a more flexible and dynamic state (Krieg & Rickli,2019:42).

In today's rapidly globalizing world, a series of revolutions have fundamentally altered the sociopolitical, socioeconomic and sociocultural aspects of societies. Consequently, this has led to a complete transformation in the dynamics between communities, communal authorities, and security providers, as well as the very nature of conflicts and their resolutions. The distinction between ordinary citizens and military personnel has been in existence for a long time. However, in today's interconnected world where conflicts transcend borders, non-state actors present unique and transnational security challenges. Moreover, the provision of security is now viewed as a global or transnational public good. As a result, the state alone is incapable of effectively carrying out security functions and must rely on alternative sociopolitical enforcement bodies that mirror the trinitarian model of society, state, and soldier (Krieg & Rickli,2019:42-43).

2.9. Economy and War

Due to the concept of total war, the conflicts witnessed in the twentieth century were characterized by states aiming to completely obliterate their adversaries by utilizing every available resource at their disposal. However, the character of war in the twenty-first century has evolved to a point where the general populace no longer actively engages in combat, and resources are employed in a more restrained manner. In essence, contemporary wars have transitioned away from being all-encompassing and no longer possess the attributes of total war. The political leaders of countries are under immense pressure from public scrutiny. They have to carefully consider the urgency of a crisis and balance it against the costs that it will impose on society and the military. This analysis of costs and benefits is a fundamental aspect of the decision-making process surrounding war and peace in the modern age of information. Unlike in the past, the human and financial burdens of war cannot be hidden from the public anymore. These burdens impact not just during the conflict itself, but also before and after the war. The resources

that are allocated to the armed forces and the preparation for war come at the expense of other important public services, depriving them of necessary funding. Maintaining a strong military is a significant drain on a government's budget, requiring substantial resources. As a result, the investments made in the military have a significant impact on society, both in terms of financial implications and the toll it takes on human lives. A substantial portion of public funds is allocated to enhancing the capabilities and resources of the armed forces, with the intention of being prepared for future conflicts. However, when a nation is actually engaged in warfare, the amount invested increases exponentially. The public's awareness of the immense costs, both in terms of finances and the loss of human lives, places a heavy burden on political leaders to justify the allocation of resources towards the military, the decision to deploy troops overseas, the methods employed during warfare, and the resulting destruction caused (Krieg & Rickli,2019:62-63). Furthermore, it is important to acknowledge that in the twenty-first century, the materials and assets required to participate in armed conflicts are no longer restricted to a particular region, but rather have a worldwide reach. According to Mary Kaldor's perspective, the act of instigating aggression, which is a fundamental component of warfare, ideally should take place within a localized setting. However, the necessary resources and provisions to sustain and fuel these conflicts should ideally be obtained from external origins (2012:94).

In the 21st century, there has been a noticeable shift in the correlation between warfare and the economy, with a striking trend emerging wherein financially-strained nations have increasingly become hotbeds for conflicts. This occurrence is particularly evident in the tumultuous Middle East, where a convergence of economic and social fragility, coupled with governance challenges and a deficit of legitimacy, has given rise to a relentless cycle of wars and hostilities. Likewise, underdeveloped regions across Africa and Asia have encountered analogous circumstances, thereby reinforcing the link between economic adversity and the eruption of armed confrontations.

2.10. Media and War

In the ninteenth century, the idea of warfare was seen as a heroic and honorable way to sacrifice oneself for the benefit of their country and state. This mindset was heavily influenced by the rise of nationalism and romanticism during that era. Despite the devastating consequences of war and the immense sacrifices made by individuals and society as a whole, serving one's nation and its interests was seen as a noble endeavor. However, in today's world, where conflicts have become more globalized and transnational, and where there is a growing public aversion to violence and organized warfare, it has become increasingly challenging for policymakers to justify the sacrifices made by citizen soldiers for peripheral interests abroad. Additionally, it has become harder to legitimize the human and financial costs associated with war. At the same time, the media had familiarized the general population with the concept of warfare, thereby transforming the decision to engage in war into a complex analysis of costs and benefits, subject to scrutiny on an international, domestic, and local level. The once-celebrated act

of a citizen soldier sacrificing their life and depleting the nation's vital resources is no longer portrayed as a heroic deed, but rather as a tragic and preventable nightmare that can only be morally justified when confronted with threats that jeopardize the very existence of a nation (Krieg & Rickli,2019:49-50). To put it briefly, due to the combination of civilians residing in conflict zones and the rapid dissemination of information regarding the events occurring in these areas, the involvement of civilians in war and conflict has significantly increased. Consequently, contemporary warfare has emerged as a matter of equal concern for both civilians and soldiers, blurring the traditional boundaries between the two.

Thanks to advancements in technology, war has become a significant focus for journalists since the mid-19th century. The Crimean War marked a turning point, as the telegraph enabled rapid dissemination of war developments to the public. The telegraph's widespread use and the subsequent growth of telegraph lines further enhanced war reporting and journalism, allowing the public to receive daily updates on the battlefield. While radio broadcasting was the sole means of communication during the Second World War, the Vietnam War and the Gulf War ushered in the era of televised war images. Today, with the advent of unmanned aerial vehicles and satellite technology, real-time views of the battlefield have become possible. The media now holds the status of the fourth estate, with war planners recognizing the importance of media and propaganda in their strategic planning. Media outlets have become influential actors in defense and foreign policy, leading to the emergence of what is known as the CNN effect. The CNN effect manifests itself in three distinct ways. Firstly, it involves setting the political agenda, effectively shaping public opinion on the matter. Secondly, it obstructs political objectives by shedding light on the realities and consequences of war. Lastly, it accelerates political decision-making by putting pressure on policymakers to respond swiftly to the demands of the public (Livingston,1997:2-4).

The CNN effect, which first emerged in 1993, was triggered by the broadcast of distressing footage showing the body of a deceased US soldier being dragged through the streets of Somalia. This powerful image had a profound impact on public opinion and exerted immense pressure on the government. Consequently, the US soldiers withdrew from Somalia in just four months. This incident served as a clear demonstration of the significant influence of television broadcasting. The portrayal of poverty, hunger, and war on screens heightened the public's ability to exert pressure on governments. Since then, the integration of war reporting into military planning has given rise to a new approach known as embedded journalism. This style of reporting involves journalists collaborating with the government to provide news coverage. In the context of the Second Gulf War, the United States took it a step further by training a battalion of journalists and deploying them to the front lines. These reporters, equipped with military training and closely aligned with the army's war plans, operated within predetermined restrictions and rules. Their role extended beyond traditional journalism as they effectively engaged in pro-government propaganda (Katovsky & Carlson,2003).

In the twenty-first century, wars have transformed into highly subjective realities that are broadcasted to the world. Consequently, there has emerged a fierce rivalry among the parties involved in the conflict - the combatants engaging in warfare, the communities directly impacted by the intervention, and external third-party entities endeavoring to sway public sentiment both domestically and internationally. This intense competition revolves around the manipulation and control of the narrative surrounding war, as each faction strives to shape the perspective and understanding of the masses. Thus, in the contemporary world, war extends beyond tactical maneuvering and military strategies and encompasses the power of narratives within the global public sphere. Therefore, achieving victory in war involves not only capturing and maintaining control over territory, but also exerting influence over the narratives surrounding the conflict in the minds of individuals at local, national, and international levels (Krieg & Rickli,2019:50-51).

2.11. Securitization of War

Throughout the twentieth century, wars were frequently waged with the objective of safeguarding national interests and were often viewed as zero-sum games. These conflicts were typically fought against a clearly defined, tangible, and openly declared adversary. However, in the twenty-first century, the concept of security has evolved into a much more complicated and multifaceted issue. This transformation can be attributed to the prevailing uncertainty and intangibility surrounding the current threat environment. As a result, there has been a significant increase in the subjective perception of security, particularly in an environment where threats are no longer easily discernible or quantifiable, as they once were. The act of engaging in warfare overseas is often portrayed by nations as stabilization and reconstruction efforts, carried out by individuals involved in humanitarian work and law enforcement, benefitting the domestic society but also contributing to the welfare of local communities within the conflict zone. It is essential to recognize that ensuring communal security for individual nations is inseparable from upholding global security as a whole (Krieg & Rickli,2019:47).

Recently, policy makers have found that the traditional justifications for connecting national security with military stabilization or humanitarian operations overseas, such as the belief that homeland security begins abroad or the concept of human security as an inherent right, are no longer satisfactory. These arguments, which were once considered valid and compelling, have now been deemed insufficient for policymakers to establish a strong and credible link between the protection of a nation's security and the need for military intervention or humanitarian efforts in foreign lands. In this age of social media, information reaches even the most isolated communities, resulting in the broadcasting of wars and holding states accountable to their own citizens. Consequently, policy-making processes are subjected to intense scrutiny both within domestic borders and on a global scale. This heightened scrutiny is primarily driven by public opposition towards engaging in military operations on foreign soil, which

puts citizen soldiers at risk without yielding tangible benefits. Moreover, the allocation of government funds towards overseas wars is increasingly questioned, especially when there are pressing domestic issues that demand attention and resources.

However, in a world where transnational threats such as global terrorism, insurgency, financial crises, global warming, and mass migration are prevalent, it becomes imperative for states to take action in order to address these direct or indirect security concerns, despite the pressure from the public to do so. In response, states exercise their authority to mitigate these threats, even if they receive support from commercial entities and non-governmental organizations (Krieg & Rickli,2019:47).

States typically rely on economic or diplomatic measures in order to address these threats. However, if the economic and diplomatic efforts are hindered by coercive or insecure environment, then the military steps in to take control of containing and managing these threats. In a globalized world, conflicts have become transnational events that can arise unexpectedly and impact distant regions across borders. These conflicts can manifest in various ways, directly or indirectly, and can persist for an indefinite duration. What makes them even more complex is that they often occur simultaneously and in different domains. As a result, governments are increasingly eager to enhance their capacity to react swiftly and effectively on a global scale, even when the situation may not require a high-intensity response (Krieg & Rickli,2019:47-48).

In today's world, the security environment has become increasingly complex and interconnected. The threats we face are no longer confined within national borders, but rather transcend geographical boundaries. This global security environment is marked by the constant emergence of new and unpredictable threats, making it difficult for states to anticipate and counter them effectively. As a result, governments are now adopting proactive measures to address these potential threats even before they fully manifest or, in some cases, before they are even tangible realities. The aim is to stay one step ahead and prevent any prolonged or escalating threats from materializing and endangering the safety and stability of nations. Thus security policies are created based on risk management, which is a more subjective approach compared to threat assessment. Risk management focuses on the possibility of negative events happening in the future, while threat assessment involves identifying a concrete entity with plausible capabilities and stated intentions (Krieg & Rickli,2019:48).

Thus, in order to ensure the safety of their citizens, governments expand the realm of their security measures by adopting a precautionary approach. This approach aims to address any potential risks that can be reasonably anticipated in our modern society, which is characterized by a growing aversion to risk. This shift towards risk-aversion is a hallmark of the postmodern era, as described by Ulrich Beck who coined the term risk society. In this society, traditional notions of security are being replaced by ever-changing and unpredictable threats. Consequently, the concept of warfare has undergone a transformation, now focusing on the construction, prevention, and management of risks. Within an

enviroment of global risks which can have far-reaching consequences, both preventive diplomacy and war are reluctantly embraced as means of minimizing the political fallout of neglecting potential risks. In fact, society now tends to view overreacting to a potential risk as more acceptable than underreacting. The state, as the governing body, has been faced with a paradoxical situation due to its attempts to manage the uncertainties on a global scale. In this scenario, the distinction between logical decision-making and irrational fear has become increasingly unclear (Krieg & Rickli,2019:48).

CHAPTER III
War in the 21st Century

Throughout history, war has been an enduring aspect of human civilization, serving as a prominent and forceful expression of conflict. Despite its enduring presence throughout the ages, the character of warfare has undergone profound changes due to globalization and rapidly advancing technology as we enter the 21st century. This transformation has resulted in wars taking on an entirely new dimension. When examining studies on the evolving characteristics of war, it becomes apparent that there have been significant changes that can be categorized into nine key areas. These areas encompass various aspects of warfare and provide insights into the transformations that have occurred over time. The first area of interest is the objectives of the war, exploring how they have shifted and evolved. Another area explores the actors involved in the conflict, investigating how the parties engaged in war have changed. Additionally, the target group of the war is examined, delving into the alterations in those affected by the conflict. The fourth area focuses on the field or front of the war, analyzing the changes that have taken place in the physical locations where battles occur. Methods and strategies of warfare are also explored, shedding light on the advancements and modifications that have shaped military tactics. The sixth area of examination is the economy of war, scrutinizing the changes in how resources are mobilized and utilized during conflicts. Furthermore, the weapons used in war are studied, highlighting the developments and advancements in military technology. The eighth area investigates the beginning and end of wars, exploring how these crucial stages have transformed over time. Finally, the symmetry in warfare is analyzed, providing insights into how the balance of power and equality between opposing forces has shifted. In this section, we will try to examine the areas in which the character of war has changed with reference to the works of important academics and authors involved in the new generation of war studies.

3. Changing Character of War

The concept of war, which has existed for as long as the history of mankind, has undergone transformations over time under the influence of political, economic, social and technological developments. The collapse of the Soviet Union and the end of the Cold War had far-reaching consequences that significantly altered the global power dynamics and created a period of uncertainty. This period of uncertainty necessitated a reevaluation of national security and warfare strategies as the world grappled with a void of power. As a result, the traditional concept of interstate warfare underwent a profound transformation. Throughout history, numerous factors such as social, cultural, and technological changes have continuously influenced the character of war. These factors have had a profound impact on the definition and understanding of war.

The devastating effects of two world wars have led societies to refrain from bearing the financial and human burden of war and states to reconsider their attitudes on this issue. In the past, martyred soldiers and fighting for the security of the country and the protection of national interests were considered sacred, and the public was mobilised behind wars by offering support in various ways. However, in the new era, there has been a change in mentality in which both the human losses and the material and moral burdens imposed on society due to wars are seen as undesirable consequences that states should avoid. This change can be attributed to developments in technology, especially the integration of communication and media tools into the battlefield. The exponential growth of social media has played an important role in shaping public opinion and has led to a widespread aversion to traditional methods of warfare, which can cause serious financial and human costs. As a result, states have been reluctant to engage in inter-state wars and have been forced to explore alternative means of conflict resolution. Moreover, due to the influence of international law and the possession of nuclear weapons, the occurrence of wars between nations has significantly decreased and become rare. Entering the 21st century, conflicts have taken on a different character, limited in scale and intensity, but highly violent and lacking regulation. These conflicts often find their roots in so-called failed states, where religious, tribal and ethnic tensions fuelled violence.

Researchers have conducted comparative studies between old wars and new wars, revealing striking differences in various aspects of warfare. Whether it is called new war or hybrid war, it is important to determine what kind of characteristics the 21st century wars have. At this point, a number of questions will be asked in this sub-heading to identify the characteristics of the new wars. When studies on the changing characteristics of war are analysed, it is seen that there are changes that can answer nine main questions.

These are:

1) What changes have occurred in the aims of the war?

2) What changes have occurred in the actors of the war?

3) What changes have occurred in the target group of the war?

4) What changes have taken place in the field / front of the war?

5) What changes have occurred in the methods and strategies of warfare?

6) What changes took place in the economy of the war?

7) What changes have occurred in the weapons used in the war?

8) What changes occurred in the beginning and end of the war?

9) How has symmetry in warfare changed?

At the point of answering these questions, the answers given by the authors in their works will be summarized. In this context, the views of Mary Kaldor, one of the leading figures of the new war literature, are important in answering the first question. According to Kaldor, who makes a distinction between old and new war and compares the aims of these two categories of wars, in the past, wars were primarily driven by geopolitical and ideological motives, such as the acquisition of land or the promotion of specific political systems like democracy or socialism. However, according to Kaldor's analysis, warfare has undergone a transformation, with contemporary conflicts being fueled by identity-based factors such as ethnicity, religion, or tribal associations. Rather than fighting for the interests of a nation or ideology, these battles revolve around the aspirations of particular groups, whether they are local or transnational, to attain power and control over the state. This shift in focus can be attributed to several factors, including advancements in communication technology, increased migration, and the diminishing influence of state-centric political ideologies due to globalization. As Kaldor emphasizes, identity, which was previously employed as a strategic tool in traditional wars, has now become the ultimate objective that propels political mobilization in modern conflicts (2013a:2).

To answer the second question, almost all authors agree that there has been a change in the actors of war, that states have lost their monopoly on the use of force, and that non-state actors have become players in the international system and have gained the capacity to use force, especially after the end of the Cold War (Creveld, 1991; Krztoń, 2022 ; Krieg & Rickli, 2019 ; Gürcan, 2012; Kaldor, 2013; Mello, 2010; Tuck, 2014). In the aftermath of the Cold War, a series of events unfolded that ultimately led to the rise of non-state actors as prominent figures in global affairs. These events included the displacement of populations, uprisings driven by identity politics, and the existence of ineffective and illegitimate governments and state institutions. As a result, various autonomous armed groups and organized crime organizations emerged, showcasing their prowess in employing force and subsequently exerting a considerable influence on the character and outcome of present-day conflicts. Instead of traditional wars between states, we now see conflicts led by rebels, organized crime groups, local militias, guerrillas, and similar non-state actors taking center stage.

Globalization, has had a profound impact on various aspects of society, including the sociopolitical, sociocultural, and socioeconomic realms. This transformation has resulted in the emergence of transnational flows, which have challenged and weakened established institutions, organizations, authorities, and values that were once dominant. Nation states and state authorities have found it increasingly difficult to exert control over these supranational flows, as they require a certain level of cooperation with international organizations. In the current world order, trans-nationality has taken precedence over national and international boundaries as the primary unit of analysis. Morever, communities are now questioning the traditional perspective of the state-controlled security and the perpetuation of violence. Instead, these communities perceive themselves as transnational entities, emphasizing their existence beyond the boundaries of a single nation-state and asserting their identity as societies that transcend national affiliations. This shift has resulted in non-state actors playing a significant role in the regulation and management of global affairs, often undermining the authority of nation-states. Despite the formal sovereignty of states, the increasing process of globalization has led to a reconfiguration of power dynamics, as the influence of non-state actors grows (Krieg & Rickli,2019:40-42).

In the 21st century, security is being handled by private companies and non-state actors, rather than solely by governments. In today's complex global world, where conflicts transcend national boundaries, addressing these transnational disputes requires collaboration between private businesses, public organizations, and global institutions. The privatization of security has led to non-state actors

competing with the state in providing security. Some states have chosen to collaborate with these emerging actors to maintain control. This challenges the traditional idea of the state having a monopoly on legitimate force. The commercialization of security originated in the 1980s, allowing for the creation of a market focused on violence. This sector has expanded and now offers a wide range of services. With globalization, it is difficult for the state alone to ensure public security. Thus, the state no longer holds monopoly over violence and delegates security responsibilities to various non-state agents. (Krieg & Rickli,2019)

Similar to this view, Gürcan states that as a result of the interconnectedness of the world, the meaning of citizenship has gradually diminished, leading to a reduced sense of connection between individuals and their respective countries. This weakening bond, coupled with the emergence of entities that are not governed by states, has greatly weakened the power and influence of nation-states, thereby impeding their ability to maintain control and authority in present-day conflicts. Consequently, the conventional understanding of security no longer depends solely on the military forces of states, but has transformed into a marketable service provided by private military companies. He suggests that the state will resort to alternative methods to avoid the negative consequences of political, economic, and socio-psychological costs. These alternative methods may include indirectly employing criminal organizations and ethnically violent movements, as well as participating in hybrid wars by supporting non-state actors or non-governmental organizations influenced by extremist religious movements. Consequently, the state will be forced to give up some or all of its monopoly on the use of force to these entities mentioned above. (Gürcan, 2012:96-97).

In parallel with this idea, Kaldor also says the advent of globalization has played a significant role in empowering non-state actors, ultimately resulting in the erosion of state authority. Unlike traditional conflicts that primarily involved the engagement of nation-states with their established military forces, the dynamics of new wars entail a diverse range of actors. These include non-state entities such as private security contractors, paramilitary groups, mercenaries, alongside the traditional armed forces of nation-states (2013b:2). In terms of actors, Münkler argues that states have lost their dominant role as the primary actors in warfare and are no longer the exclusive wielders of military power. Instead, they have been gradually supplanted by alternative entities such as parastatal structures and private actors. This shift in the landscape of warfare indicates a departure from the conventional understanding of wars being solely orchestrated and conducted by nation-states. Consequently, the traditional monopoly over the means and conduct of warfare that states once possessed has been eroded, giving rise to a more diverse and multifaceted array of actors engaged in conflict (Krztoń, 2022:19).

In contrast to the viewpoints expressed by the afore-mentioned authors, Creveld (1991) posits that the conventional state as we know it will eventually cease to exist, paving the way for the emergence of war organizations. Mello (2010: 2-3), on the other hand, contends that the state will gradually relinquish its exclusive control over the utilization of force. In a similar vein, Tuck (2014: 215) asserts that the state will no longer hold the primary role as the ultimate arbiter, as warlords and private military companies will take center stage, leading to a transformation of the very nature of warfare that surpasses the boundaries set by Clausewitz's traditional paradigm.

In answer to the third question, it is observed that there is a shift from the traditional enemy-centered approach to a people-centered approach in the new generation wars. In summary, the enemy-centered approach states that the main purpose of war is to end the physical existence of the adversary and to break his determination and will to fight. In this approach, which is based on kinetic and conventional military power, all military and quasi-military efforts are directed against the physical

existence of the enemy. This approach aims to destroy the enemy at all costs. On the other hand, in the new generation of wars, concrete objectives such as the occupation and control of a territory or the destruction of the enemy's physical presence have ceased to be the main military objective, and the ultimate objectives have started to be defined more socio-psychologically and politico-ideologically in order to achieve the abstract objective of "the enemy's determination and resolve to fight". In this people-centered approach, the main goal is to gain the support of the majority of public opinion by strengthening the positive perceptions and opinions of friendly public opinion, winning neutral public opinion, and winning or deterring hostile public opinion. The target audience in the new generation of warfare is public support and legitimacy in the eyes of the public (Gürcan, 100-104)

The reason for this change is as the nation has taken on a more prominent role in warfare, shouldering the majority of the financial and human costs, the public has also gained more influence over how the nation's resources are invested. The act of waging war has evolved into a matter of discussion and negotiation between the government and the public, rather than simply relying on physical force on the battlefield. The traditional understanding of war, as described by Clausewitz, no longer solely pertains to physical violence to compel the enemy, but also encompasses winning over the hearts and minds of the people. This requires the shaping of perception, both domestically and internationally, as well as locally. This is mainly because, states as well as other actors involved in conflict are subject to public scrunity, where global, domestic, and local legitimacy play a crucial role in determining the outcome of a war. That is to say that the power of states lies in their legitimacy and their ability to effectively communicate, sway public opinion, manipulate perceptions, and shape narratives surrounding war, thereby establishing it as a justifiable cause (Krieg & Rickli,2019:62).

This is also achieved through the strategies that prioritize the well-being and support of the local population rather than resorting to acts of violence and destruction. The ultimate goal is to garner the backing of the people residing in the operational area. To achieve this aim, there is a prevalent emphasis on the role of individuals commonly referred to as "men of peace," who prioritize the peaceful persuasion and conversion of the local population by winning over their hearts and minds, instead of resorting to acts of violence and destruction. Their main focus centers around safeguarding the lives and welfare of the people situated in the conflict zone, rather than engaging in aggressive and hostile actions. These individuals possess a deep understanding of the emotions, thoughts, perspectives, and beliefs of local communities and they exhibit a high level of cultural adaptability, proficiency in the local language, and they possess an expertise in disciplines such as socio-psychology and anthropology at both the individual and group levels. In this regard, it has become difficult for conventional armies, which try to win battles by terminating and intimidating the physical existence of their enemies, to keep up with the 'people'-centered and increasingly civilian combat environments (Gürcan,2012:110).

The answer to the fourth question is that there has been a change in the perception of the front in war. The concept of front in traditional wars has already begun to disappear with the use of nuclear weapons and intercontinental missiles (Çöpoğlu, 2018:39). In new generation wars, concrete goals such as the destruction of the enemy's physical existence have ceased to be the main military objective and have been carried out with the aim of achieving the abstract goal of breaking the enemy's determination and resolve to fight. Therefore, the objectives in wars have started to be defined in socio-psychological and political-ideological terms. In addition, the distinction between soldiers and civilians has disappeared, war has transformed from a political-military struggle into a political-social struggle, and the parties have become more inclusive of both soldiers and civilians. Therefore, the traditional physical definitions of the "battlefield" based on terrain, weather conditions and the enemy have expanded and it has been realized that the battlefield also has ‘informational’ and ‘spiritual domains’. The fact that

civilians can also become targets is not unique to new generation warfare. However, the new generation enemy has become undefinable and the concept of the front has ceased to be a spatial phenomenon and the battlefield has expanded to include cyberspace (Gürcan,2012:103).

In new wars, the method of warfare has also changed. In the past, individuals who risked or sacrificed their lives in war were revered as heroes, and wars fought for the sake of public security or nationalist sentiments were considered sacred. However, there has been a shift in this perspective in the twenty-first century. Both soldiers and society at large no longer wish to bear the burdens and casualties of war, and the use of violence is increasingly seen as socially unacceptable. In today's world, major powers perceive themselves to be facing hypothetical threats that are often created or prioritized by decision-makers from both state and non-state actors. These actors operate in a complex battlespace that spans across borders and is heavily reliant on interconnected networks (Krieg & Rickli,2019:8). Furthermore, there is a widespread broadcasting of wars, which enables them to be observed and analyzed by the global public, thereby subjecting them to intense scrutiny. Consequently, the strategies employed in warfare have become more complex, extending beyond traditional military tactics. In the current era, wars have evolved from being solely focused on conquering territories to also encompassing the objective of influencing the thoughts and sentiments of adversaries. Thus, parties involved in conflicts strive not only to secure geographical advantages but also to influence the thoughts and sentiments of their adversaries, aiming to win over their hearts and minds (Yılmaz,2021:90).

Kaldor explains this situation in a similar way as follows: The conventional method of solely relying on physical destruction and diminishing the enemy's military capabilities to intimidate them has become outdated in the current security landscape. In the past, wars were often decided in a single crucial battle, where military tactics were used to capture land and protect national interests. However, in modern warfare, these decisive battles are becoming less common. Instead, territory is now acquired through political means and control over the population. Rather than targeting enemy forces, violence is directed towards civilians in order to gain control over a particular area. The military's main objective is no longer solely to defeat the enemy physically, but also to shape the perceptions and interests of the people in the target country. This is done by convincing them that cooperating with the opposing power would be safer and more beneficial in the long run, rather than supporting their own political authority (2013a:9).

As a result, instead of completely destroying the enemy's military unit, as in old wars, the main goal in new generation wars is to break the determination and will of the people of the target country to fight and to weaken the faith of the target people in their own government and army. This change in approach can be attributed to the rising human and material costs associated with traditional conventional wars. As the economic, political, and socio-psychological implications of such conflicts become more apparent and as the cost of war weapons increases as a result of the developments in war Technologies, states are actively seeking alternative methods of warfare that allow them to mitigate these costs.Thus breaking the target country's will to fight will also mean that the other side will accept the desired policies without the need for these costly conventional wars and weapons. By doing so, they are also able to achieve their objectives while minimizing the negative repercussions typically associated with conventional wars.

In today's era, warfare has evolved to encompass a multitude of facets and dimensions. As a result, nations engage in operations across a wide range of areas, including political, diplomatic, economic and like. These operations occur not only on land, but also in the air, at sea, in space, and in cyberspace. What sets modern warfare apart is the ability to conduct simultaneous actions at both the physical and

cognitive levels, allowing states to effectively operate and counteract their adversaries on multiple fronts. Due to the rapid advancements in technology, wars have now been broadcasted and as a result, the way in which wars are conducted and perceived has undergone a significant transformation. With the advent of unmanned aerial vehicles and satellite technology, battlefields have become easily accessible and their events can now be witnessed almost instantaneously. This has resulted in a heightened level of public interest and engagement in the losses and progress experienced on these battlefronts. In essence, the interplay between technology, media, and warfare has created a complex dynamic. It has enabled the public to be more closely connected to the realities of war, while also empowering governments to manipulate perceptions through strategic media tactics. As a result, the role of technology in modern warfare extends beyond the battlefield, encompassing the realm of public opinion and the use of propaganda for political gain. Furthermore, the media and the internet have evolved into influential platforms that possess the ability to shape public opinion. As a consequence, governments and states have recognized the potential of utilizing these tools to their advantage and have incorporated media and propaganda strategies into their overall military plans. This integration serves as a means to exert pressure and sway public sentiment in order to further their own objectives and agendas during times of conflict (Yılmaz,2021:231-232).

The advent of mobile phones, the widespread availability of internet access, and the proliferation of social media networks have revolutionized the character of warfare. These technological advancements have shattered the rigid chain of command that traditionally characterized military operations, allowing parties involved in conflicts to organize themselves in a more horizontal manner. This decentralization has enabled dispersed planning and execution, granting greater flexibility and adaptability to combatants. Additionally, the use of psychological operations and cyber warfare techniques has further transformed the dynamics of warfare. These strategies can now be employed irrespective of a physical front or the absence of hostilities, enabling combatants to discredit their adversaries, manipulate the perceptions and opinions of target audiences in line with their own interests, and sabotage the enemy's information processing infrastructure by infiltrating their information systems (Gürcan,2012:111).

It is anticipated that unconventional security threats, such as those related to cyber security, limited energy resources, water disputes, and trade conflicts, will continue to grow in significance in the coming years. With the advent of a new era marked by strategic uncertainties and the emergence of transnational threats, the character of conflicts has undergone a transformation. In response to this changing security environment, nations have recognized the need to transform their armed forces, which were initially designed to combat inter-state conflicts. However, in this new era, military forces must also be prepared to confront non-state adversaries and address non-traditional threats (Yılmaz,2021:102). For instance, the U.S. Army has established a specialized Cyber Command, comprising of cyber experts who are trained to engage in both offensive and defensive cyber operations (U.S. Cyber Command, n.d.).

In response to the sixth question, the economics of the new generation of wars has also changed, giving rise to a concept called 'war economy'. In the past, conflicts were funded by governments through taxes or support from external sources. However, in modern times, a new phenomenon has emerged known as the war economy, which relies on the perpetuation of violence. This means that war has become commercialized, with financial gain playing a significant role in motivating conflicts. Some experts, like Kaldor, go as far as suggesting that economic interests drive wars, but it can be challenging to differentiate between those who exploit political violence for economic purposes and those who finance their political causes through economic activities. In these contemporary conflicts, funds are

generated through various illegal means such as kidnapping, smuggling of items like oil, diamonds, drugs, and other illicit goods (Kaldor,2013b:3).

The war economies seen in the two world wars were centralized, all-encompassing, and self-sufficient. However, the new globalized war economies differ greatly in that they are decentralized, have low participation in the war effort, and suffer from high unemployment rates. Additionally, these economies heavily rely on external resources. As a result, domestic production drastically declines due to global competition, physical destruction, or disruptions in normal trade, leading to a decrease in tax revenue. To compensate for this, the fighting units resort to financing themselves through illegal means such as plunder, hostage-taking, and the black market, or by seeking external assistance. This assistance can come in various forms, including remittances from diaspora communities, exploitation of humanitarian aid, support from neighboring governments, or engaging in illicit trade such as arms, drugs, valuable commodities like oil or diamonds, or even human trafficking. It is important to note that all of these sources of funding can only be sustained through the perpetuation of violence, which becomes ingrained within the functioning of the economy. This regressive system of social relationships, which is reinforced by war, has a tendency to spread across borders through the movement of refugees, organized crime, or the marginalization of ethnic minorities (Kaldor,2013a:10). Additionally, in his 1994 study, Duffield delves into the complex connections between localized conflicts and the global war economies. His research sheds light on the extensive networks that exist, ranging from legal to illegal trade, arms and drug trafficking, as well as the involvement of corrupt governments and diasporas that contribute to the initiation and continuation of violent conflicts.

Regarding the seventh question, in terms of the weapons utilized in the new generation wars, Creveld argues that they will not be as costly or heavy as those used today. Instead, he predicts the emergence of weapons that are affordable, compact, easily mass-produced, and versatile in their deployment. However, he also cautions against the misconception that these weapons would make warfare less deadly. As the involvement of private military units and terrorist organizations in conflicts becomes more prevalent, there is a growing demand for simple, portable, and cost-effective weapons (1991:229). Additionally, Gürcan highlights the increasing threat posed by cyber weapons, which have become a concern for countries due to the rapid advancement of technology and the proliferation of internet-based critical infrastructure systems (2012:107).

To answer the eighth question, Kaldor argues that new wars are intricately linked to the process of globalization, where the traditional boundaries and distinctions between state and non-state actors, the public and private sectors, domestic and foreign affairs, the realms of economy and politics, and even the notions of war and peace become increasingly hazy and indistinguishable (Kaldor, 1999:24). In today's world, the distinction between periods of peace, crisis, and war has become less clear in contemporary conflicts. This shift has had a profound impact on global security, as it has allowed nations to utilize unconventional methods and strategies to achieve their strategic goals, regardless of the current state of affairs. Unlike in the past, states now have the capability to sustain their involvement in conflicts through unconventional means, such as cyber attacks, terrorism, manipulating information, and employing various other tools. This ability remains active even during times that would traditionally be considered peaceful or in crisis (Gürcan, 2012:109). In the realm of traditional warfare, the commencement of conflicts is typically marked by formal declarations, and these battles are often constrained by specific timeframes for their initiation and conclusion. However, the landscape of warfare has undergone a significant transformation in contemporary times, giving rise to what is known as new generation wars. Within this context, the precise demarcation of when a war begins and ends has become increasingly intricate and convoluted (Mello, 2012:3). In the context of modern warfare, a

distinct blurring of boundaries has materialized, particularly with regards to the intentional targeting of non-combatants and the mounting challenge in discerning between friend and foe. This has effectively eroded the once clear-cut distinctions that separated soldiers from civilians, thereby muddling the lines that were once so firmly drawn (Yılmaz, 2021:209).

In previous times, it was widely accepted that a powerful and technologically advanced military, both in terms of numbers and capabilities, would always emerge victorious. However, this belief no longer holds true in the present day. Furthermore, victory is no longer determined by a single war or a series of short conflicts, but rather it is achieved over a longer period of time and is spread out. The character of war has undergone a transformation, where the ultimate objective has shifted towards intangible and hard-to-quantify factors. These factors include undermining the enemy's determination and resolve. As a result, the concept of victory has become unclear and there is a lack of consensus on how it should be defined and measured. Different perspectives on the matter have emerged, further adding to the complexity of understanding what constitutes victory in modern warfare (Gürcan,2012:109).

In response to the last question, the symmetry of wars has also changed and wars have become asymmetric. Modern conflicts are carried out by unconventional, that is, asymmetrical force elements. One the one hand, there are well-equipped states that possess advanced resources and capabilities, yet face challenges such as insufficient backing from the public, intense global scrutiny, and restrictions imposed by political and moral considerations within the boundaries of international laws and norms. On the other hand, we have irregular fighters who operate in a completely different manner. These fighters are typically organized into small, decentralized groups and rely on light weaponry rather than sophisticated military hardware. Unlike well-equipped states, these irregular fighters do not conform to international law, but instead, they are driven solely by their unwavering commitment to their cause. Despite their limited resources and military power, they draw immense strength from the support they receive from their local communities, which fuels their determination to continue their struggle (Yılmaz,2021:103). In his analysis, Mello highlights the increasing significance of asymmetric warfare strategies in contrast to the traditional notion of symmetrical encounters between regular military units. Furthermore, he emphasizes that terrorism has emerged as a pivotal component within the context of contemporary warfare tactics (2010:5-6).

In Münkler's analysis, the concept of the asymmetricalisation of war refers to the scenario where unequal adversaries engage in conflict. He posits that a strategic approach that prolongs the duration of war and slows down the progression of events can provide an opportunity for a weaker party to mount a successful armed resistance against a stronger opponent who possesses an advantage in terms of both military technology and organization. Typically, a militarily superior force with advanced technological capabilities tends to hasten the pace of war. However, this accelerated approach comes with a cost, and sometimes that cost is simply too high to bear. It is important to note that victory in war is not solely determined by the side with greater material resources and more sophisticated technological advancements. In addition, he contends that future wars will exhibit a distinct asymmetry in the competition between high-tech and low-tech weaponry. The mere possession of highly advanced technological armaments does not guarantee victory in these conflicts. He asserts that the deliberate slowing down of violence, as witnessed in guerrilla warfare, can only be effectively employed when a vast majority of the population perceives no alternative solutions to their social, economic, and political dilemmas apart from engaging in warfare that will inevitably result in significant casualties and extensive devastation. This scenario could plausibly unfold due to the multitude of emerging challenges

in the twenty-first century security landscape, prompting the population to view armed conflict as their sole opportunity for a better future (Münkler,2003:7-10).

As previously discussed, new and old wars share some similarities but also possess significant differences. To provide a comprehensive understanding, the following table summarizes the most notable and essential characteristics that distinguish new wars from old wars. By examining these distinctive features, a clearer picture can be formed in terms of the evolution and transformation of warfare over time.

Table 1: 'Old' Wars vs. 'New' Wars

Components	**Old Wars**	**New Wars**
Aim	– Realization of national and state interests – Geopolitical, ideological and financial motives	– Political control – Identity politics (ethnic, religious or tribal)
Actors	– Nation-states;conventional armies	– Non-state actors; paramilitary groups, mercenaries, cyber warriors, criminals. PMCs etc.
Target Group	– Enemy-centered approach; the physical existence and the determination/will of the enemy	– People-centered approach; the hearts and minds of the people
Field/Front	– Traditional physical battlefield	– Informational and spiritual domains – Cyberspace
Methods and Strategies	– Conquering territories – Physical destruction of the enemy – Traditional military tactics – Use of force	– Influencing the hearts and minds of people: information operations and propaganda etc. – Spreading fear – Use of intimidation and suppression
Economy of War	– Government funds through taxes and external sources; – Centralized	– Financing through illegal means and perpertuation of violence – Commercialized – Decentralized
Weapons	– Traditional, costly, heavy	– Affordable, compact, mass-produced,versatile

Beginning and End of War	– Defined beginning and end – Declaration of War – Clear distinctions	– Hazy and indistinguishable boundaries between war, peace and crises – Continued employment of unconventional means in times of peace
Symmetry	– Symmetric Force Elements: regular military units	– Asymmetric Forces

3.1. Understanding the Change in War : Generations of Warfare

The post-Cold War era, marked by a period of strategic uncertainty, has brought about significant shifts in the way wars and security are perceived due to the forces of globalization and advancements in technology. These changes have not only affected the actors involved, but also the objectives pursued, the financing mechanisms employed, and the weapons and tactics used in modern warfare. In order to better understand the distinctions between past and present conflicts, some scholars have proposed a generational framework that categorizes wars based on the internal changes and transformations they have undergone. This section aims to delve into the analysis of wars by categorizing them into four generations.

3.1.1. First Generation Warfare

First generation wars refer to the form of conflict that took place between the signing of the Peace of Westphalia, following the religious wars in Europe, and the American Civil War of 1860. These wars predominantly involved a considerable number of infantry soldiers armed with smoothbore musket rifles, and they employed line and column tactics. Soldiers were strategically positioned in a linear formation, standing side by side, typically on large and flat battlefields (Gürcan,2012:87-88). In this particular form of warfare, the primary tools of combat are cannons and muskets that require loading from the muzzle. Technological advancements and strategic movements are limited. The effectiveness of artillery and cavalry is constrained, as they can only provide partial support to the infantry. The battlefield becomes obscured by a thick cloud of smoke from the gunpowder gases released by rifle and artillery fire, making it difficult to see and navigate. Any soldiers who deviate from the established line order are at risk of being killed either by their own comrades or by the enemy forces. Traditional tactics such as deployment, maneuvering, and deception are discouraged (Aras,2022:12). The primary goal of the military is to acquire and retain authority over a particular region, without considering the potential sacrifices that might be necessary in the process (Yılmaz,2021:116).

In the first generation of warfare, the battlefield was systematically organized, and this organization played a crucial role in the establishment of structured military units. This traditional form of warfare involved a clear differentiation between soldiers and civilians, which was achieved through the utilization of various symbols such as salutes and military uniform rank grades. The purpose behind incorporating these symbols was to foster a sense of discipline and adherence to military hierarchy, ultimately cultivating a culture centered around military order. As stated by Hammes this approach was deemed effective in maintaining control and ensuring the smooth functioning of the armed forces (2005: 196).

During the 19th century, significant changes occurred on the battlefields that disrupted the established order and ushered in a new era of warfare. This transformation was primarily driven by technological advancements and innovations such as the invention of barbed wire, machine guns, and rifled muskets. These developments marked the end of the first generation wars, which were characterized by line and column tactics. Traditional armies struggled to adapt to these changes and were forced to develop new strategies and tactics to effectively engage in combat on the disorganized battlefields (Lind et al.,1989:24).

3.1.2. Second Generation Warfare

During the early to mid-20th century, a new style of warfare known as second generation warfare emerged, particularly during the First World War. This approach to warfare was heavily influenced by the French, who developed the concept of using firepower and attrition as key strategies. The primary objective of second generation warfare was to gradually wear down the enemy by causing significant losses in combat power, while simultaneously capturing and occupying territories using heavy weapons like artillery fire and infantry units. Overall, second generation warfare represented a significant shift in military strategy, emphasizing the importance of firepower, central control, and the utilization of various auxiliary classes. This approach laid the groundwork for future developments in warfare and set the stage for further advancements in the field of military tactics and technology. To effectively execute this strategy, a high level of coordination and central control was required. Commanders would meticulously synchronize the use of firepower, infantry, tanks, and artillery, issuing detailed plans and orders to ensure their forces worked in harmony. With advancements in technology and the Industrial Revolution, the importance of weapons like machine guns and artillery grew significantly, as they provided increased firepower on the battlefield. The complexity of the battlefields during this period led to the development of various auxiliary classes alongside the traditional combat units. These auxiliary classes, such as personnel, maintenance, and quartermaster, played crucial roles in supporting the overall war effort. As warfare became more intricate and demanding, it became evident that specialized roles were needed to handle the logistical and administrative aspects of combat (Yılmaz,2021:116-117).

During this era of warfare, a new class known as "divisions" and a staff class emerged, which played a crucial role in providing the commander with technical information and headquarters support. Their assistance was invaluable in the decision-making process and navigating the complexities of military operations. Additionally, this period saw the removal of nobles who lacked strong leadership skills from officer ranks, and the establishment of a merit-based promotion system and a formal military education system. The development of railways in the 1850s revolutionized the relocation, control, and coordination of large troops and ammunition, making it quicker and easier. Trains also facilitated force shifts and strategic maneuvers, while the introduction of telegraphy greatly improved communication speed and aided in the command and administration of troops. Moreover, the utilization of steam engines and advancements in armor technology in warships led to the creation of a more formidable and lethal naval force (Aras,2022:13-14).

With the advancements in weaponry, particularly infantry rifles and artillery, the scope of the battlefield expanded significantly. Moreover, these technological developments also led to a substantial increase in the size of armies. During the early 20th century, headquarters underwent a transformation, becoming more comfortable spaces where issues like nutrition, heating, and hot water were properly addressed. The use of telegraph communication became increasingly prevalent in these headquarters as well. As a groundbreaking milestone, military use of airplanes commenced in 1908, and by 1914, major European powers such as England, France, and Germany had established formidable air forces. In the context of the First World War, airplanes were primarily utilized for reconnaissance missions on the battlefield. Furthermore, the second wave of warfare witnessed the inclusion of women in professional military service, marking a significant shift in the composition of armed forces (Gürcan,2012:88-89).

In the context of the second generation war, the utilization of technology played a pivotal role in shaping the strategies employed. It is noteworthy that this era of warfare placed a significant emphasis on upholding a sense of structure and organization. The adherence to rules, procedures, and orders became of utmost importance, surpassing the value of individual initiative. The military forces did not encourage or require their members to take independent action, as it posed a potential threat to the synchronized efforts of the entire unit. The enforcement of discipline cascaded down from the highest ranks to all levels within the military establishment (Yılmaz,2021:118).

3.1.3. Third Generation Warfare

During the second generation wars, there were close-range and hot conflicts that heavily relied on firepower and attrition. These battles resulted in significant military and economic setbacks. Consequently, military strategists began devising a new approach to warfare, one that aimed to achieve victory by compelling the enemy to surrender through swift movements and agile tactics. The objective was to prevent the enemy from having the opportunity to establish defensive or offensive formations by

swiftly overpowering them. This era of warfare became synonymous with the German's innovative 'lightning tactics,' which were centered around non-linear maneuvers and the utilization of speed as a crucial element (Şengönül,2018:25). According to the 'Blitzkrieg doctrine', the primary objective was to identify the weakest point in the enemy's defense, typically located on their flanks, in order to draw them towards the center and ultimately encircle and gain control over them. This strategy involved penetrating deep into the enemy's rear and launching attacks from the sides, effectively cutting off their supply routes, isolating them from external assistance, and fragmenting their forces into smaller units that could be either annihilated or forced to surrender. The ultimate goal of this approach was to catch the enemy off guard, utilizing highly skilled maneuvers and rapid movements to achieve a decisive advantage in the battlefield (Gürcan,2012:90-91). To put it differently, an army that experiences a breakdown in its integrity, fails to address its logistical requirements, and lacks a cohesive command structure is destined to fall apart. Consequently, rather than functioning as a unified and formidable force, the objective shifts towards dismantling the enemy's defenses by deploying fragmented and inadequate units (Yılmaz,2021:119).

Third-generation warfare centers around the principles of speed, tempo, and maneuverability, aiming to exhaust the adversary both physically and mentally by constantly placing them in unforeseen and perilous circumstances at a pace they struggle to keep up with. Unlike previous generations of warfare, the current era allows leaders at various levels of command to exercise their own judgment and take independent actions, unencumbered by strict hierarchical structures. Instead, they are encouraged to closely analyze the situation, assess the capabilities and intentions of the enemy, and determine the most appropriate course of action accordingly (Hammes,2005:199-200).

During this era, the tank emerged as a highly influential weapon of power on the battlefields. Its introduction brought about a significant multiplier effect due to its unique combination of manoeuvrability and superior firepower. Furthermore, advancements in torpedo and submarine technologies, the rise of aircraft carriers, the expansion of fighter aircraft's range and capabilities, and the evolution of naval and air manoeuvre tactics have greatly enhanced and expanded the scope of warfare (Lind,2004:13). Once again, as technology continued to advance, the notion of "total war" emerged, where not only military targets, but also economic infrastructures and innocent civilians within the enemy's territory became subject to attacks from fighter aircraft, missiles, and even the devastating power of nuclear weapons. This concept of "total war" was a direct result of the experiences and lessons learned from the horrors of World War I, and it further solidified the doctrine of total warfare. Moreover, the successful implementation of encircling manoeuvre warfare during World War II completely transformed the traditional battlefield, rendering the notion of a linear front line obsolete (Gürcan,2012:91).

The era of third generation warfare is characterized by a shift in tactics from direct combat and annihilation of enemy forces to a more strategic approach. Instead of engaging in hand-to-hand combat, the focus is on infiltrating enemy lines, surrounding them, and breaking them down into smaller, more manageable units that are harder to defend against. This new approach also involves the development of defensive strategies that go beyond traditional straight-line fronts, adopting a more multidimensional and in-depth approach to warfare. Ultimately, this change in tactics transforms the character of war into a more transverse and multi-faceted phenomenon (Gürcan,2012:91-92).

3.1.4. Fourth Generation Warfare

In 1989, the US Marine Corps Journal published an article titled "The Changing Face of Warfare: Towards Fourth Generation Warfare," written by William S. Lind, Keith Nightengale, John Schmitt, and Joseph Sutton. This article aimed to analyze the power vacuum created by the collapse of the USSR during the Cold War in the 1980s, as well as the new challenges brought about by globalization. The authors introduced the concept of fourth generation warfare, which they defined as a type of warfare that blurs the lines between war and peace, as well as between civilian and military aspects. Unlike previous generations of warfare, where battles were confined to specific battlegrounds, fourth generation warfare infiltrates every aspect of society. It is characterized by its asymmetric nature and involves the use of military, semi-military, and sometimes even civilian elements (Lind et al.,1989:22-26).

One of the main reasons why the distinction between war and peace becomes blurry in this type of warfare is because states are engaged in a continuous state of conflict with terrorist organizations that do not adhere to traditional warfare tactics. What sets the Fourth Generation Warfare apart from previous generations is the involvement of at least one party that is not a conventional military force operating under the control of a state government. Instead, this party is often an organization that surpasses national borders. In essence, Fourth Generation Warfare can be described as a transformation into a decentralized form of warfare that blurs the boundaries between war and politics, military and civilian, peace and conflict, as well as the concepts of battlefield and security. (Lind, 2004:13-14).

In situations where clear borders are absent, transitional areas emerge, creating an informal environment where it becomes challenging to distinguish between civilians and soldiers, war and security zones, and peace and conflict. This complexity necessitates a comprehensive approach that utilizes political, economic, social, and military tools to persuade enemy decision-makers that their objectives are unattainable and too costly to pursue. Unlike traditional warfare, fourth generation warfare is not solely focused on achieving military victory; rather, its primary objective is to politically incapacitate the enemy through disinformation campaigns and prolonged low-intensity conflicts, thereby weakening the resolve of enemy decision-makers. As a result, the notion of victory in fourth

generation warfare has become abstract and difficult to define, leading to varying interpretations and debates on how to assess and measure success (Aras,2022:15:16).

According to Thomas X. Hammes, fourth generation warfare can be seen as an evolved version of insurgency tactics that leverage the interconnected networks within societies to sustain the ongoing conflict. In this type of warfare, the primary objective for practitioners is to persuade political leaders on the opposing side that their strategic goals are either unachievable or not worth pursuing in light of their loftier aspirations. Hammes supports this notion by emphasizing the critical role of strong political determination, which, when effectively employed, can triumph over superior economic and military might (2005:201).

Fourth Generation Warfare employs new tactics that have not been seen in previous generations. These tactics are used to weaken the resolve of a stronger adversary, with the ultimate goal of demoralizing them and reducing their will to win. It is important to note that 4GW is not solely a military revolution, but also encompasses political, social, and moral aspects. This multifaceted nature of 4GW means that military power plays a distinct and crucial role, different from its role in previous generations of warfare. In fact, 4GW is often described as an unconventional form of warfare that prioritizes political, diplomatic, and economic initiatives as much as traditional military strategies (Hammes, 2005: 201-202).

In the modern era of warfare, the traditional concept of war being solely controlled by the state has evolved. Instead of state armies being the primary actors in conflicts, we now see non-state entities asserting themselves as powerful forces. This shift is a result of both globalization and localization, which have weakened the sense of citizenship and national identity that once bound individuals to their states. Consequently, the notion of the nation-state has also been diminished. The character of war has been altered, allowing various non-state actors like individuals, criminal organizations, religious extremists, and ethnic violent movements to exert influence alongside the state's uniformed law enforcement forces. The emergence of non-state organizations that rely on warfare for economic gain has led to prolonged and inconclusive conflicts. Furthermore, the presence of private military companies has turned the field of security into a commercialized venture, transforming "security" into a marketable service. Faced with increasingly complex security threats, nation-states have sought less risky and less expensive alternative methods of warfare. Instead of engaging in costly conventional wars, they now employ indirect tactics to gradually wear down their adversaries. Another factor contributing to the erosion of the nation-state's monopoly on warfare is the influence of non-governmental organizations (Gürcan,2012:96-100).

In the traditional concept of warfare, power was primarily concentrated within states, with their armies serving as the primary actors. However, in the modern era of fourth generation wars, the dynamics have shifted dramatically. These conflicts now involve not just uniformed soldiers

representing the state, but also a plethora of unconventional participants such as unarmed saboteurs, propagandists, cyber warriors and sympathizers. This expanded spectrum of warfare has blurred the lines between state and non-state actors, as self-proclaimed power groups and specialized agents now play significant roles in the field (Lind, 2004:13).

An additional characteristic of fourth-generation wars is the shift from traditional approaches that rely on kinetic and conventional military power. In these modern conflicts, the objective is no longer solely centered on physically eliminating the enemy or breaking their will to fight. Instead, the focus is on achieving victory through psychological and ideological influence on the enemy. This change in strategy is driven by the fact that conflict environments now often involve densely populated areas where civilians reside, prompting a shift towards a people-centric approach to warfare. As a result, the primary goal of these new generation wars is not to destroy the enemy's physical presence or gain control over specific territories. Rather, it revolves around gaining control of the population and garnering popular support. Although this approach may require a significant investment of time and resources, it is imperative to carry out the effort in a methodical manner, divided into several distinct phases. These stages encompass a comprehensive plan to eliminate the presence of the enemy’s hostile forces within the region, gain the trust and cooperation of the local inhabitants, restore or strengthen governmental control, initiate the process of reconstruction and rehabilitation, and ultimately foster a lasting and mutually beneficial connection with the individuals residing in the area (Gürcan,2012:103-104).

The concept of traditional warfare, where soldiers were driven by the instinct to kill before being killed, has drastically changed in modern warfare. The focus has shifted from a mindset of conquering and eliminating the enemy through physical force to strategies that prioritize the well-being of the people. In 4th generation wars, the primary objective is to preserve the lives of the people in the targeted area, to gain their trust and support, and to win over their minds and hearts. These wars revolve around legitimacy in the eyes of the local population, requiring individuals who are intimately familiar with the region's social and psychological dynamics, culturally adaptable, fluent in the local language, and capable of comprehending the emotions, thoughts, perceptions, and opinions of the local people (Gürcan,2012:110).

According to David Kilcullen, there are two important aspects to consider when it comes to public support: the emotional and sociopsychological element, referred to as the "hearts" dimension, and the cognitive aspect, known as the "minds" dimension. The concept of hearts involves the art of influencing individuals by demonstrating how their own personal well-being and prosperity are intricately tied to your achievements. It entails convincing them that supporting and aligning themselves with you is the most beneficial course of action. On the other hand, the notion of minds revolves around the ability to win over people's trust and confidence by assuring them that you possess the necessary capabilities to safeguard their interests. It entails demonstrating your competence and reassuring them that opposing

or resisting you would ultimately prove futile and unproductive. In essence, the fundamental objective within the realm of fourth generation warfare is to establish a deep-rooted connection and common ground between the populace's beliefs and their personal interests, as this is pivotal in order to garner widespread support (2006:5).

Due to this reason, the approach centered around individuals is not limited to military and security strategies alone. Instead, it necessitates a comprehensive understanding of various behavioral sciences, including sociology, social psychology, theology, economics, international relations, business, management, organization, and foreign languages. Consequently, the application of this approach demands an interdisciplinary perspective. Hence, it is highly preferable for the personnel responsible for implementing the 4GW to possess a hybrid profile, encompassing both military and civilian expertise (Gürcan,2012:106).

In the modern era of warfare, the traditional notion of a physical front has been redefined due to the emergence of the Fourth Generation Warfare. This new form of warfare transcends physical boundaries, as the cyber world has emerged as a critical battleground. Cyber-attacks have become a significant aspect of warfare, capable of being executed from multiple dimensions and across various scenarios – be it during peacetime, times of crisis, or even in the midst of war. These attacks have now become a pivotal element in shaping the dynamics of contemporary warfare (Gürcan,2012:107). In Fourth Generation Warfare, the tactics employed have expanded beyond just traditional military strategies. Now, there is a recognition that military, political, economic, and socio-psychological means can all be utilized to undermine the enemy's resolve. By employing techniques such as psychological operations and cyber warfare, it is now possible to weaken the enemy's credibility, manipulate public opinion to align with friendly interests, target and disrupt the enemy's information infrastructure, and gather valuable intelligence by infiltrating their information systems. These tactics can be employed not only during times of crisis or war, but even in times of peace, blurring the lines between traditional battlefronts and the virtual realm (Gürcan,2012:109).

The media plays a crucial role in the implementation of the 4GW, as it not only controls the flow of information but also shapes public perception. Its significance cannot be overstated when it comes to managing how the 4GW is executed. Nowadays, there is a deliberate attempt to blur the lines between reality and fiction, with the aim of creating a virtual battleground where historical narratives of victimization are intertwined. This approach essentially positions today's conflicts as a natural progression of past confrontations. Additionally, another significant aspect that sets fourth generation warfare apart from traditional warfare is the specific arena in which the operations are carried out. While the armed forces of states place great emphasis on the tactical battlefield, this aspect holds less significance for the fighters engaged in 4GW (Lind, 2004: 13-14).

In the realm of 4th generation warfare, the traditional divisions of peace, crisis, and war have become blurred and intertwined. The clear separation between these periods no longer exists. States now have the ability to actively combat new elements of warfare, such as information operations and terrorism, even during times of peace and crisis. The belief that a strong and technologically advanced military will always be victorious is no longer valid. Instead of a single war or a series of short-term conflicts determining the outcome, warfare now extends over a longer duration and spans a greater period of time. Furthermore, the goal of war in 4th generation warfare has shifted towards abstract and difficult-to-measure objectives, such as breaking the enemy's resolve and determination. As a result, the concept of victory has become ambiguous, and numerous conflicting perspectives on what constitutes victory and how to measure it have emerged (Gürcan,2012:109). The 4GW primarily involves non-state actors who are engaged in conflicts against one or more states. These actors have distinct perceptions, values, and battlefield strategies, resulting in ongoing asymmetric conflicts. Consequently, the character of these conflict environments is becoming increasingly complex. Unlike traditional warfare where success is evaluated based on certain parameters, the criteria for success vary significantly for the warring parties involved. Thus, even if the state side possesses greater strength, it does not guarantee victory in practical terms. This can be attributed to the notion that states are inherently more politically vulnerable in asymmetric environments and tend to suffer greater losses as the weaker side (Jayachandran,2009:174).

In general, it is commonly believed that the occurrence of convetional conflicts will be rare within the framework of the 4GW. Furthermore, if conflicts do arise, they are likely to be less brutal compared to traditional military conflicts in terms of the magnitude of violence, the deployment of troops, or the number of casualties. However, this does not imply that the overall level of violence within the 4GW will be lower than in a conventional war. On the contrary, given that the 4GW encompasses cultural and religious disputes, it is anticipated to evoke a heightened level of emotional intensity. Consequently, the animosity and hostility experienced in individuals' minds may surpass that experienced in realpolitik wars. Hence, conflicts within the 4GW may not always follow rational patterns or logical reasoning (Lind et al.,1989:25-26). By employing every possible resource at their disposal, they will make concerted efforts to impede and overcome the aspirations of the opposing faction or society. Simultaneously, they may strive to instill their beliefs and recruit potential allies through targeted dissemination of accurate or misleading information, bolstered by meticulously planned and executed physical demonstrations. In the realm of the 4GW, it is ultimately the psychological and emotional resilience of the populace that will wield the most profound influence in determining the ultimate outcome (Jayachandran,2009: 174-175).

Given that 4GW practitioners typically consist of regionally based trans-national groups lacking traditional armies, their approach to tactics differs greatly from conventional armed forces. Instead of employing uniformed militants, they rely on a combination of terror, revolutionary methods, and

unconventional strategies. Many of their actions bear resemblance to guerrilla warfare or low-intensity conflict. These tactics involve carrying out distributed operations, engaging in sabotage, targeting civilians with violence, and even resorting to ethnic cleansing. Moreover, the systematic elimination of leaders within the targeted community or group is an inevitable aspect of their approach. Furthermore, it is distressingly evident that numerous groups exploit the vile act of gang rape and sexual harassment as a means of defilement (Jayachandran,2009:175).

The phenomenon of globalisation has brought about noteworthy progress in communication, and information technologies. These modern-day technologies have become increasingly accessible, affordable, and user-friendly, thereby simplifying the ability of actors involved in the Fourth Generation Warfare to operate in dispersed, small groups. Through these advancements, these groups are able to communicate, coordinate, and campaign over a network without the need for a central command, all while effectively concealing the identity of their leaders. Consequently, this poses a challenge in identifying and reaching the individuals accountable for acts of warfare that states encounter (Jayachandran, 2009:176).

CHAPTER IV
Cyber Warfare And The Changıng Character Of War

4. Cyber Warfare and the Changing Character of War

Throughout the course of human history, war has been a constant presence, with individuals harnessing its power for various reasons. However, as we enter the 21st century, the character of warfare has undergone profound changes due to globalization and rapidly advancing technology. This transformation has resulted in wars taking on an entirely new dimension, with a wide range of actors becoming involved compared to previous eras. Today, conflicts are not limited to battles between two nations and their respective armies; they now encompass a diverse array of non-state entities. What further amplifies the significance of this evolution is the fact that cyberspace has become a platform where all types of actors can thrive, granting them the capability to wield power.

With the rapid advancements in communication technologies, the incorporation of the internet into various aspects of our daily lives has not only made things more convenient but has also exposed us to potential security risks. Deliberate actors with malicious intentions are actively leveraging cyber attack tools to exploit these vulnerabilities for their personal gain. Additionally, the battle between nations has now extended into the realm of cyberspace. This is primarily due to the heavy reliance on internet-based critical infrastructure systems, public and private services, and information systems. Consequently, the security of information and services in this domain has become a pressing issue of great importance.

The emergence of cyberspace has raised the notion that the destructive potential traditionally associated with conventional warfare can now be achieved through the use of a single computer, all at a significantly reduced expense. This is particularly relevant in light of the escalating tolls, both in terms of human lives and financial resources, that have been exacted by wars over the course of the past century. Furthermore, there is a growing societal aversion towards violence, with the general public expressing a negative perception towards such acts. Consequently, cyber attacks have garnered increased appeal and are viewed as a more desirable substitute to the physical and kinetic conflicts that have characterized historical warfare.

This shift in warfare has also led to a redefinition of what constitutes a strong or weak state. Today, merely having a large military force and extensive weaponry is not enough to be deemed strong. A state is now considered strong based on its ability to adapt to technological advancements, shield itself from surrounding threats, and act as a deterrent. The realm of cyberspace has emerged as a battleground where forces of varying strengths can clash. In this domain, victory is no longer determined by who possesses more ammunition, but rather by who can effectively control and manipulate information, as well as wage a psychological war to win over hearts and minds.

This section will examine the same questions that were raised in the previous chapter regarding the transformation of the character of warfare, but this time focusing specifically on cyber warfare. A comprehensive analysis will be conducted to explore the significance and position of cyber wars within the present-day landscape of conflicts. Although cyberspace undoubtedly alters the character of warfare, there are ongoing debates regarding its classification as a distinct form of warfare within the realm of new generation war concepts. This section will also address and explore these debates in detail.

4.1. How Does Cyber Warfare Change the Character of War?

4.1.1. Aims

In cyberspace, state and non-state actors engage in a constant struggle driven by a myriad of motivations, including geopolitical interests, ideological beliefs, religious affiliations, economic ambitions, political agendas, and even military objectives. The nature of this virtual environment is fraught with uncertainties, making it challenging to ascertain the true identities and motives of those behind cyber attacks. However, it is crucial to recognize that such attacks can serve a multitude of purposes. From an old war perspective, to fully comprehend the geopolitical and ideological backdrop of attacks, one must possess a deep understanding of the regional dynamics, historical context, and political landscape within which the actors and their organizations operate. In essence, when attempting to identify the state responsible for an attack and decipher its underlying purpose, it is imperative to consider and analyze the wealth of regional, historical, and political information available. If we were to analyze the denial of service attacks in Estonia in 2007 and the cyber-attacks during the Russia-Georgia War in August 2008 from a broader geopolitical and ideological perspective, it becomes evident that both Estonia and Georgia were once part of the Soviet Union, and Russia, as the successor state, aimed to assert its geopolitical and ideological influence over these nations. Consequently, it can be inferred that these attacks were orchestrated by Russia as a means to safeguard its interests in these countries.

An argument can be made that the motivation behind Stuxnet is connected to the desires of certain countries to restrict Iran's nuclear capabilities. While territorial expansion is not a factor in this case, the objectives of Stuxnet can be discussed in terms of geopolitical interests, political power, and financial gains. The states' interest in limiting Iran's nuclear facilities is believed to be directly tied to their defense policies, as they aim to eliminate the risk of new nuclear weapons. Some argue that the United States and its allies' position in the Middle East is at risk due to Iran's dominant presence, and if Iran were to possess nuclear weapons, the influence of the US and its allies would diminish. After the Shiite ulama rose to power in Iran following the revolution, there was a notable shift in the country's foreign policy objectives and priorities, leading to a significant change in how Iran perceived its allies and adversaries. Gone were the days when Iran was considered a crucial ally of the Western nations in the Middle East; instead, it transformed into a nation that actively promoted policies that were vehemently against the

West. With a strong anti-Israel stance, Iran has now become one of the "enemy" countries that not only disrupts the regional order, but also challenges the global system, all while possessing nuclear capabilities. Consequently, it becomes imperative for the Western powers to engage in a relentless battle against Iran (Küpeli, 2016:44). Taking into account the intense regional competition involving Iran, whose stance towards Israel has grown increasingly hostile following the revolution, Israel, perceiving Iran's nuclear activities as a direct security concern, has escalated its assertiveness in response. Israeli officials firmly assert that Iran's nuclear program not only jeopardizes Israel's national interests but also poses a substantial threat to the stability of the entire region and the global order (Mercan, 2021:3).

However, if cyber attacks in Estonia and Georgia were evaluated in identity politics context, it can be argued that the Estonian and Georgian wars were identity-based conflicts. The identity based conflict in Estonia can be seen in the situation surrounding the 'Bronze Soldier' statue which serves as a symbol of the Soviet Union's triumph over Nazi Germany during World War II. However, it is important to note that the significance of the "Bronze Soldier" varies greatly within Estonian society, leading to much controversy. While some view the statue as a tribute to the soldiers who fought against the Nazi army and liberated Estonia, others see it as a reminder of the Soviet aggression that impacted the rest of the Estonian population. The dependence of Russian-speaking citizens in Estonia on Russian media outlets for information has created an ideal environment for spreading Russian propaganda and easily reaching these individuals. The core of this propaganda is based on the belief that those who fail to acknowledge and honor the Red Army's role in defeating Nazi Germany in Europe are sympathetic to fascist ideology and Nazi Germany as a whole. To effectively disseminate their message, Russia employs various propaganda techniques, such as circulating videos showcasing the Estonian police accompanied by Nazi music, defaming high-ranking Estonian officials by portraying them as fascists, and constructing narratives that depict Russian-speaking citizens as martyrs who have fallen victim to the violent clashes that occurred in Tallinn surrounding the "Bronze Soldier" monument (Khmelidze,2021).

According to Valeriano and Maness, the Estonian cyber-attack had a specific purpose: to teach Estonia a lesson for disrespecting Russian culture, history, and identity. This disrespect was perceived when Estonia decided to relocate the Bronze Soldier from its central location in Tallinn to a military cemetery (2015:143). Therefore, the main driving force behind these cyber attacks can be understood as identity politics. On one side, there were Pro-Russian activists who saw the Bronze Soldier as a symbol of the strong bond and shared history between Estonia and Russia. They felt grateful to Russia for liberating Estonia from Nazi control. On the other side, pro-Estonians viewed the statue as a symbol of oppression, specifically Soviet and now Russian, and found it offensive to their national pride and identity. Moving on to the conflict in Georgia, the goals were centered around identity and self-determination. Separatists in Abkhazia and South Ossetia used their Russian identity as a justification

to break away from Georgian authority, as they believed it would allow them to preserve their unique identities and determine their own fate.

In the context of the 21st century warfare, the focus has shifted from using identity as a mere tool to mobilize large groups of people, to making it a primary objective in contemporary conflicts. However, it is important to note that identity still serves as a means to an end, rather than being the ultimate goal in itself. The realm of cyberspace, which offers a unique platform for activities to occur rapidly and without geographical limitations, has the ability to leverage civilian nationalists, diasporas, seperatists, and geographically disconnected supporters ready to execute influence programs and DDoS attacks coordinated to complement national objectives. It is crucial to recognize that the objectives of wars cannot be simply reduced to identities, as they are shaped by a complex interplay of various factors including ideologies, economic considerations, and geopolitical aspirations. Nonetheless, it can be argued that it is, in fact, the means of achieving the goals that distinguishes the old and new wars from each other. In the light of these evaluations, it can be said that cyberspace provides the opportunity to act in line with the purpose of the actors, regardless of the type of purpose. Even though it does not provide the opportunity to physically seize a region, it can be said that it can be used as a force multiplier in this direction or it can be effective by mobilising all international people around the identity in attacks carried out for identity politics.

4.1.2. Actors

To begin with, cyberspace is a diverse environment that caters to a wide range of users, encompassing both ordinary internet users and highly skilled professionals working in crucial sectors of the government. This virtual realm transcends geographical boundaries and traditional limitations, providing a platform for non-state actors to connect on a global level, collaborate effectively, and orchestrate cyber-attacks with specific objectives in mind. Moreover, the accessibility and affordability of cyberspace have rendered it an attractive avenue for individuals and organizations alike, enabling them to partake in lucrative cyber activities. Additionally, the lack of governing bodies or regulations in the realm of cyberspace allows individuals and groups to operate with a certain degree of autonomy and flexibility, free from immediate repercussions or limitations. This unregulated environment of the digital world presents an enticing opportunity for various actors, both state and non-state, to engage in their activities. Consequently, within the vast expanse of cyberspace, one can encounter a diverse array of individuals driven by personal motives, as well as criminal organisations or entities supported by governments, all working towards their own larger and often intricate goals.

Following two destructive wars, individuals no longer desire to endure the severe repercussions and burdensome tolls of warfare. Furthermore, the ability to closely monitor battlefields through advancing technology and witness the devastating consequences of war in real time has intensified the negative perception towards armed conflicts. In the present age of social media, people are questioning the necessity of deploying ordinary citizens to fight on the frontlines, particularly when there are no

tangible advantages or when the government could allocate those resources towards addressing urgent domestic concerns. Thus, nations strive to address complex and worldwide threats in the 21st century while evading large-scale conflicts and the risks of mutual destruction through a combination of methods that fall both below and above the thresholds of violence.

In this context, the realm of cyberspace offers a unique opportunity to engage in combat without endangering civilians and soldiers, as well as to carry out operations against hostile forces while avoiding the threshold of traditional warfare. As of late, governments have increasingly turned to cyber actors to take on the responsibilities of warfare. The cyber domain, in particular, provides an ideal platform for utilizing surrogates due to the nature of cyber weapons. These powerful tools offer the patron state a level of plausible deniability, as it becomes exceedingly difficult to definitively attribute cyber-attacks to their source. The resulting ambiguity surrounding the origins of these attacks allows the patron state to distance itself from any potential consequences and simplifies the engagement of both state and non-state actors in cyber activities, all without the fear of direct retaliation or repercussions.

The collaboration between states and non-state actors is also evident in the situations involving Iran, Estonia, and Georgia. Although the accused states have not acknowledged their involvement in these incidents, there are ongoing discussions regarding their potential role. Regarding the Stuxnet attack, experts in computer security have concluded that it is highly likely that one or more nation states are responsible due to the significant resources, complexity, and risks associated with the cyber worm (Bloomberg Originals, 2012). However, despite these accusations against the US and Israel, neither country has confessed to the crime, which is to be expected considering the covert nature of weaponized codes like Stuxnet that can be easily denied, unlike physical acts of aggression such as bombing (Kaspersky, 2014).

In the present era of globalization, governments are actively establishing horizontal and transnational ties. This trend towards interconnectedness and decentralization of power, traditionally associated with non-governmental organizations (NGOs), is now also observed within nation states. Consequently, the global political landscape is undergoing a transformative process, wherein the relationships between nation states, NGOs, and corporations are becoming increasingly intertwined (Kaldor, 2013:76). A prime example that showcases the collaborative relationship between nation-states and corporations is Iran's allegations against Siemens, a renowned engineering company responsible for developing the industrial control system for Iran's nuclear program. It is believed that Siemens aided the United States and Israel in initiating the notorious Stuxnet cyberattack. Iran's civil defence chief, Gholamreza Jalali, has called for a legal investigation into the role of Siemens SCADA software in the Stuxnet case. Jalali argues that there are strong indications suggesting that the United States and Israel could not have carried out the cyber-attack without the assistance and information provided by Siemens. Specifically, Siemens is accused of sharing valuable details about the control system of the Iranian

nuclear program, including the existence of a default password, which ultimately facilitated the successful execution of the cyber-attack (Dehghan, 2017).

In the wake of the Georgian cyber-attack, similar to many instances of nation-state cyber operations, Russia vehemently denied any involvement. Despite the lack of concrete evidence directly linking the cyber-attacks on Georgian government websites to Russia, it is evident that Russia's offensive cyber-operations against Georgia were facilitated by surrogates, aligned hacktivists, supporters, criminals, and sympathizers. Interestingly, Russian criminal organizations seemingly made no attempt to conceal their participation in the cyber campaign against Georgia, as they sought recognition and credit for their actions (Kirk, 2009). Although establishing direct connections to the Russian government may be challenging, there are certain groups whose actions significantly align with the strategic goals of the Russian military.

Although there is no definitive proof connecting the cyber attacks in Estonia in 2007 to their culprits in the virtual world, both Estonian officials and scholars who extensively examined the incident and conducted interviews with Estonian officials in the aftermath of the attacks concurred with the belief that the aggression originated from two nation-states, namely Estonia and Russia (Schmidt, 2013:76). Nevertheless, it should be noted that there are indications of involvement from non-state actors in this particular attack, as well as in other previously mentioned instances of cyber warfare. Konstantin Goloskokov, who is the commissioner of Nashi, a youth organization supported by the Russian government, openly confessed their involvement in these cyber attacks. (NATO Stratcom, n.d.:61) In addition to these activist surrogates, the Russian government also sought support from cybercrime entities like the notorious Russian Business Network. This organization, believed to have connections with the Russian mafia, was instrumental in launching cyber attacks against Estonia (Krieg & Rickli,2019:99). Furthermore, as stated in Roussi's report, the responsibility for the attack has been attributed to KillNet, a well-known Russian organization, which proudly announced their involvement through their Telegram channel. This group consists of highly adept hackers who strongly advocate for the pro-Russian government, making their actions in line with Russia's broader interests in both Ukraine and the Western world (Roussi, 2022).

4.1.3. Target Group

In contrast to past conflicts where the aim was to completely annihilate the adversary's military forces, the primary objective of modern warfare has shifted towards undermining the determination and resolve of the people within the targeted nation, as well as eroding their faith in their own government and armed forces. This shift can be attributed to the evolution of conventional warfare technologies. With the exorbitant costs and devastating consequences associated with modern weaponry, the pursuit of obliterating the enemy would only escalate the economic burden of war. However, by breaking the opposing country's will to fight, the desired policies can be imposed upon them without the need for such costly armaments. In the context of these objectives, the occurrence of cyber-attacks targeting

essential infrastructure systems of nations and various internet-dependent public and private services has the potential to yield significant outcomes by undermining the resolve and determination of states to engage in conflicts. To illustrate, with the growing reliance on internet connectivity for national security and military operations, carrying out cyber-attacks that disrupt military units and other related entities (Libicki, 2009) can have detrimental effects on the willingness and commitment of states to engage in combat.

In the realm of cyberspace, there is a significant advantage for those seeking to carry out information attacks and spread propaganda. This advantage lies in the ability to exploit the vast digital landscape to achieve their objectives by undermining the determination and resolve of the people within the targeted nation, as well as eroding their faith in their own government and armed forces. One such objective could be the extraction of immensely crucial information pertaining to national security using cyber espionage techniques, which can then be utilized against nations. Additionally, the manipulation, erasure, or modification of such vital information through cyber sabotage tactics can have detrimental consequences, ultimately undermining the trust and faith that the target population places in their own government and military.

Lastly, the advancements in information and technology have allowed the public to closely monitor and understand wars. As a result, the decision to go to war has become a complex evaluation of costs and benefits, which is subject to scrutiny from the international, domestic, and local levels. Therefore, it can be argued that the public serves as a powerful force that influences a state's war policies, acting as both a source of support and a potential obstacle. In this regard, psychological operations conducted through propaganda and information warfare in the digital realm can have a negative impact on a state's resolve and the public's willingness to engage in combat. This kind of propaganda strategy can be seen in the situation surrounding the "Bronze Soldier" statue in Estonia. The dependence of Russian-speaking citizens in Estonia on Russian media outlets for information has created an ideal environment for spreading Russian propaganda and easily reaching these individuals. The core of this propaganda is based on the belief that those who fail to acknowledge and honor the Red Army's role in defeating Nazi Germany in Europe are sympathetic to fascist ideology and Nazi Germany as a whole. To effectively disseminate their message, Russia employs various propaganda techniques, such as circulating videos showcasing the Estonian police accompanied by Nazi music, defaming high-ranking Estonian officials by portraying them as fascists, and constructing narratives that depict Russian-speaking citizens as martyrs who have fallen victim to the violent clashes that occurred in Tallinn surrounding the "Bronze Soldier" monument (Khmelidze,2021).

Another form of this strategy involves launching cyber attacks. In 2007, Russia was accused of orchestrating large-scale cyber attacks against Estonia. The motive behind this cyber offensive can be traced back to the controversial decision of replacing the "Bronze Soldier," which sparked a wave of protests among Russian-speaking citizens in Estonia. Various official websites belonging to

governmental bodies, political parties, media outlets, and banks and so on were targeted for the purpose of distrupting the functioning of these instutions, hinder online operations and spread specific propaganda. The overarching objective behind these cyber attacks was to undermine the credibility of the institutions responsible for ensuring security in Estonia. Additionally, the attackers sought to portray Estonia as an unstable and insecure nation while highlighting Russia's advantageous role as a stabilizer (Khmelidze,2021).

Similary, in Georgia in 2008, a series of assaults were carried out against various targets including the websites of the president, government entities, the Ministry of Foreign Affairs, the Parliament, informational portals, media platforms that support Georgia, online forums, and even the banking systems. On August 11, a malicious act occurred where the President's website became a target of a defacement attack. During this attack, fascist symbols were inserted onto the website, along with photographs that compared President Saakashvili to Hitler (Gotsiridze, 2019). In cyber-attacks on 54 sites of official Georgian state institutions, the links were crashed. Thus, Georgia's connections with the fighting troops were cut. At the same time, it became difficult for the public to get information about the events (Hollis, 2011:2).

4.1.4. Field/Front of War

The utilization of cyber warfare tools marks a significant shift in the nature of warfare, as it eliminates the need for direct confrontation between opposing forces on traditional battlefields. Instead, the realm of cyberspace has emerged as a new battleground, eradicating the relevance of national boundaries and replacing them with technological defenses such as firewalls, air-gapped networks, and such. Morever, since the primary objective of the contemporary wars has shifted towards undermining the enemy's determination and will to fight, which is achieved through more abstract means, the objectives of warfare are now being defined in socio-psychological and political-ideological terms, rather than purely physical terms. Consequently, the traditional concept of the battlefield, which was primarily based on geographical terrain, has evolved to encompass additional dimensions such as the "informational" and "spiritual" domains (Gürcan,2012:103). In today's modern warfare, the battlefield has expanded beyond physical boundaries to encompass the thoughts and emotions of individuals. This shift has necessitated the use of war tactics such as propaganda, disinformation, misinformation, and manipulation, which have become increasingly crucial. Among the various platforms available, cyberspace has emerged as the most suitable arena for executing these tactics due to its ability to conduct operations simultaneously across different regions of the world, thereby disregarding geographical limitations. Consequently, the internet and social media platforms have become the primary battlegrounds, surpassing traditional zones dominated by conventional military forces, bombs, and warplanes. It is within these virtual realms that perception management and the production of consent occur, ultimately determining the course and outcome of modern conflicts.

In the past, the focus of warfare was on targeting physical assets on battlefields or frontlines. However, with the emergence of cyberspace, this dynamic has shifted. Now, targets extend beyond the traditional battlefield and can include critical infrastructure, information and communication systems, and even countries located far from the frontline. This shift has been particularly pronounced in the 21st century, as digital environments have become integral to the provision of public services, states have connected their critical infrastructures to the internet, the private sector relies on internet connectivity for its operations, and e-commerce has gradually replaced traditional trade practices. Consequently, the nature of attacks carried out in cyberspace has evolved accordingly. One of the most significant aspects of cyber attacks is that they transcend physical borders, enabling them to target multiple points simultaneously (Schreier, 2015: 7). This is made possible through the utilization of electromagnetic forces, which serve as a means of transportation within this virtual realm. As a result, any action taken within cyberspace has the ability to transcend national boundaries instantaneously, a concept that would be unimaginable in the physical world (Department of Defense, 2006:4). In traditional forms of warfare, it has been customary for nation-states to dispatch their troops or operatives to foreign territories in order to execute physical operations against enemy states. However, with the rise of cyber warfare, this scenario has significantly transformed. Unlike before, where agents had to physically step foot in foreign territories to carry out their missions, the battleground has shifted to the realm of computer terminals, making it much more challenging to trace and identify those responsible for the attacks (Bates,2020.:64).

Lastly, the scope and impact of cyber weapons are primarily determined by the extent of network connectivity that enables the transmission of malicious code to intended targets. The remarkable aspect of this virtual battleground is its fluidity, as it can be altered instantaneously with a simple switch. Consequently, targets can vanish into thin air or reemerge as swiftly as they disappeared. Moreover, countries have the option to employ air-gapping techniques, a method that involves electronically isolating a nation in the digital realm, thereby facilitating the reduction or even elimination of their cyber presence (Stimpson, n.d.:5). Moreover, it is possible that the targeted state may have already resolved its vulnerabilities prior to the initiation of the attack, resulting in potential failure or a lack of the desired impact for the operation (Schreier, 2015).

4.1.5. Methods and Strategies

In this age of the Internet, the struggle to win over people's hearts and minds has become even more crucial. Social media, a network built on trust, has become a breeding ground for gathering intelligence, spreading propaganda, and conducting psychological operations with the aim of influencing public opinion or luring adversaries into dangerous situations. As we navigate through the complexities of modern-day operations, cyberspace has assumed an increasingly significant role. When an adversary launches a targeted attack in the cyber realm, it is essentially an assault on the computer systems that are integral to our daily lives and businesses, the functioning of critical infrastructure, and the facilitation of financial transactions, among various other essential activities. However, as Richard

Clarke says we face the risk of cyber attacks that involve an adversary strategically disseminating misleading information to manipulate our understanding of a given situation and influence our decision-making processes. These attacks, although conducted in the digital realm, can have dire real-world consequences that are comparable to those of a direct assault on a vital infrastructure (Lange-Ionatamishvili & Svetoka & Geers,2015:104).

Cyberspace has the potential to serve as a platform for executing narrative-focused endeavors where the primary objectives are not the machines or networks themselves, but rather the minds of individuals. With the internet and social media platforms offering the capability to rapidly disseminate information at minimal cost, the utilization of these mediums for propaganda, information warfare, and influence operations has become increasingly prevalent. These endeavors possess the ability to significantly alter the perception and behavior of the target audience. Cyberspace, being a highly dynamic and user-centric environment, is in a constant state of flux, making it effortless for messages to go viral. Moreover, it presents challenges in terms of tracking the original source of information, verifying its authenticity, and distinguishing fact from fiction (Lange-Ionatamishvili et al.2015:104-105).

Social media platforms provide a means for individuals to engage in interactive communication with one another, regardless of their physical location, time availability, or limitations on personal expression. Additionally, these platforms afford users the ability to share and exchange a wide range of content, including visual images, audio recordings, and written messages (Krieg & Rickli,2019:94). Due to the rise of smartphones and advancements in mobile technology, the virtual communities formed on social media platforms have gained significant influence, capable of connecting and rallying potentially millions of people worldwide. In this regard, Lucas Kello says, information has tranformed from being merely a means of acquiring power to becoming a potent force in its own right (2017:5). This shift emphasizes the significant impact and influence that information holds in today's society.

Social media, when exploited, has the potential to have a subversive impact, especially when it is used to sway and rally individuals and communities. The concept of empowerment can have both positive and negative implications, particularly in modern conflicts where narratives hold significant strategic value. In the realm of insurgency and counterinsurgency, social media has proven to be remarkably influential as it molds perceptions and galvanizes the support of insurgent sympathizers within the local community or the home base of the counterinsurgent in foreign lands. As a result, social media becomes a formidable tool for both sides, effectively projecting the disruptive consequences of traditional warfare onto the global cyber stage, where information is disseminated instantly to a worldwide audience (Krieg & Rickli,2019:95).

The primary goal of the insurgent movement is to undermine the legitimacy of the governing authority through a variety of clandestine tactics, including but not limited to the dissemination of

propaganda and the utilization of force and acts of terrorism against the authority. As a result, insurgency can be considered as a type of conflict that occurs within a society, wherein a group that is not in power seeks to dismantle, reshape, or weaken the credibility and public backing of the existing governing body. Insurgents employ strategies such as political activism, subversion, the spread of persuasive information, and instilling fear among the population to accomplish their objectives and garner support for their alternative mode of governance. Insurgents employ various strategies such as engaging in political activism, subverting existing systems, spreading propaganda, and intimidating the population in order to accomplish their goals and garner support for their alternative form of governance. However, in the modern era, insurgencies have evolved beyond solely physical warfare and are increasingly being fought in the virtual realm of cyberspace, where the battle revolves around shaping and controlling narratives. These narratives play a crucial role in influencing public opinion and garnering support, making the online landscape an essential battleground for insurgents (Krieg & Rickli,2019:95).

Social media has become a powerful tool for insurgents as it enables them to effortlessly reach a much larger audience compared to the past. It allows them to do so instantly, universally, and at a lower cost. This accessibility to a wide range of potential recruits, supporters, and allies comes with the added benefit of reduced risk of being discovered. The geographical constraints that previously hindered the recruitment process are now eliminated thanks to social media. Moreover, social media enables insurgencies to expand their support base by gathering and uniting the anger, frustration, and resentment prevalent in many societies. The emergence of social media has completely transformed the way local grievances are collected and shared, as it has shifted the entire process to the global cyber sphere. This digital realm provides a convenient, cost-effective, and secure platform for individuals to reach out to a vast audience of like-minded individuals who share their grievances. Consequently, this makes it significantly easier for insurgent groups to identify and approach potential recruits who are particularly susceptible to their persuasive narratives. Furthermore, thanks to the diverse array of communication channels available in cyberspace, such as chat rooms, mobile applications, and email, insurgents have the ability to pinpoint individuals who may serve as human surrogates for their cause. These potential surrogates are individuals who are more likely to align themselves with the values and ideologies of the insurgent group. By leveraging these digital platforms, insurgents are able to establish connections and foster relationships with individuals who are more likely to embrace their cause and actively participate in their activities (Krieg and Rickli,2019:95-96).

When the case of Stuxnet including the denial of service attacks in Estonia in 2007 and the cyber-attacks during the Russia-Georgia War in August 2008 are analysed in regards to method of new generation wars, it can be argued that the method involves control through political means where the primary objective is to win over people's hearts and minds. For example, In an article written by Kenneth Corbin, it was highlighted that the Russian cyber attacks had a specific objective: to undermine the Georgian population by isolating and silencing them. These malicious cyber assaults not only succeeded

in silencing the Georgian media but also had the detrimental consequence of cutting off the country from the global community. As a result, the Georgian people were left feeling defeated, both in terms of their access to information and their ability to communicate the dire circumstances they were facing to the outside world (Shakarian, 2011:65)

The subsequent cyber conflict between Georgia and Russia revolved around manipulating and upholding public sentiment on the internet. Russia and its supporters utilized a range of cyber tactics, such as Distributed Denial of Service (DDoS) assaults and the establishment of counterfeit websites, in order to dictate the manner in which their preferred version of reality was conveyed to the public (Thomas, 2009). Through their control over the narrative across cyber, electronic, and conventional channels, Russia endeavored to mold popular opinion and influence the worldwide audience to embrace a pro-Russian stance.

Throughout the duration of the Russo-Georgian War, a persistent and far-reaching storyline emerged which aimed to undermine and invalidate the Georgian government. This narrative was skillfully employed by Russia both prior to and following the conflict, as they sought to portray themselves as defenders of ethnic Russians while simultaneously highlighting alleged atrocities committed by Georgia. In an effort to shape public opinion, Russia strategically positioned Georgia as a subordinate nation to the United States, thereby justifying their military intervention in Abkhazia and South Ossetia by framing it as a necessary response to genocide. The Russian side provided a rationale for their military intervention by claiming that their main objective was to put an end to what they believed was an ongoing genocide being carried out by the Georgian forces against the Ossetian population. Additionally, they asserted that their intervention was meant to safeguard both Russian citizens living in South Ossetia and the Russian contingent of the joint peacekeeping forces stationed in the region (Traynor, 2009).

The operational environment was greatly affected by the infiltration and pollution of messages and narratives, which had a detrimental impact on the data available to policymakers. Moreover, these false narratives played a significant role in diminishing the trust that the general population had in institutions like the Georgian government and various media outlets. The Russian political content, in particular, had a clear objective of tarnishing the reputation of democratic leaders and undermining the credibility of institutions by making allegations of voter fraud, election rigging, and political corruption (MacFarquhar, 2016). For example, on August 11, a malicious act occurred where the President's website became a target of a defacement attack. In order to sway public opinion, during this attack, fascist symbols were inserted onto the website, along with photographs that compared President Saakashvili to Hitler (Gotsiridze, 2019).

4.1.6. War Economy

In stark contrast to the centralized and self-sufficient war economies of World War I and II, the financing of modern conflicts is facilitated by the globalized war economy, as described by Kaldor (2013:7-10). With the Internet being both decentralized and integral to globalization, the potential for funding conflicts in cyberspace is vast. The vastness and intricacy of cyber warfare have become so extensive that it has become increasingly difficult to distinguish between state and non-state actors. These actors, in turn, are taking advantage of the rapidly growing cyber war economy. This is further fueled by the widespread prevalence of cybercrime, which provides a thriving market for cyber mercenaries motivated by political and economic gains. The use of crypto-currencies has also played a significant role in amplifying these activities.

While conflicts in various regions around the world, particularly in Africa, have historically been fueled by the lucrative trade of diamonds and oil, the landscape of conflicts has shifted in cyberspace. The catalyst for these digital conflicts lies in the ease and virtual anonymity provided by cryptocurrencies like Bitcoin, which have become the preferred method of payment in the cyber black market. As time has progressed, the once fragmented and disparate individuals involved in this illicit underworld have coalesced into highly organized networks. These networks often have connections with established criminal organizations and even nation-states. This convergence has led to an exponential growth of the cyber black market, offering an ever-increasing range of illicit goods and services (Ablon & Libicki & Golay,2014). There is a major and growing internet-based illicit trade market for illegally traded species, cultural property, human trafficking and illegal drugs. Additionally, there is a burgeoning data industry that deals with the sale of unlawfully obtained information gathered through covert cyber activities. These include stolen records like credit card information, contant lists, GPS locations, and exploit kits, as well as highly sought-after items like zero-day vulnerabilities and valuable intellectual property (Global Initiative Against Transnational Organized Crime (GIATOC), 2021:18). Some of these underground organizations have amassed a staggering global presence, with reported revenues reaching into the hundreds of millions of dollars (Ablon & Libicki & Golay,2014). According to predictions from Cybersecurity Ventures, the expenses incurred due to cybercrime are projected to increase at a rate of 15 percent annually in the upcoming five years. This escalating trend is anticipated to result in a staggering annual cost of $10.5 trillion USD by the year 2025. Furthermore, it is noteworthy that this astronomical figure will surpass the combined profitability of the illicit drug trade on a global scale (Cybercrimemag,2021).

The defense sector, responsible for developing safeguards against cyber threats, and the offense, consisting of cyber-crime actors, are both leveraging the advantages of cyber-war economy offered by the cyber realm. As governments and private entities increasingly recognize the need for robust cybersecurity measures, the demand for cyber protection is on the rise. Consequently, a flourishing global market of private cybersecurity firms has emerged to cater to this escalating demand. Private

military and security companies (PMSCs) are increasingly venturing into the realm of cybersecurity, a domain that was traditionally not their core focus. These PMSCs are either establishing their own dedicated cybersecurity teams or opting to acquire smaller, specialized firms that offer cyber tools and services. While private security contractors are not a novelty in the industry, the cybersecurity sector presents a more favorable landscape for establishing such companies due to its reliance on intellectual capabilities and technology rather than traditional weaponry. Consequently, the barriers to entry in this business are relatively low (Maurer & Hoffman, 2019:5).

4.1.7. Weapons

In contrast to conventional weapons, which require significant financial resources and are only possessed by a number of countries, cyber weapons are relatively inexpensive and accessible to not just nation-states but also criminals and malicious individuals. Moreover, while the paths of conventional weapons can be easily tracked, cyber weapons traverse the intricate network of fibre-optic cables spread across the world, making it easier to attribute their actions to other entities and create a sense of plausible deniability. In contrast to traditional weapons, cyberweapons operate in a highly decentralized manner and demand considerably fewer resources for acquisition. Developing conventional weaponry like weaponized drones or ballistic missiles necessitates immense investments of human, financial, and physical resources. However, when it comes to cyberweapons, all that is required is access to a computer, an Internet connection, and proficient computer engineering abilities. This means that not only states but also substate groups and even individuals now have the ability to become significant actors in the cyber warfare domain (Thomas, 2018).

In contrast to the exclusive groups of individuals involved in the development of nuclear weapons or drones, the remarkable aspect of cyber weapon creation is that it can be done remotely and collaboratively. Through online forums, a diverse range of people can come together and instantly share their expertise in crafting sophisticated malware. This unique form of crowd-sourcing has revolutionized the field, making it accessible to anyone with the dedication and time to acquire the necessary knowledge. Consequently, the playing field has been leveled, erasing the distinction between the capabilities of nation-states and non-state actors in the realm of cyber warfare. This unprecedented scalability has led to a convergence of power, granting individuals and smaller organizations the ability to engage in cyber operations at a scale previously limited to major powers (Thomas, 2018). According to postings on some Russian hacker websites, many “hacktivists” were thought to be members of Russian youth movements during the cyber operations in Georgia in 2008. Additionally, StopGeorgia.ru provided easy-to-use tools and instructions to launch DDoS from private machines. It even featured a user-friendly button called “FLOOD” which, when clicked, deployed multiple DDoS on Georgian targets. One hacktivist notes that the instructions provided were very accessible, even for a novice user (Shakarian,2011).

4.1.8. The Beginning and End of the War

In the realm of modern warfare, there exists a complex intermingling of three distinct periods: peace, crisis, and war. Traditionally, these periods have been clearly defined and separate from one another. However, in the new generation of wars, the boundaries between peace and war have become increasingly blurred. States now possess the capability to engage in active combat even during times of peace and crisis, thanks to emerging techniques such as cyber warfare and information operations. An illustrative example of this dynamic is the cyber attacks that occurred in Georgia. These attacks serve as a stark reminder of how cyber warfare has evolved and become an integral part of modern conflict. The ability to launch cyber attacks during peacetime not only demonstrates the changing character of warfare but also highlights the importance of bolstering cybersecurity defenses to protect against such malicious actions.

Although conventional war broke out on 8 August following the dispute over South Ossetia, the first conflicts related to this dispute started in cyberspace before the conventional conflict. Russia for the first time combined kinetic attacks and cyberattacks in an international military operation against Georgia. For several weeks prior to the Russian offensive in Georgia, however, non-attributable Russian "hacktivists" conducted a similar computer network attack (CNA) with the strategic focus of severing Tbilisi's command and control of the Georgian armed forces, rallying ethnic Russian, Ossetians, and Abkhazians to the Russian cause, and to isolate Georgia from the rest of the world (Dayspring,2015:98). The initial attack occurred prior to the commencement of conventional operations, happening on July 19, which targeted the official website of the Georgian President by means of a DDos attack. Subsequently, a series of assaults were carried out against various targets including the websites of the president, government entities, the Ministry of Foreign Affairs, the Parliament, informational portals, media platforms that support Georgia, online forums, and even the banking systems. On August 11, a malicious act occurred where the President's website became a target of a defacement attack. During this attack, fascist symbols were inserted onto the website, along with photographs that compared President Saakashvili to Hitler (Gotsiridze, 2019).

4.1.9. Symmetry

Asymmetrical warfare can be described as the confrontation between two opposing forces that possess unequal levels of power. Usually, the entity with greater conventional power, which is often a nation-state but not limited to it, boasts a significantly superior military capability, greater resources, and access to advanced technology compared to the weaker force. This power disparity compels the weaker force to resort to unconventional tactics in order to stand a chance against the stronger adversary. In asymmetrical warfare, the weaker force tends to be decentralized and relies on unconventional tactics, predominantly engaging in smaller-scale attacks of low intensity. These tactics are strategically aimed at eroding the enemy's willpower and undermining their overall strength (Martins,2017:98-99).

Due to the unique characteristics of the online realm, individuals or groups with limited conventional power can still exert significant influence over much stronger opponents. The interconnected structure of the Internet allows for instantaneous communication among billions of people worldwide, resulting in a remarkable decentralization of cyber armies across various geographic locations. Furthermore, hostile actions in cyberspace possess unconventional attributes, as they are cost-effective, rapid, anonymous, and capable of disrupting or denying critical services at the most critical moments. Although cyber attacks cannot replicate the physical impacts of traditional combat, they predominantly manifest as low-intensity conflicts, necessitating persistent and dedicated efforts to gradually erode the determination of the adversary over time (Martins,2017:102).

The following table provides a comprehensive analysis and comparison of the distinctive qualities of the 'new' war in contrast to cyber war. Moreover, this analysis seeks to explore the transformative impact of cyber warfare on the character of war in the 21st century, as well as the evolving significance and role of cyber warfare within the broader context of the changing character of war.

Table 2: New Wars vs. Cyber War

Components	**New Wars**	**Cyber War**
Aim	– Political control – Identity politics (ethnic, religious or tribal)	– Myriad of motivations, including geopolitical interests, ideological beliefs, economic ambitions, political agendas etc.
Actors	– Non-state actors: paramilitary groups, mercenaries, cyber warriors, criminals, PMCs etc.	– States – Non-state actors: individuals, cyber patriots, hacktivist, cyber mercenaries etc.
Target Group	– People-centered approach; the hearts and minds of the people	– People-centered approach; the hearts and minds of the people – Internet of things, critical infrastructure and information systems
Field/Front	– Informational and spiritual domains – Cyberspace	– Virtual realm of cyberspace, the global network – Informational and spritiual domains – Social media platforms etc.
Methods and Strategies	– Influencing the thoughts & interests and sentiments of adversaries – Information operations and propaganda	– Influencing the hearts and minds of people – Intelligence, propaganda and psychological operations

Economy of War	– Financing through illegal means and perpertuation of violence – Commercialized – Decentralized	– State-sponsored cyber operations – 'Cyber-War Economy': Darkweb, Black Market, Online trade of illicit goods and services – Commercialized – Decentralized
Weapons	– Affordable – Compact – Mass-produced – Versatile	– Cost-effective – Compact – Asymmetrical – Easy to hide and deploy – High-speed – Not constrained by physical boundaries
Beginning and End of War	– Indistinguishable boundaries between times of war, peace and crises; continued employment of unconventional means in times of peace	– Indistinguishable boundaries between times of war, peace and crises; covert operations during peace times
Symmetry	– Asymmetric Forces	– Asymmetric Forces

4.2. Shift From Traditional Warfare?

During the 19th century, the act of engaging in warfare was regarded as a noble and honorable sacrifice made by individuals for the betterment of their respective nations. This perception was heavily influenced by the rise of nationalism and romanticism during that era. However, the catastrophic consequences of two world wars have significantly impacted societies, causing them to reconsider their stance on war and its associated costs. Previously, soldiers who lost their lives in battle were revered as martyrs, and the act of fighting for the security of one's country and the protection of national interests was considered sacred. The public rallied behind wars, offering support in various forms. However, in the current era, there has been a noticeable shift in mentality, whereby the human casualties and the economic and moral burdens imposed on societies due to warfare are viewed as undesirable outcomes that states should strive to avoid. There is now a growing aversion to violence and military interventions, as the use of force is widely regarded as socially unacceptable. The concept of war itself has become a ghastly reminder of a bygone era. Consequently, the international community, as well as the general public and individuals living in conflict-affected regions, are keenly observing and scrutinizing any instance of coercive action, resulting in a heightened sense of awareness and the need for accountability.

In the modern world, policy makers face a challenge when it comes to justifying the costs and advantages of engaging in war, as the media has made the public more aware of its consequences of such conflicts. The rise of social media platforms has made it possible for wars to be broadcasted to even the most isolated communities, leading to a shift in accountability. Now, states are being held responsible for their actions by their own citizens. Moreover, the decision-making processes behind policies related to warfare are being closely examined both at home and on a global scale, as the public expresses opposition. People are now questioning the justification for sending ordinary citizens to fight in foreign battles, particularly when there are no tangible benefits involved or when the government could allocate those funds towards addressing urgent domestic issues. As a result, the media and the internet have played a significant role in familiarizing the general population with the concept of warfare, causing the decision to go to war to be scrutinized from a cost-benefit perspective under international, domestic, and local scrutiny.

In the past century, conflicts were driven by the need to safeguard national interests and were viewed as battles where one side's gain meant the other's loss. However, as we entered the 21st century, the concept of security has become more intricate and harder to define due to the presence of uncertainty and intangible threats. The understanding of security has become highly subjective, particularly when faced with threats that are not easily identifiable. Nowadays, countries justify their military interventions by emphasizing the importance of stabilization and reconstruction efforts, which are believed to bring benefits to both domestic and local communities. Nevertheless, the traditional justifications for military interventions, such as the notion that ensuring homeland security begins overseas, no longer satisfy the public. As a result, there has been an increase in public scrutiny and opposition towards military operations, raising questions about the allocation of resources. In light of these pressures, it is imperative for states to confront and tackle transnational challenges such as terrorism and global warming head-on. In our increasingly interconnected and globalized world, conflicts can emerge unexpectedly and have far-reaching implications on distant regions. Consequently, governments are driven to respond rapidly and efficiently on a global level, even when faced with lower-intensity threats. The security landscape has evolved into a complex web of interconnectedness, with threats that transcend national boundaries. As a result, governments are now embracing proactive measures to preemptively address potential threats before they fully materialize. Despite facing public pressure, it is of utmost importance for states to adopt a comprehensive strategy that enables them to effectively combat these threats without escalating into a full-scale war.

In the present circumstances, the domain of cyberspace presents a unique opportunity to partake in combat without endangering civilians and soldiers. It also provides a means to carry out operations against adversarial forces while sidestepping the threshold of conventional warfare. As a result, cyber warfare has emerged as a cost-effective alternative that allows nations to intervene in conflicts abroad without attracting undue attention or facing backlash from the international community and their own

domestic population. The inherent characteristics of cyberspace enable states to distance themselves from the conflict, thereby avoiding direct attribution and potential repercussions like retaliatory measures or international condemnation. As of late, there has been a growing trend among governments to employ cyber actors for military purposes. The cyber realm has emerged as a highly favorable arena for utilizing cyber-surrogates due to the unique characteristics of cyber weapons. These potent tools provide the sponsoring state with a certain level of plausible deniability, making it extremely challenging to definitively trace cyber-attacks back to their origin. This lack of clarity surrounding the source of such attacks enables the sponsoring state to distance itself from any potential consequences, facilitating the involvement of both state and non-state actors in cyber operations. This, in turn, eliminates concerns about direct retaliation or repercussions.

In the 21st century, wars have taken on a new dimension that is characterized by subjectivity and a fierce battle for control over the narrative surrounding the conflicts. This shift can be attributed to the transformative power of the internet and mobile devices, which have revolutionized the way information is shared and made it increasingly challenging for any single nation to effectively regulate. Consequently, achieving victory in war now hinges on the ability to influence and shape the narratives that emerge from these conflicts. This evolution in the character of warfare reflects the growing recognition that controlling public perception can be just as important, if not more so, than traditional military strategies. Governments and non-state actors alike are now engaged in a battle to shape the narrative surrounding conflicts, employing various tactics to gain an upper hand. This can range from disseminating propaganda and misinformation to leveraging social media influencers and conducting sophisticated online campaigns. The consequences of this shift are far-reaching. The ability to control the narrative surrounding a conflict can have profound implications for the outcome of a war, as it can shape public opinion, garner support, and even influence the international community's response. Moreover, the reliance on these non-traditional methods of warfare has the potential to mitigate some of the financial and human costs typically associated with armed conflicts. One of the key factors driving this phenomenon is the exponential growth of social media platforms, which have become a powerful tool in shaping public opinion. The widespread usage and accessibility of these platforms have allowed individuals from all walks of life to become active participants in the discourse surrounding war. As a result, traditional methods of warfare, with their significant financial and human costs, are increasingly met with aversion by the public.

Moreover, the advent of social media has granted ordinary citizens a greater degree of influence over the allocation of the nation's resources. The traditional concept of warfare has undergone a transformation, shifting from a reliance on brute force on the battlefield to a more nuanced process involving discussions and negotiations between the government and the general public. Consequently, in this new security landscape, states find themselves compelled to win not only military victories but

also the hearts and minds of their populace, as well as shape the perception of their actions domestically, internationally, and locally. In essence, the power of a state is contingent upon its legitimacy and its ability to effectively communicate, sway public opinion, manipulate perceptions, and control the narratives surrounding warfare, thus justifying its cause (Krieg & Rickli,2019:62).

Consequently, due to the reluctance of states to involve themselves in inter-state conflicts, they have had to explore alternative methods of resolving conflicts. This has led to a shift in the objectives of warfare in the modern era. Instead of focusing solely on concrete goals like occupying territories or destroying the physical presence of the enemy, military objectives have become more focused on socio-psychological and politico-ideological factors. The ultimate aim now is to undermine the enemy's determination and resolve to fight. This approach places a strong emphasis on the people involved, with the primary goal being to gain the support of the majority of public opinion. This is achieved by strengthening positive perceptions and opinions among friendly public opinion, winning over those who are neutral, and either winning or deterring hostile public opinion. In the new generation of warfare, the target audience is the public themselves, as the main aim is to gain their support and legitimacy (Gürcan, 2012:100-104). In this regard, cyberspace cyberspace presents an exceptional chance to effortlessly connect with a significantly broader audience in comparison to conventional methods. It enables the execution of disinformation, misinformation campaigns, propaganda dissemination, and psychological operations in a manner that is immediate, widespread, and more economical. The limitations imposed by geography, which used to impede the process of recruiting individuals, have now been eradicated thanks to the advent of social media. Additionally, the growing significance of both military and personal data has further bolstered the prominence of cyber warfare strategies.

Additionally, the influence of international law and the possession of nuclear weapons have played a significant role in reducing and making rare the occurrence of wars between nations. Engaging in a war between major powers entails severe repercussions, including the degradation of the international order and, in the worst-case scenario, the potential annihilation of humanity if weapons of mass destruction (WMD) are deployed. To prevent such a catastrophic event, most countries adopt the strategy of using WMD as a deterrent, aiming to dissuade enemies from attacking or attempting to coerce them. Consequently, conflicts between major states tend to avoid traditional warfare as a means of resolution since the risk of escalation and the utilization of WMD becomes too immense. This avoidance leads to the implementation of alternative methods, such as cyber warfare, which are considered less aggressive yet still effective in exerting influence and control (Wooding, 2019).

Over the course of the past century, technology has advanced significantly, leading to the emergence of the internet and various communication tools. As a result, cyber space has become an integral part of our daily lives. The level of reliance on technology has experienced a substantial increase in the last decade or so. This heightened dependence is evident in almost every sector of our society,

including defense, finance, healthcare, education, government, and critical infrastructure. These sectors have become heavily reliant on technology, to the extent that reverting to non-technological methods is nearly impossible. Moreover, many of these systems are interconnected, meaning that a failure in one area can have far-reaching consequences on a larger network of societal functions. Our society's reliance on technology has grown to such an extent that it has become a prime target for those with malicious intentions, posing a significant threat to our well-being (Sweet, 2017). Destructive cyber-attacks have the potential to cause immense damage and can be executed with minimal effort and cost. These attacks can be orchestrated by a small group of individuals and possess the ability to inflict destruction on a scale previously only achievable through physical attacks. The reason behind their formidable capabilities lies in the advanced technological infrastructure that permeates our modern society. In essence, we have become reliant on technology, placing us at the mercy of potential breaches in our computer systems and networks, which can result in catastrophic consequences.

Furthermore, in contemporary societies, the prominence of technology has had a profound impact on warfare, leading to a shift towards technology-driven conflicts. This transformation is evident through the increasing reliance on various information systems like GPS, unmanned vehicles, and automated systems. As societies become more inclined towards the utilization of robotic and digitized systems, digitized conflict has emerged as a more enticing prospect, especially when it offers reduced risks and resource burdens. The concept of cyber warfare is believed to have the ability to greatly influence, disturb, and incapacitate both traditional military operations and civilian systems, particularly vital infrastructure. The emergence of cyber capabilities has opened up new avenues for achieving political objectives without resorting to full-scale warfare, which typically come with immense human and financial costs. Given the interconnected and interdependent nature of our modern society, activities pertaining to cyberspace, ranging from spreading false information to launching aggressive cyber-attacks, have the potential to play a crucial role in achieving significant outcomes with reduced risks and less attribution. One significant aspect of cyber warfare is its ability to diminish the display of hostility and avoid provoking further escalation, which is often associated with conventional military force. As a result, the cyber domain has gained prominence and is now considered an integral component of a nation's power and strategic planning (Wooding, 2019).

In today's society, which increasingly depends on digital infrastructures, there has been a significant shift in the way conflicts are waged. This shift has rendered the traditional notion of a physical front obsolete, as the lines between times of war and peace have become increasingly blurred. The inception of cyber operations is not easily discernible, making it challenging to precisely identify when and where these actions begin. Furthermore, the objective of these cyber operations is not necessarily to achieve a decisive victory that brings an end to the conflict. Instead, their aim is to utilize cyber tools for the purpose of engaging in destructive sabotage, specifically targeting the enemy's information infrastructures in order to disrupt their operations and gain a strategic advantage.

Furthermore, in addition to their primary purpose of gathering intelligence through covert methods, cyber espionage attacks are also employed as a means to tarnish the reputation and diminish the morale of opposing powers. This multifaceted approach allows states to achieve their desired objectives, whether they be political, economic, or of another nature, without completely severing the possibility of negotiation or diplomatic and economic relations. Unlike traditional warfare, cyber warfare offers an unparalleled strategic advantage that comes with significantly lower costs and risks. As there is no formal declaration of war or open conflict between two states, the option to engage in peaceful discussions and negotiations always remains. Compared to conventional warfare, cyber warfare is easier to initiate as it allows for the evasion of direct responsibility, requires less logistical complexity and economic investment, and poses fewer political risks, as the ultimate goal is not necessarily military victory (Bargues ve Bourekba, 2022).

In contemporary conflicts, the historical distinction between civilian and combatant populations has become obsolete. This is due to the presence of non-state actors who seamlessly blend into the civilian population, making it challenging to differentiate between friend and foe. One of the contributing factors to this phenomenon is the absence of a clearly defined battlefield in modern warfare. Military operations can occur anywhere and everywhere, making it difficult to pinpoint a specific location where battles take place. Furthermore, the emergence of cyber warfare has further eradicated the physical battlefield, as conflicts can now be waged in the virtual realm. In this current security environment, where the primary threat to national security emanates from non-state actors, it is plausible to expect a wider utilization of technologies of war, especially those that have low barriers to entry. These non-state actors often lack the conventional military forces possessed by nation-states, and they compensate for this disadvantage by employing cyberweapons. The accessibility and affordability of cyberspace have contributed to power imbalances, allowing smaller non-state actors to challenge the dominance traditionally held by nation-states (Rosenzweig, 2013).

This strategy allows actors to compensate for any weaknesses they might have in terms of weaponry and other conventional forms of power. Instead of investing in training soldiers and acquiring and operating armored vehicles to physically disrupt a power plant through traditional methods, a group of hackers can efficiently and cost-effectively launch a cyber attack on the same target. The advent of advanced weapon systems and their possession by dominant states has rendered weaker states and non-state groups incapable of resisting these powerful entities. As a result, smaller, irregular forces have resorted to asymmetric conflict, employing tactics such as cyber warfare while leveraging technology, networks, cyberspace, and media (Indianstrategicknowlegdeonline,2009).

Former Secretary of Defense Donald Rumsfeld draws a comparison between kinetic warfare (traditional armed conflict) and cyber warfare, highlighting the drawbacks of massing an army and the advantages of training cyber warriors. Rumsfeld points out that assembling a large army is a time-

consuming and costly process, which also brings negative publicity when citizens' children are killed or return home with physical and psychological injuries. In contrast, training cyber warriors presents its own set of challenges, but the advantage lies in the fact that hackers rarely face the risk of physical harm or debilitating injuries in the realm of cyberwar. Furthermore, when compared to conventional weapons like fighter aircrafts, tanks, or bombs, the tools used in hacking are relatively more cost-effective. While the maintenance and sustainment of a massed army and traditional weapons systems incur exorbitant costs, cyber warfare offers a comparatively lower operational cost (CyberCecurity, 2023).

In regards to cyberweapons, in contrast to traditional weapons, cyberweapons possess a distinct characteristic of being widely dispersed and demanding considerably fewer resources for acquisition. The development of conventional weapons, such as weaponized drones, ballistic missiles, or even nuclear bombs, necessitates substantial investments in terms of human capital, financial backing, and physical infrastructure. Conversely, cyberweapons solely require a computer, access to the Internet, and proficient computer engineering expertise. This fundamental disparity has resulted in a paradigm shift, as it has enabled not only nation-states but also substate factions and even individuals to emerge as significant contenders in the cyber domain. In contrast to the limited accessibility of nuclear weapon or aircraft carrier development, the internet has enabled a unique phenomenon where individuals can collaborate remotely and instantly connect with a vast number of people (Thomas,2018).

In conclusion, when considering the potential risks associated with traditional warfare, such as political instability, economic consequences, human casualties, and the possibility of failure, as well as considering the costs in terms of human and economic factors, the speed of execution, and the scalability of traditional warfare in contrast to cyber warfare, it becomes evident that cyber warfare presents a significantly more appealing option for state and non-state actors inclined towards causing harm.

4.3. Cyber War Debate

As analyzed in the previous section, it can be said that cyber warfare has changed the character of war. In particular, the easy accessibility of cyberspace, its ability to accommodate all kinds of actors, its asymmetric structure, its ability to conceal identity and source, its ability to target the enemy's resolve and determination by staying below the threshold of war and using information and psychological warfare methods, and the fact that it does not adhere to geographical boundaries or rules and laws while doing all these, have been very effective factors in changing the character of war. It is precisely at this point that some researchers have brought new war debates to the agenda in light of the changing character of war and started to ask questions about the possibility of cyber warfare. There is a group of researchers who argue that cyber tools may cause destruction equivalent to conventional attacks in the future and that conventional wars will be replaced by cyber wars, and an opposing group of researchers who completely reject the possibility of cyber warfare. Another group of researchers has argued that cyber warfare can be effective as a means of supporting conventional warfare. The character of war is a

dynamic phenomenon and has changed over the years due to political, military, technological and other factors. The existence of cyberspace has certainly changed the character of warfare, but so far, cyber attacks have not had an impact equivalent to conventional wars. It has been shown that cyber warfare has been waged in coordination with conventional warfare to impose its demands on another state, to destroy the critical infrastructures of hostile countries, and to gain psychological superiority over the public opinion of the adversary country during a political dispute. This issue will be discussed in more detail by analyzing the arguments of researchers and academics who consider cyber warfare as a force multiplier of conventional warfare and reveal the reasons for this situation.

4.3. Cyber Warfare As A Complement To Conventional Warfare

This particular school of thought puts forth the argument that cyber warfare, on its own, will not occur independently, but rather, it will act as a supplement to traditional physical warfare. British General Sir Nicholas Houghton supports this viewpoint by suggesting that contemporary physical wars incorporate an online dimension, wherein cyber networks are exploited to manipulate public opinion and shape perceptions (Lemmerling, 2017:53). This group of thinkers firmly believes that the internet will serve as a battleground for future conflicts, but they remain skeptical about the ability of cyber attacks alone to determine the ultimate outcome of such conflicts.

The scope of cyberattacks is currently restricted due to the intrinsic connection between cyberspace and the physical realm. One prominent case of cyber sabotage, known as Stuxnet, serves as a remarkable example, as it likely necessitated human intervention and the use of a flash drive to bypass the protective barrier separating the Iranian nuclear centrifuge systems from external intrusion. Furthermore, cyberattacks often exhibit limitations in terms of their duration and the ease with which their effects can be reversed when compared to traditional kinetic attacks. Stuxnet, for instance, managed to impede the progress of the systems it targeted, yet failed to completely destroy their capabilities. Lastly, it is crucial to note that cyberattacks do not provoke substantial destabilization in international relations, primarily due to the fact that nations exercise self-restraint when utilizing their cyber power (Brantly & Van Puyvelde, 2019).

According to Erik Gartzke, the discussion surrounding cyber warfare has been disproportionately fixated on the methods and consequences of cyberattacks, such as their destructive potential and lethality. Insufficient attention has been paid to comprehending the motivations driving individuals or entities with the capability to engage in such actions (Gartzke,2013). There are several reasons why a state might choose to use cyberattacks as a means to target an adversary. Traditionally, force has been employed to punish, conquer, and compel enemies to comply with certain demands. However, Gartzke argues that the majority of actors capable of causing harm to their adversaries, whether through cyberattacks or other means, often refrain from doing so because they lack sufficient motivation. Similarly, Valeriano and Maness (2015:2) also contend that cyberattacks alone do not pose a significant

enough threat to influence the political decisions of a sovereign nation. Although cyberattacks may result in costs for the targeted adversary, such as the disruption of their electricity grid, these damages can typically be repaired, and there would be no lasting harm that could potentially shift the balance of power between the two parties involved (Gartzke,2013).

In order to engage in cyber warfare, actors must first locate weaknesses in secure critical systems. With each new operation, the attacker may be required to discover a fresh vulnerability, as the targeted state will likely take steps to address and rectify its weaknesses following an attack. Moreover, it is possible that the targeted state may have already resolved these vulnerabilities prior to the initiation of the attack, resulting in potential failure or a lack of the desired impact for the operation (Schreier, 2015). According to Gartzke's standpoint, cyber warfare has the potential to disrupt power grids, immobilize airports, and hinder communication systems, thereby causing financial harm to the targeted nation. Nonetheless, it is important to note that such damage is only temporary, and most of it can be rectified with relatively small investments (Gartzke, 2013:57). The consequences of cyber operations are uncertain and cannot be accurately predicted. The impact of such operations may not be as strong or significant as initially anticipated. This is primarily due to the interconnected nature of various systems, which means that an attack can inadvertently harm not only the intended targets but also the individuals or organizations responsible for initiating it, as well as their allies. Moreover, from a strategic perspective, it is illogical for any actor engaging in cyber warfare to restrict themselves solely to a specific type or category of weaponry (Schreier, 2015).

The task of attribution, or identifying the perpetrator behind a cyber-attack, is a highly intricate process in the realm of cyberspace. It is extremely difficult to provide concrete evidence that definitively links a state to an attack. This challenge arises from the fact that attackers have numerous means to conceal their actions within the complex web of cyberspace. One common method involves the use of a botnet network, wherein a virus or worm takes control of a network of computers. This network, also known as a zombie network, is often situated in a different geographical location than the attacker, and the individuals whose devices are part of this network are typically unaware of their involvement in the malicious activities being carried out. In addition, states are constantly enhancing their ability to carry out covert cyber operations against other states, making it incredibly challenging to identify the responsible party unless they willingly accept accountability. This particular characteristic of cyberspace poses a significant obstacle in categorizing an attack as an act of cyber warfare due to the absence of attribution. Moreover, this challenge also renders it nearly impossible to respond outside of the cyber realm, as it becomes exceedingly arduous to establish the necessary political circumstances that would allow for pinpointing a specific country as the perpetrator of a particular cyber-attack (Novaković & Rizmal, 2018:254). According to Gartzke, the lack of attribution poses a significant challenge for attackers. Cyber attacks, by their very nature, are unable to serve as a demonstration of

power or a means of issuing threats. This raises the question of why an adversary would choose to launch an attack while remaining anonymous. While anonymity may provide protection against potential retaliation, it also hinders the attacker from receiving recognition for their actions. In other words, as Gartzke points out, when anonymity shields an aggressor from consequences, it also diminishes the acknowledgment they would receive for their deeds (2013:46). When considering the perspective of the victim, it becomes apparent that surrender is not an option if the attacker cannot be identified. Consequently, the attacker must come to the realization that cyberattacks hold limited power without being linked to more traditional forms of military aggression, where identifying the perpetrator is less challenging. In this particular scenario, cyberattacks are expected to retain their secondary role, as they are overshadowed by the utilization of conventional kinetic forces that have the capability to cause intolerable damage to an enemy (Brantly & Van Puyvelde, 2019).

There are additional factors that contribute to states' reluctance to partake in a purely independent cyber war. One such factor is the limited scope for signaling and deterrence within the cyber domain. This constraint is primarily attributed to two key reasons. Firstly, the development of capabilities for conducting cyber warfare is predominantly shrouded in secrecy, making it challenging for states to gauge the extent of their adversaries' cyber warfare capabilities. Secondly, unlike traditional warfare where the use of nuclear weapons on Hiroshima and Nagasaki served as a powerful demonstration of their destructive potential, cyber attacks lack a similar "demonstration effect." Consequently, it becomes more difficult to showcase the potential dangers associated with cyber attacks, further reducing the effectiveness of deterrence strategies. Due to the limited understanding of the general public regarding the magnitude of risks associated with the cyber realm, implementing effective strategies for both signaling and deterrence becomes challenging. In simpler terms, it is difficult to convince people that engaging in a conflict within the cyber sphere would result in significant costs. Consequently, due to the lack of awareness among the public regarding potential dangers and threats that may arise from future cyber conflicts, decision-makers face a diminished level of pressure from the people, which is a crucial factor for the successful implementation of a deterrence strategy. Another challenge lies in the fact that cyber weapons are typically effective only for a single use. This implies that after the initial attack, the targeted entity can enhance their defenses by bolstering and upgrading their own systems. Moreover, they can also disseminate this knowledge to other potential targets. Consequently, nations tend to hesitate in deploying their most advanced and potentially hazardous cyber weapons. This cautious approach stems from the realization that in the event of a full-fledged war, when combined with conventional weaponry, these cyber weapons possess the potential to confer a strategic advantage (Novaković & Rizmal, 2018:255- 256). According to Struglinski, Stuxnet was quickly rendered ineffective and extensively analyzed by the Iranian authorities after its discovery. Consequently, the vulnerabilities exploited by the virus were promptly addressed and patched, ensuring that not only

would there be no possibility of a subsequent Stuxnet attack, but also thwarting any potential future assaults utilizing similar entry methods (Struglinski,2012).

Unlike traditional weapons, the impact of cyber attacks on nations is heavily dependent on their level of connectivity. In other words, the more interconnected a state is and the more it relies on cyberspace for its operations, the higher the potential for a cyber attack to cause significant damage. Consequently, cyber warfare is most effective when employed against states that have extensive connectivity, wherein critical systems, both military and civilian, are automated and reliant on network-based management. Consequently, states possessing advanced cyber capabilities are more likely to become targets of such attacks (Novaković & Rizmal, 2018:256). On the other hand, it is worth noting that numerous countries, particularly those with limited resources and lacking technological advancements, have governments, militaries, and citizens who possess minimal connectivity. Consequently, launching a cyber attack against these nations would yield little impact and may even escape detection. In contrast, physical weapons have the potential to be employed against any state, irrespective of their economic status or level of technological development, as long as they fall within the range of the aggressor's capabilities (Stimpson,n.d.:4).

Furthermore, it is important to acknowledge that the countries that possess the greatest cyber capabilities are also the ones that invest the most in cyber defense (Novaković & Rizmal, 2018:257). If an adversary has a robust and impenetrable cyber defense system, it becomes nearly impossible for any cyber attack to be effective. This is exemplified by the concept of air-gapping, which refers to electronically isolating a country in cyberspace, allowing them to easily reduce or eliminate their presence (Stimpson, n.d.:5). A notable example of this is the Stuxnet virus, which required entry into the target environment and subsequent spreading to reach its intended target. However, this target was protected by an 'air gap', meaning it was not connected to the insecure Internet or even internal networks. Consequently, the infection occurred through the use of a removable drive, such as a USB stick (Rid, 2013: 44). As a result, the limited accessibility and reliance on physical means for infection significantly restricts the potential use of cyber warfare as a standalone or fully-fledged branch of warfare.

Another factor that hinders the effectiveness of cyber attacks as a standalone method of warfare is the significant amount of time and effort required to prepare a sophisticated virus or worm. While it is indeed possible to initiate a cyber attack within seconds with a simple click of a button, the creation and preparation of the cyber projectile necessitates careful planning and preparation. Whether it is a retaliatory strike or a pre-emptive action, a considerable amount of groundwork must be completed beforehand (Stimpson,n.d.:6). According to Roel Schouwenberg from Kaspersky Lab, the development of the worm in its final form took a significant amount of time, specifically two to three years (Fruhlinger, 2022). Furthermore, Singer and Friedman argue that carrying out sophisticated cyber attacks necessitates the involvement of highly skilled cyber experts. Additionally, the ability to disrupt hydroelectric generators

or create malware like Stuxnet, which disrupts the operation of nuclear centrifuges, goes beyond simply gaining access to computer systems. It requires a deep understanding of the specific actions to take once inside the system. Causing substantial harm involves comprehending the intricacies of the targeted devices themselves, including their functioning, engineering, and even the underlying principles of physics. Stuxnet serves as a prime example of how successful cyberattacks require a diverse team of experts, including cyber professionals, nuclear physicists, and engineers with specialized knowledge of Siemens industrial equipment. In addition to the expertise needed, substantial financial resources are required to conduct rigorous software tests on the specific hardware targeted. Hence, the numerous prerequisites necessary to carry out a successful retaliatory cyberattack render cyber tools an unappealing option. Moreover, for a cyberattack to be effective as a pre-emptive strike, extensive knowledge of the target is essential, and ample time is required to thoroughly investigate the opponent's system for vulnerabilities prior to launching an attack (Stimpson,n.d.:6).

According to Amy Chang, a research associate in the technology and national security program at the Center for a New American Security, cyberweapons offer an enticing option for nations seeking a cost-effective and easily accessible alternative to traditional weaponry. In terms of affordability and accessibility, cyber warfare presents a significant advantage, as these digital weapons are considerably cheaper and more readily available to smaller nations (Suciu,2021). According to Ross Rustici's perspective, the affordability of cyber weapons presents a unique opening for technologically disadvantaged nations to challenge the superiority of more advanced countries in terms of their technological capabilities and conventional weaponry. In his viewpoint, it is plausible that in the near future, any nation equipped with a basic network connection could potentially exert enough influence to incapacitate an entire capital city (Rustici,2011:37). In addition, Garkze asserts that the implementation of the cyberwarfare strategy is not limited by financial or physical limitations. This implies that any entity, regardless of size or resources, is capable of accessing and utilizing cyber attack tools for the purposes of engaging in cyber warfare (Gartzke, 2013:44). Knapp and Boulton says '*cyberweapons have become more affordable and available…. An attacker can build an E-bomb, designed to "fry" computer electronics with electromagnetic energy, for as little as $400.' (2006:79).* While it is true that cyber weapons are readily available and affordable to various actors, it is important to note that this argument may not fully encompass the complexities of conducting advanced cyber operations. Liff, for instance, highlights the limitations of conventionally weaker actors in terms of their ability to incapacitate the infrastructure of more sophisticated adversaries. Such endeavors demand substantial human resources, technical expertise, and organizational capabilities that are typically beyond their grasp (Liff, 2012:411). In addition, Rid highlights that the development and deployment of Stuxnet necessitated significant resources and investment, making it evident that only a nation possessing considerable cyber capabilities could have undertaken such an operation. This underscores the notion that crafting sophisticated cyber weapons demands substantial technical expertise and

financial backing, thereby making them unlikely choices for economically disadvantaged nations (Rid, 2013:45). He adds that Stuxnet required '*time, resources, and an entire team of core developers as well as quality assurance and management. The threat also combined expensive and hard-to-get items: four zero-day exploits (i.e. previously unknown and hence highly valuable vulnerabilities); two stolen digital certificates; a Windows rootkit (software granting hidden privileged access); and even the first-ever Programmable Logic Controller rootkit* (Rid, 2013:45).

When cyberweapons are utilized in the digital realm, the user may not always have complete authority over the weapon's impact or its eventual destination. This lack of control can lead to detrimental outcomes for both the attacking state and the targeted state. For instance, a deployed cyberweapon could permeate the attacker's own networks, infecting their employer's systems and resulting in negative repercussions. In contrast to conventional weapons, the effects of cyberweapons are not easily observable or finite. It is challenging to ascertain the extent of damage caused by a cyberweapon or where a virus may ultimately infiltrate. When a state loses control over the consequences of its weapons, it runs the risk of inflicting more harm upon itself rather than the intended target. The ramifications of such cyber blowback would encompass the disruption of systems integral to the daily lives of citizens, critical infrastructures, and economic productivity (Stimpson,n.d.:8). According to Kevin Hogan, a senior director for Symantec Security Response, Stuxnet has already managed to infect a staggering 115 countries (Yeo, 2010). This alarming spread of the virus highlights the potential global consequences of utilizing cyber space to target a country's economy and industry. In today's interconnected world, attacking vital systems such as power generators, IT infrastructures, and global financial systems can have dire repercussions for both the attacker and the targeted state. The repercussions of such an attack could result in severe negative impacts on various levels, including economic, political, and societal. It emphasizes the need for governments and organizations to prioritize cybersecurity and adopt measures to protect against such cyber threats.

If we are advocating for cyberwar as a valid form of warfare, it is important to consider the aspects of deterrence and coercion. Deterrence requires two crucial components: a credible threat and the ability to effectively communicate that threat. However, the complexity of cyberspace makes it difficult to achieve either of these elements. Unlike physical means, cyber coercion is unable to compel the enemy as effectively. To establish deterrence, one must convince the adversary that an attack will result in significant pain and suffering. Unfortunately, cyber attackers face limitations in terms of what they can accomplish. While disrupting a state's industry or military communication networks may be bothersome and temporarily weaken the state, the effects are only temporary, and any resulting damage can be repaired relatively quickly. In addition, it is crucial to not only possess the means to deter a credible threat and effectively carry out operations, but also to communicate one's capabilities to the adversary. However, it is important to consider that revealing offensive and defensive capabilities in cyberspace

may inadvertently provide the attacker with valuable knowledge. For instance, if an operation showcasing offensive capabilities is conducted, it may not be as impactful because once the target detects a computer virus, they will thoroughly analyze its design and identify access points. Consequently, launching a subsequent attack using an identical or similar virus and exploiting the same vulnerabilities would be extremely difficult, if not impossible, to execute again (Stimpson,n.d.:9-11). Attribution presents a significant challenge in cyber warfare when the objective is to manipulate or intimidate an adversary. This is due to the fact that the originator of a cyber deterrence message remains unidentified, thus increasing the likelihood of misinterpretation, misreading, misidentification, or even complete failure to detect the message (Stimpson,n.d.:11).

In their study, Flemming and Rowe discuss three key factors that can have an impact on the success of cyber coercion. The first factor they highlight is the reusability of the attack method. Essentially, once a system that is being targeted by a cyber attack updates its defenses and implements countermeasures, the effectiveness of that particular attack method diminishes. This suggests that attackers need to constantly innovate and develop new strategies in order to maintain their success rate. The second factor identified by Flemming and Rowe is the uncertainty and complexity of the technological sphere in which cyber coercion occurs. The realm of cyber operations is characterized by a high level of uncertainty, making it difficult for attackers to accurately predict the vulnerabilities of their target systems. This creates a challenge for attackers, as the weaknesses they identify in a system may be addressed and fixed before they even have a chance to launch their attack. In summary, Flemming and Rowe argue that the success of cyber coercion is contingent upon the reusability of attack methods and the unpredictable nature of the technological sphere. Attackers must constantly adapt and find new ways to exploit vulnerabilities in order to maintain their effectiveness. Additionally, the uncertain and complex nature of the cyber realm poses a challenge for attackers, as their target systems may be fortified before they can execute their planned attacks. Lastly, the issue of attribution poses another significant challenge that can impact the effectiveness of cyber coercion. As previously stated, the realm of cyber operations is intricate and multifaceted, making it difficult to definitively determine the true identity of the attacker. Consequently, when the adversary lacks certainty regarding the responsible party behind the attack, they may not perceive the demands being made as highly credible or legitimate. This lack of attribution can undermine the overall success of cyber coercion tactics (Flemming and Rowe, 2015).

In his article showcased at the 17th European Conference on Cyber Warfare and Security, Andrew Liaropoulos discusses five significant hurdles that must be overcome in order to effectively establish cyber coercion. The initial challenge revolves around communication. Unlike in traditional diplomatic scenarios where the coercer's demands are straightforwardly conveyed, the realm of cyberspace presents a more convoluted landscape for communication. Consequently, the coercer must carefully select the

most appropriate method to effectively convey their true intentions behind the attacks, ensuring that the target comprehends the message clearly. One of the challenges in cyberspace is the attribution problem, which involves the difficulty of identifying the true identity of an attacker. This issue is further complicated by the fact that revealing the methods and capabilities used for attribution can diminish the effectiveness of future operations. Anonymity is often seen as advantageous for actors engaging in cyber operations, but when it comes to cyber coercion, it becomes necessary to determine and disclose the attribution in order to persuade the target and convey a clear message. Lastly, assuring the opponent that once they comply with the demands, there will be no further threats adds complexity to the coercive strategy. The nature of cyberspace introduces ambiguity regarding the origin of the attack and the clarity of the demands and intentions. This ambiguity can make it difficult for the opponent to trust the coercer's promise of no further threats, as the source and motives behind the initial attack may remain unclear. Furthermore, establishing credibility poses another obstacle in cyberspace. It is difficult to accurately measure power and demonstrate capabilities, which are crucial in convincing the opponent of the seriousness of the threats. In the virtual realm, where physical presence and tangible evidence may be lacking, establishing credibility becomes more challenging (Liaropoulos, 2018).

CONCLUSION

The phenomenon of war, which constitutes one of the most fundamental subjects of study in the discipline of International Relations, continues to be one of the most studied topics in the field. The fact that there is no clear framework on war and that there are still debates on the nature and characteristics of war, despite the high number of studies, shows the complexity of the subject. One of the most important reasons for this is that war is a dynamic, ever-evolving phenomenon that is influenced by the social, technological and economic conditions in which it takes place.

With the end of the Cold War, the change of the international system into a unipolar structure, the emergence of the globalization process, the emergence of new actors and threats, and the widespread use of rapidly developing technology and information and communication tools have brought with them a change in the character of warfare. In the period of strategic uncertainty that emerged after the Cold War, long-suppressed ethno-nationalist aspirations for autonomy and self-governance have come to the fore all over the world, and ethnic-based civil wars have increased, with most of the conflicts in the nature of civil wars occurring in failed states (Snow, 1996:2-3). With these developments, new war debates, which argue that the outlook of 21st century wars is different from the old wars, have started to come to the agenda. Accordingly, the first part of this study examines the reasons for the changing character of war.

In the second part of the study, questions about the characteristics of new generation wars were asked in the second part of the study regarding what today's wars look like, and answers were sought by reviewing the relevant literature. These questions are grouped under 9 headings focusing on the war's purpose, actors, target audience, front, strategies, economy, weapons, start-end processes and symmetry. At this point, it has been stated that new wars are mostly caused by identity-based reasons; there has been a change in the actors of war and the state has lost its monopoly on the use of force, especially with the globalization process; there has also been a change in the target audience of the war in new generation wars and it has become more important to conquer the will of the target population; as a result of this, the front of the war has expanded. Since the primary goal is to seize control of civilians, the methods and strategies of war have also changed accordingly. The importance of information operations to capture the will of civilians has increased. It has also been argued that there have been changes in the economics and financing of war. With the development of technological elements, the weapons used in warfare have also changed, especially cyber weapons have become indispensable elements of new generation wars. The requirement of a declaration at the beginning and end of the war, which traditional international law considers as one of the criteria of war, has lost its importance in new generation wars. It has been stated by the authors in the relevant literature that there are no clear boundaries for the start and end of new generation wars. And finally, it is noted that the asymmetry between the opponents in wars is becoming more and more evident. Now, there is usually a state with

better equipped and modern forces on one side, while on the other side, irregular forces, which are relatively weaker in terms of armament, financing, power and so on, fight using asymmetric means and strategies. Additionally, based on the discussions on the character of the new generation war, one of the research questions of the study was to determine what kind of an evolutionary process war goes through and what today's wars look like. In this context, the study of Lind et al. (1989), which tries to explain this evolution process by dividing war into phases or generations by putting forward the thesis that war evolves, was analyzed.

In the last part of the study, the questions asked about the changing character of war are also asked for cyber warfare and an attempt is made to examine how cyber warfare tools change the character of warfare and the meaning of cyber warfare in new generation war studies. In regards to aim, state and non-state actors engage in a constant struggle driven by a myriad of motivations, including geopolitical interests, ideological beliefs, religious affiliations, economic ambitions, political agendas, and even military objectives in cyberspace. It is crucial to recognize that the objectives of wars cannot be simply reduced to identities as Mary Kaldor argues (2013:2), as they are shaped by a complex interplay of various factors including ideologies, economic considerations, and geopolitical aspirations. Nonetheless, it can be argued that it is, in fact, the means of achieving the goals that distinguishes the old and new wars from each other. In the light of these evaluations, it can be said that cyberspace provides the opportunity to act in line with the purpose of the actors, regardless of the type of purpose. In terms of actors, the fact that cyberspace is inherently cheap and accessible to all kinds of actors has led non-state actors to develop their capacity to use force in this area. In the new generation wars, the main goal has become to break the will and determination of the people of the target country to fight and to weaken the belief of the target people in their own government and army. In line with this goal, cyber sabotage, cyber espionage, propaganda, disinformation and misinformation activities are effective in addition to targeting the critical infrastructure systems of actors who are becoming more and more dependent on cyberspace. The battlefields where traditional wars were waged and physical borders were clear have now moved to cyberspace, which is no longer bounded by geographical limitations.

In addition, in the new generation of wars, where the determination and resolve of the people are targeted instead of occupying a territory and destroying enemy forces, the target of the war has begun to be explained in socio-psychological and political-ideological terms rather than physical terms. The emergence of the 'knowledge' and 'spiritual' spheres of traditional wars based on geographical terrain has led to a change in the field of war. The targeting of this intangible sphere is carried out more effectively and quickly with the use of cyber warfare tools together with the developing information and communication technologies and the increasing use of social media. The fact that new generation wars control the public by targeting people's psychology and beliefs with political tools instead of capturing a region with military means has enabled cyber warfare to be used as an alternative war strategy, since it has become possible to discredit the adversary with psychological operations and sabotage activities

carried out in cyberspace, to shape the perceptions and opinions of the target public opinion in accordance with friendly interests, and to control the public by attacking and infiltrating the information processing infrastructure of the adversary. Researchers reveal that the financing of new wars is based on a globalized economy where the income is based on ongoing violence (Kaldor, 2013:3). With the Internet being both decentralized and integral to globalization, the potential for funding conflicts in cyberspace is vast. There is a growing cyber-crime market for state and non-state actors motivated by political and economic gains. The use of crypto-currencies has played a vital role in amplifying these activies. In terms of weapons, cyber weapons are portable, cheap, easy to access, not bound by geographical borders and legal restrictions. The beginning and end of cyber warfare are ambiguous because the nature of cyber warfare is such that cyber attacks are conducted anonymously and covertly. A declaration of war, as in conventional warfare, will result in the failure of cyber warfare as it will cause the target to close its vulnerabilities by increasing its cyber security measures. Cyber warfare is also used in times of peace and conflict as part of a larger operation to discover vulnerabilities in systems. Finally, the very nature of cyberspace, which allows access to all kinds of actors, has changed the symmetry of warfare, as attacks in cyberspace are not concerned with who is physically stronger, but who is better equipped for cyber attacks, and a relatively weaker state can target the internet-oriented systems of a stronger state in cyberspace.

In conclusion, despite cyber warfare's relative infancy, its speed, range, cost, accessibility, and range of effects undoubtedly have changed the character of war. In the cyber era, technology permits attacks at light speed and negates any barriers imposed by distance. Forces can be equipped for as little as the price of a laptop computer. In the 21st century, operations in the cyber domain provide all actors a type of force-leveling which was previously reserved for the wealthy. Cyber warfare offers low entry barriers, the capability to act without regard to boundaries, reduced risk to human life, clandestine maneuver, deniability, amplified effectiveness of the few, and blurred lines between combatant and non-combatants. Thus, while operations within the cyberspace domain are still relatively immature, its integrated use has dramatically influenced the manner in which wars are fought.

In the aftermath of two devastating world wars, people have begun to take a stance against the use of violence and the human and financial burdens that wars bring with them. In particular, the emergence of the internet and social media, and the fact that wars can now be closely monitored, has created the potential to influence societies' war policies. With these developments, states are faced with the dilemma of ensuring security in a globalizing world against globalized and more complex threats and maintaining their legitimacy while resorting to violence. Especially after taking into account the various dangers inherent in conventional warfare, like the destabilization of political systems, the negative impact on economies, the loss of human lives, and the likelihood of unsuccessful outcomes, coupled with the consideration of the toll it takes on people and finances, it becomes clear that opting for cyber warfare is an immensely attractive choice for state and non-state actors.

In line with these arguments, it has been argued that cyber warfare may replace conventional warfare in the near future. However, research indicates that cyber warfare is a strategic and often distracting or delaying force multiplier that can support the faster conclusion of conventional wars. Nevertheless, due to the nature of cyberspace, it is impossible to know the cyber attack and defense capacities of countries, and since this field is new and countries are still trying to discover their attack and defense capacities in this field, the question of what consequences cyber attack tools can cause yet and whether they can replace conventional wars in the future is still puzzling. As technology develops and dependence on technology increases, the lasting effects of cyber warfare may increase in the future, strengthening it as a singular warfare technique. In the case of Estonia, it has been demonstrated that a country's critical infrastructure systems can be targeted with cyber-attacks lasting for days, in the case of Georgia, cyber-attacks can be used in conjunction with conventional wars, and finally, in the case of Stuxnet, physical damage can be caused with a cyber-attack tool. With technology advancing at breakneck speed, it is difficult to predict what will happen next, but it is certain that cyber warfare will continue to exist on the battlefield.

REFERENCES

Ablon, L., & Libicki, M. C. (2015). Hackers' Bazaar: The markets for cybercrime tools and stolen data. *Defense Counsel Journal, 82*(2), 143–152. https://doi.org/10.12690/0161-8202-82.2.143

Aras, H. (2022). Analysis of hybrid war strategies of Russia in the context of the Syrian çivil war [PhD Dissertation]. Bursa Uludağ University.

Bargues, P., Bourekba, M., & Colomina, C. (2022). War By All Means: The Rise Of Hybrid Warfare. Bargues, P., Bourekba, M., and Colomina (Eds.) Hybrid Threats,Vulnerable Order. CIDOB Barcelona Centre For International Affairs.

Bates, N. (2020). Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks. *Egham, United Kingdom: Royal Holloway, University of London*.

Batır, K. (2017). Uluslararası Hukukta Devlet ve Başarısız Devletler: Somali Örneği. Çanakkale Onsekiz Mart Üniversitesi Uluslararası Sosyal Bilimler Dergisi, 2(4), 81-102.

Bloomberg Originals. (2012, March 23). *Falkenrath says Stuxnet virus may have origin in Israel: Video* [Video]. YouTube. https://www.youtube.com/watch?v=H6VipR0xBGo

Brantly, A. F., & Van Puyvelde, D. (2019). *Cybersecurity: Politics, governance and conflict in cyberspace*. http://eprints.gla.ac.uk/173432/

Brock, L., Holm, H., Sorenson, G., & Stohl, M. (2012). Fragile states. Polity.

Bueno de Mesquita, B., & Lalman, D. (1992). War and reason : domestic and international imperatives. New Haven (Conn.): Yale university press.

Connell, M., & Vogler, S. (2017). *Russia's approach to cyber warfare* (pp. 1-29). Arlington, VA: CNA.

CyberCecurity, S. B. (2023). *Kinetic War vs. Cyber War: The Potential Battlefields Ahead* -. MSSP Alert. https://www.msspalert.com/post/cyber-war-vs-kinetic-war-explained

Cybercrimemag. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Çöpoğlu, M. O. (2018). Examination of new generation warfare by case studies of Russian Federation [MA Thesis]. Karadeniz Technical University.

Dayspring, S. (2015). Toward a Theory of Hybrid Warfare: the Russian Conduct of War During Peace.

Dehghan, S. K. (2017, November 26). Iran accuses Siemens of helping launch Stuxnet cyber-attack. *The Guardian*. https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack

Department of Defense. (2006). *The National Military Strategy for Cyberspace Operations* (NMS-CO), Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf

Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. DIANE Publishing.

Earth', International Security, Vol. 38, No. 2

Freedman, L. (1994). Weak states and the west. Society, 32(1), 17–20. doi:10.1007/bf02693348

Fruhlinger, J. (2022). *Stuxnet explained: The first known cyberweapon*. CSO Online. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Gartzke, Erik (2013), 'The Myth of Cybewar: Brining War in Cyberspace Back Down to

Global Initiative Against Transnational Organized Crime. (2021). *The global illicit economy: Trajectories of transnational organized crime*. https://globalinitiative.net/wpcontent/uploads/2021/03/The-Global-Illicit-Economy-GITOC-Low.pdf

Gotsiridze, A. (2019). The Cyber Dimension of the 2008 Russia-Georgia War. RONDELI BLOG. Retrieved March 11, 2023, from https://gfsis.org.ge/blog/view/97

Gürcan, M. (2012). Savaşın Evrimi ve Teorik Yaklaşımlar. Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri, 71-132.

Hammes, T. X. (2005). War evolves into the fourth generation. Contemporary Security Policy, 26(2), 189-221.

Helman, G. B., & Ratner, S. R. (1992). Saving Failed States. Foreign Policy, (89), 3. doi:10.2307/1149070

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. Small Wars Journal, 6.

https://lib.ugent.be/fulltxt/RUG01/002/352/680/RUG01-002352680_2017_0001_AC.pdf

Indianstrategicknowlegdeonline. (2009). ''Conventional Wars:Emerging Perspective''. https://indianstrategicknowledgeonline.com/web/Theory%20of%20warConventional%20War%20Emerging%20Perspective%2019%20Nov%202009.pdf Accessed 10 Dec. 2023.

International Law Commission. (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supplement No. 10 (A/56/10), chp.IV.E.1, available at: https://www.refworld.org/docid/3ddb8f804.html [accessed 1 December 2023]

Jayachandran, C. J. (2009). Evolution of War into the Fourth Generation: A Historical Perspective. Claws Journal, 161-183.

Kaldor, M. (2012). New and Old Wars: Organized Violence in a Global Era (3rd ed.). Stanford University Press.

Kaldor, M. (2013a). New and old wars: Organised violence in a global era. John Wiley & Sons.

Kaldor, M. (2013b). In Defence of New Wars. Stability: International Journal of Security and Development, 2(1), Art. 4.DOI: https://doi.org/10.5334/sta.at

Kaspersky. (2014, December 9). *Eugene Kaspersky discusses the Stuxnet virus on Cybercrimes with Ben Hammersley* [Video]. YouTube. https://www.youtube.com/watch?v=4oNnSStrc38

Katovsky, B., & Carlson, T. (2003). *Embedded: The media at war in Iraq*. https://www.amazon.com/Embedded-Media-at-War-Iraq/dp/1592282652

Keely, D. M. (2011). *Cyber Attack!: Crime Or Act of War?*. US Army War College.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Khmelidze, E. (2021). The Russian hybrid Warfare: Case of Estonia. The Foreign Policy Council. https://foreignpolicycouncil.com/2021/11/04/the-russian-hybrid-warfare-case-of-estonia/

Kilcullen, D. (2006). Twenty-Eight Articles Fundamentals of company-level counterinsurgency. Marine Corps Gazette, 90(7), 50.

Kirk, J. (2009). Georgia cyberattacks linked to Russian organized crime. *Computerworld*.

Knapp, K. J., & Boulton, W. R. (2006). *Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. Information Systems Management, 23(2), 76–87.* doi:10.1201/1078.10580530/45925.23.2.20060301/92675.8

Krieg, A., & Rickli, J. (2019). *Surrogate Warfare: The Transformation of War in the Twenty-First Century*. Georgetown University Press.

Krztoń, W. (2022). Changes and Transformations of Wars and Armed Conflicts. Theoretical Approach. Journal of Security and Sustainability Issues, 12(1), 17-26. doi:10.47459/jssi.2022.12.2

Küpeli, M. Ş. (2016). The economic politic effects of the sanctions imposed against Iran in the framework of nucleer issue [MA Thesis]. Sakarya University.

Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). Strategic communications and social media in the Russia Ukraine conflict. *Cyber war in perspective: Russian aggression against Ukraine*, 103-111.

Lemmerling, N. (2017). "Could Cyber-Warfare Be Considered A New Tool of Foreign Policy?". Ghent University, Faculty of Political and Social Sciences. pp. 51-58. Available at :

Liaropoulos, A. (2018). The Uses and Limits of Cyber Coercion. In *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2* (p. 261-267).

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. http://www.jstor.org/stable/10.7249/mg877af

Liff, A. P. (2012). *Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, 35(3), 401–428.* doi:10.1080/01402390.2012.663252

Lind, W. S. (2004). Understanding fourth generation war. Military review, 84(5), 12-16.

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). The changing face of War: into the fourth generation. *Marine Corps Gazette*. https://www.academia.edu/7964013/The_Changing_Face_of_War_Into_the_Fourth_Generation

Livingston, S. (1997). Clarifying the CNN effect: An examination of media effects according to type of military intervention. *Shorenstein Center Research Paper Series*.

MacFarquhar, N. (2016). A powerful Russian weapon: The spread of false stories. *New York Times, 28.*

Martin, C. D. (2017). TAKING THE HIGH ROAD White hat, black hat: the ethics of cybersecurity. ACM Inroads, 8(1), 33-35.

Maurer, T., & Hoffman, W. (2019). The privatization of security and the market for cyber tools and services. *The Business & Security Series, 3*, 1-24.

Mello, P. A. (2010). In search of new wars: The debate about a transformation of war. European Journal of International Relations, 16(2).

Mercan, M. V. (2021). Ortadoğu'da Nükleer Gerginlik: İran-İsrail Güç Mücadelesi. Retrieved March 13, 2023, from https://www.insamer.com/tr/ortadoguda-nukleer-gerginlik-iran-israil-guc-mucadelesi_3984.html

Münkler H. (2010), Old and New Wars, in: The Routledge Handbook of Security Studies, eds. M. Dunn Cavelty, V. Mauer, Routledge, London, pp. 191–194

NATO StratCom. (n.d.). "2007 cyber attacks on Estonia", https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (Date of Accession: 05.02.2023).

Novaković, I. & Rizmal, I. (2018). Cyber warfare: New type of warfare of additional element of conventional warfare. Ministry of Defense, University of Defence Strategic Research Institute & National Defence School. Available at : http://www.isac-fund.org/wp-content/uploads/2019/01/Cyber-Warfare_Novakovic-Rizmal.pdf

Rid, T. (2013). Cyber war will not take place. Oxford University Press, USA.

Rosenzweig, P. (2013). Cyber warfare: how conflicts in cyberspace are challenging America and changing the world. ABC-CLIO.

Rotberg, R. I. (2002). Failed States in a World of Terror. Foreign Affairs, 81(4), 127. doi:10.2307/20033245

Roussi, A. (2022). Estonia fends off 'extensive' cyberattack following Soviet monument removal. POLITICO. https://www.politico.eu/article/estonia-extensive-cyber-attack-following-soviet-war-monument-removal/

Rustici, R.M. (2011) Cyberweapons: Leveling the international playing field. Parameters. 41 (3), 32–42.

Schmidt, A. (2013). The Estonian cyberattacks. *Atlantic Council.*

Schreier, F. (2015). "On Cyberwarfare". DCAF HORIZON 2015 Working Paper No.7. Available at : https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Shakarian, P. (2011). The 2008 Russian cyber campaign against Georgia. Military Review-English Edition, 91(6), 63.

Shearer, D. (1998). Outsourcing War. Foreign Policy, (112), 68. doi:10.2307/1149036

Snow, D. M. (1996). *Uncivil Wars: International Security and the New Internal Conflicts*. Lynne Rienner Publishers.

Stimpson, M. R. T. (n.d.). *CYBERWARFARE WILL NOT REPLACE CONVENTIONAL WARFARE* [MA Thesis]. CANADIAN FORCES COLLEGE. Available at : https://www.cfc.forces.gc.ca/259/290/317/305/stimpson.pdf

Struglinski, D. (2012). How Serious is the Threat of Cyber Warfare? *E-International Relations*. https://www.e-ir.info/2012/05/22/how-serious-is-the-threat-of-cyber-warfare/

Suciu, P. (2021, April 24). Why cyber warfare is so attractive to small nations. *Fortune*. https://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/

Sweet, C. (2017). State-sponsored cyberattacks are now the preferred method of warfare. *CSO Online*. https://www.csoonline.com/article/563413/state-sponsored-cyberattacks-are-now-the-preferred-method-of-warfare.html

Şengönül, A. (2018). Fourth generation war strategy under discussion for Turkey [PhD Dissertation]. Selçuk University.

Thomas, K. (2018). *Cyber vs. Conventional Weapons : Five Unique Attributes of Cyberweapons and Their Implications*. Medium. https://medium.com/@kamaalthomas/cyber-vs-conventional-weapons-795653bde5eb

Thomas, T. (2009). The Bear Went Through the Mountain: Russia Appraises its Fine-Day War in South Ossetia. *Journal of Slavic Military Studies*.

Traynor, I. (2009). Georgian President Mikheil Saakashvili blamed for starting Russian war. *The Guardian, UK*.

Tuck, C. (2014). Understanding Land Warfare (1st ed.). Routledge. https://doi.org/10.4324/9781315882253

U.S. Cyber Command. (n.d.). Command history. https://www.cybercom.mil/About/History/

Valeriano, B. & Maness, R. C. (2015). *The Impact of Cyber Conflict on International Interactions. Armed Forces & Society, 42(2), 301–323.* doi:10.1177/0095327x15572997

Van Creveld, M. (1991). On future war. New York.

Waltz, K. N. (1993). The emerging structure of international politics. *International security*, *18*(2), 44-79.

Wooding, C. (2019). ‘’The Rise of Cyber and the Changing Nature of War.’’ *Grounded Curiosity Blog*. https://groundedcuriosity.com/the-rise-of-cyber-and-the-changing-nature-of-war/ Accessed 12 Dec. 2023.

Yalçınkaya, H. (2004). Transformation of war at the post-cold war era (Publication No. 146746) [Doctoral Dissertation, İstanbul University].

Yeo, V. (2010). Stuxnet infections spread to 115 countries. *ZDNET*. https://www.zdnet.com/article/stuxnet-infections-spread-to-115-countries/

Yılmaz, S. (2021). The changing character of the war in the 21st century: Hybrid warfares in Middle Eastern context [PhD Dissertation]. Police Academy.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world’s first digital weapon*. https://ci.nii.ac.jp/ncid/BB19363361