IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

The Reality of Cyber Warfare: The Ukraine-Russia Conflict as a Catalyst for New Dynamics in Cyberspace

July, 2022

2573972N
20109962
26734797

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word Count: 23157
Supervisor: Christian Kaunert
Date of Submission: 26 July 2022

University of Glasgow

DCU UNIVERSITY OF TRENTO

CHARLES UNIVERSITY

The Reality of Cyber Warfare: The Ukraine-Russia Conflict as a Catalyst for New Dynamics in Cyberspace

Table of Contents

1. INTRODUCTION 4

2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK.... 12

2.1. The Information Revolution 13

2.2. The Emergence of the Fifth Domain 14

2.3. Main Features of Cyberspace 15

2.4. Actors and Activities in Cyberspace 16
2.4.1. Hackers, Hacktivists, Cybercriminals, and Nation-States 19

2.5. Cyber Campaigns, Cyber Operations, and Cyberattacks 20

2.6. Defining 'Cyber War' and 'Cyber Warfare' 22

2.7. Can Cyber War Take Place? 26

3. RESEARCH DESIGN AND METHODOLOGY 32

3.1. Qualitative Approach 33

3.2. Case Study: Ukraine-Russia Cyber Warfare 36

4. BACKGROUND INFORMATION 38

4.1. Ukraine and Russia: History and Geopolitics 38

4.3. Russia in Cyberspace 40
4.3.1. How Russia Conceives Cyber Warfare 42
4.3.2. The Role of Russia's Intelligence Agencies in Cyberspace 42

4.4. Ukraine in Cyberspace **44**
4.4.1. Ukraine's Use of Cyber Proxies 45

5. DATA ANALYSIS **46**

5.1. Initial Phase of the Ukrainian Conflict **46**

5.2. Intermediate Phase of the Ukrainian Conflict **49**

5.3. Current Phase of the Ukrainian Conflict **51**
5.3.1. Russia's Military Invasion of Ukraine: Is a Cyber War Taking Shape? 55

6. DATA INTERPRETATION **62**

6.1.Towards a New Definition of 'Cyber War' **63**

6.2. Cyber War Exists and Is Currently Underway **66**

6. CONCLUSION **72**

7. BIBLIOGRAPHY **76**

Abstract

The world is constantly evolving, and so is technological progress, which increasingly impacts the lives of all of us. The Information Revolution, triggered by the advent of the Internet and technological development, has fostered the emergence of a more interconnected world and, thus, of a new domain: *cyberspace*. Given its ubiquity and global reach, cyberspace is redefining power dynamics by creating new opportunities that different actors are willing to seize. Because goals and ways to achieve them vary, cyber threats also vary and increase accordingly. Actors may want to steal sensitive information by orchestrating espionage operations, gain money and power by conducting criminal activities, or even sabotage and ultimately cause damage to the adversary, as in war. Cyber warfare is a very controversial topic. Despite numerous attempts by the research community to conceptualise the phenomenon, there is still much confusion as to what it really is. Specifically, the definitional ambiguity of the term 'cyber war' is such that, to date, no single universally agreed definition exists. As a result, a debate has ensued on the existence of cyber war from which different currents of thought have emerged. While some argue that cyber war is an imminent threat and is likely to permeate the conflicts of the 21st century, others are reluctant to believe that the conditions for a war in cyberspace to occur are in place.

Since they are closely related issues, this dissertation aims to define *what cyber war is* and to determine *whether cyber war can take place*. To this end, the ten-year conflict in Ukraine will be analysed in three different phases: the initial phase, from 2013 to 2015, the intermediate phase, from 2016 to 2020, and the current phase, from 2021 to May 2022. For each phase, cyberattacks will be examined by applying the following criteria. First and foremost, cyberattacks are destructive in nature, meaning that they can be destructive even when they target things, thus resulting in the destruction of information, data, and software.

Secondly, cyberattacks target the critical infrastructure of the adversary. Thirdly, cyberattacks are instrumental and political in nature. If all the criteria are fulfilled, then they constitute acts of war. Regarding the Ukraine-Russia conflict, a total of 40 destructive cyberattacks have been detected since the Russian military assault on Ukraine on February 24th, 2022. There is no doubt that such cyber operations were planned by the Russian government in pursuit of its political and military objectives and launched with the aim of harming the enemy by targeting its critical infrastructure. Therefore, cyber war not only exists, but is also currently taking place. Moreover, having analysed the new dynamics in cyberspace that have been triggered by the ongoing conflict, an updated definition of cyber war will be provided.

Acknowledgments

To my angel, who never stopped being by my side and to whom I dedicate this important milestone.

To my mother, who never stopped believing in me and never missed an opportunity to remind me how strong I am.

To Alberto, who knows more than anyone else how to reassure me, support me, be there.

To Veronica, Aurora, and Aidana, precious pearls in my life. Thank you for listening to me even in my most deafening silences.

To my family, a safe haven to which I am always happy to return. Thank you for the immense love you show me every day.

To my colleagues, who have always supported and encouraged me.

to my professors, who have enriched my knowledge and lit my way.

And to myself, for NEVER giving up.

1. Introduction

Is cyber war taking place? The world is constantly evolving, and so is technological progress, which increasingly impacts the lives of all of us. The Information Revolution, triggered by the advent of the Internet and technological development, has fostered the emergence of a more interconnected world and, thus, of a new dimension: *cyberspace*. Cyberspace is an easily accessible virtual domain with no physical boundaries in which actors engage in both offensive and defensive behaviour, depending on the purpose for which they act. On the one hand, actors launch offensive operations seeking to control the information with the aim of affirming their power over the adversary. On the other hand, they continuously need to improve their defensive posture to maintain control of the information with the aim of preventing the adversary from attempting to gain power (Fanelli, 2016). In the last two sentences, the word 'power' has already been used twice, but what is power in cyberspace? Unlike the concept of power to which we are accustomed, the concept of *cyber power* takes on a slightly different meaning. Indeed, it consists of the ability to influence adversaries and gain a strategic advantage over them by owning the information in terms of confidentiality, integrity, and availability (Kuehl, 2009; Czosseck, 2013; Fanelli, 2016). In a nutshell, power belongs to those who hold the information, which can be accessed by anyone with strong computer skills, from single individuals to the intelligence units of a nation-state.

Thus, the dynamics of influence and power in cyberspace, which differ from those in the real world, create new opportunities that both state and non-state actors are willing to seize by using different tactics and techniques. As a result, the variety of goals, means, and ways to achieve them inevitably increases threats that take shape in the cyber arena every day (Choucri and Clark, 2018). In this respect, actors may want to steal sensitive information by orchestrating espionage operations, gain money and power by conducting criminal activities, or even sabotage and ultimately cause damage to the adversary, as in war.

Cyber war is a very controversial topic. Over the years, scholars have repeatedly attempted to define cyber war over the past decades, but without success. Consequently, to date, there is no universally accepted definition capable of adequately conceptualising the phenomenon. The ambiguity of the concept led to a debate from which different currents of thought on the actual existence of cyber war have arisen. While Arquilla (2012) and Stone (2013) argue that the conditions for the occurrence of cyber war exist, Rid (2012) firmly claims that cyber war has never taken place, does not take place, and will never take place in the future (Rid, 2012; Arquilla, 2012; Stone, 2013). Specifically, Rid (2012) draws these conclusions by applying the notion of war in conventional terms to the cyber domain and states that cyberattacks cannot be potentially violent, instrumental, and political in nature. Stone (2013) counter-argues Rid's statements claiming that cyberattacks can actually be lethal if we do not consider the term in its strict sense (Stone, 2013). It is a fact that no cyberattack has caused the physical death of millions of people, as is usually the case in a war in the real world, yet the destructive nature of some attacks has nevertheless proven to have devastating effects.

As can be seen, the problem of defining cyber war and the ensuing debate on its actual existence are intrinsically linked. Therefore, the first research question this dissertation aims to answer within a more definitional framework is: *what is cyber war?*. This question is followed by a second research question that emerged from a more theoretical framework encompassing the aforementioned debate, that is: *can cyber war take place?,* to which is then added, in consideration of the latest events concerning the war in Ukraine: *is a cyber war taking place?*. The attempt to contribute to the existing literature by providing an up-to-date definition of cyber war and determining whether conditions for its occurrence exist can serve as a basis for developing future research.

To answer these questions, we will delve into the heart of the Ukrainian crisis, triggered by escalating tensions with the Russian Federation following the then-

Ukrainian President's refusal to sign the Association Agreement with the EU. The long-lasting conflict in Ukraine, which started in November 2013 and erupted into a large-scale military conflict in February 2022, is one of the most representative cases of hybrid warfare. Hybrid warfare, in Russian strategic thinking, consists of the use of two sources of power, namely kinetic and cyber means, to combat the adversary (Covington, 2016). Over the years, in fact, we have witnessed a series of cyber operations and campaigns aimed at disorienting, sabotaging, and even damaging the adversary, especially by the Kremlin and affiliated cyber proxies. Beginning with the increase in DDoS attacks coinciding with the Euromaidan protests, the annexation of Crimea, and the conflict in Donbas, going through cyber espionage campaigns, such as Operation Armageddon, orchestrated by Russian Advanced Persistent Threat (APT) groups, to the relentless and destructive cyberattacks against Ukrainian critical infrastructure that began to be launched by Russia shortly before the military assault, the conflict will be closely analysed from a cyber perspective in three different phases: the initial phase, from 2013 to 2015, the intermediate phase, from 2016 to 2020, and the current phase, from 2021 to the events up to May 2022. For each phase, the following criteria will be tested to assess whether the detected cyberattacks constitute 'acts of war'. In order to be classified as an 'act of war', a cyberattack must be destructive, political, and instrumental in nature and target critical infrastructure.

The reasons for deep diving into a single, specific case study are manifold. First and foremost, it has not yet been studied and researched. The advantage of exploring a still largely unexplored topic - from the Russian military invasion of Ukraine onwards - is twofold: firstly, to provide insights from which to draw for future research and, secondly, to be able to contribute to the existing literature in a completely original way. Furthermore, besides being fought in cyberspace, this conflict has been evolving over time. Indeed, cyberspace is a fluid dimension in which actors constantly refine their techniques thanks to incessant technological development. This favours the creation of new

dynamics, as well as the use of increasingly destructive cyberattacks, which will emerge in the case study analysis. Last but not least, the involvement of non-state actors, such as Anonymous and KillNet, which publicly sided with Ukraine or Russia and declared war on each other, is something we have never seen in the cyber domain. That said, I conclude with the same question with which I deliberately opened this chapter: Is a cyber war taking place?

The subdivision of the chapters is structured as follows. Besides providing the setup for the entire dissertation, the present introduction contains the background information that allows the reader to understand the research topic and the research questions this dissertation aims to answer. The following chapter reconstructs the existing literature on the main concepts belonging to the cyber sphere, focusing mainly on those that will be referred to during the dissertation. Specifically, clarity will be shed on cyberspace and its main characteristics, the conceptual difference between cyberattacks and cyber campaigns, the use of cyber proxies by state actors, and how cyber power can be achieved and by whom. This chapter also provides the reader with an overview of the research topic and lists a number of definitions of 'cyber war' and 'cyber warfare' to highlight any conceptual differences between the two terms that are often used interchangeably. In particular, the concept of cyber war has been generating so much confusion over the years that no single universally agreed definition exists to date. Due to the ambiguity of the term, several currents of thought have emerged whose proponents argue *for* or *against* the existence of war in cyberspace. The ensuing debate, whose main arguments are introduced and explained, constitutes the theoretical framework within which this study is embedded. Based on the existing literature, the criteria used throughout the analysis to determine whether a cyberattack can be classified as an act of war are set. At this point, the main objectives of the dissertation are outlined. Firstly, to provide the existing literature with an up-to-date definition of cyber war that considers the most recent events related to the ongoing war in

Ukraine. Secondly, to contribute first-hand to the debate on the potential occurrence of wars in cyberspace.

The third chapter illustrates the research design and the methodological approach adopted during the research. Based primarily on a qualitative approach, which allows for a deeper understanding of the phenomenon, this study is conducted by drawing on both primary and secondary sources. While the former are mostly official documents, reports, newspaper articles, and social media posts, the latter are dictionaries, academic and conference papers, and academic books. Subsequently, the case study used to answer the identified research questions is introduced. In this regard, the reasons why only one case study was selected and why this case study specifically, namely the Ukraine-Russia cyber warfare, are explained. Lastly, a brief overview of the case study, highlighting what it is about, the actors involved, and the chosen time frame, is followed by an in-depth analysis of the case study in the most extensive and informative chapter of this dissertation.

Here, the conflict in Ukraine is analysed in detail, from the Euromaidan protests, in November 2013, to the declaration of cyber war between Anonymous and KillNet, in May 2022. For the purposes of the analysis, three phases of the conflict have been identified based on major military and geopolitical events in the real world. In other words, the first phase, from 2013 to 2015, and the current phase, from 2021 to the present, are those in which tensions between the two countries are most acute. Before going deeper into the case study, the historical background of the tensions between the countries since the end of the Cold War is provided so that the reader is clear about the geopolitical context and the reasons that led to such a latent and long-lasting conflict over the years. Then, official military and cyber documents of both countries are explored to give an insight into how Ukraine and Russia approach cyberspace and warfare.

The time span considered was consciously chosen to show how the conflict has evolved over the years from a cyber perspective, although particular attention is

dedicated to the last part of the conflict, more precisely since the Russian military invasion of Ukraine in February 2022. In conducting the analysis, not only cyber events but also real-world political and military events in the context of the Ukrainian crisis are taken into account. Any potential correlation is indeed crucial to understanding why certain attacks, operations, and campaigns have been planned and launched in cyberspace, especially by the Russian Federation. The considerable amount of qualitative data resulting from the analysis of this case study is then used in chapter five to elaborate on my thoughts on the subject. This fundamental chapter focuses on the interpretation of the qualitative data that emerged throughout the analysis in order to achieve the objectives set while researching cyber warfare. After carefully examining the existing definitions in chapter two, an updated definition of 'cyber war' is formulated based on the cyber events that have been observed in the context of the Ukrainian war. Then, once the main theories and arguments of the cyberwar debate have been discussed and the criteria on cyberattacks observed during the three phases have been applied, the existence of wars in cyberspace is demonstrated. The final chapter draws conclusions on what emerged in the previous chapter and aims to give some advice for future research.

2. Literature Review and Theoretical Framework

This chapter reviews the literature on the main concepts belonging to the cyber sphere and identifies the theoretical framework within which the main arguments on the potential existence of cyber war will be explained in detail below. Because the notion of 'cyber war' still generates confusion, this dissertation aims to provide the existing literature with an updated definition based on the latest events concerning the ongoing conflict between Ukraine and Russia in cyberspace by using drivers such as *actions*, *actors*, *effects*, *targets*, *aims,* and *context*. The conceptual ambiguity of cyber war is such that a debate on the existence of cyber war has ensued. In this regard, this dissertation intends to contribute to the existing debate by analysing the events observed in

cyberspace since the beginning of the Ukrainian conflict by applying the following criteria: a) cyberattacks are destructive in nature; b) cyberattacks target critical infrastructure; c) cyberattacks are instrumental and political in nature. If all the criteria are fulfilled, then cyberattacks constitute acts of war.

2.1. The Information Revolution

The Information Revolution, dating back to the 1990s, refers to the information explosion triggered by an extraordinary revolution in computer technology (Robertson, 1990: 235). Like the Industrial Revolution, the Information Revolution has caused major changes not only in the global economy, greatly affecting development and productivity, but also in society. Unlike the Industrial Revolution, however, the transformations have occurred more quickly (Mathews, 2000: 63). Thanks to the development of the Information and Communication Technologies (ICT), which encompass technologies concerning integrated communication systems, such as computers and related software, people around the world started to create and exchange a huge amount of information (Moshood, 2020).

Besides being linked to technological development, the Information Revolution is extremely tied to the birth of the Internet. The Internet, a global network of computer networks facilitating communication worldwide, emerged in the 1970s and started to be widely used by the population in the 1990s (Dennis and Kahn, 2022). Since then, the number of internet users has considerably increased throughout the years. In 2021, *Statista* published a detailed graph showing the number of internet users worldwide year by year (ITU, 2021). From 2005, when people with access to the Internet were estimated to be approximately 1 billion, there has been an increment of about 380%. Last year, in fact, the number of users rose to 4.9 billion, which corresponds to almost two-thirds of the world's population (Statista Research Department, 2022), and is foreseen to be rising to 5.3 billion by 2023 (Cisco Systems, 2022). Having access to the Internet means being part of a virtual environment in which all

users can interact with each other, easily access any sort of information, and, consequently, collect, store and exchange that information. As a matter of fact, these numbers indicate how increasingly interconnected the world has become.

2.2. The Emergence of the Fifth Domain

Besides being revolutionary in the sense of enabling real-time connections amongst people and the exchange of huge amounts of information, the advent of the Internet marked the emergence of a new dimension, the so-called "cyberspace". The term 'cyberspace' first appeared in a short story written by William Gibson in 1982 and subsequently in his science fiction novel, *Neuromancer*, published in 1984 (Brussell, 2013). The book is set on a planet inhabited by artificially intelligent beings where cyberspace is described by the author as the creation of a computer network (Gibson, 1984). As time went by, several notable institutions and organisations sought to define the new digital domain properly. However, there still seems to be no universally agreed definition of cyberspace.

To date, the most widely adopted definition was formulated by the U.S. Department of Defence, according to which cyberspace is "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JP 1-02, 2010: 55). In other words, cyberspace is a *global information-based domain* consisting of *interconnected networks*. In this dissertation, cyberspace is also viewed as an *operational space*, not only where information can be created, modified, stored, exchanged, and, at worst, exploited or manipulated (Kuehl, 2009), but also where cyber operations are conducted alongside 'kinetic' military operations in the physical domains, namely land, sea, space, and air (Fanelli, 2016).

2.3. Main Features of Cyberspace

Undoubtedly, cyberspace has become one of the most important features of our world. First considered a matter of "low politics", it is now a matter of "high politics" in the same way as violence, conflicts, and political tensions. As with any other aspect of high politics, cyberspace represents a source of vulnerability, as well as a threat to national security. Given its ubiquity and global reach, the new domain is redefining influence and power dynamics by creating new opportunities that different actors are willing to seize in the cyber arena. Because there are different types of actors and goals to be achieved, the mechanisms through which both state actors and non-state actors pursue their goals also vary, and cyber threats increase accordingly (Choucri and Clark, 2018).

Choucri (2012) identifies seven general features of cyberspace: *temporality*, *virtuality*, *permeation*, *fluidity*, *participation*, *attribution*, and *accountability*. When talking about temporality, the author means the possibility of instant interaction between human beings. In this sense, the virtual environment enables real-time connections, contrary to all other physical domains. As for virtuality and permeation, reference is made to the ability of cyberspace to transcend geographical constraints and, therefore, easily penetrate boundaries and jurisdiction. Fluidity encourages constant changes, which means that the 'playing field' is promptly created and destroyed by the players within it. Participation refers to the increase of activism and political expression. Because the barriers to entering the virtual domain are relatively low - people only need a computer and a good connection to connect to the network - the number of internet users is particularly high. Furthermore, given the structure of cyberspace and the elements of which it is composed, users can freely express their own opinions and ideas. Last but not least, most of the time, actors act without their identities being revealed. In this way, they are hardly traced back to the activities they carry out and, therefore, held accountable for those activities. Together, these elements seem to be at odds with the vertical power

structures and the principle of state sovereignty inherent in the international system as we know it (Choucri, 2012; Choucri, 2013; Choucri and Clark, 2018).

Specifically, anonymity has often been mentioned as one of the most potentially menacing characteristics of cyberspace (Libicki, 2009; Clark and Landau, 2011). The difficulty of matching an offender to a cyber offence not only undermines the credibility of a state, as it may be seen as unable to protect its infrastructures and citizens, but also constitutes a significant advantage for those operating with malicious intentions (Reveron, 2012). This encourages more would-be threat actors to orchestrate and conduct cyberattacks, as they are unlikely to be detected and targeted, ultimately making it more challenging for the victim to retaliate (Libicki, 2009). In theory, coercion would be indeed possible when the attack is attributed to a specific threat actor, who is often not identified. In practice, only the suspicion that the attack comes from a certain threat actor often leads the victim to counterattack.

2.4. Actors and Activities in Cyberspace

Actors in cyberspace are many and of different types. Since the Peace of Westphalia (1648), which marked the emergence of the *modern state system* based on the inviolable principle of *state sovereignty*, states have monopolised power (The Editors of Encyclopaedia Britannica, 2019). Over time, various non-state actors have appeared on the international scene, potentially undermining the traditional vertical structures of power and influence (Choucri and Clark, 2018: 10). For its part, cyberspace can only exacerbate this situation. Being easily accessible and apparently borderless and lawless, the virtual domain encourages the emergence of new actors and extends power to all players within the cyber arena (Reveron, 2012; Czosseck, 2013). As a result, no one actually holds an effective monopoly on cyber power.

Due to the increasing number of actors holding cyber power, new asymmetries, new opportunities, and new dynamics are created. On the one hand, the fact that there are more actors implies that there are more entities with different objectives and mechanisms through which to achieve them. Consequently, conflicts between actors are likely to rise. On the other hand, the increasing interactions among different actors are subverting the balance of power to such an extent that potentially weaker actors are able to influence and threaten stronger ones (Choucri and Clark, 2018: 14). Taking everything into account, we can conclude that both state and non-state actors play a key role in the cyber arena.

But what specifically is *power* in cyberspace? Broadly speaking, it corresponds to the ability to influence others in doing what you want them to do (Cambridge Dictionary, 2019). In other words, the more one is able to influence others to do what they would not otherwise do, and vice versa, the more power one gains. In the attempt to adapt this concept to cyberspace, Czosseck (2013) identifies *cyber power* as "the ability to act and influence through, and by means of, cyberspace" (Czosseck, 2013: 1). In this regard, Kuehl (2009) provides a more detailed definition, seeking to apply one of the core concepts of military operations to a non-physical domain. This led to the definition of cyber power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" (Kuehl, 2009: 38). The meaning of the latter definition will come in handy when the focus of the review shifts to activities in cyberspace, especially with regard to cyber offensive and defensive operations.

Klimburg (2011) identifies three different dimensions that help measure the ability of states to exercise power in cyberspace, namely *integrated government capability*, *integrated system capability*, and *integrated national capability*. Based on this differentiation, Czosseck (2013) observes that each state addressed each dimension in its own way and achieved a certain degree of

success depending on the approach used. On the one hand, in most cases, states proved a good ability to coordinate within their governmental structures. On the other hand, they struggled to create a system-wide policy coherence through international alliances. As for the integrated national capability, which refers to the ability of a state to coordinate the activities of non-state actors both within its borders and structures, the difference in the approach adopted by each state is particularly evident (Czosseck, 2013: 2). In this regard, Western states gave relatively little importance to developing their integrated national capabilities in order to increase their power in cyberspace. On the contrary, states such as Russia, China, North Korea, and Iran invested in the so-called "proxies" to conduct malicious activity, namely non-state actors who have proven to be highly capable players in cyberspace (Klimburg, 2011).

Cyber proxies are usually hacker and organised crime groups that are used by states to obtain and project power (Collier, 2017). In fact, they either conduct offensive cyber operations on a state's behalf or help a state to carry them out (Maurer, 2018). In this regard, proxies may be involved in one or more steps of the 'cyber kill chain', namely *planning and preparation*, *cyber intrusion*, *persistent access and management*, and *execution of payload*, that corresponds to the final phase in which the desired effect of the cyber operation is achieved (Lockheed, 2015). Moreover, proxies occupy different levels within the cyber threat hierarchy drawn up by the US Defense Science Board based on how sophisticated their attack methods are. Those who conduct offensive cyber operations are ranged from Tier I, which involves the use of known exploits and methods, to Tier IV, which entails the use of zero-day vulnerabilities and malware. From Tier V upwards, proxies usually support states such as the United States, Russia, and China (Defense Science Board Washington DC, 2013). When asked about the effectiveness of their actions in cyberspace, many cyber experts agree that proxies may be more powerful but not necessarily more dangerous than states. That said, what are the main actors operating in cyberspace?

2.4.1. Hackers, Hacktivists, Cybercriminals, and Nation-States

Although the types of actors operating in cyberspace are more than those listed below, four categories have been identified consistently with the topic under analysis: hackers, hacktivists, cybercriminals, and nation-states. Firstly, hackers are "younger individuals, taking an interest in hacking into information technology (IT) services, primarily out of curiosity and the thrill of the challenge" (Ziolkowski, 2013: 4). In other words, they usually hack computer systems bypassing security mechanisms or exploiting vulnerabilities. When acting with good intentions, hackers are called 'white hats'. Conversely, when acting with bad intentions, they are referred to as 'black hats' (Ziolkowski, 2013).

Secondly, hacktivists are "individuals or groups of individuals who conduct cyberattacks primarily for political rather than monetary reasons" (Denning, 2001: 243). They usually act by denying access to the IT service, overloading the system, so it does not work properly, or defacing the web with images or messages of an offensive or political nature. Indeed, the ultimate ideological purpose is to achieve the desired changes (Ziolkowski, 2013).

Thirdly, cybercriminals are groups of hackers, programmers, and other technology bandits who combine their skills and resources to commit major crimes. They engage in cybercrime, which is "criminal activity that targets or uses a computer, computer network or networked device" for personal reasons, namely, to obtain money and power (Kaspersky, 2019).

Finally, nation states tend to involve national intelligence services that in turn use cyber tools for espionage purposes. They may engage in cyber warfare activities with the aim of undermining the national security of other nations, in acts of sabotage used to exploit vulnerabilities, and in cyber espionage operations**,** which correspond to "the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage"

(Weissbrodt, 2013: 370-371). Nation states act mainly for geopolitical purposes, by seeking to compromise critical infrastructures and block access to systems of national importance.

2.5. Cyber Campaigns, Cyber Operations, and Cyberattacks

Before moving on to the subject matter of this dissertation, it is worth dwelling on some key cyber-related concepts that can generate confusion and, therefore, need to be brought into focus and clarified as much as possible. This step is indeed crucial for two reasons. First, it will provide the reader with an overview of activities in cyberspace. Second, it will serve as a guide throughout the analysis section, in which reference will be often drawn to such concepts. Thus, the reader is being given the necessary tools to fully understand the topic of research in many of its facets.

As Richard Harknett and Max Smeets (2020) point out, many cyber-related concepts are often mixed up and, as a result, wrongly used. More specifically, terms such as *cyber campaign* and *cyber operation* are frequently treated as if they were synonymous, but they are not. Therefore, these two concepts should be carefully distinguished in order to dispel any doubts. For the purposes of this study, reference will be made to the definitions of 'cyber campaign' and 'cyber operation' provided by Richard Harknett and Max Smeets. On the one hand, a cyber operation is "a series of coordinated actions directed towards a computer or network in order to achieve a certain operational objective" (Harknett and Smeets, 2020: 541). On the other hand, a cyber campaign is "a series of coordinated cyber operations, which take place over time, to achieve a cumulative outcome leading to strategic advantage" (Harknett and Smeets, 2020: 541). Thus, any cyber campaign conducted in cyberspace is composed of multiple cyber operations that ultimately aim to secure a strategic advantage for the actors orchestrating the campaign.

With regard to the term *cyberattack*, it has been conceptualised in the *Tallin Manual on the International Law Applicable to Cyber Warfare*, written from 2009 and 2012 by an international group of experts and released in 2013. *Rule 30* of this academic study defines cyberattack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2013: 106). What emerges from this definition is that cyberattacks are regarded as cyber operations, and vice versa. Although the definition provided by the Tallin Manual is more specific in terms of effects that a cyberattack could entail, these terms will be used interchangeably throughout this study. Like cyberattacks, in fact, operations in cyberspace may be offensive or defensive in nature, depending on the ultimate goal.

In this regard, whilst offensive operations aim to control information resources, thus increasing one's power in cyberspace and affirming it on the adversary, defensive operations are intended to maintain control of information resources, trying to defeat the opponent's attempts to gain power. Cyber power, in fact, belongs to those who control information in terms of its *confidentiality*, *integrity,* and *availability*. These three principles are referred to as the “CIA Triad” (Skytland, 2019) and are defined as follows: confidentiality “requires that information is disclosed only to those who are authorized”, integrity “requires that information can only be modified by those authorized, and only in the ways intended”, and availability “requires that the information is accessible when needed” (Fanelli, 2016: 55).

Accordingly, the offensive, which aims to find a flaw in an IT system to facilitate attacks by the offender, is designed to compromise the confidentiality, integrity, and availability of information. Conversely, the defence “seeks to preserve control by eliminating cooperation with attackers and reducing confidentiality for their capabilities and activities” (Fanelli, 2016: 59) Hence, in order to preserve control of information, the level of confidence, integrity and

availability must be maximised. Therefore, while offensive measures have a transitory effect and a low degree of persistence since, once implemented, they leave the defender with the possibility of restoring and reinforcing the system in order to defend themselves, defensive measures must be based on static and active security measures to be effective (Fanelli, 2016). In particular, active defence leads the adversary to spend more time and resources to evade detection, overcome the defence and achieve its objectives. That said, active defence is crucial to enable defenders to plan and implement effective countermeasures. In a nutshell, creating a synergy between offensive and defensive measures would be ideal for asserting and maintaining control over information resources, which is equivalent to controlling their confidentiality, integrity, and availability.

2.6. Defining 'Cyber War' and 'Cyber Warfare'

Now that the existing literature on the main cyber concepts has been reviewed, the following paragraphs will be dedicated to the topic of this dissertation and the theoretical framework in which the research project was carried out. Since the beginning, cyber warfare has been a widely contested topic that has lately received great attention from many cyber experts, researchers, and scholars worldwide. Given the growing importance of the phenomenon in international relations and strategic studies, much literature has been written on the subject (Green, 2016). However, as is often the case, there is no universal agreement on a standard definition of 'cyber warfare', and so on 'cyber war'. Moreover, although the most used term in the literature is 'cyber warfare' (Green, 2016), the term 'cyber war' often appears in academic papers, journal articles, and newspaper articles as if to replace it. In other words, they happen to be used as if they were easily interchangeable synonyms, but is this really the case? The question still seems to be left open.

Cyber warfare "is a more open-ended term, more useful in exploring an environment that is not only virtual but also largely uncharted" (Cornish e*t al*.,

2010: 2). This would explain why most academics write on the subject using 'cyber warfare' instead of 'cyber war'. Whether it is more appropriate to use one or the other, it is worth noting that the most authoritative international organisations and institutions have been fairly cautious about the explicit use of these terms. For instance, the United Nations (UN) seems much more inclined to refer to activities in cyberspace aimed at damaging other nation-states simply as cyberattacks. In the 2021 Edition of *Glossary of Terms and Definitions*, NATO officially adopts notions such as 'cyberattack', 'cyber operation', and 'cyber defence' (Nato Standardization Office, 2021). The same can be said for the U.S. Department of Defense and the U.S. National Institute of Standards and Technology. As a matter of fact, there has been a clear intention to address these issues without necessarily confining such a complex phenomenon to a specific term.

Considering the recent events surrounding the Ukrainian-Russian war, however, we should ask ourselves whether speaking of cyber war is still too rash or not. Indeed, what is currently happening in cyberspace is something we have never seen before. This might lead us not only to deem the use of the term 'cyber war' more appropriate under the circumstances, but also to formulate a definition that takes into account the type of actors involved and the dynamics triggered by the conflict. In this regard, this dissertation aims to answer the first research question that I identified during the research, namely, *what is cyber war?*. To answer this question, a new definition of 'cyber war' will be formulated. A careful review of the best-known definitions offered by the research community that can be found below is the first logical step toward achieving the desired goal. In doing so, the definitions of both cyber warfare-related concepts will be considered in order to better define the concept under investigation. Secondly, key variables that often appear in definitions, such as *actions*, *actors*, *effects*, *aims,* and *targets* will be taken into account during the formulation process. To these variables I will add *context*, which I believe is of crucial importance. Last but not least, cyber events arising from the ongoing war between Ukraine and

Russia will serve to bring this definition up to date. Given the constant advancement of technology, the dynamics within cyberspace are constantly evolving, and the threats that emerge from it and can have real-world effects are continuously increasing. This makes it necessary to formulate a new definition that takes into account the latest cyber events related to the war in Ukraine.

The first scholars who wrote on cyber war were John Arquilla and David Ronfeldt. In their 1993 report *"Cyberwar is Coming!,"* they introduced to the public the concept of 'cyber war'. According to the authors, cyber war "refers to conducting, and preparing to conduct, military operations according to information-related principles" (Arquilla and Ronfeldt, 1993: 146). The main objective of carrying out such operations, they say, is to disrupt - *if not destroy* - the information and communications systems of an opponent in order to exert some form of control over them eventually. Strategically speaking, knowing the adversaries more than they know themselves constitutes a great advantage and could tip the balance of information and knowledge in favour of the attacker at the expense of the victim. In the early 2000s, a cyber security expert from U.S. President Bush's entourage described cyber war as "actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010: 292). Although they are very similar to each other, the definition given by Richard Clarke is more specific on the type of actor conducting the attack, namely nation-states.

Based on the latter definition, Billo (2004) and Taddeo (2012) also provided the research community with definitions of cyber warfare focused primarily on nation states. In 2004, Billo defined cyber warfare as "units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means" (Billo, 2004: 4). When looking at this statement, it is not clear what is meant by 'boundaries', since cyberspace apparently has no borders within it (Robinson *et al.*, 2014: 73). Moreover, no reference is made to the objectives of 'offensive and defensive

operations', which makes it hard to classify a cyberattack properly. With regards to 'units', it might give an idea of the variety of actors actually involved despite being a quite vague term.

After about a decade, Taddeo contributed to the literature on cyber warfare, defining it as "warfare based on certain uses of ICTs within a state-approved offensive or defensive military strategy". Such a military strategy, he continues, aims at "the immediate disruption or control of the enemy's resources, [...]". As for the targets of such operations, he states, they belong to both the physical and non-physical domains (Taddeo, 2012: 114). This is undoubtedly the most comprehensive definition to this point. It is clear *who* conducts such cyber-warfare attacks (states), *why* (immediate disruption or control), *by what means* (ICTs) and the *targets* (both physical and non-physical). Robinson, Jones and Janicke (2014) made a couple of observations on this definition, pointing out that while defining the effects on the enemy's resources as 'immediate' is not entirely appropriate, as sometimes cyberattacks have late effects, clarification of the type of target was absent in other definitions (Robinson *et al.*, 2014: 73). As a matter of fact, claiming that the targets of cyber warfare also belong to the physical domain is acknowledging the possibility of achieving kinetic effects through cyber means.

However, the closest definition to the ongoing events appears to be that of Cornish et al. (2012), who state that cyber warfare is "a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare, it is extremely difficult to direct precise and proportionate force; the target could be military, industrial, or civilian, or it could be a server room that hosts a wide variety of clients, with only one among them the intended target" (Cornish *et al*., 2010: 3). This definition is certainly vague and considers different situations and types of targets. However, it introduces a new element that had never been taken into account before, namely non-state actors as perpetrators of cyberattacks. As will emerge in the analysis section, non-state actors can indeed

play a considerable role in cyber warfare. In view of the formulation of a new definition that considers the most recent events in cyberspace, the importance of this significant element will be borne in mind.

2.7. Can Cyber War Take Place?

As already pointed out, there is still much confusion over the concepts of cyber warfare and cyber war. The inability of the research community to reach a single definition, as well as the apparent reluctance of the most authoritative international organisations to refer to certain cyberattacks as acts of war, shows how controversial the topic is. It is therefore not surprising that numerous debates have emerged over the years. One, in particular, has aroused the curiosity of many academics about the actual existence of cyber war. Two main currents of thought have emerged from this debate, the 'alarmist' and the 'sceptic' currents. On the one hand, alarmists conceive cyber war as an imminent threat (Arquilla and Ronfeldt, 1997; Arquilla, 2012; Gartzke, 2013; Stone, 2013). Broadly speaking, they argue that anyone can wage cyber war. This means that non-state actors can also engage in acts of war in cyberspace, with ultimate responsibility resting with the state that funded them. Moreover, they assert that the targets of cyber war are primarily critical state infrastructure, which, if damaged, greatly impacts the functioning of society. Critical infrastructure is, in fact, the heart of a state and includes "the vast network of highways, connecting bridges and tunnels, railways, utilities and buildings necessary to maintain normalcy in daily life. Transportation, commerce, clean water and electricity all rely on these vital systems" (The Department of Homeland Security, 2022). On the other hand, sceptics believe it is inappropriate to consider cyber war as an existential threat unless it is overused. They are reluctant to consider cyberattacks as actual acts of war. Unlike the alarmists, they claim that a cyber war can mainly be waged by state actors, as they have the necessary resources to design sophisticated attacks. Like the alarmists, they consider critical state infrastructure among the main targets of

an act of war in cyberspace, assuming this can ever occur. In general, sceptics assert that the acts of war, as conceived by alarmists, are merely acts of espionage, sabotage, or subversion, which in turn cause disruption rather than destruction (Ashraf, 2021).

This research project has been conducted within the theoretical framework of this heated debate in order to make a further contribution to the arguments that have already been put forward by scholars. After they are introduced and explained in detail, these arguments will be analysed based on the events surrounding the Ukrainian-Russian conflict. This, in a nutshell, will allow me to approach the debate by trying to offer a new point of view and potentially give a meaningful answer to the question that many have been asking for decades: *can cyber war take place?* This seemingly simple but, in fact, very complex question will accompany us throughout the analysis of data and beyond.

Moving to the core arguments of the aforementioned debate, the first academic who challenged the concept of cyber war is Dr. Thomas Rid, the leading exponent of sceptics. In his 2012 article provocatively titled *'Cyber Will Not Take Place!'*, Rid (2012) criticised the 1993 RAND report that cyber war was coming (Arquilla and Ronfeldt, 1993) and countered that "cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future." (Rid, 2012: 5). In order to support his main argument, Rid recalls the three features of war conceptualised by Prussian general Carl von Clausewitz in *'On War'*, a philosophical work on military strategy written mostly after the Napoleonic Wars and published for the first time by his wife, Marie von Clausewitz, in 1832.

Clausewitz (1832; 1980) identified three elements characterising wars occurring in the real world. Firstly, he stated that "war is an act of force to compel the enemy to do our will" (Clausewitz, 1832; 1980: 27). According to Rid (2012), defining an act of war as an act of force means that all wars must be potentially

violent to be regarded as such. Hence, when acts do not escalate into violence, they are not real acts of war (Rid, 2012: 7). Secondly, wars are instrumental, meaning that there is always a means as well as an end (Clausewitz, 1832; 1980: 29). In this regard, the *means* usually corresponds to physical violence, through which the offender forces the enemy to do what the offender wants the enemy to do. For this to happen, the enemy must be put in a position where it no longer has any defences. To succeed in this is to achieve the typical *end* of all wars (Clausewitz, 1832; 1980: 29). Lastly, wars are fought for a greater purpose, which is usually political and transcends the use of force. The larger political intention of each adversary must be conveyed to both sides of the confrontation so that the attribution of any act of violence and its related political intention is made possible (Clausewitz, 1832; 1980: 35).

By analysing the most significant and potentially violent cyberattacks in history, namely a Siberian pipeline explosion that occurred in 1982, the massive cyberattacks on Estonia in 2007, the hybrid war between Georgia and the Russian Federation in 2008, and a cyber-espionage operation against the United States in the late 1990s, Rid (2012) states that most of them have none of the above requirements to be classified as acts of war. In fact, they did not involve violence, often had no clear purpose, and could not be attributed to any adversary most of the time. Therefore, Rid (2012) concludes that cyber war is a misnomer since cyberattacks do not have any *violent*, *instrumental*, or *political* character and, consequently, cannot be defined as acts of war (Rid, 2012: 8). Rather, he asserts that all the cyberattacks conducted until such time had been aimed at *subverting*, *spying*, or *sabotaging*. The purpose of these activities is indeed to be effective, not to be violent. Moreover, adversaries may want to act politically through cyber, but are much more inclined to maintain anonymity to avoid attribution (Rid, 2012: 15). As a matter of fact, subversion, espionage, and sabotage are activities as old as war and are often combined with military operations for real-world-wars to succeed, but they do not correspond to war for the reasons just stated (Rid, 2012: 29).

Thomas Rid's arguments on cyber war were readily challenged by John Arquilla, among the leading exponents of alarmists, in a journal article published by Foreign Policy in 2012. "Cyberwar is here, and it is here to stay, despite what Thomas Rid and other skeptics think" (Arquilla, 2012), so begins the article in response to the words of the Professor of War Studies. To support his main argument, Arquilla recalls the 2008 Georgian-Russian conflict, during which a massive campaign of offensive cyberattacks on Georgia, allegedly orchestrated by a group of Kremlin-linked hackers, helped Russia weaken the adversary. By bringing offline numerous Georgian government websites and compromising communication within the country, the Russian Federation gained a considerable strategic advantage over Georgia (International cyber law: interactive toolkit contributors, 2021). Referring to this conflict, Arquilla points out that waging wars through cyber would become even more destructive over time (Arquilla, 2012). And so, it was. As a result, cyberspace began to be conceived as a war-fighting domain, and many cyber warfare-related concepts are now central to U.S. military strategy. For instance, the declassified version of the *2018 National Defense Strategy of the United States of America* emphasises the urgency of investing in cyber defence, as well as integrating cyber capabilities into military operations, to cope with growing cyber threats (Department of Defense, 2018).

Additionally, Arquilla (2012) observes that the notion of cyber war has been often coupled with the term 'strategic' over the years, indicating that cyber war is mainly used to covertly defeat the enemy by attacking their critical infrastructures without necessarily conducting conventional military operations first. This mode of virtual attack proved to be particularly effective. Just think of the damaging effects of the 2007 cyber war against Estonia. Despite being relatively small, Estonia is one of the most wired countries in the world, meaning that its people rely extensively on the Internet to carry out ordinary activities. At the time, in fact, an estimated 97% of Estonians were banking online. It is therefore not surprising that the total costs resulting from those

cyberattacks amounted to millions of euros. At this point, Arquilla expresses concerns over the fact that these activities can only scale up and, consequently, be more impactful. This is due to the increasing sophistication of cyber weapons, which make cyber offences more effective than existing defences. As it is increasingly easy to exploit vulnerabilities of communication systems, cyber warriors are likely to be encouraged to carry out such offensives. Thus, the question is not whether cyber war is real or not, but how to improve defence capabilities to tackle this growing threat (Arquilla, 2012).

Thomas Rid's remarks have indeed triggered the debate. Following Arquilla, John Stone (2013) argued that the reason why we cannot fully understand whether cyberattacks can constitute acts of war or not is that we have little understanding of what war actually is. Key concepts of strategic studies often remain poorly explored and clarified by strategic theorists. Thus, in making his contribution to the debate, Stone focuses on the terms *force* and *violence* and their link to *lethality*. In this regard, he points out that while attempting to determine the features of cyber war, Rid (2012) states that in addition to being political in motivation and instrumental in character, any act of war must be lethal in potential. In explaining this last feature, he asserts that an act of force implies violence, which in turn implies lethality (Rid, 2012). On the contrary, Stone (2013) advocates that there is no causal relationship between these elements and adds that an act of war damages not only people, but also things. To insist that violence is necessarily lethal would be to deny certain attacks - such as the Schweinfurt raids - the status of acts of war. And this would not be correct. Therefore, in his view, acts of war produce violent effects, but these do not have to be necessarily lethal in character (Stone, 2013: 106-107).

Moreover, the Senior Lecturer at King's College London recalls the definition of war by Clausewitz and observes that there is no explicit reference to the fact that acts of war must be attributable, as Thomas Rid argues instead. That said, Stone (2013) emphasises that cyberattacks could constitute acts of war even if

they are unattributable, as long as they are violent in the effects they produce. Also, claiming that there is no broader political purpose behind wars through cyber could not be entirely true. Perhaps it is simply not made known (Stone, 2013: 105). Finally, Stone emphasises how small acts of force can result in large amounts of violence when it comes to technology (Stone, 2013: 107). Therefore, he concludes that it is too rash to say that cyber war will never happen. In fact, the conditions for it to take place are there (Stone, 2013: 108).

Having examined the various arguments for and against the actual existence of cyber war, and, in particular, the characteristics that make a cyberattack an act of war, it is now possible to set up the criteria that will be tested in the course of the analysis to determine whether cyber war exists and whether, with reference to the conflict in Ukraine, it is currently taking place. First and foremost, cyberattacks are destructive in nature. Destructive attacks are defined by The Centre for Cybersecurity (2021) as cyberattacks that can result in death, physical damage, or destruction of information, data, and software to such an extent that their recovery is not possible (Centre for Cyber Security, 2021: 4). As pointed out by Stone (2013), with whom I fully agree, a cyberattack can be destructive and, therefore, constitute an act of war even when it aims to destroy things, not necessarily by causing the death of people (Stone, 2013: 106-107). That said, the first criterion is crucial when it comes to determining whether or not a cyberattack constitutes an act of war. It serves as a sort of 'threshold', an element without which an act of cyber war cannot be regarded as such. Therefore, the following criteria can only be considered if this criterion is met. Secondly, cyberattacks aim to target the critical state infrastructure of the adversary. As mentioned above, critical infrastructure constitutes the heart of a state and, therefore, if compromised or damaged, can have damaging effects on society as a whole. Thirdly, cyberattacks are instrumental and political in nature. In setting the third criterion, I agree with Rid (2012) that an attack is instrumental when it constitutes a means to an end. Therefore, a destructive cyberattack is the means by which the attacker intends to achieve their desired

end, namely, to force the adversary to bend to their will (Rid, 2012: 7). As for the political element, a cyberattack must follow a political motivation, which is what drives and places the cyberattack within the context of cyber war.

3. Research Design and Methodology

This chapter shows the methodological approach adopted in the realisation of the research project, focusing in particular on the type of material, sources, and data used to achieve the desired aim of this dissertation, namely, to fill a gap in the literature. While researching cyber warfare, I noticed that the terms 'cyber warfare' and 'cyber war' are often used interchangeably despite having different, albeit subtle, nuances. Of the two, however, academics and researchers seem to prefer the use of the term 'cyber warfare', as it is more "open-ended" and, therefore, probably better suited to express a concept that, to date, is still little explored (Cornish *et al*., 2010: 2). There is, in fact, much ambiguity surrounding the term 'cyber war', of which no universally agreed definition exists. As evidence of this, Hughes and Colarik (2017) found that there were 56 explicit and 103 implicit definitions of 'cyber war' in use in 2017 (Hughes and Colarik, 2017). Given the general confusion originating from such a concept, this dissertation aims to provide the existing literature with a new definition of 'cyber war', by using key variables such as *actions*, *actors*, *effects*, *targets*, and *aims,* to which I will add *context* since I consider it essential in order to formulate a definition that seeks to be as comprehensive as possible. Furthermore, the latest events concerning the ongoing conflict in cyberspace between Ukraine and Russia will be taken into account in order to come up with an updated definition.

Due to the definitional ambiguity of this concept, over time, several currents of thought have emerged from which a debate has ensued, as explained in detail in the previous chapter. The debate I am referring to concerns the real possibility of a cyber war occurring. While some, otherwise known as 'alarmists', argue that all the conditions are in place for a cyber war to take place, others seem to

be more sceptical in this regard and claim that cyber war is unlikely to take place (Arquilla and Ronfeldt, 1997; Gartzke, 2013; Arquilla, 2012; Rid, 2012; Stone, 2013). As this topic is still being debated today, this dissertation aims to develop a new point of view by analysing the events observed in cyberspace since the beginning of the Ukrainian conflict. To this end, the conflict will be analysed in three different phases, within which cyberattacks will be tested using the criteria established in the previous section. In particular, it will be determined whether, for each phase of the conflict, the cyberattacks are destructive in nature, whether they target critical infrastructure and whether they are instrumental and political in nature.

3.1. Qualitative Approach

For the purpose of researching cyber warfare, I adopted mainly a qualitative approach by drawing on both primary sources, such as official documents, reports, newspaper articles, and social media posts, and secondary sources, such as dictionaries, academic and conference papers, and academic books. Specifically, the use of secondary sources has been fundamental to gaining a thorough overview of the topic, as well as a deep understanding of how scholars and researchers have approached it over the years. This helped me not only to reconstruct a framework of the existing literature tailored to cyber warfare, but also to find the aforementioned gaps on which I then built the research questions that this dissertation aims to answer. During the research, I relied mainly on Google Scholar, a freely accessible web search engine that provides a comprehensive range of academic literature based on the keywords entered in the search bar, on IEEE Xplore and ScienceDirect, through which I gained more technical insights given the subject matter, as both of these platforms deliver content in science and technology, and on Taylor & Francis Online and Routledge, which offer a wide variety of open sources available online. With regard to the keywords entered in the search bar to narrow down the search field and, thus, construct the literature review, the following were the most frequently

used: ‘Cyberspace’, ‘Cyberattack’, ‘Cyber Warfare’, ‘Cyber War’, ‘Hybrid Warfare’, ‘Offensive Cyber Operation’, ‘Defensive Cyber Operations’, ‘Cyber Espionage’, ‘Hacker’, and ‘Hacktivism’.

As for the central chapter of the research project, namely the analysis, both primary and secondary sources were examined. Because this chapter deals with the facts concerning the long-lasting conflict in Ukraine, I mainly used online articles published by Western news outlets such as Al Jazeera, The Guardian, The New York Times, The Washington Post, BBC News, CNBC, and CBS News, as well as the Russian news agency TASS, to reconstruct the historical chronology of events from 2013 to the present day. Despite looking for objective historical data, a Russian media outlet was also taken into account in order to avoid potential bias in the narration of events. Furthermore, considering the topic and the main actors in the case study, I searched for any official Ukrainian and Russian cyber-related documents on the website of the United Nations Institute for Disarmament Research (UNIDIR), specifically in the ‘Cyber Policy Portal’, in which I found the cyber strategies and doctrines of the two countries that allowed me to understand their approach to cyberspace. As far as Russia is concerned, the Cybersecurity & Infrastructure Security Agency (CISA) website was very useful for finding information on the type of activities conducted by Russia in cyberspace, pro-Russian hacker groups, and Russian intelligence agencies allegedly involved in offensive cyber campaigns and operations aimed at targeting the West.

In general, various technical and strategic reports released by the world’s best-known cybersecurity technology companies such as Kaspersky, CrowdStrike, Microsoft, and McAfee were analysed to gain an in-depth understanding of certain cyberattacks, such as NotPetya in 2017, the alleged threat actors behind them, the Tactics, Techniques and Procedures (TTPs) used, and the alleged purpose of such attacks. These reporters also proved useful when I needed detailed explanations about more technical concepts, such as ‘malware’, ‘spear

phishing', 'web defacement', and so on and so forth. Again, not only Western-based firms were considered, but also Kaspersky, the multinational cybersecurity provider headquartered in Moscow, Russia, for the reasons stated above. To analyse cases of cyberattacks of my interest, I also browsed the GitHub online platform. GitHub is the largest and most advanced platform in the world, where developers and programmers, who can also be hackers, make their techniques and skills available to everyone. Within this platform, there are a number of folders named by year in which information on various cyberattacks detected is shared.

Especially with regard to the latest events since the outbreak of the current war in Ukraine, I have kept myself informed via Twitter, a microblogging and social networking service on which users post and interact with messages. Most of the content that I came across was posted by the Anonymous collective, which utilises this platform to keep its followers updated on the cyberattacks it launches, sometimes by even publishing the sensitive data and information stolen from the victims. The hacktivist group has lately used Twitter to send war-like messages to the Russian Government, as well as to the pro-Russian cybercriminal group KillNet, which in turn used the platform for the same purposes. In addition to this, I relied on this platform for government announcements and appeals, especially from the Ukrainian government.

Overall, when searching for information in the most common search engines on Ukraine, Russia, and their confrontation both in the real world and in cyberspace, the following keywords were entered in the search bar: 'Russian Military Invasion', 'Hybrid warfare', 'Hybrid War', 'Russia in Cyberspace', 'Ukraine in Cyberspace', 'Ukrainian Conflict', 'Pro-Russia Hacker Groups', 'Pro-Ukraine Hacker Groups', 'Anonymous', 'KillNet'.

3.2. Case Study: Ukraine-Russia Cyber Warfare

As I have already mentioned, one of the aims of this research project is to investigate whether there are any concrete possibilities for war in cyberspace to occur. Since this is an unresolved issue, I have included the use of a case study in the research design in order to reach a potential conclusion on the topic under debate or at least provide the literature with new insights on which to debate. Generally speaking, case studies lend themselves easily to different types of research. Indeed, they allow us to delve deeper into the subject matter being researched with respect to a single event, in this case with respect to a single conflict, and thus narrow the field of research. In other words, case studies explore every aspect of that single event, generating predominantly qualitative data (Burnham *et al*, 2008). As Bradshaw and Wallace (1991) claim, it would be advisable to compare multiple case studies in order to have more empirical evidence and, thus, a complete framework on the subject matter (Bradshaw and Wallace, 1991). Although this approach is correct in principle, it was not adopted for this research project for a certain reason. Technological advancement allows actors in cyberspace to refine their modes of attack continuously. Therefore, it would be inappropriate to compare the current war in Ukraine and the resulting dynamics in cyberspace with past cyberattacks that could potentially be classified as 'acts of war' and have already been widely studied by academics. In a nutshell, because cyberspace is a fluid domain in which dynamics, opportunities, and actors involved in such dynamics are constantly changing, it would be pointless to determine whether a cyber war is likely to occur on the basis of past empirical data. In this regard, the confrontation between Ukraine and Russia in cyberspace is purposefully analysed from its origins to show how it has evolved over time.

Now that it has been explained the reason behind the use of a single case study, it is worth dwelling on the reason why this specific case study has been chosen. The Russian full-scale military invasion of Ukraine on February 24th, 2022 triggered a series of new dynamics in cyberspace that have not yet been studied,

at least from this point of view. In the past, in fact, case studies such as the Stuxnet worm allegedly designed by the United States and Israel to hit the Iranian nuclear power plant, and the massive cyberattacks on Estonia (2007) and Georgia (2008) by the Russian Federation have been extensively studied in the context of cyber warfare. Scholars wondered whether these events in cyberspace constituted actual 'acts of war', but the question remained pending as many had conflicting views and opinions. Therefore, besides the fact that it is still little researched, this case study could provide new insights into the debate on the potential occurrence of cyber war. In going through the analysis section and the subsequent data interpretation section, the reader should keep the following question in mind: in the context of the current war in Ukraine, can we assert that there is also a cyber war underway?

I now deem it appropriate to give some information about *what* this case study is about, *who* is involved, and the *time frame* considered. As already anticipated, the main actors are Ukraine and Russia, who are engaged in a conflict that has been going on for a decade now. The events will be analysed from November 2013 to May 2022. The Ukrainian crisis is perhaps one of the most representative case studies of 'hybrid warfare'. Since the beginning of the conflict, the cyber component has been of great strategic importance for Russia in particular, whose unique approach to hybrid warfare reflects, in turn, its unique approach to defence and security. Russia sees hybrid warfare as a single form of warfare involving the use of two different sources of power that, when employed simultaneously, favour the achievement of a particular goal. Accordingly, 'ambiguous' means of warfare (i.e., cyberattacks, information warfare) must be coupled with 'non-ambiguous' means of warfare (i.e., conventional and nuclear forces). Although, in fact, the former help destabilise and disorient the enemy, especially in the early stages of the conflict, the latter are indispensable for gaining ground on the battlefield and possibly accomplishing the intended outcome of a military campaign (Covington, 2016).

4. Background Information

Because the geopolitical context is crucial for conducting this type of analysis, especially for identifying any links between events in the real world and events in cyberspace, this chapter will provide a historical overview of relations between Ukraine and Russia since the end of the Cold War, by highlighting how tensions between the two countries have escalated and why. Subsequently, some background information regarding the approach adopted by the two countries in cyberspace will be added. A special focus will also be dedicated to how Russia conceives cyber warfare. This will help the reader become familiar with the case study used and gain a deeper understanding of why certain events took place.

4.1. Ukraine and Russia: History and Geopolitics

During the Cold War, the former Union of Soviet Specialist Republics (USSR) was one of the two leading powers of the international system. Its internal disintegration began in 1989 and ended in 1991, when the USSR formally ceased to exist as a sovereign state (History Editors, 2022). Since then, the Presidents of the current Russian Federation, Boris Nikolaevič Él'cin, Dmitry Medvedev, and Vladimir Putin, have ensured that the legitimate heir to the USSR plays a key role on the international stage. Especially with Putin in power, the country has experienced considerable growth, internal stability and various foreign policy successes for years, proving to be an assertive country capable of pursuing its geopolitical interests both regionally and internationally (Ferrari, 2014; Rezvani, 2020). However, Russia's political agenda has often collided with the interests of the West, representing a significant source of tension among these two actors.

Indeed, because most of the USSR states had declared their independence near the end of the Cold War, Russian foreign policy has been oriented towards the creation of an exclusive sphere of influence on the territory of the former Soviet Union, in particular over the countries of the Southern Caucasus and the states bordering the European Union (Kraemer and Otarashvili, 2014; Center for

Strategic and International Studies, 2020). To this end, Moscow founded the *Eurasian Customs Union* (EACU) in 2010, aimed at creating a rival to the European Union and counteracting its eastward expansion (Dreyer and Popescu, 2014; Kraemer and Otarashvili, 2014). The main purpose of the project was to extend the EACU not only to strengthen economic ties amongst its members, but also to promote future political integration (Ferrari, 2014). As time went by, Russia began to exert pressure on some former USSR republics and satellite states, such as Armenia, Georgia, Moldova, and Ukraine, to join the project and abandon the idea of moving closer to the European Union (Dreyer and Popescu, 2014).

Putin's strategy of restoring the glory of the Soviet Union and protecting its historical borders from the expansion of the EU and North Atlantic Treaty Organization (NATO) has led Russia to intervene, usually by supporting separatist forces and authoritarian regimes, in the former USSR republics to hold them out of the grip of the Western powers (Ferrari, 2014, Kotkin, 2016; Rezvani, 2020). One only has to think of the long military presence in Transnistria, a portion of territory internationally recognised as part of Moldova, and of the military actions in Georgia (2008) and subsequently in Ukraine (2014), not to mention Russia's interventions beyond its near abroad (Kraemer and Otarashvili, 2014; Rezvani, 2020). As for Ukraine, among the countries at the heart of this dissertation, its relations with Russia have been particularly strained since the first election of Vladimir Putin as President of the Russian Federation in 2000.

The earliest tensions between the two nations date back to 2004 during the Ukrainian presidential elections and increased as Ukraine developed closer relationships with the European Union. This led Russia to persuade the then-Ukrainian President Yanukovych not to sign the Association Treaty with the European Union at the Vilnius summit on 28-29 November 2013. Following his decision, the political framework in Kyiv was completely overturned by pro-

Western Ukrainian political forces, and simultaneously several protests, known as the Euromaidan Protests, were organised in Ukraine's capital Kyiv (Center for Preventive Action, 2022). The power of those demonstrations was so intense that Yanukovych was ousted and forced to leave the country in February 2014. At this point, it should come as no surprise why the annexation of Crimea was so lightning fast. In Putin's eyes, Ukraine was slipping out of Moscow's orbit, making Ukraine's chances of joining the Eurasian Union practically nil. Frustrated by the idea of losing internal consensus, Putin agreed to complete the annexation of Crimea in March 2014 after submitting a referendum to the population, later defined as illegitimate by the whole international community (Ferrari, 2014).

Putin's new political agenda differs significantly from that of his first two terms in office. The will to build positive relations with the West has clearly disappeared. Today, in fact, an aggressive political line prevails, which inevitably leads to a position of perpetual confrontation with the West (Ferrari, 2014). As Fëdor Luk'janov points out, the referendum in Crimea put an end to any attempt at dialogue. Moscow no longer cares about the possible damage to its relations with the West, which risk being seriously undermined (Luk'janov, 2014: 175). To validate his position, Putin introduced a relatively new concept in connection with the Ukrainian crisis, namely 'Novorossiya', referring to a territory conquered by the Russian Empire in the XVIII century that included much of present-day Ukraine (Basora and Fisher, 2014). With the excuse of claiming a territory that historically belongs to Russia, this concept has been widely used by Moscow to justify the invasion of the Crimean Peninsula and its annexation to the Russian Federation, the military action in Donbas, and the more recent full-scale military invasion of Ukraine.

4.3. Russia in Cyberspace

Russia's conceptualisation of 'cyber' is encapsulated in its 2014 *Military Doctrine*, its 2015 *National Security Strategy,* its 2016 *Information Security*

Doctrine, its 2016 *Foreign Policy Concept*, and its 2016 *Conceptual Views on the Activity of Armed Forces in the Information Space* (Hakala and Melnychuk, 2021; UNIDIR, 2022). Unlike the West, Russia conceives of 'cyber' as something that can be mainly traced back to 'information' and employs cyber capabilities accordingly (Connell and Vogler, 2017; Hakala and Melnychuk, 2021). Not surprisingly, Russia's cyber strategy aims to achieve information superiority and emphasises the importance of controlling information and content on its network (The International Institute for Strategic Studies, 2021). As a result, 'cyberspace' becomes 'information space' or 'information sphere', perceived as a continuation of its physical borders, which are being continuously infringed by foreign intrusions. Following the same principle, 'information security' and 'information-technological confrontation' are the equivalent of 'cyber security' and 'cyber warfare', respectively (Hakala and Melnychuk, 2021).

Russia's approach to cyberspace reflects the sense of insecurity caused by the enlargement of NATO and the European Union. This security threat can only be countered by extending the areas under Russian control, thus making the enemy feel less secure. Just as in the real world, Russia perceives that it is in perpetual information confrontation with the West and, therefore, that it is constantly under attack and legitimised to counterattack (Pynnöniemi and Kari, 2016). Consequently, Russia's behaviour in cyberspace appears rather aggressive. Because it has strong offensive cyber capabilities, Russia tends to make extensive use of them with the aim of disrupting and competing with perceived enemies. In this regard, cyber operations are mainly used for espionage purposes, namely to gather strategically important information from adversaries. In addition, Russia has demonstrated the use of a wide range of techniques, including the publication of hacked sensitive data, access to communication networks, and the use of trolls and bots to disseminate disinformation (Hakala and Melnychuk, 2021).

4.3.1. How Russia Conceives Cyber Warfare

Adversaries do not behave in the same way in cyberspace. Some might calculate risks and interpret escalation differently from others. This depends on the actor's perception of cyber threats and their potential impact on its security. Over the years, Russia has behaved rather aggressively and demonstrated to possess strong cyber capabilities, as well as perseverance in conducting cyber operations (Connell and Vogler, 2017). In this regard, former Director of National Intelligence James Clapper claimed that "Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny" (Clapper, 2016: 3). As already mentioned, Russia tends to link anything cyber-related to the concept of 'informatisation'. Consequently, the Western concept of 'cyber warfare' takes on a broader meaning that is encapsulated in the Russian concept of 'information warfare' (Connell and Vogler, 2017). Information warfare (IW) is a holistic term, which includes intelligence, surveillance, and reconnaissance (ISR), psychological operations (PSYOP), electronic warfare (EW), and information operations (IO) (Jasper, 2020; Whyte *et al*., 2021) and encompasses "actions intended to protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantage, objective or victory over the adversary" (Valeriano, 2018).

4.3.2. The Role of Russia's Intelligence Agencies in Cyberspace

Over time, Russia has increasingly improved its cyber capabilities to the point of conducting sophisticated cyberattacks on a global scale, the success of which has been largely determined by the involvement of various Russian agencies and intelligence units. Russia, in fact, is known to often rely on these actors to carry out the information confrontation in cyberspace (Bowen, 2022). With the collapse of the Soviet Union, the former State Security Committee (KGB) was split into two agencies serving the Russian Federation: the Federal Security

Service (FSB) and the External Intelligence Service (SVR), which deal with internal and external matters respectively. The Main Directorate of the General Stuff (GRU), which, unlike the FSB and SVR, is under Russian military command, retained its main role of controlling the military intelligence service (The International Institute for Strategic Studies, 2021: 106). To date, these three Russian intelligence agencies are believed to possess and extensively use both intelligence and offensive cyber capabilities (The International Institute for Strategic Studies, 2021: 110).

Among the most dangerous Russian cyber threat actors we know to be linked to Russian intelligence agencies and that primarily conduct espionage and cyber warfare activities are APT28, APT29, and SandWorm (Cybersecurity and Infrastructure Security Agency, 2022). APT28, also known as *Fancy Bear*, *Sofacy, Group 74*, and *Strontium*, is a highly sophisticated cyber hacking group operating on behalf of GRU Unit 26165 (Müller, 2019). Although it had been active since 2004, its cyber activities were disclosed by cybersecurity firms from 2014 onwards (Rid, 2020). Among the numerous cyber operations attributed to this malicious actor, APT28 was identified as responsible for interference in the 2014 Ukrainian elections and the 2016 US elections (Hakala and Melnychuk, 2021). Sandworm, also known as *IRIDIUM*, *Telebots*, *Vodoo Bear*, and *Iron Viking* has also been linked to GRU, but to Unit 74455. This state-sponsored group is believed to be behind the most dangerous cyberattacks by deploying some of the most destructive malware in the world, such as *KillDisk* against Ukraine in 2016, *NotPetya* against Ukraine in 2017, and *Olympic Destroyer* aimed at targeting the PyeongChang Winter Olympics in 2018 (Hakala and Melnychuk, 2021). Finally, APT 29, also known as *Cozy Bear*, *The Dukes*, *CozyCar*, and *CozyDuke* is a Russian-affiliated hacker group whose cyber activities are suspected to be tied to the SVR (Hakala and Melnychuk, 2021).

Russia also relies on cyber proxies for various reasons. Cyber proxies can be cybercrime groups, which are typically financially motivated by the Kremlin to extort money from the victims (Cybersecurity and Infrastructure Security Agency, 2022). However, they can also be groups of hackers, who do not need much technical training, and hacktivists, who often operate for free. Overall, cyber proxies are very good at ensuring anonymity, thus providing the Kremlin with plausible deniability (Connell and Vogler, 2017).

4.4. Ukraine in Cyberspace

The Ukrainian conceptualisation of 'cyber' is encapsulated in the *2015 National Security Strategy*, the *2016 Cyber Security Strategy*, the *2017 Information Security Doctrine*, and the *2020 National Security Strategy* (UNIDIR, 2021). Overall, Ukraine's cybersecurity strategy is oriented towards strong cooperation with the West particularly on cyber defence and cybercrime and recalls several Western cyber-related concepts. For instance, unlike Russia - for which cyberspace is a continuation of the real world that knows no temporal or physical boundaries and where confrontation with adversaries is perennial - Ukraine conceives of cyberspace as a domain of hostility separate from the physical domains (Connell and Vogler, 2017; Spînu, 2020). As for the willingness to align its cybersecurity strategy with that of Western actors, Ukraine signed and ratified the Budapest Convention on Cybercrime (ETS No. 185), which then entered into force in 2006 (Spînu, 2020; Convention on Cybercrime, 2001). The primary goal of these strategy documents is to improve Ukraine's cyber resilience in cyberspace, especially with regard to critical infrastructure. This was highlighted in the 2016 Cyber Security Strategy and in the 2020 National Security Strategy, in light of the numerous cyberattacks that have targeted Ukrainian critical infrastructure in recent years (Tkachenko, 2017).

On the one hand, the 2016 Cyber Security Strategy of Ukraine aims to create the conditions for a more secure cyberspace, by increasing the cyber capabilities

of the country and enhancing the resilience of its critical and governmental infrastructure (Tkachenko, 2017). On the other hand, the 2020 National Security Strategy of Ukraine is based on three fundamental pillars, namely *cyber deterrence*, *cyber resilience,* and *interaction* with foreign partners. Furthermore, special focus has been placed on Russia, which has been identified on more than one occasion as particularly aggressive towards Ukraine (Getmanchuk, 2020; Spînu, 2020). In this regard, the new NSS underlines a growing concern over the Kremlin's deployment of hybrid warfare operations, perceived by Ukraine as a major threat to its national security (Getmanchuk, 2020). The document also addresses a purely geopolitical issue, emphasising Ukraine's urgency to join the EU and NATO (Getmanchuk, 2020). This further alignment with the West, together with other factors, may have prompted Putin's decision to invade the country militarily on February 24th, 2022.

4.4.1. Ukraine's Use of Cyber Proxies

Like Russia, Ukraine extensively relies on cyber proxies when it comes to conducting operations in cyberspace (Baezner, 2018). As already pointed out, cyber proxies provide the state with a considerable advantage, namely plausible deniability. Should a cyberattack be successful, the state would benefit from the effects of that attack. Conversely, should a cyberattack be unsuccessful, the state could distance itself from the attack and claim to have no connection with the cyber proxy (Maurer, 2015: 81). Based on their activity in cyberspace and the targets they tend to strike, some hacker groups have been identified as pro-Ukraine. These groups are known as Cyber Hunta, Cyber Hundred, Null Sector, and the Ukrainian Cyber Army (Baezner, 2018).

Cyber Hunta and Cyber Hundred are both hacktivist groups. While the former is committed to revealing Russia's involvement in the Ukrainian crisis, the latter operates mainly to protect Ukrainian networks from pro-Russia hacker groups and teach Ukrainians how to counter-attack in cyberspace (Miller, 2016). As far as Null Sector and the Ukrainian Cyber Army are concerned, they are hacker

groups and respectively target Russian websites using mainly DDoS attacks and pro-Russian separatists in Ukraine (Baezner, 2018). In particular, the Ukrainian Cyber Army attempts to trace and flag the bank accounts of pro-Russians so that they can be closed (Kerkkänen e Kuronen, 2016).

5. Data Analysis

This chapter analyses the Ukrainian conflict from November 2013 to May 2022. In particular, it focuses on the cyber confrontation between Ukraine and Russia and how this confrontation has evolved over time. Indeed, as the analysis will show, the cyber element has been a constant throughout the conflict, even in times of apparent détente between the warring parties.

Specifically, this chapter is divided into three macro chapters that correspond to three phases of the Ukrainian conflict: the initial phase, from 2013 to 2015, the intermediate phase, from 2016 to 2020, and the current phase 2021 to May 2022. For each phase, the nature of the attacks launched and, more generally, the dynamics created in cyberspace will be analysed by testing the criteria established in the second chapter. This will ultimately allow me to determine whether or not these criteria have been met and, thus, the potential existence of the cyber war.

5.1. Initial Phase of the Ukrainian Conflict

The peculiarity of the Ukrainian-Russian conflict lies in a constant confrontation in both the *real* and *cyber* worlds, especially since tensions began to escalate with Ukraine's rapprochement with the EU and NATO in late 2013 and early 2014. The initial ambition of Yanukovych to sign the Association Agreement, which would have significantly increased trade with the European Union and, thus, undermined Putin's project of a Eurasian Union, prompted the Kremlin to make a series of *promises* and *threats* to dissuade the then President of Ukraine from signing (Heritage and Golubkova, 2013; Herszenhorn, 2013; Mankoff, 2022). After Yanukovych's decision to reject the bilateral agreement with the

EU and to reach an agreement with Putin on the price of natural gas, Kyiv was overrun by the 'Revolution of Dignity', that has repeatedly been violently repressed by police forces (Diuk, 2014; Pakharenko, 2015).

Coinciding with the Euromaidan protests, the annexation of Crimea by the Russian Federation, and the Russian military intervention in Donbas, a series of Distributed Denial of Service (DDoS) attacks were launched on both sides of the conflict targeting Russian and Ukrainian websites (Baezner, 2018). Generally speaking, DDoS attacks aim to saturate the communication bandwidth of a computer system, often via botnets, to prevent legitimate users from accessing the content of that system (Rijtano, 2018). In this case, Russian hackers apparently started defacing the websites of several Ukrainian TV stations and newspapers with DDoS attacks in November 2013 (Weedon, 2015). Shortly after, the websites of the opposition of the Ukrainian government were targeted on December 2nd, 2013, followed by numerous DDoS attacks against the websites of the Ukrainian government from hacktivists supporting the opposition. The most sophisticated cyberattacks were carried out on February 18th-20th, 2014, in conjunction with a bloody shootout against protesters that resulted in the death of a hundred people, not counting those injured (Traynor, 2014; Pakharenko, 2015). On that occasion, opposition members' telephones were flooded with calls and text messages in order to prevent them from planning and coordinating defence operations in a timely manner (Pakharenko, 2015).

In the aftermath of the 'Revolution of Dignity', Russia invaded and annexed the Crimean Peninsula, triggering a further increase in cyber activity. In addition to several DDoS attacks on Ukrainian and Russian websites, Russia not only took control of the Crimean TV networks, but also managed to connect to internal Ukrainian systems and to regularly intercept conversations in order to exfiltrate valuable information for Russian intelligence (Pakharenko, 2015; Baezner, 2018). In parallel, pro-Ukraine hacker groups launched various cyberattacks on

Crimean websites during the occupation. As soon as the separatists partially took control of the Donetsk and Luhansk oblasts in the Ukrainian region of Donbas in early April 2014, where pro-Russian groups were organising massive anti-government demonstrations, cyber operations were increasingly deployed alongside kinetic ones. Russian intelligence agencies, in fact, spread propaganda to feed the pro-Russian narrative in eastern Ukraine and conducted cyber espionage operations to plan military operations against the Ukrainian army (Pakharenko, 2015).

The types of cyberattacks that have permeated the Ukrainian conflict also include malware infections. On this matter, a computer and network security company, FireEye, reported an increase in the use of malware since the beginning of the war between Ukraine and Russia. By tracking and analysing the evolution of callbacks from 2013 to 2014, FireEye identified a sort of correlation between the rise of callbacks to Ukraine and Russia and the intensification of political and military events related to the conflict (Peters, 2014). For instance, there was a significant increase in the number of Ukrainian machines infected by *Snake*, also known as *Uroburos* or *Turla*, a malware that appeared to have targeted mostly government agencies for espionage purposes (Sanger and Erlanger, 2014). According to the report published by BAE Systems, 14 files allegedly containing the espionage toolkit were submitted for analysis in early 2014 alone, compared to 8 files in the whole of 2013. What made the experts think that those cyberattacks came from Russia was the Moscow time zone in which developers used to operate and the presence of Russian words in the malicious code (BAE Systems, 2016). Overall, Snake is a cyber espionage toolkit that provides attackers with “full remote access to the compromised system” (BAE Systems, 2016: 33). Due to their ability to “hibernate" in the system, attackers can remain undetected for months, if not years. Snake, in fact, is believed to have been active since 2010.

Simultaneously, a Russian state-sponsored cyber espionage campaign dubbed *Operation Armageddon*, apparently active since mid-2013 and uncovered in 2014 by the LookingGlass Cyber Threat Intelligence Group (CTIG), allegedly targeted the Ukrainian government, law enforcement, and military officials through spear phishing emails containing compromised Word attachments (Hackett, 2015; Lewis, 2015). The CTIG noted that the earliest campaign-related cyber activities date back to Ukraine's rapprochement with Europe and gradually intensified, especially in the wake of the Russian intervention in Donbas (Lewis, 2015). It should therefore come as no surprise that the primary purpose of Operation Armageddon was to steal sensitive information in order to gain a strategic and military advantage in the kinetic warfare against Ukraine (Weedon, 2015).

The early part of the conflict saw mainly DDoS attacks aimed at causing disruptions by pro-Ukrainian and pro-Russian hacker groups, a cyber espionage operation against Ukrainian government agencies, and Operation Armageddon launched by Russian intelligence to steal sensitive information for strategic and military advantage given the continuous clashes in the Donbas region. Since no destructive cyberattack was launched, the first criterion that serves as a threshold in determining whether a cyberattack is an act of war or not is not fulfilled. Therefore, regardless of the other identified criteria, we can undoubtedly conclude that no cyber war occurred.

5.2. Intermediate Phase of the Ukrainian Conflict

Despite numerous attempts by the parties involved to agree on a ceasefire, clashes between separatist groups and the Ukrainian army in the Donbas region continue to this day (Bigg, 2022). As a result, the conflict has never stopped being fought both on the battlefield and in cyberspace. Of the multiple malware attacks detected during this hybrid war, *BlackEnergy3* and *NotPetya* deserve particular attention. On the one hand, BlackEnergy3 belongs to the malware family and corresponds to an updated version of BlackEnergy and

BlackEnergy2 (Baezner, 2018). This third version usually targets Supervisory Control and Data Acquisition (SCADA) systems and can easily disable machines thanks to a new component called KillDisk. On December 23th, 2015, BlackEnergy3 was used to conduct a series of cyber attacks on the Ukrainian electronic systems targeting three regional electricity distribution companies - Kyivoblenergo, Prykarpattyaoblenergo and Chernivtsioblenergo - and causing major power outages throughout the regions (Cybersecurity and Infrastructure Security Agency, 2021; FireEye, 2016; Global Research & Analysis Team, 2016). Besides sending spear phishing emails containing compromised Microsoft Office attachments, the attackers also flooded the call centres of the targeted energy companies with phone calls in order to prevent customers from reaching them and reporting outages (E-ISAC, 2016). Given their ability to vary their tactics and techniques depending on the environment, cyber experts assumed that a highly-skilled, well-structured, and resourceful actor was behind the attack (E-ISAC, 2016). In this regard, the U.S. Government officially attributed this malicious cyber campaign aimed at targeting Ukraine's critical infrastructure to Russian state cyber actors (CISA, 2021). More specifically, since BlackEnergy is a distinctive tool of a Russian APT group, many believe that Sandworm is the real culprit of the cyberattack (Paganini, 2016).

On the other hand, NotPetya is known to be one of the most destructive malware attacks in history. Although it looked like ransomware, as part of the code was taken from the Petya ransomware, and some of its features resembled those of the WannaCry ransomware, the NotPetya worm was not employed by attackers to obtain a ransom (Hern, 2017; Baezner, 2018). On the contrary, when in use in 2017, besides distracting the targets from other ongoing cyber operations, it managed to render data impossible to recover once encrypted. First designed to target Ukrainian critical infrastructure, the malware then spread beyond the borders of Ukraine. As of 2017, approximately 16,500 machines had been infected worldwide, causing $10 billion in economic damage by permanently encrypting machines (Palmer, 2017; Milmo, 2022). After analysing the worm

that indiscriminately disrupted several European and Russian organisations, the UK Government attributed the attack to the Russian government, specifically to Sandworm (Baezner, 2018; National Cyber Security Centre, 2018).

In the intermediate phase of the conflict, in which there were several ceasefires attempts and moments of détente, the Ukraine-Russia conflict in cyberspace did not end. The two cyberattacks examined above are the most noteworthy in the time span considered. Compared to the attacks detected in the first phase of the conflict, however, these do not seem to be linked to any particular geopolitical event. The execution of the BlackEnergy3 and NotPetya malware was allegedly launched by the same threat actor, Sandworm, which belongs to Russian military intelligence. Although both BlackEnergy3 and NotPetya were designed to target critical Ukrainian infrastructure, only NotPetya proved to be a real destructive cyberattack with severe consequences worldwide. This allows me to continue with the testing of the second criterion for NotPetya on critical state infrastructure, which is already fulfilled. As far as the third criterion is concerned, it seems to be partially met. On the one hand, NotPetya can be regarded as political in nature in the sense that it carried a clear political message warning people not to do business in Ukraine (Greenburg, 2018). On the other hand, it is unclear whether this cyberattack was a means to a certain end, since even its programmers were apparently not aware of the effects it would have globally. Therefore, because not all the criteria are fully met, NotPetya cannot be properly considered an act of war in cyberspace.

5.3. Current Phase of the Ukrainian Conflict

As already pointed out, the Ukrainian conflict never ceased once it broke out. However, although tensions had particularly escalated recently, no one expected the Russian President to conduct a large-scale military invasion of Ukraine. No one except the U.S. intelligence community, which for months has been warning the whole world of Putin's plans to attack the country, stating that “a major assault was imminent” (CNBC, 2022). Earlier this year, such predictions proved

correct, and Russia officially invaded Ukraine on February 24th, this time with the intention of putting an end once and for all to Kyiv's continued attempts to align with the West. As justification for unleashing the biggest war on the Old Continent since World War II, Putin stressed that Ukraine was posing an ever-growing security threat to Russia (Kirby, 2022). In a speech to the Russian population on the day of the invasion, the Russian President pointed out that the main purpose of the military operation was to "demilitarise and denazify Ukraine, as well as bring to trial those who perpetrated numerous bloody crimes against civilians, including against citizens of the Russian Federation" (Putin, 2022). According to Moscow's narrative, in fact, the Kyiv regime has been perpetrating genocide against the Russian-speaking population of the Donetsk and Luhansk regions for years, particularly since the first clashes between the Ukrainian army and separatists in 2014 (Al Jazeera, 2022a).

Consistently with Moscow's strategically unique approach to hybrid warfare, based on the employment of both ambiguous means of warfare, such as cyberattacks, and conventional forces, numerous Russian nation-state actors began executing operations in cyberspace a year before the military assault on Ukraine. In this regard, the Microsoft Threat Intelligence Centre (MSTIC) observed in early 2021 an increase in malicious cyber activities against organisations within or allied to Ukraine aimed at gaining permanent access to networks to collect strategic battlefield intelligence and to facilitate future destructive cyberattacks during the military conflict. When Moscow began mass deployment of its troops on the border with Ukraine in April 2021, several large-scale phishing campaigns were launched on Ukrainian military targets to gather information on Ukraine's defence and its foreign military partnerships (Bielieskov, 2021; Microsoft's Digital Security Unit, 2022). As evidence of this, DEV-0257, a Russian threat actor also known as *Ghostwriter*, attempted to get

hold of e-mail accounts by hacking into Ukrainian military networks (Microsoft's Digital Security Unit, 2022).

In mid-2021, Russian-aligned groups conducted a series of cyberattacks to gain strategic network positioning against suppliers in Ukraine's supply chain. For instance, DEV-0586, a hacker group suspected of being affiliated with the GRU, hacked the network of an IT firm that supplies systems to the country's Ministry of Defence. In addition, NOBELIUM, otherwise known as UNC2452/2652 and allegedly connected to the SVR, attempted to gain access to some IT companies that supply government customers of NATO member states, and sometimes managed to steal sensitive data from Western foreign policy organisations by exploiting privileged accounts (Microsoft's Digital Security Unit, 2022). Besides being aimed at espionage, these cyber operations allow Moscow to obtain insights on potential responses from the West to Russian offensives against Ukraine. Without considering Ukraine, the most targeted countries were the United States, the United Kingdom, Norway, Germany, and Turkey between July 2020 and June 2021 (Microsoft's Digital Security Unit, 2022).

In late 2021, Russian threat actors sought to secure permanent access to Ukraine's critical infrastructure networks to conduct destructive cyberattacks from within before and during the military conflict. Of all, the technology and energy sectors were the most targeted (Microsoft's Digital Security Unit, 2022). In particular, KitSoft, a Ukrainian IT firm developing digital services for the government and businesses, was compromised by the hacker group DEV-0586 to more easily launch destructive attacks on the customers of the company. On January 13th and 14th, 2022, when diplomatic efforts between Ukraine, Russia, the United States, the Organization for Security and Co-operation in Europe (OSCE), and NATO to de-escalate border tensions failed, two government agencies technologically supported by KitSoft were hit by several destructive cyberattacks (Al Jazeera, 2022b; Krebs and Kwon, 2022; Microsoft Threat Intelligence Center, 2022). Dozens of computers were wiped following the

installation of a destructive malware dubbed WhisperGate (aka WhisperKill) by Microsoft. According to the MSTIC, in fact, although it resembles ransomware, this malware is designed to render targeted machines unusable rather than to obtain a ransom (Microsoft Threat Intelligence Center, 2022). Simultaneously, about 70 websites of central and regional authorities were targeted by what Ukrainian officials believed to be part of the same cyber operation. Following an investigation, it was discovered that some of the systems of KitSoft had also been infected with WhisperGate, which allowed hackers to deface customer websites (Krebs and Kwon, 2022; Microsoft's Digital Security Unit, 2022; Zetter, 2022).

At that point, the Ukrainian crisis had already entered an escalation phase. On January 24th, 2022, NATO reinforced its military presence in Eastern Europe following the failure of diplomatic meetings aimed at preventing the conflict from escalating (Al Jazeera, 2022b). Two days later, U.S. President Biden responded to the request made last December by Russian President Putin not to allow former Soviet republics to join NATO and that the organisation would continue to stick to its so-called 'open-door' policy (Al Jazeera, 2021; Al Jazeera, 2022b). From the Kremlin's perspective, the U.S. and NATO did not take Russia's security demands too seriously. As a consequence, while both sides were reinforcing their military forces on the border and tensions between Ukraine and Russia were rising, in early February, a DDoS campaign was launched by the GRU against several Ukrainian banking and defence institutions (Fendorf and Miller, 2022). On February 17th, the Kremlin pointed out that if Washington continues to refuse to negotiate firm and legally binding guarantees for its security, Moscow will be forced to respond by deploying military and technical measures (TASS, 2022). A few days before Russia invaded Ukraine, Putin declared the independence of the Russian-backed separatist regions of Luhansk and Donetsk, breaking the 2015 Minsk agreements (Teslova, 2022). Subsequently, malicious activity in cyberspace against Ukraine intensified, and a new malware, dubbed FoxBlade (aka

Hermetic Wiper) by Microsoft, was detected in more than 300 systems by the MSTIC (Microsoft's Digital Security Unit, 2022). Deployed by Sandworm, this malware targeted mainly the government, technology, energy and financial sectors, and, unlike NotPetya, which was designed by the same threat actor in 2017, the effect was more limited to specific targets (Smith, 2022).

5.3.1. Russia's Military Invasion of Ukraine: Is a Cyber War Taking Shape?

On February 24th, 2022, the Russian Federation officially began its military offensive against Ukraine. Since then, military operations have been conducted in concert with computer network operations to ensure that Russia achieved its goals on the battlefield. According to Microsoft, the cyber component of this large-scale hybrid war in Ukraine is destructive as well as unstoppable. In fact, the MSTIC observed continuous intrusion attempts, especially into Ukrainian government networks and critical infrastructure, by six Advanced Persistent Threat (APT) actors and other hacker groups suspected of being affiliated with Russia. The main techniques used by these actors range from phishing campaigns to exploiting unpatched vulnerabilities and compromising IT service providers in order to conduct destructive operations, exfiltrate sensitive data, and position themselves in targeted networks for espionage purposes (Microsoft's Digital Security Unit, 2022). As outlined above, part of these cyber activities started to be carried out by Russian state-sponsored groups in the escalation phase to prepare Russia for war.

Overall, cyber and kinetic attacks appear to have been launched simultaneously on similar military targets or geographical locations. Moreover, the high intensity fighting often coincided with a high concentration of malicious activity in cyberspace. In total, around 40 destructive cyberattacks were discovered by Microsoft from 23 February to 8 April, with an average of 2.5 attacks per week. So far, these cyber operations have been primarily aimed at preventing the Ukrainian population from accessing reliable information and essential life

services, undermining the credibility of Ukrainian President Volodymyr Zelensky and his entourage, deterring the Ukrainian army from continuing to fight, and continuing to collect valuable intelligence information that provides significant strategic and tactical advantages to Russian military forces (Microsoft's Digital Security Unit, 2022).

In the early morning of the day of the Russian full-scale military assault, Ukraine was invaded on four main axes: in the North from Belarus towards Kyiv, in the North-East from the Russian western military district towards Sumy and Kharkiv, in the East on the border with Donbas towards the Russian-backed separatist regions of Luhansk and Donetsk, and in the South from the Crimean Peninsula towards Mariupol, Kherson, and Odesa. The ground incursions were also supported by the launch of a hundred missiles from land and sea. (Watson, 2022). A few days before the Russian army crossed the border, there was an increase in disruptive DDoS attacks targeting Ukrainian government websites and financial institutions, which caused connectivity issues and, at times, significant disruptions in strategically important areas for the country, such as military and nuclear bases (Doyle, 2022; Scroxton, 2022). These cyberattacks were then publicly attributed by the US and the UK governments to Russia's Main Directorate of the General Staff of the Armed Forces (GRU) (National Cyber Security Centre, 2022b; Paganini, 2022b). Around the same time, critical infrastructures in Odesa, and Sumy were most likely compromised by Russian-aligned threat actors (Microsoft's Digital Security Unit, 2022). An hour before the invasion, Russian hackers managed to hinder satellite communications in Ukraine by compromising the systems of Viasat, an American provider of high-speed broadband satellite services and secure network systems that the Ukrainian government relies on. It is suspected that the Viasat attack was intended to prevent the "Command and Control" exercise from being triggered in the first critical hours after the military assault began (Sanger and Conger,

2022). Like other cyberattacks, it went beyond Ukraine and reached other critical infrastructures across Europe. Forensic analysis of the malware used in the attack, AcidRain, led cybersecurity researchers and intelligence officials to link the denial of service (DoS) attack to the GRU and showed how vulnerable the global communications systems are (Guerrero-Saade and van Amerongen, 2022; National Cyber Security Centre, 2022a; Sanger and Conger, 2022). The hackers, in fact, did not have to hack the space satellites themselves but the devices that connect to the satellites. Not being a particularly sophisticated cyberattack, the entire US intelligence community and the Pentagon now fear that similar vulnerabilities could be exploited in the future (Sanger and Conger, 2022).

As soon as the Russian Federation declared war on Ukraine by physically invading the country and waging the first military strikes, the hacker group known as *Anonymous* published a tweet at 10:50 p.m. (CET) claiming that it was officially in cyber war against the Russian government (YourAnonOne, 2022). In the following days, the collective claimed credit for massive DDoS attacks on the websites of the Kremlin and the Russian Ministry of Defence, as well as on a Russian-backed news service called 'Russia Today'. These cyber intrusions into Russian state television channels were intended to combat disinformation by showing the Russian population the atrocities and war crimes committed by the Russian army against the Ukrainian population, as well as to broadcast Ukrainian songs and their national anthem (Milmo, 2022)

First emerged on 4chan in 2003, Anonymous is a decentralised and non-structured hacktivist movement that acts in a collective and coordinated manner in pursuit of a common goal. Over the years, the hacktivist collective has attacked several governments, institutions, and organisations that misused power, supported censorship, or fostered inequality (Huddleston Jr., 2022). For instance, in 2011, Anonymous launched the so-called 'OpTunisia' in defence of freedom of speech, with the aim of attacking Tunisian government websites and

compromising the software used by the government to spy on citizens for surveillance purposes (Coleman, 2013: 7). Therefore, its actions are mainly socially and politically motivated, usually directed at specific targets, and typically consist of data leaks and the exposure of security vulnerabilities. The geopolitical power of Anonymous lies in its ability to draw media attention and its unpredictability when it comes to taking concrete action (Coleman, 2013: 2). Given that Anonymous has repeatedly intervened in support of the causes it believes in, the declaration of war on Putin following the invasion of Ukraine should come as no surprise. In addition to the Anonymous collective, another hacker group also took sides against the Russian Federation. A few days after the Russian military assault, the Ukrainian Deputy Prime Minister issued a Twitter appeal to digital talents around the world to join the "IT Army of Ukraine" on Telegram to help Ukraine protect its critical infrastructure and, most importantly, conduct cyberattacks against Russia (Euronews and Reuters, 2022; Lyosu, 2022).

According to an interview conducted by CNBC, the group reached 311,000 members within a couple of days only (Shead, 2022). The interviewees, who are actively participating in this cyber mission, told the US news channel that a list of specific Russian targets is shared daily so that the hackers know where to focus their efforts. In an attempt to level the playing field between Russia and Ukraine, the IT Army of Ukraine carried out several cyber intrusions into Russian government websites and banks. More specifically, it was reported that the Kremlin and Duma websites, along with media websites supporting the Kremlin and spreading disinformation, were affected by some interruptions (RHC, 2022a). With regard to the most commonly used techniques by the IT Army for conducting an attack, DDoS attacks seem to be the most frequently used (Shead, 2022).

In the first weeks since the beginning of the conflict, the Ukrainian networks most targeted by Russian threat actors were mainly those of broadcasting

companies, military, government, and, more generally, critical infrastructure. Specifically, while missile strikes were fired against a TV tower in the Ukrainian capital Kyiv, threat actors suspected of being affiliated with Russia hacked a major Kyiv-based broadcasting company by launching the DesertBlade malware on the same day (Harding, 2022; Microsoft's Digital Security Unit, 2022). Considering the type of target attacked, the primary aim of these kinetic and cyber actions appears to be consistent with the Russian vision of information operations, namely, to attack the main sources of information, take control of information, and, ultimately, spread disinformation.

In order to destabilise the enemy, Russia continued to conduct psychological operations during the current conflict. As evidence of this, several public information sources and Ukrainian critical infrastructure have been compromised by threat actors aligned with the Kremlin. In this regard, while Russian troops were attempting to take control of the defunct Chornobyl nuclear power plant and the Europe's largest nuclear power plant, Zaporizhzhya, which was officially seized by the Russian military on March 4th, Russian state media claimed that Ukraine, together with the United States, was working on the development of chemical and biological weapons (Finnegan, 2022; World Nuclear Association, 2022). In the meantime, Russian threat actors sought to meddle in the networks of organisations whose data would potentially help the Kremlin support its disinformation narrative aimed at damaging Ukraine's reputation internationally (Microsoft's Digital Security Unit, 2022).

In the wake of this information warfare, the Anonymous collective addressed Russian people in mid-March, urging them not to be victims of propaganda produced by the national media, especially after Putin's decision to shut down a number of social media, including Facebook and Instagram (Castelletti, 2022). To combat censorship, the hacktivists took a series of actions. On the one hand, Squad303 designed the portal *1920.in* through which people from all over the world could send an SMS to Russian telephone numbers, thus informing the

recipients about war-related events in Ukraine (RHC, 2022b). On the other hand, GostSEC, operating on behalf of Anonymous, hacked hundreds of Russian government and military printers with the aim of repeatedly printing as many documents as possible containing the same message reminding the Russian population that they are victims of their own government (ANSA, 2022; RHC, 2022f). On March 15th, the hacker collective consisting of Anonymous, GhostSec, SHDWSec and Squad303 published online a letter in which it declared its determination to strike Russia "by any means necessary" (RHC, 2022d). Below is an extract from the letter.

In the second half of March, Russian threat actors targeted logistics support providers with the alleged aim of disrupting the supply chain to conflict hotspots. In this regard, IRIDIUM conducted a destructive cyberattack against a transport provider based in eastern Ukraine, where foreign humanitarian aid is particularly concentrated. Moreover, just when peace negotiations were being held in Turkey between representatives of Russia and Ukraine, pro-Russian hacker groups compromised Ukrainian civil support organisations (Microsoft's Digital Security Unit, 2022; Spicer and Garanich, 2022). Specifically, Ukrtelecom, the country's largest telecommunications provider, was the victim of the most severe cyberattack since the beginning of the invasion (Brewster, 2022). Between the end of March and the beginning of April, cyberattacks on energy infrastructure increased. According to Microsoft (2022), while IRIDIUM attempted to launch an attack on an electricity supplier from the networks of some companies it had broken into at the beginning of March, DEV-0586 launched a psychological operation to turn Ukrainian citizens against their government. In short, the Russian threat actor sent e-mails whose senders seemed to be residents of Mariupol, a city besieged by the Russian army. The content of these emails was aimed at discrediting the Ukrainian government, which was blamed for abandoning its citizens in the grip of the enemy (Microsoft's Digital Security Unit, 2022).

As Russian military forces continued to advance towards Kyiv, and concurrently Russian threat actors attempted to intrude into Ukrainian networks for the purposes of espionage, information control and, in some instances, data destruction, Anonymous declared that it was officially at cyber war with KillNet, a cybercriminal group believed to be acting on behalf of Russia because it has been acting in line with the Kremlin's political objectives (Cybersecurity and Infrastructure Security Agency, 2022; YourAnonOne, 2022). Shortly after the declaration of war, Anonymous published a new tweet announcing the destruction of the official Killnet website. By attacking the Russian-affiliated group, the collective hopes to break the chain of attacks by these cyber criminals. Indeed, the pro-Russian hacker group has been held responsible for conducting malicious activities in cyberspace against Ukrainian and European targets in recent months. Specifically, KillNet claimed credit for a series of Distributed Denial-of-Service (DDoS) attacks against the websites of the governments of the United States, Romania, Italy, Estonia, Poland, the Czech Republic, and other NATO members (Paganini, 2022a; RHC, 2022c).

The response of KillNet was not long in coming. On May 25th, after four days following the provocation by Anonymous, the pro-Russian hacker group published on Telegram a message announcing the recruitment of about 3,000 *кибер бойцы* (literally "cyber fighters") willing to join the group. The new legionnaires would participate in the so-called "Panopticon" cyber operation aimed at countering the "Operation Russia" launched by Anonymous against the Russian government. As in any war, in fact, the warring parties need soldiers to advance their cause (RHC, 2022e). Overall, the threat posed by KillNet is not to be underestimated. Technical analysis conducted at the end of May revealed thousands of unique IP addresses used by the group to conduct DDoS attacks worldwide, totaling thousands of compromised machines in more than 130 countries (RHC, 2022g).

In the escalation phase of the conflict, which lasts throughout 2021, operations in cyberspace by Russian threat actors were initiated about a year before the military invasion of Ukraine. These operations, mainly aimed at gathering intelligence and gaining permanent access to Ukrainian critical infrastructure networks in order to facilitate the launch of cyberattacks in view of a potential armed conflict, were not destructive in nature. The first truly destructive cyberattack was launched in January 2022, followed by the spread of the FoxBlade malware, which hit the government, energy, technology, and financial sectors a few days before the military invasion. This destructive cyberattack started a series of relentless and destructive attacks against Ukraine's critical infrastructure. Thus, the first criterion is met from January 2022 onward. Indeed, between February 23rd and April 8th, Microsoft (2022) detected about 40 destructive attacks that caused the permanent destruction of files within hundreds of Ukrainian systems. Of these, an estimated 40 percent were aimed at targeting Ukrainian critical infrastructure (Microsoft's Digital Security Unit, 2022: 3-4). At this point, it can also be concluded that the second criterion is fulfilled. As far as the third criterion is concerned, these ongoing destructive cyberattacks on Ukraine's critical infrastructure appear political and instrumental in nature. These cyberattacks are part of a broader political purpose, which is to advance the Russian political agenda in an effort to bend the adversary, Ukraine. Moreover, they constitute a means aimed at supporting kinetic operations on the battlefield to achieve the ultimate goal, which is to take over Kyiv. Because all the criteria are fulfilled, these cyberattacks can be considered acts of war.

6. Data Interpretation

This chapter aims to interpret the qualitative data that emerged from the case study analysis. Indeed, this step is crucial in order to achieve the two objectives that this research project has set itself from the outset, namely to define the concept of 'cyber war' and to establish, on the basis of the latest developments

relating to the war in Ukraine, whether cyber war exists and whether it is currently underway.

6.1.Towards a New Definition of 'Cyber War'

As has been repeatedly stated, various scholars have been trying to define cyber war for almost thirty years. Despite numerous attempts, however, there is no clear, complete, and universally accepted definition of this perennially debated concept to date. On the contrary, different and conflicting definitions have been provided in the literature. Due to the confusion generated by the ambiguity of the term, over time, scholars have been divided between those who are convinced that cyber war is an imminent threat with serious and large-scale effects and those who believe that there are not and never will be the conditions for it to occur.

As emphasised in the opening part, the first research question that this dissertation seeks to answer concerns cyber warfare in its essence. In order to formulate a new definition of cyber war, which is intended to be as comprehensive as possible, the best-known definitions listed in chapter two were carefully examined. Moreover, the events surrounding the ongoing Ukrainian-Russian hybrid warfare have inevitably and widely inspired the definition of a concept that seemed too nebulous to be defined. The reality of cyber warfare, in fact, may have acquired more meaning in the face of what the whole world is currently witnessing. That said, what is cyber war then?

Cyber war occurs when state and non-state actors conduct a range of offensive activities in cyberspace with the aim of gaining a strategic advantage over adversaries. These activities encompass espionage and information operations, as well as disruptive and destructive cyberattacks. Accordingly, critical infrastructure, military targets, and government institutions are the most affected targets.

Aware of the difficulty of defining an already complex concept, this ambitious attempt to contribute to the existing literature with an up-to-date conceptual definition is aimed at framing the phenomenon by considering some variables that, in my humble opinion, are essential to ensure a certain degree of completeness to the definition itself. However, before delving into the various elements of the above definition, a premise must be made. Looking not only at the current military conflict in Ukraine, but also at other past conflicts in which the cyber component was extensively employed to achieve certain ends, one can conclude that the use of cyber means to strike the enemy is often triggered by conflicts or tensions between states in the real world. Therefore, a preliminary analysis of the geopolitical context is fundamental when it comes to determining whether a cyber event can be classified as an act of 'cyber war'. If there is no conflict underlying the relationship between two or more state entities in the physical domain - be it openly declared wars, as in the case of the current conflict in Ukraine, or geopolitical tensions - it is much more likely to be cyber espionage. Every day, in fact, we witness breaches of computer systems with the aim of gathering intelligence. Yet cyber war is more offensive than mere espionage: it is not about breaking into computer systems and looking for intelligence; it is about breaking into the computer systems of adversaries to damage them. Consequently, analysing the context and establishing whether the threshold of mere cyber espionage has been crossed with the launch of destructive cyberattacks is crucial to assess whether we are dealing with a real case of cyber war.

In the attempt to construct a definition that was neither too broad, which would have risked generating more confusion, nor too specific, which would have inevitably excluded certain events from being categorised as acts of war in cyberspace, *actors*, *actions*, *aims*, *effects,* and *targets* were taken into account. Having these in mind, I concluded that cyber war consists of a series of offensive activities aimed at gaining a strategic advantage over opponents by controlling their information resources. Here, the non-coincidental use of the terms

‘offensive’, ‘strategic advantage’, and ‘adversaries’ alludes to the real-world conflictual dimension I mentioned above. Moreover, these activities are carried out by both state and non-state actors. In most definitions currently in use, the concept of cyber war is almost always linked to the concept of ‘state vs. state’. Yet, it is crucial to stress that non-state actors are also involved, as we have largely seen in the ongoing Ukraine-Russia conflict. That nation-states increasingly rely on cyber proxies to conduct cyber operations on their behalf is now a given. Despite providing great support to the governments they act for, non-state actors cannot act alone to be effective. Indeed, states not only have more resources at their disposal to perform highly sophisticated attacks, for instance, using zero-day exploits costing from USD 30,000 upwards, but they also know how critical state infrastructure is generally protected and through which protocols and procedures (Rosenfield, 2009; Ablon and Bogart, 2017). Therefore, state and non-state actors can be both perpetrators of offensive activities when referring to cyber war.

Activities conducted during a cyber war include espionage and information operations. While the former aim to gather intelligence in order to gain a strategic and, possibly, military advantage over opponents in the event of a real-world conflict, the latter are intended to control and manipulate information in order to disorient opponents and damage their reputation both within and outside their borders. In this respect, Russia has demonstrated to be particularly adept at planning and launching these types of cyber operations against its adversaries. In the case of Ukraine, Russian threat actors positioned themselves in the enemy’s computer systems a year before the military invasion of February 24th, 2022, and then conducted destructive cyberattacks once the conflict broke out. Speaking of ‘destructive’, this is exactly the effect that the actors waging war in cyberspace want to achieve. Together, in fact, disruptive and destructive cyberattacks are used to cause significant harm to the enemy. In particular, destructive cyberattacks can result in physical damage to industrial control

systems, which can ultimately cause physical injury, and the destruction of data, software, and information (Centre for Cyber Security, 2021).

Taking everything into account, it should come as no surprise that critical infrastructure, as well as the military and governmental institutions have been identified as the targets primarily affected during a cyber war. Indeed, they represent the heart of the state. On the one hand, critical state infrastructure includes vital physical and cyber assets that, if damaged or destroyed, could negatively impact national security, public health and safety, and the well-being of citizens (Council Directive 2008/114/EC, 2008). On the other hand, military networks, if hacked, provide the attacker with sensitive information about military strategies and capabilities of a state. Furthermore, military and intelligence institutions rely heavily on digital solutions and are connected via wired networks that, if violated, risk giving the attacker power over the control of the military system and, therefore, of a country's military decisions. Apart from this last type of cyber intrusion, which is rarely the case, we have so far witnessed cyber espionage and information operations, as well as disruptive and destructive cyberattacks in the current Ukrainian-Russian conflict.

6.2. Cyber War Exists and Is Currently Underway

Having defined what is meant by 'cyber war' through the formulation of an updated definition based on the events surrounding the war in Ukraine, this dissertation also aims to provide a new perspective on a heated debate that has been dividing the most distinguished experts in this field for years: *does cyber war exist?* Two main currents of thought have emerged on the actual existence of cyber war, the 'alarmists' and the 'sceptics'. Whilst the former claim that cyber war not only exists but is also likely to permeate, if not replace, the conflicts and wars of the 21st century, the latter assert that cyber war should not be considered 'war' in the narrowest sense of the term and is unlikely to take place (Ashraf, 2021).

As emerged in the chapter concerning the review of the literature in the cyber field and the theoretical framework within which this study has been carried out, John Arquilla and John Stone appear to be among the main proponents of the existence of cyber war, as opposed to Thomas Rid. Relying on Clausewitz's classic definition of 'war', Rid argues that a cyberattack must, through the use of force, be aimed at bending the enemy to the attacker's will, have a distinct political purpose, and result in lethal effects in order to be classified as an 'act of war'. As none of the cyberattacks we have witnessed to date meet these characteristics, it is very unlikely that a war in cyberspace will occur (Rid, 2012).

That cyberspace is considered a domain of war and, therefore, mentioned in the military strategies of several countries in the world is now a given. However, while it is certainly a good starting point, it might be too rash to use a concept suited to the physical domains to refer to the virtual domain, which inevitably has somewhat different characteristics and internal dynamics. In cyberspace, in fact, power is measured by the control of information and can be gained by state and non-state actors, as well as individuals. In this regard, I personally agree with the point made by Stone (2012) about the link between force, violence, and lethality identified by Rid, according to which force generates violence, which in turn generates lethality. In Stone's view, there is not necessarily a causal relationship between these three elements. Moreover, claiming that a cyberattack is an 'act of war' *only* if it is lethal in potency, that is, only if it is capable of harming people, sometimes even causing their death, is not entirely correct (Stone, 2013). Cyberattacks may not be lethal if we consider the term 'lethal' in its strict sense, but they can be destructive when they target things. As already mentioned, destructive cyberattacks are designed to damage and destroy essential physical and ICT assets of a nation, with the risk of also impacting human beings in some form. It is no coincidence that they were included in the definition formulated above.

Bearing these arguments in mind, the aim is now to determine whether there are, in fact, conditions for a war in cyberspace to occur on the basis of the analysed case study with respect to the three identified criteria that were applied in each phase of the conflict. As pointed out when describing the methodology used to carry out the research project, the time span in which the most relevant events of the war in Ukraine are examined is from November 2013 to the present, specifically up to the events of May 2022. Besides providing an overview of the conflict and its development from a cyber perspective over time, there is a specific reason why less recent events were also subject to analysis and will soon become clear.

In the early stages of this decade-long conflict, namely between 2013 and 2015, the most frequently detected activities in cyberspace include DDoS attacks, as well as cyber espionage and information operations against Ukraine. After the Euromaidan protests, an increase in DDoS attacks against Ukrainian government websites and telecommunications infrastructure was observed, with the aim of disrupting communications and the flow of information within the country. In addition, a series of information operations 'à la Russe' were launched to manipulate information and spread misinformation about what was happening in the Crimea and Donbas regions. These operations were accompanied by relentless cyber espionage campaigns orchestrated by Russian threat actors to steal sensitive information and, thus, gain a strategic advantage over Ukraine. Two of the best-known examples are the Turla malware which targeted dozens of Ukrainian government agencies, and Operation Armageddon, which allegedly hacked the Ukrainian government, law enforcement, and military officials through spear phishing e-mails that contained compromised Word attachments. Both attacks were attributed to the Kremlin-linked group known as Sandworm.

Basically, Russia waged war against Ukraine through strategic information theft and manipulation. Is this enough to conclude that a war in cyberspace was taking

place at the time? Definitely not. In describing the new definition, I emphasised that cyber espionage operations, which are intended to know the enemy and possibly anticipate their moves, are carried out every day. In the event that the threshold of mere espionage is crossed, then one can speak of cyber war if cyberattacks are destructive in nature, thus fulfilling the first criterion that was identified before carrying out the analysis. Although there were a few attempts by Russian-aligned groups to disrupt Ukrainian government websites, there is no evidence of cyberattacks aimed at destroying the computer systems of the enemy. In light of these considerations, we can conclude that the cyber activities detected up to that point do not constitute 'acts of war'. On the contrary, as Libicki (2015) and Weedon (2015) pointed out, they were much less impactful than the cyberattacks against Estonia in 2007 and Georgia in 2008, which were closer to the concept of 'cyber war' (Libicki 2015; Weedon, 2015).

Things began to change in 2017, when the NotPetya malware, which was created and released by Russian military hackers tied to the GRU, infected countless machines, first in Ukraine and then worldwide (Greenburg, 2018; Nakashima, 2018). Several critical infrastructures, such as hospitals in Pennsylvania, and multinational corporations, such as the pharmaceutical company Merck, were paralysed by the virulent worm, which is estimated to have caused $10 billion in economic damage (Greenburg, 2018). The effects resulting from the spread of NotPetya were so devastating that most agreed that it was an act of cyber war, whatever definition one wanted to consider. The then-Homeland Security Advisor of former US President Donald Trump, Tom Bossert, stated that "while there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory" (Greenburg, 2018), referring to a tactical victory for Russia in the undeclared war with Ukraine that had begun more than four years earlier and had already claimed thousands of Ukrainian lives. Craig Williams, director of Cisco's global Talos Outreach team, also commented on the phenomenon, saying that it was the fastest-spreading malware he had ever seen until then and that it carried a clear political message:

anyone who wanted to do business in Ukraine would pay dearly for it (Greenburg, 2018; Greenberg, 2019: 183). This last aspect, coupled with the destructive nature of the attack, could partially challenge Rid's main arguments based on which an act of war in cyberspace that meets certain characteristics would have never occurred. Although it proved to be destructive and political in nature, its instrumental character is not clear, thus making it difficult to classify it as a real act of war. Despite this, it cannot be denied that NotPetya turned out to be a real cyber weapon that a nation-state, in this case, the Russian Federation, used against its enemy and that ultimately caused, perhaps even unexpectedly, from the point of view of its programmers, collateral damage all over the world.

Regarding the current phase of the conflict, which was analysed from the beginning of 2021 to May 2022, the nature of cyberattacks has clearly changed, as have the dynamics in cyberspace. According to the MSTIC (2022), Russian threat actors started to position themselves in Ukrainian networks as early as 2021. Their goal was twofold: to gather strategic intelligence and to facilitate the launch of cyberattacks in view of a foreseeable invasion. To this end, some groups of hackers belonging to Russian intelligence agencies, namely DEV-0257, DEV-0586, and NOBELIUM, broke into the networks of Ukraine and some NATO member states to acquire information on the military apparatus and defence system of the enemy, as well as on the Western response capabilities in the event of any military offensives by Russia on Ukrainian territory (Microsoft, 2022). Considering the nature of these cyber activities, none of the cyber operations launched were destructive in nature, so there was no cyber warfare going on at the time. However, in the most acute escalation phase of the conflict and during the current war, we have been witnessing a series of relentless destructive and disruptive cyberattacks targeting mainly Ukraine's critical infrastructure, government websites and financial institutions. In this regard, the MSTIC (2022) identified six Advanced Persistent Threat (APT) actors and other allegedly Kremlin-affiliated hacker groups conducting offensive operations

against Ukraine. From February 23rd to April 8th, a total of 40 destructive cyberattacks were detected and 8 malware were executed compromising dozens of machines and systems. (Microsoft, 2022). There is no doubt that such cyber operations were planned by the Russian government in pursuit of its political and military objectives and launched with the aim of harming the enemy by targeting its critical infrastructure. Therefore, while a war with conventional weapons was being fought in the physical domain, a war in cyberspace was also beginning to take shape according to the criteria used to analyse potential acts of war in cyberspace.

It should be noted that this conflict has triggered a number of new dynamics in cyberspace, namely the involvement of non-state actors and their declared alliance with Ukraine or Russia. On the one hand, as soon as the Russian military invaded Ukraine on February 24th, the Anonymous collective declared to be in cyber war against the Kremlin. After a couple of days, the so-called 'IT Army of Ukraine' attracted hackers from all over the world eager to make their computer skills available to attack Russia. Both groups mainly targeted Russian government websites by launching DoS and DDoS attacks that most often resulted in the interruption of systems and web defacement to display political messages. On the other hand, the cybercriminal group, KillNet, is believed to have acted in support of the Russian government by targeting Ukrainian and European institutions and organisations in the past few months. As a result, Anonymous has also recently declared war on KillNet.

The declaration of war in the physical domain was de facto followed by a declaration of war in the cyber domain by Anonymous, first against the Kremlin and then against its cyber proxy, KillNet, which in turn responded by launching a counteroffensive. The current war between Ukraine and Russia is thus not only being fought by conventional and non-conventional means, but also on *three* different levels in cyberspace. It is, in fact, a war between state actors (Russia versus Ukraine), between state and non-state actors (pro-Russia groups versus

Ukraine and pro-Ukraine groups versus Russia), and, finally, between non-state actors (Anonymous versus KillNet). In other words, we are witnessing something that has never happened before, which is the reason why this specific case study deserves to be analysed.

6. Conclusion

Technological evolution, combined with the birth of the Internet, has fostered the emergence of an increasingly interconnected world and, consequently, of a new domain: cyberspace. The fluidity of this digital reality is such that new opportunities are constantly being created and exploited by different types of actors at their will. As a result, new threats are constantly taking shape, from espionage to alleged war activities. In this regard, academics around the world wondered whether a cyberattack could constitute an act of war, and a debate thus ensued. Since there is still much confusion on the subject and, to date, there is no universally accepted definition of 'cyber war', the debate on whether a war can actually take place in cyberspace is still ongoing. However, as it will soon become clear, it was not a matter of *if*, but *when* a cyber war would occur. Cyber war does in fact exist and, to quote John Arquilla, is already upon us.

Among the various currents of thought that have emerged from the aforementioned debate, two deserve particular attention. On the one hand, those better known as 'alarmists' argue that cyber war is an imminent threat and is likely to permeate the conflicts of the 21st century. On the other hand, the more sceptical are reluctant to believe that the conditions are in place for war in cyberspace to occur. Of them, Thomas Rid refers to Clausewitz's 1832 definition of 'war' and claims that a cyberattack must be violent, instrumental, and political in nature in order to be classified as an 'act of war'. With respect to the violent nature of a cyberattack, which assumes the death of people as its ultimate effect, John Stone argues that an attack can also be violent when it aims to destroy things. On the basis of this argument, the first criterion used to analyse cyberattacks that have been launched during the decade-long conflict in Ukraine

was formulated. This criterion is decisive in determining whether we are dealing with a case of cyber war. Every day, in fact, nation-states carry out espionage operations in cyberspace to gain a strategic advantage over their *perceived* adversaries. From this point of view, we are all someone's perceived enemy. Yet, in war, the enemy is *pure,* and the ultimate end is to destroy them at any cost. Therefore, mere cyber espionage activities establish a kind of *threshold* beyond which one could speak of cyber war, as long as the cyberattacks are *destructive* in nature. Destructive cyberattacks are, in fact, designed and launched to cause significant harm to the adversary intentionally. By definition, they can result in physical damage to industrial control systems (ICS), which can eventually cause the destruction of data, software, and information. This criterion is followed by the two criteria identified by Rid, according to whom cyberattacks must be *instrumental* and *political* in character, and an additional criterion, which takes into account the type of target targeted, namely, critical infrastructures. These, in fact, represent the heart of a state, and any damage to them could have severe effects on society as a whole.

In analysing the ten-year conflict in Ukraine, a typical case of 'hybrid warfare' in which the cyber component has been extensively used, it emerged that no destructive cyberattack was detected in the initial phase that coincided with major real-world political and military events such as the Euromaidan Protests, the Russian annexation of Crimea, and the Russian military intervention in Donbas. On the contrary, the most frequently observed activities in cyberspace between 2013 and 2015 included DDoS attacks aimed at disrupting communications within Ukraine, cyber espionage operations launched by the Russian threat actor, Sandworm, with the aim of obtaining strategic intelligence, and information operations intended to spread disinformation about what was happening in Donbas. Because there is no evidence of any cyberattack deployed to damage the adversary, none of the cyber activities detected up to that point constitute 'acts of war'.

During the conflict, cyberattacks have decreased in frequency but not in intensity. Technological advancement allows threat actors to refine their tactics, techniques and procedures (TTPs), making cyber threats increasingly difficult to control and contain. NotPetya is a good example. This malware, designed and distributed in 2017 by Russian military hackers linked to the GRU, targeted critical Ukrainian infrastructure and then spread worldwide, affecting hospitals, multinationals and pharmaceutical companies. The effects resulting from the spread of NotPetya were so devastating that most experts in the field agreed that it was an act of cyber war, no matter what definition one wanted to consider. In fact, NotPetya proved to be a real destructive cyberattack which caused collateral damage all over the world. But is that enough to consider it a real act of war? Not really. When testing the criteria used to determine whether a cyberattack constitutes an act of war, not all of them seem to be met when applied to this malicious software. NotPetya was a cyberattack aimed at damaging Ukraine's critical infrastructure and apparently carrying a certain political message, that of not doing business in and with Ukraine. However, it is unclear whether this worm was a means to achieve the typical purpose of a war, namely, to bend the enemy, in this case, Ukraine.

This brings us to the current phase of the conflict, when, at the beginning of 2021, Russian threat actors started to infiltrate Ukrainian critical infrastructure networks with the aim of gaining a strategic position in view of a possible invasion, as well as gathering valuable information that would give Russia an advantage over the enemy. However, the first real destructive cyberattacks, WhisperGate and FoxBlade, date back to earlier this year. In particular, the FoxBlade malware, which, unlike NotPetya, managed to limit and focus its effects on a specific target, the Ukrainian critical infrastructure, initiated a series of incessant and destructive cyberattacks against Ukraine. Between February 23rd and April 8th, 8 malware deployed by at least six Russian Advanced Persistent Threat (APT) groups and other Kremlin-affiliated hacker groups were detected, amounting to a total of 40 destructive cyberattacks in less than two

months. Forty percent of them targeted the critical infrastructure of the country, with the clear aim to weaken and damage the adversary. From the attacker's point of view, there is no doubt that these cyberattacks were part of a broader political purpose, namely, to hinder Ukraine's rapprochement with the West once and for all by invading the country on a large scale, and that they were used as a means to gain a tactical advantage on the battlefield in advancing towards Kyiv. In short, many of these cyberattacks against Ukraine meet the criteria set at the beginning of the analysis. They are destructive, political, and instrumental in nature, as well as aimed at targeting Ukraine's critical infrastructure, thus constituting acts of war. Therefore, it can be concluded that, while a war with conventional weapons is being fought in the physical domain, a war with cyber weapons is also taking place in cyberspace.

The peculiarity of the current war in Ukraine lies in the fact that a series of new dynamics have been triggered in cyberspace, including the involvement of non-state actors who have openly sided with Kyiv, such as the transnational collective Anonymous, or with Moscow, such as the cybercriminal group KillNet, thus deciding not to act anonymously. Since the start of the Russian military invasion of Ukraine on February 24th, 2022, the war has not only been fought on the battlefield between the Ukrainian and Russian armies, but also on three different levels in cyberspace involving state and non-state actors. It is, in fact, a war between state actors (Russia versus Ukraine), between state and non-state actors (pro-Russian groups versus Ukraine and pro-Ukrainian groups versus Russia), and, finally, between non-state actors (Anonymous versus KillNet).

This is the first time in history that a clash of this magnitude has involved state-sponsored hacker groups (KillNet), hacker groups organised into one or more collectives (Anonymous), and individuals who make their computer skills available to support Ukraine (members of the IT Ukraine Army). To date, the cyberattacks conducted by these hacker groups have not been destructive but

rather disruptive in nature and often aimed at publishing sensitive data and sending political messages. The damage caused, therefore, is definitely limited. At this point it would beg the question: what would be the impact if these groups upped their game further, hitting strategic or nationally important infrastructure?

To conclude, based on the results of my analysis that *cyber war exists* and is *currently taking place*, I provide below an updated definition of 'cyber war', taking into account the latest cyber events and dynamics related to the war in Ukraine and, more generally, the definitions currently in use in the existing literature on cyber warfare.

Cyber war occurs when state and non-state actors conduct a range of offensive activities in cyberspace with the aim of gaining a strategic advantage over adversaries. These activities encompass espionage and information operations, as well as disruptive and destructive cyberattacks. Accordingly, critical infrastructure, military targets, and government institutions are the most affected targets.

Because the war between Ukraine and Russia is still ongoing, the question arises whether non-state actors will be able to raise their game in the near future. In addition to continuing to examine current events in cyberspace and the kind of impact cyberattacks have, or will have, during the ongoing war, a suggestion for future research could therefore be to analyse whether the new definition of cyberwar, which I formulated at the end of my analysis, will actually be applicable in future conflict scenarios and what role non-state actors will play.

7. Bibliography

1. Ablon, L. and Bogart, A. (2017). *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corporation. doi:10.7249/rr1751.

2. Al Jazeera (2021). *Russia demands Ukraine, ex-Soviet nations be barred from NATO*. [online] www.aljazeera.com. Available at: https://www.aljazeera.com/news/2021/12/17/russia-demands-ukraine-ex-soviet-nations-barred-from-nato.
3. Al Jazeera (2022a). *'Smells of genocide': How Putin justifies Russia's war in Ukraine*. [online] www.aljazeera.com. Available at: https://www.aljazeera.com/news/2022/3/9/smells-of-genocide-how-putin-justifies-russias-war-in-ukraine.
4. Al Jazeera (2022b). *Timeline: How the Ukraine-Russia crisis reached the brink of war*. [online] www.aljazeera.com. Available at: https://www.aljazeera.com/news/2022/2/13/timeline-how-the-ukraine-russia-crisis-reached-the-brink-of-war.
5. ANSA (2022). *Anonymous viola stampanti militari russe - Tlc*. [online] ANSA.it. Available at: https://www.ansa.it/sito/notizie/tecnologia/tlc/2022/03/14/ucraina-anonymous-viola-stampanti-militari-russe_fa95a0f1-d9f8-480f-b509-b154c8c64da6.html [Accessed 28 Apr. 2022].
6. Arquilla, J. (2012). *Cyberwar Is Already Upon Us: But can it be controlled?* [online] Foreign Policy. Available at: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ [Accessed 23 Apr. 2022].
7. Arquilla, J. and Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), pp.141–165. doi:10.1080/01495939308402915.
8. Arquilla, J. and Ronfeldt, D. eds., (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. RAND Corporation. doi:10.7249/mr880.
9. Ashraf, C. (2021). Defining cyberwar: towards a definitional framework. *Defense & Security Analysis*, 37(3), pp.1–21. doi:10.1080/14751798.2021.1959141.
10. BAE Systems (2016). *The Snake: Campaign Cyber Espionage Toolkit*. Surrey Research Park.

11. Baezner, M. (2018). Cyber and Information warfare in the Ukrainian conflict, Version 2, October 2018, Center for Security Studies (CSS), ETH Zürich.
12. Basora, A.A. and Fisher, A. (2014). Putin's 'Greater Novorossiya' – The Dismemberment of Ukraine?. *Foreign Policy Research Institute*. [online] Available at: https://www.fpri.org/article/2014/05/putins-greater-novorossiya-the-dismemberment-of-ukraine/ [Accessed 19 Apr. 2022].
13. Bielieskov, M. (2021). *The Russian and Ukrainian Spring 2021 War Scare*. [online] Center for Strategic and International Studies (CSIS). Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210921_Bielieskov_War_Scene.pdf?1LcoLhk8Qe3cswhqsQPNN6HJg0XvrdNa.
14. Bigg, M.M. (2022). A timeline of the tensions between Russia and Ukraine. *The New York Times*. [online] 18 Feb. Available at: https://www.nytimes.com/2022/02/18/world/europe/russia-ukraine-timeline.html [Accessed 22 Apr. 2022].
15. Billo, C. and Chang, W. (2004). *Cyber warfare an analysis of the means and motivations of selected nation states*. Dartmouth College.
16. Bowen, A.S. (2022). *Russian Cyber Units*. Congressional Research Service.
17. Bradshaw, Y. and Wallace, M. (1991). Informing Generality and Explaining Uniqueness: The Place of Case Studies in Comparative Research. *International Journal of Comparative Sociology*, 32(1-2), pp.154–171. doi:10.1177/002071529103200108.
18. Brewster, T. (2022). *'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider*. [online] Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=19bccb4e7dc2 [Accessed 4 May 2022].
19. Burnham, P., Lutz, K.G., Grant, W. G. and Layton-Henry, Z. (2008). Research Methods in Politics (2nd edition). Houndmills Palgrave Macmillan, Basingstoke.

20. Bussell, J. (2013). *Cyberspace*. [online] Encyclopedia Britannica. Available at: https://www.britannica.com/topic/cyberspace [Accessed 13 April 2022]
21. Cambridge Dictionary (2019). Power. In: *Cambridge English Dictionary*. [online] Available at: https://dictionary.cambridge.org/dictionary/english/power [Accessed 12 May 2022].
22. Castelletti, R. (2022). *Putin spegne anche i social: oscurati Instagram e Facebook*. [online] La Repubblica. Available at: https://www.repubblica.it/economia/2022/03/11/news/putin_spegne_anche_i_social_oscurati_instagram_e_facebook-341072829/ [Accessed 30 Apr. 2022].
23. Center for Preventive Action (2022). *Conflict in Ukraine*. [online] Global Conflict Tracker. Available at: https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine [Accessed 21 May 2022].
24. Center for Strategic and International Studies (2020). *Four Myths about Russian Grand Strategy*. [online] Center for Strategic and International Studies. Available at: https://www.csis.org/blogs/post-soviet-post/four-myths-about-russian-grand-strategy.
25. Centre for Cyber Security (2021). *The threat of destructive cyber attacks*. [online] Available at: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-threat-of-destructive-cyber-attacks.pdf [Accessed 19 Apr. 2022].
26. Choucri, N. (2012). Cyberpolitics in international relations. Cambridge: Mit Press, Cambridge, Massachusetts. Available at: https://www.jstor.org/stable/j.ctt5hhkrs
27. Choucri, N. (2013, October 13–15). *Co-evolution of cyberspace and international relations: New challenges for the social sciences*. World Social Science Forum (WSSF) 2013 Montreal, Canada. Version: Author's final manuscript.
28. Choucri, N. and Clark, D.D. (2018). *International relations in the cyber age : the co-evolution dilemma*. Cambridge, Ma: The Mit Press.

29. Cisco Systems. (2020). *Internet user growth worldwide from 2018 to 2023 (in billions)*. *Statista*. Statista Inc.. Accessed: July 10, 2022. https://www-statista-com.ezp.biblio.unitn.it/statistics/1190263/internet-users-worldwide/
30. Clapper, J.R. (2016). *Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*. [online] Available at: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf [Accessed 15 Apr. 2022].
31. Clark, D.D. and Landau, S. (2011). *Untangling Attribution*. [online] Harvard National Security Journal. Available at: https://harvardnsj.org/2011/03/untangling-attribution-2/ [Accessed 19 Apr. 2022].
32. Clarke, R.A. and Knake, R.K. (2010). *Cyber War : the Next Threat to National Security and What to Do About It*. New York: Harpercollins E-Books.
33. Clausewitz, C.V. (1832, 1980). *Vom Kriege*. Berlin: Ullstein
34. CNBC (2022). *U.S. intel accurately predicted Russia's invasion plans. Did it matter?* [online] Available at: https://www.cnbc.com/2022/02/25/us-intel-predicted-russias-invasion-plans-did-it-matter.html [Accessed 30 Apr. 2022].
35. Coleman, G. (2013). Anonymous in Context: The Politics and Power behind the Mask. *Internet Governance Papers*, (3).
36. Collier, J. (2017). Proxy Actors in the Cyber Domain: Implications for State Strategy. *St Antony's International Review*, [online] 13(1), pp.25–47. Available at: https://www.jstor.org/stable/26229121.
37. Connell, M. and Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. [online] Center for Naval Analyses (CNA). Available at: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf [Accessed 23 Apr. 2022].
38. Convention on Cybercrime (ETS No. 185). (2001). Council of Europe. November 23. Budapest

39. Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2010). *On cyber warfare*. London: Chatham House (The Royal Institute of International Affairs).
40. Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (2008). Official Journal of the European Union. L345/75
41. Cybersecurity and Infrastructure Security Agency (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure | CISA*. [online] Available at: https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.
42. Cybersecurity and Infrastructure Security Agency (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. [online] Available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
43. Czosseck, C. (2013). State Actors and their Proxies in Cyberspace. In: *Peacetime regime for state activities in cyberspace : international law, international relations and diplomacy*. Talinn: Nato Cooperative Cyber Defence Centre Of Excellence.
44. Defense Science Board Washington DC (2013). *Resilient Military Systems and the Advanced Cyber Threat*. [online] Defense Technical Information Center. Available at: https://apps.dtic.mil/sti/citations/ADA569975 [Accessed 24 Apr. 2022].
45. Denning, D.E. (2001). Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy. In: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation. doi:10.7249/mr1382.
46. Dennis, M.A. and Kahn, R. (2022). *Internet*. [online] Encyclopedia Britannica. Available at: https://www.britannica.com/technology/Internet#ref255529 [Accessed 10 Apr. 2022].
47. Diuk, N. (2014). EUROMAIDAN: Ukraine's Self-Organizing Revolution. *World Affairs*, [online] 176(6), pp.9–16. Available at: https://www.jstor.org/stable/43555086.

48. Doyle, P. (2022). *Major DDoS attacks increasing after invasion of Ukraine*. [online] TechTarget. Available at: https://www.techtarget.com/searchsecurity/news/252521150/Major-DDoS-attacks-increasing-after-invasion-of-Ukraine [Accessed 13 Jun. 2022].
49. Dreyer, I. and Popescu, N. (2014). *The Eurasian Customs Union: The economics and the politics*. [online] The European Union Institute for Security Studies. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_11_Eurasian_Union.pdf.
50. E-ISAC (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*. [online] Electricity Information Sharing and Analysis Center. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.
51. Euronews and Reuters (2022). *Ukraine to launch new 'IT army' to fight off Russian cyberattacks*. [online] Euronews. Available at: https://www.euronews.com/next/2022/02/26/ukraine-war-ukrainians-announce-the-launch-of-an-it-army-to-fight-off-russian-cyberattacks#:~:text=Ukraine%20will%20create%20an%20%22IT [Accessed 28 Apr. 2022].
52. Fanelli, R. (2016). Cyberspace Offense and Defense. *Journal of Information Warfare*, *15*(2), 53–65. Available at: https://www.jstor.org/stable/26487531
53. Fendorf, K. and Miller, J. (2022). *Tracking Cyber Operations and Actors in the Russia-Ukraine War*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.
54. Ferrari, A. (2014). *Oltre la Crimea Russia contro Europa?* Milano: ISPI – Istituto per gli Studi di Politica Internazionale.
55. Finnegan, C. (2022). *Russia escalates false chemical weapons claims about US, Ukraine by bringing them to UN*. [online] ABC News. Available at:

https://abcnews.go.com/Politics/russia-escalates-false-chemical-weapons-claims-us-ukraine/story?id=83366504 [Accessed 27 Apr. 2022].

56. FireEye (2016). *Cyber attacks on the Ukrainian grid: what you should know*. [online] Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.
57. Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *Quarterly Journal: International Security*, 38(2), pp.41-73 .
58. Getmanchuk, A. (2020). *Russia as aggressor, NATO as objective: Ukraine's new National Security Strategy*. [online] Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/russia-as-aggressor-nato-as-objective-ukraines-new-national-security-strategy/ [Accessed 3 May 2022].
59. Gibson, W. (1984). *Neuromancer*. New York: Ace.
60. Global Research & Analysis Team (2016). *BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents*. [online] Securelist by Kaspersky. Available at: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.
61. Green, J.A. (2016). *Cyber warfare : a multidisciplinary analysis*. London ; New York: Routledge, Taylor & Francis Group.
62. Greenberg, A. (2020). *Sandworm : a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Doubleday.
63. Greenburg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. [online] WIRED. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 2 May 2022].
64. Guerrero-Saade, J.A. and van Amerongen, M. (2022). *AcidRain: A Modem Wiper Rains Down on Europe*. [online] SentinelOne. Available at: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ [Accessed 30 Apr. 2022].
65. Hackett, R. (2015). *Russian cyberwar advances military interests in Ukraine, report says*. [online] Fortune. Available at:

https://fortune.com/2015/04/29/russian-cyberwar-ukraine/ [Accessed 25 Apr. 2022].

66. Hakala, J. and Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*. Riga: NATO Strategic Communications Centre of Excellence.
67. Harding, L. (2022). *Ukraine says Russia targeting civilians as missiles hit Kyiv TV tower*. [online] The Guardian. Available at: https://www.theguardian.com/world/2022/mar/01/ukraine-russia-civilians-missiles-kyiv-tv-tower [Accessed 29 Apr. 2022].
68. Harknett, R.J. and Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4), pp.534–537. doi:10.1080/01402390.2020.1732354.
69. Heritage, T. and Golubkova, K. (2013). Russia eyes loan, gas deal to keep Ukraine in its orbit. *Reuters*. [online] 16 Dec. Available at: https://www.reuters.com/article/us-ukraine-russia-idUSBRE9BF0GV20131216 [Accessed 17 Apr. 2022].
70. Hern, A. (2017). *WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017*. [online] The Guardian. Available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware [Accessed 29 Apr. 2022].
71. Herszenhorn, D.M. (2013). Facing Russian Threat, Ukraine Halts Plans for Deals with E.U. *The New York Times*. [online] 21 Nov. Available at: https://www.nytimes.com/2013/11/22/world/europe/ukraine-refuses-to-free-ex-leader-raising-concerns-over-eu-talks.html [Accessed 23 Apr. 2022].
72. History Editors (2019). *Fall of the Soviet Union*. [online] HISTORY. Available at: https://www.history.com/topics/cold-war/fall-of-soviet-union [Accessed 27 Apr. 2022].
73. Huddleston Jr., T. (2022). *What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia*. [online] CNBC. Available at: https://www.cnbc.com/2022/03/25/what-is-anonymous-

the-group-went-from-4chan-to-cyberattacks-on-russia.html [Accessed 29 Apr. 2022].

74. Hughes, D. and Colarik, A. (2017). The Hierarchy of Cyber War Definitions. *Intelligence and Security Informatics*, pp.15–33. doi:10.1007/978-3-319-57463-9_2.
75. International cyber law: interactive toolkit contributors (2021). *Georgia-Russia conflict (2008)*. [online] cyberlaw.ccdcoe.org. Available at: https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008) [Accessed 25 Apr. 2022].
76. ITU. (2022). Number of internet users worldwide from 2005 to 2021 (in millions). *Statista*. Statista Inc. Available at: https://www-statista-com.ezp.biblio.unitn.it/statistics/273018/number-of-internet-users-worldwide/ [Accessed: June 13, 2022]
77. Jasper, S. (2020). *Russian cyber operations : coding the boundaries of conflict*. Washington, Dc: Georgetown University Press.
78. JP 1-02. (2010). *Department of Defense Dictionary of Military and Associated Terms*. Available at: https://irp.fas.org/doddir/dod/jp1_02-april2010.pdf
79. Kaspersky (2019). *Tips on How to Protect Yourself against Cybercrime*. [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime [Accessed 22 Apr. 2022].
80. Kerkkänen, T. and Kuronen, A. (2016). *Russia's Cyberwar in Ukraine is Relentless – This Hacktivist Strikes Back*. [online] Yle. Available at: http://yle.fi/uutiset/osasto/news/russias_cyberwar_in_ukraine_is_relentless__this_hacktivist_strikes_back/8918200 [Accessed 5 May 2022].
81. Kirby, P. (2022). Why has Russia invaded Ukraine and what does Putin want? *BBC News*. [online] 9 May. Available at: https://www.bbc.com/news/world-europe-56720589 [Accessed 13 May 2022].
82. Klimburg, A. (2011). Mobilising Cyber Power. *Survival*, 53(1), pp.41–60. doi:10.1080/00396338.2011.555595.

83. Kotkin, S. (2016). Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern. *Foreign Affairs*, [online] 95(3), pp.2–9. Available at: https://www.jstor.org/stable/43946851 [Accessed 17 Apr. 2022].
84. Kraemer, R. and Otarashvili, M. (2014). *Geopolitica Implications of the Ukraine Crisis*. [online] Foreign Policy Research Institute. Available at: https://www.fpri.org/article/2014/04/geopolitical-implications-of-the-ukraine-crisis/ [Accessed 24 Apr. 2022].
85. Krebs, K. and Kwon, J. (2022). *Cyberattack hits Ukraine government websites*. [online] CNN. Available at: https://edition.cnn.com/2022/01/14/europe/ukraine-cyber-attack-government-intl/index.html.
86. Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In: *Cyberpower and National Security*. Washington, D.C.: National Defense University Press, pp.26-28
87. Lewis, J. (2015). *Cyber Espionage as a Component of Russian Modern Warfare*. [online] LookingGlass Cyber Solutions. Available at: https://lookingglasscyber.com/blog/threat-intelligence-insights/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/ [Accessed 17 Jul. 2022].
88. Libicki, M. (2015). The Cyber War that Wasn't, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 49–54.
89. Libicki, M.C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, Ca: Rand.
90. Lockheed, M. (2015). *Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense.* [online] Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.
91. Luk'janov, F. (2014). Promemoria per l'occidente: la Russia è tornata. *Limes*, [online] 14(4). Available at:

https://www.limesonline.com/cartaceo/promemoria-per-loccidente-la-russia-e-tornata [Accessed 16 Apr. 2022].

92. Lyosu [Twitter] 26 February. Available at: https://twitter.com/FedorovMykhailo/status/1497642156076511233?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497642156076511233%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.euronews.com%2Fnext%2F2022%2F02%2F26%2Fukraine-war-ukrainians-announce-the-launch-of-an-it-army-to-fight-off-russian-cyberattacks
93. Mankoff, J. (2022). *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic and International Studies.
94. Maurer, T. (2015). Cyber Proxies and the Crisis in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 79–86.
95. Maurer, T. (2018). *Cyber Mercenaries The State, Hackers, and Power*. Cambridge University Press.
96. Microsoft Threat Intelligence Center (2022). *Destructive malware targeting Ukrainian organizations*. [online] Microsoft. Available at: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ [Accessed 3 May 2022].
97. Microsoft's Digital Security Unit (2022). *Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine*. Microsoft Corporation.
98. Miller, C. (2016). *Inside The Ukrainian 'Hacktivist' Network Cyberbattling The Kremlin*. [online] RadioFreeEurope/RadioLiberty. Available at: https://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html [Accessed 17 Jul. 2022].
99. Milmo, D. (2022). *Anonymous: the hacker collective that has declared cyberwar on Russia*. [online] The Guardian. Available at: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia [Accessed 4 May 2022].

100. Moshood, T.D. (2020). *Information and Communication Technology*. [online] Encyclopedia. Available at: https://encyclopedia.pub/entry/3009 [Accessed 24 Jul. 2022].

101. Müller, R.S. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice.

102. Nakashima, E. (2018). Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes. *The Washington Post*. [online] 12 Jan. Available at: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html [Accessed 3 May 2022].

103. National Cyber Security Centre (2018). *Russian military 'almost certainly' responsible for destructive 2017 cyber attack*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

104. National Cyber Security Centre (2022a). *Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion [Accessed 10 Jun. 2022].

105. National Cyber Security Centre (2022b). *UK assesses Russian involvement in cyber attacks on Ukraine*. [online] GOV.UK. Available at: https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine [Accessed 26 Apr. 2022].

106. Nato Standardization Office (2021). *NATO glossary of terms and definitions = Glossaire OTAN de termes et définitions*. North Atlantic Treaty Organization (NATO). Available at: http://www.nato.int/docu/stanag/aap006/aap6.htm.

107. Paganini, P. (2016). *BlackEnergy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure*. [online] Infosec Resources. Available at: https://resources.infosecinstitute.com/topic/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/ [Accessed 6 May 2022].

108. Paganini, P. (2022a). *Pro-Russian group Killnet launched DDoS attacks on Romanian govt sites*. [online] Security Affairs. Available at: https://securityaffairs.co/wordpress/130732/hacking/russian-hacktivists-ddos-romanian-govt.html [Accessed 18 May 2022].

109. Paganini, P. (2022b). *White House and UK Gov attribute DDoS attacks on Ukraine to Russia's GRU*. [online] Security Affairs. Available at: https://securityaffairs.co/wordpress/128174/cyber-warfare-2/russia-gru-ddos-ukraine.html [Accessed 29 Apr. 2022].

110. Pakharenko, G. (2015). Cyber Operations at Maidan: A First-Hand Account, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 59–66.

111. Palmer, D. (2017). *Petya ransomware attack: How many victims are there really?* [online] ZDNet. Available at: https://www.zdnet.com/article/petya-ransomware-attack-how-many-victims-are-there-really/ [Accessed 27 Apr. 2022].

112. Peters, S. (2014). FireEye: Malware Traffic to Ukraine, Russia Spiked During Peak of Conf. *Dark Reading*. [online] 29 May. Available at: https://www.darkreading.com/analytics/fireeye-malware-traffic-to-ukraine-russia-spiked-during-peak-of-conflict [Accessed 25 Apr. 2022].

113. Putin, V. (2022). *Address by the President of the Russian Federation*. [online] *President of Russia*. Available at: http://en.kremlin.ru/events/president/news/67843.

114. Pynnöniemi, K. and Kari, M.J. (2016). Russia's New Information Security Doctrine: Guarding a besieged cyber fortress. *Finnish Institute of International Affairs*, 26/2016.

115. Reveron, D.S. (2012). *Cyberspace and national security : threats, opportunities, and power in a virtual world*. Washington, Dc: Georgetown University Press.

116. Rezvani, B. (2020). Russian Foreign Policy and Geopolitics in the Post-Soviet Space and the Middle East: Tajikistan, Georgia, Ukraine and Syria. *Middle Eastern Studies*, 56(6), pp.1–22. doi:10.1080/00263206.2020.1775590.

117. RHC (2022a). *300.000 hacker volontari si uniscono per combattere la Russia*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/300-000-hacker-volontari-si-uniscono-per-combattere-la-russia/ [Accessed 5 May 2022].

118. RHC (2022b). *Anonymous chiede ai russi di rimuovere Putin dal potere*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/anonymous-chiede-ai-russi-di-rimuovere-putin-dal-potere/ [Accessed 5 May 2022].

119. RHC (2022c). *Anonymous dichiara guerra a Killnet. E ora è guerra tra bande rivali*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/anonymous-dichiara-guerra-a-killnet-ora-e-guerra-tra-bande-hacktiviste/ [Accessed 4 Jun. 2022].

120. RHC (2022d). *Anonymous e affiliati: dobbiamo 'colpirli con tutto ciò che abbiamo'*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/anonymous-e-affiliati-dobbiamo-colpirli-con-tutto-cio-che-abbiamo/ [Accessed 5 May 2022].

121. RHC (2022e). *Anonymous e Killnet arruolano nuovi legionari*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/anonymous-e-killnet-arruolano-nuovi-legionari/ [Accessed 4 Jun. 2022].

122. RHC (2022f). *Anonymous viola le stampanti russe esortando di fermare la guerra*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/anonymous-viola-le-stampanti-russe-esortando-di-fermare-la-guerra/ [Accessed 5 May 2022].

123. RHC (2022g). *La Botnet di Killnet possiede migliaia di IP in 132 paesi compresa l'Italia*. [online] Red Hot Cyber. Available at: https://www.redhotcyber.com/post/la-botnet-di-killnet-possiede-migliaia-di-ip-in-132-paesi-compresa-litalia/ [Accessed 4 Jun. 2022].

124. Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, [online] 35(1), pp.5–32. doi:10.1080/01402390.2011.608939.

125. Rid, T. (2020). *Active Measures : the secret history of disinformation and political warfare.* S.L.: Profile Books Ltd.

126. Rijtano, R. (2018). *Attacco DDoS (Denial of Service): Cos'è, come funziona, come difendersi - Cybersecurity360*. [online] Cyber Security 360. Available at: https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/ [Accessed 17 Apr. 2022].

127. Robinson, M., Jones, K. and Janicke, H. (2014). Cyber warfare: Issues and challenges. *Computers & Security*, [online] 49, pp.70–94. doi:10.1016/j.cose.2014.11.007.

128. Rosenfield, D.K. (2009). Rethinking Cyber War. *Critical Review*, 21(1), pp.77–90. doi:10.1080/08913810902812156.

129. Sanger, D.E. and Conger, K. (2022). Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds. *The New York Times*. [online] 10 May. Available at: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html [Accessed 3 Jun. 2022].

130. Sanger, D.E. and Erlanger, S. (2014). Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government. *The New York Times*. [online] 8 Mar. Available at: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html [Accessed 29 Apr. 2022].

131. Schmitt, M.N. ed., (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. [online] Cambridge: Cambridge University Press. doi:10.1017/cbo9781139169288.

132. Scroxton, A. (2022). *New wave of cyber attacks on Ukraine preceded Russian invasion*. ComputerWeekly.com.

133. Shead, S. (2022). *'We want them to go to the Stone Age': Ukrainian coders are splitting their time between work and cyber warfare*. [online] CNBC. Available at: https://www.cnbc.com/2022/03/23/ukrainian-coders-splitting-their-time-between-day-job-and-cyberwar.html [Accessed 29 Apr. 2022].

134. Skytland, N. (2019). *Confidentiality, Integrity, Availability – Future of Work*. [online] National Aeronautics and Space Administration (NASA). Available at: https://blogs.nasa.gov/futureofwork/2019/04/12/confidentiality-integrity-availability/ [Accessed 29 Apr. 2022].

135. Smith, B. (2022). *Digital technology and the war in Ukraine*. [online] Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ [Accessed 5 May 2022].

136. Spicer, J. and Garanich, G. (2022). Ukraine and Russia resume peace talks with 'no handshake'. *Reuters*. [online] 29 Mar. Available at: https://www.reuters.com/world/europe/ukraine-sets-ceasefire-goal-new-russia-talks-breakthrough-looks-distant-2022-03-29/ [Accessed 29 Apr. 2022].

137. Spînu, N. (2020). *Ukraine Cybersecurity Governance Assessment*. [online] Geneva Centre for Security Sector Governance. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment_dec2021.pdf [Accessed 22 Apr. 2022].

138. Statista Research Department (2022). *Internet usage worldwide - statistics & facts*. [online] Statista. Available at: https://www.statista.com/topics/1145/internet-usage-worldwide/#dossierKeyfigures.

139. Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies*, 36(1), pp.101–108. doi:10.1080/01402390.2012.730485.

140. Taddeo, M. (2012). An analysis for a just cyber warfare. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. [online] Available at: https://www.semanticscholar.org/paper/An-analysis-for-a-just-cyber-warfare-Taddeo/9a8b0bc14d336e5d2a599f9bf9ae163ff95f7ff5 [Accessed 25 Apr. 2022].

141. TASS (2022). *Russia's reaction to the US response on security guarantees.* [online] Available at: https://tass.ru/politika/13744013?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com [Accessed 28 Apr. 2022].

142. Teslova, E. (2022). *Putin says Minsk Agreement on Ukraine exists no more*. [online] Anadolu Agency. Available at: https://www.aa.com.tr/en/asia-pacific/putin-says-minsk-agreement-on-ukraine-exists-no-more/2510573 [Accessed 27 Apr. 2022].

143. The Department of Homeland Security (2022). *Critical Infrastructure*. [online] U.S. Department of Homeland Security. Available at: https://www.dhs.gov/science-and-technology/critical-infrastructure#:~:text=Critical%20infrastructure%20includes%20the%20vast%20network%20of%20highways%2C [Accessed 29 Apr. 2022].

144. The Editors of Encyclopaedia Britannica (2019). Peace of Westphalia. *Encyclopædia Britannica*. [online] Available at: https://www.britannica.com/event/Peace-of-Westphalia.

145. The International Institute for Strategic Studies (2021). *Cyber Capabilities and National Power: A Net Assessment*. [online] The International Institute for Strategic Studies. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

146. Tkachenko, O. (2017). Cybersecurity in Ukraine: National Strategy and international cooperation. *Global Forum on Cyber Expertise*. [online] 7 Jun. Available at: https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/ [Accessed 2 May 2022].

147. Traynor, I. (2014). Ukraine's bloodiest day: dozens dead as Kiev protesters regain territory from police. *The Guardian*. [online] 21 Feb. Available at: https://www.theguardian.com/world/2014/feb/20/ukraine-dead-protesters-police [Accessed 4 May 2022].

148. UNIDIR (2022). *Russian Federation*. [online] Cyber Policy Portal. Available at: https://cyberpolicyportal.org/states/russian-federation [Accessed 11 Jun. 2022].

149. UNITED STATES. (2018). *Summary of the 2018 national defense strategy of the United States of America: sharpening the American military's competitive edge*. Available at: http://purl.fdlp.gov/GPO/gpo91947.

150. Valeriano, B. (2018). *The United States*. *Oxford Scholarship Online*. Oxford University Press. doi:10.1093/oso/9780190618094.003.0007.

151. Watson, E. (2022). *100 days of war in Ukraine: A timeline*. [online] CBS News. Available at: https://www.cbsnews.com/news/ukraine-russia-war-timeline-100-days/ [Accessed 12 Jun. 2022].

152. Weedon, J. (2015). Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 67–77.

153. Weissbrodt, D. (2013). Cyber-Conflflict, Cyber-Crime, and Cyber-Espionage. *Minnesota Journal of International Law*, [online] 22. Available at: https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles.

154. Whyte, C., Thrall, A.T. and Mazanec, B.M. (2021). *Information warfare in the age of cyber conflict*. Abingdon ; New York: Routledge.

155. World Nuclear Association (2022). *Ukraine: Russia-Ukraine War and Nuclear Energy*. [online] World Nuclear Association. Available at: https://world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine-russia-war-and-nuclear-energy.aspx [Accessed 19 Jun. 2022].

156. YourAnonOne (2022). [Twitter] 24 February. Available at: https://twitter.com/YourAnonOne/status/1496965766435926039

157. Zetter, K. (2022). *Dozens of Computers in Ukraine Wiped with Destructive Malware in Coordinated Attack*. [online] Zero Day. Available at: https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r [Accessed 29 Apr. 2022].

158. Ziolkowski, K. (2013). *Peacetime regime for state activities in cyberspace : international law, international relations and diplomacy*. Talinn: Nato Cooperative Cyber Defence Centre Of Excellence.