LUISS

Department of Political Sciences
Master's Degree in International Relations
Major in Security

Chair of Security Policies

Cyber Operations and Information Campaigns: An Analysis of European Cyber Diplomacy in the Context of Russian Hybrid Warfare

Prof. Carlo Magrassi
SUPERVISOR

Prof. Pasquale Ferrara
CO-SUPERVISOR

ID. 650392

Margherita
Zoppi

CANDIDATE

Academic Year 2022/2023

Index

Introduction

With the invention of the computer and the advent of the Internet, people all around the world have started to communicate with each other through a complex network of information systems. These developments allowed individuals to conduct most of their activities online, from buying and selling goods and services in the form e-commerce, to the digitalization of the institutional processes that characterize most countries, such as online payment of taxes, as well as systems of electronic voting for national and local elections. As a result, because of the widespread access to digital devices fostered by the process of globalisation, many believed that the digitalization of communication and the popularization of the Internet would be accompanied by an overall democratization of the international scenario; in other words, the idea was that increased interconnectedness and interdependence of systems would make the possibility of entering into conflict an unlikely and disadvantageous scenario, just like the invention and diffusion of the nuclear bomb, and the concept of mutually assured destruction, made the prospect of launching a nuclear missile undesirable (Samabaluk, 2022, p. 54). However, for what concerns cyberspace, this was not the case.

While democratic countries sought to use new digital technologies for the welfare of their citizens, authoritarian states started exploiting the weaknesses of cyberspace as a new and more efficient way to pursue their political and military agendas. In particular, Russia, China, Iran and North Korea represent the four main countries engaged in malicious cyber activities targeting other nation states, either directly by employing their own security and intelligence apparatuses, or indirectly, by delegating their activities to proxies and cyber mercenaries (Microsoft, 2022, p. 33). In particular, Russia and Iran have been mainly targeting the IT sector to gain access to the customers of tech companies, but other frequently targeted sectors by state actors include Think Tanks, Non-Governmental Organizations (NGOs), universities and government institutions (Microsoft, 2022, p. 35). Moreover, the energy sector also features among the most common targets of cyber-attacks in recent years, which have expanded and intensified following the Russian invasion of Ukraine that took place on February 24, 2022 (Pasquazzi & Savarino, 2023).

As a matter of fact, the ongoing war in Ukraine has given new impetus to the use of cyber aggression as an element of warfare, leading scholars to label the Ukrainian conflict as a case of hybrid war, in which elements of traditional kinetic warfare are combined with cyber warfare as well as the use of propaganda. In fact, the Russian Federation represents an illustrative and relevant case of a nation state exploiting digital instruments, like the Internet and social media, to launch influence operations in cyberspace, both domestically and abroad, where its information warfare campaigns aim to erode trust in local governments and sow doubt concerning the current and real state of international affairs (Microsoft, 2022, p. 72). Indeed, if we look at Ukraine, the Russian Federation has been able to maximize its war efforts by combining information operations to cyber-attacks and traditional kinetic operations on the ground (Microsoft, 2022, p. 76), therefore bringing a multidimensional approach to modern conflict. Scholars of the balance of power theory have argued that Moscow's resort to cyber aggression stems from its relative military and economic weakness compared to its rivals, the United States in particular, therefore allowing Russia to challenge its enemies in an asymmetric confrontation (Pytlak & Mitchell, 2016). Indeed, Russian cyber operations have provided pro-Kremlin forces on the ground a substantial support in undermining Ukraine's government and military forces.

Furthermore, while authoritarian regimes like Russia are able to harness the information environment to their advantage, the spread of malicious cyber activities and disinformation represents a grave threat to democracies around the world, as they are subject to increasingly sophisticated foreign influence operations. In recent years, these operations have found fertile ground in Western countries, as online communication and information systems have been overflowed with often contradictory narratives, which have, in turn, generated higher levels of social and political polarization, particularly around issues like race and immigration (Unver, 2017, pp. 127–128). Member states of the European Union (EU) are not immune to these issues, and European societies have been experiencing increased levels of polarization, especially during the COVID-19 pandemic of 2020: as daily activities moved to cyberspace because of the imposition of lockdowns, increased activity in the digital realm opened the door for authoritarian regimes to spread their propaganda narratives, therefore creating a tsunami of fake news and disinformation

(Kalathil, 2020, p. 39). Furthermore, European citizens have been increasingly targeted by cyber-attacks, which aim to disrupt the functioning of daily online activities, as well as democratic institutional processes, especially elections. As a response to the threats emanating from cyberspace and the insidious effects of information operations, the EU has been developing a framework of cybersecurity policies aimed at transforming the Union into a leading geopolitical player in the fight against cyberthreats through diplomatic initiatives. As Moscow's actions in Ukraine demonstrate how the use of information and communications technologies (ICTs) can be used to erode trust in political institutions and weaken democratic processes, the EU has been providing support to Ukraine to contrast cybersecurity and disinformation threats (Ringhof & Torreblanca, 2022).

Overall, the digitalization of the world's social and political systems makes countries vulnerable to those entities willing and capable of exploiting the weaknesses of their citizens and institutions. Furthermore, while cyber-attacks are generally, but not always, detected the moment they are launched due to their immediate effects, in the case of what is known as Foreign Influence Manipulation and Interference (FIMI), targets are oftentimes unaware of being the subjects of foreign influence operations, therefore making their detection an incredible difficult task. Nonetheless, cyber-attacks and influence operations are inextricably connected to each other, given that disinformation and influence operations are launched in cyberspace through the use of digital instruments, which amplify their reach and impact; yet, the literature on this particular and recent phenomenon is still developing, and it would benefit from more research on the conjunction of cyber and information operations (ENISA, 2022b). Indeed, these types of operations are generally conducted during both times of conflict and peacetime, thereby making them a pervasive and permanent threat to the health and functioning of our democratic societies. For this reason, this thesis will attempt to investigate the role of cyber and information operations in the context of inter-state hybrid campaigns. In practice, the present work will try to assess the role of EU cyber policies, in particular European Cyber Diplomacy, in the prevention, defence against and response to threats in cyberspace. To do so, this thesis will investigate the case study of Russian hybrid warfare conducted in Russia's neighbouring countries and Europe, with a particular focus given to the conflict in Ukraine.

Before delving into the analysis presented in this thesis it is necessary acknowledge the limited nature of this work, which gives a concise overview of the topic analysed here; moreover, it is important to mention that due to the ongoing nature of the war in Ukraine, the findings reported in this work do not assume to be exhaustive nor definitive, but seek to shed light on the conflict through the knowledge gathered so far by researchers and experts. The present work will be divided into four chapters, structured in the following way. The first chapter will provide a concise literature review on cyberspace and interstate hybrid warfare, focusing on the development of cyberspace, cyber warfare in inter-state conflicts and modern information warfare in cyberspace. The second chapter will present an overview of European Cyber Regulation, starting with a brief overview of its evolution, and then focusing on the EU's external approach to cybersecurity through the policy of Cyber Diplomacy. The third chapter will focus on Russian hybrid warfare, particularly the use of cyber campaigns and information manipulation, through the illustration of a set of case studies, namely Estonia, Georgia, and the US, but also inside the EU, with Germany, the United Kingdom and France. The fourth chapter, starting with synthesis of Russo-Ukrainian relations, will analyse Russian hybrid campaigns in Ukraine, from the 2014 annexation of Ukraine to the 2022 invasion, focusing on the cyber and information elements of the conflict, and investigating the EU's response to Moscow's hybrid warfare in Ukraine. The final part of this thesis will present the results that emerged from the analysis and will draw the conclusions with some suggestions for further research.

1. Cyberspace and Inter-State Hybrid Warfare

Ever since the invention of computers and the advent of the Internet, cyberspace has become a realm deeply connected with every aspect of our daily lives, therefore making it a foundational element in the functioning of modern societies. The democratisation of digital connections has increased the number of people capable of using computer technologies, therefore pushing both state and non-state actors to move their operations in the digital battlespace (Nissen, 2016, p. 196). Indeed, billions of people connect to the Internet every day: in April 2023, 5.18 billion internet users were registered around the world, amounting to 64.6 percent of the total population, of which 4.8 billion were users of social media (Petrosyan, 2023). Yet, despite its pervasive presence, there is still a lack of clear and overwhelming consensus on what cyberspace actually is (Bindt et al., 2017, p. 8). Nevertheless, this section will attempt to provide an exhaustive, albeit limited, overview of the common grounds that can be found in the literature on cyberspace and cyber conflict. First, an overview of the emergence of cyberspace will be presented, followed by its conceptualisation and a brief account on the functioning of international cyberspace governance; next, the second section of this chapter will investigate the phenomenon of cyber warfare and the related concept of cyberattacks, and will give a brief overview on the issues of attribution in cyber conflict and the emerging threat of Artificial Intelligence. Finally, the third section will present a concise analysis of information warfare in cyberspace, and the role social media play in the spread of disinformation in the context of influence operations.

1.1 Cyberspace: Origin and Development of the 5th Domain

In order to better understand what cyberspace is, and the type of activities that take place within it, this section should begin with an overview of its history and origins. To this end, Huansheng Ning's (2022) *A Brief History of Cyberspace* provides us with a comprehensive account on the origins and development of cyberspace. Ning (2022) starts with the

etymological definition of 'cyberspace', which derives from the Ancient Greek word '*kybernētēs',* that "stands for steersman, governor, pilot or rudder" (p. 1). While some argue that the concept of "cyberspace" emerged in 1844, the same year the telegraph was invented (Even & Siman-Tov, 2012, p. 9), the term became popular after being employed in the science fiction series *Neuromancer* by American author William Gibson in the 1980s, and a decade later the term cyberspace became a concept that was commonly used to refer to computer networks as well as the Internet (Ning, 2022, pp. 1–2).

Yet, despite becoming a widespread term only in the 1990s, the development of cyberspace is directly linked to the birth of the computer in 1946, and to its mass commercialization in the following years, leading to the establishment of the Advanced Research Projects Agency Network (ARPANET) in 1969, which is considered the ancestor of today's Internet and whose goal was to set up communication networks between different computers in order to share and transmit information (Ning, 2022, pp. 2–3). ARPANET was born out of the Advanced Research Projects Agency (ARPA), established by American President Dwight Eisenhower in 1958 to enhance national security through investments in technological research and development; this project was triggered by the 1957 launch of the first artificial satellite, Sputnik 1, by the Soviet Union (USSR), during a time in which the United States and the USSR were competing to achieve technological and military supremacy (Puddephat, 2020, p. 13). What is significant about ARPANET is the way in which it developed the various processes involved in the delivery and reception of data, mainly through transmission control protocol (TCP) and the internet protocol (IP), whose application to communication networks gave birth to the modern "Internet", which became the commonly used name for the process of "inter-networking" (Puddephat, 2020, p. 14).

When the commercialisation process of the Internet was completed in 1995, cyberspace allowed for the widespread interconnection of things as well as humans, leading to the birth of the so-called 'Internet of Things' (Ning, 2022, p. 4). This complex coupling and interdependence of networks, which has been accelerated by the process of globalisation, has made our society increasingly interconnected, guaranteeing the delivery of information and services with almost lighting speed; yet, our overreliance on the Internet

and the construction of interlinked global systems has made us particularly vulnerable to any kind of threat or malign actor found in cyberspace (Nye, 2017, p. 44). In turn, as the cyberspace realm became fertile ground for both non-state and state malicious activity (Klimburg, 2014, p. 1), the concept of cyberspace has been also defined and conceptualized by the military literature, and an important definition comes from the Joint Publication 3-12 (R) on Cyberspace Operations by the Department of Defence (DoD) of the United States, which describes cyberspace as:

> *"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."* (Department of Defense, 2013).

This conceptualization includes the main elements that scholars and experts in the field generally agree on for what concerns the makeup of cyberspace. First of all, it is a domain where we find an interconnection of computer networks in which information is shared at a very high speed, almost lightning-like (Guyonneau & Le Dez, 2019, p. 105). Furthermore, given the various systems and infrastructures that comprise this domain, cyberspace is made widely accessible to virtually any individual or entity that has access to the Internet (Gomez, 2021, p. 135). However, while this interconnection may have given a voice to emarginated communities around the world, cyberspace has also allowed unfriendly actors to continue their activity in a new digital environment (Guyonneau & Le Dez, 2019, p. 105). The increased availability of computer network resources has expanded the number of cyber actors, going from terrorist groups and organized crime, as well as the so called 'hacktivists', but also to state-controlled proxies operating in the virtual world under the direction and control of state governments (Siers, 2018, p. 558).

Several actors are found operating on the Internet, but before delving into an analysis of cyber activities, it is important to begin by giving a concise overview of the structure of cyberspace. To do so, a further definition of cyberspace must be provided. The United Nations International Telecommunications Union (ITU) defines cyberspace as "*the physical and non-physical terrain created by and/or composed of some or all of the*

following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users." (ITU, 2010, p. 11). From this conceptualisation Shmuel Even and David Siman-Tov (2012) have argued that three interconnected layers are found in cyberspace: the human layer, the logical layer, and the physical layer (p. 10). First, the human layer concerns the human use of computer networks and devices, which involves activities such as reading and exchanging information; second, the logical layer is where software activity takes places, involving Graphic Users Interface (GUI), applications and operating systems; third, hardware such as chips and electronical impulses form the main element of the physical layer (Even & Siman-Tov, 2012, pp. 12–13). Similarly, Ning (2022) divides cyberspace into a physical, logical, and content layer, where the latter represents Even and Siman-Tov's human layer; indeed, it is in the content layer that human behaviour is regulated (p. 143). A further conceptualisation of the structure of cyberspace divides its structure into four layers, where the first two remain the physical (hardware) and logical layer (information), and the remaining two levels are the cyber-persona layer, which are the network users, and the social layer, namely the entities operating the Information Communication Technologies and the hardware (Bindt et al., 2017, p. 10). While some attempts at structuring cyberspace have been made, this domain is incredibly complex, fostering a high degree of unpredictability on the activities that can take place within it (Gomez, 2021, p. 136).

Layer	**Type of Activity and its purpose**	**Contents (examples)**	**Developing Trends (examples)**
1. The human layer			
The user	Human use of computerization products	Reading, trading, investing, finding information, exchanging information, maintaining contact with friends, contact between citizens and	An increase in the phenomenon of user communities (WEB2) and the use of mobile and integrative devices (smart phones); the start of sophisticated internet use (WEB3)

		government offices, crime, cyberwar	
2. The logical layer	Software activity		
Graphic user interface (GUI)	Translating information from user language to computer language (digital information) and back	Pages of text, pictures, videos, audio, buttons	Increase in types and levels of applications presented at the interface; rise in graphic presentation; transition to 3D
Applications software	Processing information from user interfaces, network management software	Instructions and flow charts in programming language (algorithms)	More applications; more and more layers of software between the hardware and user interface
Operating systems	Running software and translation from computer language to machine language	Information in programming language relevant to the layer	
3. The physical layer			
Hardware	Electromagnetic physical infra- structure doing machine operations	Chips, electronic cards, etc; electrical impulses	Growth in volume of information about electronic components, miniaturization, mobility, flash memory
Communications and energy systems (electromagnetic infrastructure)	Providing conditions for existence and activity of computerization in electromagnetic field	Infrastructure and maintenance; laying cables, computer tables, etc; RF signals, light and electricity waves	Growth in variety and spread of communications systems: cellular, Bluetooth, router, satellite, ocean cable. Improved energy utilization and miniaturization
Hardware and software carriers	Provide additional conditions to maintain		People carrying smart computers and phones;

	cyber- space on land, at sea, in the air, and in space.		computer embedded installations, systems, and tools; equipment with integrated processors and controllers; and devices with input options (scanners), sensors, and effectors. This is where the connection between cyberspace and the physical realms occurs.

Table 1 - The Three Layers of Cyberspace (Source: Even, S., & Siman-Tov, D. (2012). Cyberspace and the Security Field: A Conceptual Framework. http://www.jstor.com/stable/resrep08940.4)

As illustrated above, definitions of cyberspace describe it not as a technology (Klimburg, 2014, p. 3), but as a 'domain'. Indeed, scholars of cyberspace agree on the classification of the cyber realm as an environment in which both public and private actors communicate (Hodges & Creese, 2015, p. 36), with some defining cyberspace as the 'fifth domain', together with the four main physical domains, land, sea, air and space (Even & Siman-Tov, 2012, p. 13), with cyberspace connected to each of these domains (Bindt et al., 2017, p. 14). Consequently, being cyberspace a new realm in which humans act and interact to perform their daily activities, this cyber domain has become the object of governance, bringing with it issues of state sovereignty (Ning, 2022, p. 128). One significant element to be kept in mind when discussing cyberspace governance is that the private sector possesses and manages cyberspace through a series of standards and procedures that constitute some kind of market governance (Puddephat, 2020, p. 17). Nonetheless, states have developed an interest in exercising their digital sovereignty in order to protect critical infrastructures and assets in the cybersphere, however, the virtual nature of this dimension makes it incredibly difficult to establish a unanimously recognized system of governance (Liaropoulos, 2016). Furthermore, this difficulty also stems from the fact that 'Internet governance' can have various meanings: governance can be some-kind of state government, technical protocols for the functioning of the system, crisis management system for harmful issues within the system, or even an instrument to contrast the power

of those companies, mainly US-based, that hold state-like power in cyberspace (Puddephat, 2020, p. 20).

Because of its commercial origin, cyberspace was born as a virtual space in which limited and unorganised, non-state governance did not seek to control information (Liaropoulos, 2016, p. 17); however, as soon as the Internet expanded in the 1970s and its use drastically grew at the global level, the need to regulate and govern the cyber domain developed with it (Ning, 2022, p. 140). International organizations aimed at creating international standards for the uniform development of cyberspace were established, going from the founding of the *International Network Working Group* (INWG) in 1972 (Ning, 2022, p. 146), to the creation of the *Internet Corporation for Assigned Names and Numbers* (ICANN) in 1998, a private non-profit institution (Muller, 2016, p. 168) tasked with coordinating Internet addresses and names (Klimburg, 2014, p. 6). The creation of ICANN was pushed by the US government's desire for a market-like governance of the Internet managed by private non-governmental organisations; however, the involvement of governments in the managing of cyberspace turned governance of the Internet into a political issue, as the European Union wished for the establishment of a 'multilateral institutional framework', where governments would have a relevant role in the management of the Internet alongside the private sector (Puddephat, 2020, pp. 14–15).

Initially, the Internet was considered an English-language system available to only a few privileged people (Puddephat, 2020, p. 16), but it eventually developed into a platform available to virtually anyone using a computer or other electronic devices. From the 1990s onwards, sovereignty in cyberspace and cyber governance gradually became important issues on states' political agendas, and in 2005 the United States DOD declared cyberspace as a 'global commons' together with the four other domains; however, due to the increase in malicious cyber activities, governments have increasingly sought to assert their presence in this domain and have a say in its governance (Ning, 2022, p. 132). To this end, the United Nations took an active role in coordinating governments to discuss issues related to Internet governance. In particular, the UN International Telecommunications Union (ITU) took the lead and convened the *World Summit on the Information Society* (WSIS) to discuss the future governance of the Internet, leading to the creation of the

Internet Governance Forum (IGF), a multi-stakeholder UN-based governance group with the goal of setting cyber governance norms (Puddephat, 2020, pp. 18–19). These initiatives were followed by the United Nations General Assembly (UNGA) 2002 Resolution 57/239, which stated that all participants of cyberspace, including governments, organisations and individual, are responsible for ensuring the security of cyberspace and information technologies (Liaropoulos, 2016, p. 20), and 2004 saw the establishment of the *UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN GGE), a body aimed at governing state behaviour in cyberspace (Chernenko et al., 2018, p. 5).

When looking at cyberspace governance, there are three main models that have been studied: distributed governance, multilateral governance, and multi-stakeholderism. As mentioned above, the early days of the Internet were characterised by freedom and unorganized governance, therefore representing a distributed model of governance that was based on self-regulation of a limited network. Multilateral governance, instead, is based on the idea that chaos reigns in cyberspace, and that countries have the right to govern cyberspace through their own regulations, given the presence of physical hardware within the sovereignty and jurisdiction of the state (Ning, 2022, p. 135). This type of governance can be said to fall within the International Relations theory of Realism, which focuses on the primacy of states and the conceptualisation of the international system as anarchic (Pytlak & Mitchell, 2016, p. 99), and it is supported by countries like Russia and China (Ning, 2022, pp. 135–136). In the third system, the multi-stakeholder model, all Internet users must participate in the formulation of institutions and policies governing cyberspace to enhance the legitimacy of state governance in cyberspace (Ning, 2022, p. 136), an issue that gained importance and relevance in 2013 when Edward Snowden, former contractor for the US National Security Agency (NSA), revealed the existence of a network of Western governments spying on their own citizens in cyberspace (Libicki, 2021a, p. 34). An example of the application of the multi-stakeholder approach was the creation of the ICANN organisation, which represents a governance institution based on the neo-liberalist approach to cooperation between governments and non-state entities (Muller, 2016).

International cooperation in cyber governance and the formulation of regulations have become fundamental elements in state prevention of cybercrime and cyber-attacks (van der Meer, 2018, p. 7). Indeed, because of the international and widespread nature of the cyber domain, cooperation with foreign governments is essential to mitigate the effects of border-crossing malicious cyber activity (Even & Siman-Tov, 2012, pp. 32–33). In fact, while cyberspace gives the idea of being a virtual and borderless realm, it still relies on the existence of a physical architecture, and its geographical location (Steed, 2015, p. 87). For this reason, governments and international organisations have cooperated to establish institutions aimed at protecting security in cyberspace against the growing number of cyberthreats, as our society's digital interconnection deepens and expands. In particular, a code of norms to regulate cyberspace as a domain of warfare have been set out in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, released by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) (M. N. Schmitt, 2013).

The creation of the Tallinn Manual stems from the events that took place during the 2007 cyber-attacks against Estonia. As a way to strengthen NATO's defence, the NATO CCD COE was set up in Estonia's capital, Tallinn, and in 2013 the Centre produced the Tallinn Manual on the international law applicable to cyber warfare, given the lack of any treaty regulating warfare in cyberspace; yet, this Manual does not completely fill the legal gaps concerning conduct in cyber warfare, but only provides a generally agreed guide on cyberspace behaviour (Steed, 2015, pp. 85–86). For what concerns the main content of the Tallinn Manual, we find that the document argues that cyber-attacks can be compared to conventional kinetic warfare, to a certain degree (Libicki, 2021a, p. 656); as a result, the International Group of Experts agreed that "both the *jus ad bellum* and *jus in bello* apply to cyber operations" (M. N. Schmitt, 2013, p. 5) or that, in other words, international law standards apply to cyberspace (M. N. Schmitt, 2013, p. 13). When discussing sovereignty, the Manual emphasised that "A State may exercise control over cyber infrastructure and activities within its sovereign territory" (M. N. Schmitt, 2013, p. 15) and that "Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty" (M. N. Schmitt, 2013, p. 22). Furthermore, Rule 6 on the Legal Responsibility of States sets that states are legally

responsible for cyber operations violating international law, if such an operation is attributable to that state (M. N. Schmitt, 2013, p. 29). This Rule raises one of the most fundamental issues in cyberspace and warfare, the issue of attribution, which will be analysed in the following section within the context of cyber warfare. In 2017, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* was released (Ning, 2022, p. 134), and it includes more detailed rules concerning states and their proxies engaged in malicious cyber activities outside of warfare (Garon, 2018, p. 21).

In sum, cyberspace has seen its transformation from an unorganized and small-scale system of networks into a global web of interconnected computer systems. As a result, international organizations and common standards were created to harmonize the Internet and cyberspace, but as this domain grew, so did the actors inside it, whether benevolent or malignant, leading to the emergence of cyberthreats. In turn, this new security issue has pushed governments to exercise their sovereignty in the digital realm, as cyberspace has become a new domain of warfare where governance and international law are still lacking clear and defined consensus.

1.2 Cyber Warfare: The Digital Frontier of Inter-state Conflict

Following an analysis of the main characteristics and development of cyberspace, this section will investigate the phenomenon of cyber warfare and its origins, but first, it is crucial to place this digital security issue within the context of so-called Hybrid Warfare (HW). Indeed, cyber-attacks are generally performed in combination with traditional and unconventional elements of warfare, therefore making cyber-attacks an asset inside what Bernard Siman calls the "Hybrid Warfare 'Toolbox'" (Siman, 2022, p. 1). The concept of hybrid warfare became popular during the annexation of Crimea by Russia in 2014 and, despite the concept's lack of a clear conceptualization, we can find the following characteristics attributed to HW: "*it is asymmetric and multi-modal along a horizontal and a vertical axis, and to varying degrees shares an increased emphasis on creativity, ambiguity, and the cognitive elements of war"* (Reichborn-Kjennerud & Cullen, 2016, p. 2). In particular, hybrid warfare's main attribute is the synergy of different strategies and

attack elements, which result in a high level of uncertainty and ambiguity for the enemy (Danyk et al., 2017, p. 9). The synchronization and coordination of conventional and unconventional components multiply the effects of these instruments of power, whose ambiguity makes attribution of an attack extremely difficult, therefore giving plausible deniability to the attacker thanks to the use of unrelated proxies and anonymous cyber-attacks (Reichborn-Kjennerud & Cullen, 2016). In fact, what distinguishes cyber warfare from traditional kinetic conflicts is the degree of uncertainty and ambiguity surrounding the impact of cyber-attacks (Libicki, 2021b, p. 18), making the line between conflict and peace increasingly blurred (Reichborn-Kjennerud & Cullen, 2016, p. 2). As a result, the integration of cyber elements into hybrid warfare will have profound impacts on the future of conflict (Danyk et al., 2017, p. 13).

Now that we have clarified the position of cyber conflict within the broader phenomenon of hybrid warfare, a brief overview on the origin and development of cyber warfare will be presented here to lay the basis for a better understanding of the threat conflict in cyberspace poses in today's world. According to Richard Stiennon (2015), cyber warfare finds its origins in Electronic Warfare (EW), a phenomenon now under the umbrella of cyber warfare that is connected to radar and radio communication technology; since the 1990s, the expansion of states' military presence in cyberspace has led to a growth in national interest for what concerns cyberthreats, also fostered by the increased interconnection of computer networks and information systems brought about by the development of the Internet (p. 7). To this date there is no consensus on the existence of a pure and solely cyber conflict (Smith, 2013, p. 82), but cyber warfare has been used as a strategic tool in several instances, including the notorious examples of cyber-attacks in Estonia (2007), Georgia (2008), Iran (2010) and Ukraine (2014) (Steed, 2015). But what exactly is cyber warfare?

Cyber warfare is generally used to describe "a systematic campaign of cyberattacks for political or related military end" (Libicki, 2021a, p. 66) and its operational form is in constant evolution (Ning, 2022, p. 186). More specifically, cyber warfare has been defined as:

> *"An extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."* (Stiennon, 2015, p. 8)

From this definition we can infer that cyber conflict involves state actors, like traditional warfare, who employ digital or cyber means to threaten their enemy's national security. Furthermore, there is also the possibility for cyber proxies to take action under the command and control of belligerent states, such as individuals, groups or criminal entities (ENISA, 2017, p. 7). While some definitions focus on the use of cyber-attacks to cause "direct damage or destruction" (Even & Siman-Tov, 2012, p. 20), others look at the malicious use of Information and Communication Technologies (ICTs) to "change or modify state behaviour" (Pytlak & Mitchell, 2016, p. 98). Ultimately, cyber warfare does not take place for its own sake, but it is a strategy used by states and their surrogates to gain a military, economic, political or societal advantage (Guyonneau & Le Dez, 2019, p. 103). In other words, cyber warfare is an ensemble of cyberthreats and cyber-attacks.

While some scholars have argued that cyber-attacks taking place during political confrontations are not to be considered serious elements of warfare, but only "Weapons of Mass Annoyance" (Smith, 2013, p. 84), others considers them more like "Weapons of Mass Disruption" (Rühle, 2016, p. 18). Depending on the definition one adopts, the intensity of the effects of cyberattacks can vary, and it can be argued that the conceptualisation attributing to cyberattacks the highest level of intensity comes from Rule 30 of the *Tallin Manual*, which gives us the definition of a cyberattack:

> "*A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"* (M. N. Schmitt, 2013, p. 106)

This definition implies that cyber operations can have a physical impact, whereas Martin Libicki (2021a) argues that while it is electronic warfare operations that can have concrete repercussions in the physical realm, cyberattacks use information technology to

"interfere with an information system's operations" (p. 64). Furthermore, the European Union Agency for Cybersecurity (ENISA) makes another distinction, between "cyber incident", "cyber accident" and "cyber attack". A cyber-attack is defined as "Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions is called cyber incident", while they define cyber accidents as "any occurrence associated with cyber space causing significant damage to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing personal injury", consequently, "Cyber attacks cover all cyber incident triggered by malicious intent where damages, disruptions or dysfunctionalities are caused" (ENISA, 2017, pp. 6–7). Finally, Duncan Hodges and Sadie Creese (2015) argue that the purpose of a cyber-attack is to "compromise the confidentiality, integrity or availability of digital assets" (p. 34).

In light of this brief overview on the conceptualisation of cyberattacks, different forms of cyber operations take place during cyber conflicts, which include activities like website vandalism, denials of service, and intrusions (Pytlak & Mitchell, 2016, p. 98), but also propaganda operations and manipulation of information infrastructure (Yasin, 2020). ENISA's 2022 Threat Landscape Report identified eight main cyber threats: ransomware, malware, social engineering threats, threats against data, threats against availability (Denial of Service and Internet threats), disinformation-misinformation, and supply-chain attacks (ENISA, 2022, p. 4). These cyber threats make up the majority of cyber events that take place around the world, whether for commercial or political motives. Instead, if we consider inter-state cyber warfare, Even and Siman-Tov mainly differentiate between three different kinds of activities that take place in cyberspace: espionage, soft cyber war, and cyber war (Even & Siman-Tov, 2012, p. 20).

Among the multitude of cyberattacks that comprise the arsenal of malicious cyber actors, cyber espionage represents a significant, if not the most important component of cyber warfare, since it is considered the necessary step preceding the delivery of cyberattacks during conflicts (Stiennon, 2015, p. 28). Defined as the "unauthorized

extraction of information from a computer system or network" (Libicki, 2021a, p. 66), cyber espionage can be divided into industrial espionage, involving businesses and enterprises, and state espionage, which concerns the collection of intelligence by state actors (ENISA, 2017), like in the case of the 2004 'Titan Rain' cyber operation against American military laboratories (Stiennon, 2015, p. 8). Espionage conducted in cyberspace represents the most common type of cyberactivity, and falls under the attack category of computer network exploitation (CNE), whereas degrade attacks fall under the computer network attacks (CNA) typology (Nye, 2017, p. 47) which, despite being less frequent than espionage activities, are more successful in achieving coercion (Foote et al., 2021, p. 56).

In between cyber espionage and cyber warfare we find 'Soft Cyber War', which Even and Siman-Tov (2012) have divided into 'Informational Message Warfare' and Sanctions. Starting with Informational Message Warfare, which will be analysed into more detailed in the following section, this kind of warfare's main element is the manipulation of information and it includes activities like "psychological warfare, fraud, propaganda, and disclosure of secret information", whose aim is to influence the enemy and its public to adopt a behaviour favourable to the interests of the attacker, without resorting to the physical use of force (Even & Siman-Tov, 2012, p. 22). As the expansion of the Internet was accompanied by an increase in the use of information warfare in cyberspace, public diplomacy rose in prominence as a way to contrast these operations by providing reliable information to both domestic and international audiences, meaning that informational message warfare takes place in the human layer of cyberspace, while other attacks target information at the logical or physical level (Even & Siman-Tov, 2012, pp. 22–23). The second element of soft cyber war are sanctions. Sanctions, defined as "cyberspace ostracism", represent a 'soft' operation used to coerce the enemy into altering its behaviour and to achieve some kind of deterrence against future inimical activity, with the added advantage of giving states a high level of impact with a low level of technical capabilities required (Even & Siman-Tov, 2012, p. 24).

While cyber network operations (CNO) that include espionage are not meant to deliver some kind of damage or destruction, CNA are destructive in nature (Siers, 2018, p. 558), which means that they fall under Even and Siman-Tov's third category of

cyberwar. Within this category of cyber-attacks we find cyber sabotage and disruption, more specifically, Distributed Denial of Service (DDoS) attacks, which are aimed at disrupting information systems' essential services (Yasin, 2020, p. 3). The methodology behind this type of attacks is to make websites crash by overflowing them with a wide array of hits taking place at the same time, therefore annihilating the websites ability to withstand the attack, as well as their ability to attribute the attack given the use of non-identifiable servers and hackers (Even & Siman-Tov, 2012, p. 27). The most notorious examples of large DDoS attacks include the operations in Estonia in 2007 and in Georgia in 2008 (Nye, 2017, p. 47). DDoS attacks are believed to violate state sovereignty without leading to physical destruction in the attacked state, however, because of the lack of certainty in attributing these damaging cyber operations to another state, denial of service attacks represent a widely legally unsettled phenomenon in international law (M. Schmitt, 2021, pp. 193–194). Indeed, when talking about inter-state cyber warfare, attribution is probably the greatest issue concerning cyber-attacks.

Attribution**,** defined as "the ability to hold a cyber actor responsible for a specific cyber operation or action" (Siers, 2018, p. 559), represents the most significant dilemma in cyberspace, especially for what concerns deterrence during cyber conflicts (Nye, 2017, pp. 49–50). Among the reasons that make attribution in cyberspace extremely complicated we find the widespread use of computers and networks, which can be easily turned into cyber weapons by anyone with a certain level of computer knowledge, and without the need to be physically located near the target. Furthermore, among the unique characteristics of cyberattacks we find that: cyber weapons do not leave physical traces and they can be easily hidden, the delay of cyberattacks' effects makes it hard to establish a relationship with a particular weapon, and, finally, the similarity with cyber espionage's *modus operandi* makes the latter harder to separate from cyber-attacks (Rowe, 2015, pp. 61–62). Given the ambiguity, asymmetry and anonymity of cyberattacks (Yasin, 2020), achieved through the use of elements such as encryption and proxies (Bindt et al., 2017, p. 12), activities in cyberspace are surrounded by a dense 'cyber fog of war' (Guyonneau & Le Dez, 2019, p. 108) that raises the level of doubt and uncertainty concerning the actions and intentions of entities operating in cyberspace (Libicki, 2021b, p. 19).

While different methods exist to establish attribution of files and network traffic, achieving attribution for states is much more complicated, since backtracking an attack to a device located in a state does not automatically attribute the cyber operation to that state (Rowe, 2015, p. 67). In addition, even when a state is found to be the source behind a cyber-attack, official attribution to a state raises technical, political, and legal issues concerning the consequences of establishing responsibility for cyberattacks (Steed, 2015, p. 84). Indeed, establishing credible and reliable attribution is necessary before responding to a cyber-attack (van der Meer, 2018, p. 7). However, both the attacker and the victim may have different strategical interests in failing to establish responsibility for cyberattacks, for instance, attribution of a cyberattack may not always be desirable because it would mean admitting to having suffered from a cyberattack, while distorting or hiding information presented to the public about cyber-attacks may constitute a form information warfare itself (Libicki, 2020, p. 80).

Adding to the uncertainty of cyberspace operations is the emergence of new threats, such as the Pegasus malware created by the Israeli NSO Group, consent phishing, data compromise, attacks on Machine Learning (ML) models, and AI-enabled disinformation and deepfakes (ENISA, 2022a, p. 5). In particular, the rise of Artificial Intelligence (AI) in Cyber Warfare has exacerbated the problem of attribution in cyberspace. This new technological development consists of different kinds of technologies that include machine learning, deep learning, and data analytics (Garon, 2018, p. 42), technologies which revolve around the processing of information, therefore making AI an important player for cyber warfare (Guyonneau & Le Dez, 2019, p. 104). Differently from the collective imagery of AI as a malicious entity taking over humanity, a belief also supported over the years by tech-billionaire Elon Musk, who claims that AI poses an "existential threat to human civilisation" (Gibbs, 2014; Metz & Schmidt, 2023; Sulleyman, 2017), evidence on the current development of AI demonstrates that it does not pose a threat to human society. Nonetheless, there have been international efforts by the AI epistemic community to establish a set of principles guiding the research and development of Artificial Intelligence called 'Asilomar AI Principles' (Garon, 2018, p. 48), therefore supporting the idea that AI can become a dangerous tool when its technology is used in an unregulated way.

Within the context of cyber warfare, Artificial Intelligence poses a significant threat to the integrity and confidentiality of information that resides in cyberspace, since military use of AI can enhance the ability of states to access and manipulate data (Goldfarb & Lindsay, 2022), making AI an enabler (Sweijs, 2018, p. 4), a tool capable of multiplying the effects of other technological developments and tools (Johnson, 2020, pp. 18–19). For this reason, AI can have a substantial impact on state security and international conflict, whether it is used to help the military to process information with the goal of achieving more clarity in cyber fog of war (Guyonneau & Le Dez, 2019), or if its technology is used to accelerate the speed of cyber conflict (Sweijs, 2018, p. 7). Consequently, it can be argued that Artificial Intelligence represents one of the main challenges in the future of cyber warfare; however, the impact of this technology still represents an uncharted territory, making further research on the subject an essential element for the study of the future of cyber warfare. Moving on, the next section of this chapter will focus on the phenomenon of Information Warfare within the context of cyber conflict, whose relevance stems from the acknowledgement that control over data and information represents a strong source of power in today's world (Guyonneau & Le Dez, 2019, p. 103).

1.3 Modern Information Warfare in Cyberspace

As it has been illustrated above, cyberwar takes place within the wider context of hybrid conflict, which combines elements of conventional and unconventional warfare. Among these we find different activities aimed at producing a distorting effect at the informational level, which include psychological warfare, disinformation, fake news, propaganda and influence operations (Kalathil, 2020). As a matter of fact, the weaponization of data has revealed itself to be an effective instrument in a society in which information is power, and governments around the world have also come to use this new strategy to pursue their interests, as it has been shown, for instance, by the information crisis produced by the COVID-19 pandemic (Kalathil, 2020, p. 33). Indeed, cyber and information warfare as elements of hybrid warfare have an important role in reducing states' employment of military forces (Abdyraeva, 2020, p. 21). One country in particular has found the

manipulation of information in cyberspace particularly fruitful for the achievement of both domestic and international political goals: unsurprisingly, this particular country is Russia and several of its attacks fall under the fuzzy category of information warfare (Nye Jr, 2017, p. 49). Given the relevance of Russia for what concerns the use of cyber-attacks and information operations, Chapter 3 will be dedicated to an in-depth analysis of Russian activities as a representative case study of this phenomenon, while the present section will focus on the role of Information Warfare (IW) in inter-state cyber warfare.

We have already touched upon the concept of information warfare in the previous section, with Even and Siman-Tov's categorisation of 'Informational Message War' as a form of soft-cyber warfare (Even & Siman-Tov, 2012, p. 22). Other authors see information warfare as one of the main elements of hybrid warfare, along with military use of force (Reichborn-Kjennerud & Cullen, 2016, pp. 3–4). While information warfare seems a relatively new phenomenon because of its increased relevance in today's cyber conflicts, the experts that first started looking into IW in the 1990s used the writings of the Chinese military general, and philosopher, Sun Tzu to support their claim on the primacy of information as an element of warfare (Libicki, 2021b, p. 15). Indeed, historians have confirmed that information warfare under the form of intelligence gathering, military deception (MILDEC) and information support operations was already waged by military leaders in the Eighteenth and Nineteenth century (Bastian, 2019, p. 31). For instance, Frederick the Great, King of Prussia, established a network of spies in the territory of the enemy to gather strategic information; however, as military theorist Carl von Clausewitz noted, even though the information gathered was often flawed or untruthful, its use was still highly valuable (Bastian, 2019, p. 32). Furthermore, while military leaders in the 18th century employed MILDEC to influence the adversary's perceptions by misleading the decision-making process of the target, army men of the 19th century, like French general Napoleon Bonaparte, also employed Military Information Support Operations (MISO), an additional form of activity aimed at exploiting information to manipulate the enemy's behaviour to the advantage of the attacker's interests, while he also adopted forms of Operation Security (OPSEC) to guarantee the integrity of sensitive information (Bastian, 2019, pp. 33-34).

However, despite the acknowledgment of the historical importance of the informational elements during conflicts, scholars have struggled to produce a standardized conceptualisation of information warfare (Libicki, 2021b, p. 15). Consequently, because information warfare entails a wide array of elements that involve information and communication, therefore adding to the ambiguous nature of activities in cyberspace (Foote et al., 2021, p. 55), it is important to provide a general definition of this activity. Keeping in mind the definition of information as facts and data and "the meaning that a human assigns to data" (Department of Defense, 2006), the 2006 Joint Publication (JP) 3-13 US Joint Chiefs of Staff defines 'Information Operations' (IO) as:

> "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." (Department of Defense, 2006).

As we can see from the definition above, Information Operations' main strategy is to distort or conceal information with the goal of influencing the enemy's behaviour or state to the advantage of the attackers interests (Hutchinson & Warren, 2001, p. 1). If we then look at cyber warfare, scholars have argued that manipulation of information takes places in the form of Cyber-enabled Information Operations (CIO): "*state-based actions, in the context of an ongoing cyber action, seeking to communicate a message or manipulate the reception of digital information for malicious purposes among a targeted population*" (Foote et al., 2021, p. 57). While information operations concerning data include denial of access, disruption and destruction and theft (Hutchinson & Warren, 2001, p. 3), disruption activities such as 'vandalism' are the most commonly employed methods during CIO, mainly through the use of propaganda, disinformation and psychological operations, tactics employed to influence behaviour (Foote et al., 2021, p. 60).

What differentiates the various information operations, all aimed at gaining the information advantage, are the methods and means used within the different activities, with

Psychological Operations focusing on the content of information (Libicki, 2021b, p. 15). Under the category of PYSOP we find propaganda operations, which can have far-reaching implications for the political and societal landscape of the attacked country, with some authors arguing that the effects of propaganda campaigns resemble those of traditional military activities because of the ability of such operations to influence the behavioural and cognitive patterns of the target (Abdyraeva, 2020, p. 21). Propaganda is a long-used tactic in warfare (Gomez, 2021, p. 133), but its potential has been enhanced by recent technological developments; in particular, the expansion of the Internet has created a global system of interconnections in which informational messages can be delivered to wide audiences in an almost instantaneous way, making new terms like 'computational propaganda' emerge in the literature (ENISA, 2022b, p. 6). Furthermore, thanks to the lower threshold of resources needed to operate in cyberspace, Internet-based propaganda can now be waged by a smaller state apparatus, therefore contributing to the asymmetry of modern-day hybrid conflicts, as well as the ambiguity of how to counteract persistent and non-lethal information operations (Libicki, 2021b, pp. 19–21).

In sum, what Miguel Alberto Gomez (2021) defines as Information Warfare / Information Operations (IWIO) does not represent a novelty in military activity, and cyber warfare, albeit creating some level of damage and disruption, does not surpass military force in terms of impact; instead, what is revolutionary about the employment of Information Operations in cyberspace is the latter's ability to intensify and expand cognitive mechanisms that make Internet users exposed to information manipulation (pp. 132-133). In fact, information campaigns seeking to raise disinformation and spread conspiracy theories operate in the cognitive sphere of hybrid warfare in cyberspace (Abdyraeva, 2020, p. 21). Research on human psychology has shown that human assimilation of new information into beliefs is reinforced by the association of emotions to such information; as a result, IWIO campaigns take advantage of topics that raise strong emotions in target audiences, in order to trigger in them a desired behaviour (Gomez, 2021, p. 134). For this reason, a few scholars have added a fourth layer to the structure of cyberspace previously analysed here, along with the physical, logical, and human layer: the cognitive or emotional level in the minds of audiences targeted with information in cyberspace (Gomez, 2021, p. 136). All these layers are interdependent and events at one

level can have a cascading effect on the other layers as well; in other words, cyber-enabled information operations can have significant impacts on the cognitive processes of the targeted audiences (Gomez, 2021, p. 136).

Among the tactics employed in IWIO we find propaganda campaigns, leak operations of classified information, whose goal is to erode the target's authority and reliability in the eyes of the audience, and "chaos producing operations" through misinformation (Gomez, 2021, pp. 137–138). Misinformation represents a serious threat in today's globalized society, since rapid sharing of information is allowing fake news and conspiracy theories to reach new audiences, therefore leading to a rise in social and political polarization in several countries around the world. For this reason, ENISA and the European Union External Action Service (EEAS) have tried to shed light on the threat posed by information manipulation in cyberspace by producing the 2022 report on "Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape". The report starts with the element of 'intent' to distinguish between misinformation and *disinformation*, where the latter is "*the intentional spread of false and/or misleading information for a specific purpose*" (ENISA, 2022b, p. 6). Because of the broad nature of this definition, the authors of the report propose their own conceptualisation of disinformation under the term FIMI, which is described as:

> *"a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory*." (ENISA, 2022b, p. 4)

ENISA's definition of FIMI stresses the role of the manipulation and interference elements of information operations, but, most importantly, the report also emphasises how hybrid threats involving information manipulation need to be combined with a cyber component in order to successfully achieve the desired goal (ENISA, 2022b, p. 7). Indeed, cyberattacks play a fundamental role in information operations at different levels. For what

concerns the content of information operations, cyber-tools are employed to obtain and use information for planned attacks, to develop content such as 'deep fakes', and to perform actions aimed at developing specific narratives; at the infrastructure level, cyberattacks can be used to acquire data for the dissemination of information, to create legitimate (fake) accounts while defaming existing reliable accounts, and to display false information on compromised websites, and finally, the cyber element comes into play during the dissemination phase, aimed at maximising the exposure of the information that has been manipulated (ENISA, 2022b, p. 22). It is at this stage that social media play a fundamental part as the main medium for the propagation of disinformation in cyberspace.

Social media platforms have witnessed a tremendous growth over the last years. Since social networking service Myspace reached one million users for the first time in 2004, in 2019 a third of the global population was using at least one social media platform daily (Ortiz-Espina, 2019). Today, the social networks with the largest number of registered users are Facebook (2,958 billion), YouTube (2,514 billion), WhatsApp (2 billion), Instagram (2 billion), WeChat (1,309 billion), TikTok (1,051 billion), and X, known until very recently as X, formerly Twitter (with "only" 556 million users compared to other platforms), of which Facebook, WhatsApp and Instagram are all owned by Mark Zuckerberg's tech company Meta (Dixon, 2023). As a result, because of the widespread digitalisation of the global population that began in the early 2000s, social media have become strategic resources in conflicts, and malicious activities taking place on these platforms have been defined as a sub-category of cyber warfare (Nissen, 2016). Thomas Elkjer Nissen (2016) argues that social media can be used for "military" activities in cyberspace, which include Intelligence gathering (thanks to the near-real time collection of information without the need of physical proximity to the target), coordination of targeting processes, Cyber Operations such as Cyber Network Exploitation (CNE), Cyber Network Attacks, and Cyber Network Defence (DNC), command and control operations for internal organisation and, finally, propaganda activities (pp. 190-195). In the context of military utilisation, social media platforms use for propaganda purposes has proven to be more successful than traditional channels of communication, mainly thanks to the amplifying effect of cross-media communication (Nissen, 2016, p. 194). As a result, in order to attain

the desired political objectives, social media platforms become the theatre of operations aimed at influencing behaviour through the manipulation of information.

Given their ability to deliver messages almost instantaneously to any user or platform that is connected to the global information environment, social media have become the best-suited platform to conduct Information Warfare and Influence Operations. As we have mentioned before, the main goal of IWIO is to influence populations' behaviour and erode the trust they have in their governments, and social media have enhanced the ability of malicious actors to take advantage of the interconnectedness of our society, making social media the "nexus of information operations and cyber warfare" (Prier, 2021, pp. 88–89). The distortion of information and messages on social media is made possible thanks to the presence of User Generated Content (UGC), which allows platform users to interact with the content they consume on a daily basis (Nissen, 2016, pp. 195–196), making it an essential element of social media-based propaganda operations.

An example of this process can be found on X (Twitter), where behaviour and interests are influenced by spreading a particular narrative through 'trending topics'. In practice, the operation starts from a core group of strong believers in a specific narrative; then, a team of cyber warriors and an army of 'bots' work to reproduce the propaganda message by flooding the feed of narrative outsiders; in turn, because of the 'echo chamber' phenomenon in which people tend to believe what aligns with their beliefs, as the message gets shared by more and more people, its content is gradually accepted as legitimate; as a result, since the original source has gained credibility, fake news finally enter mainstream media and the public is exposed to propaganda under the form of viral news reported on generally reliable and legitimate channels (Prier, 2021).

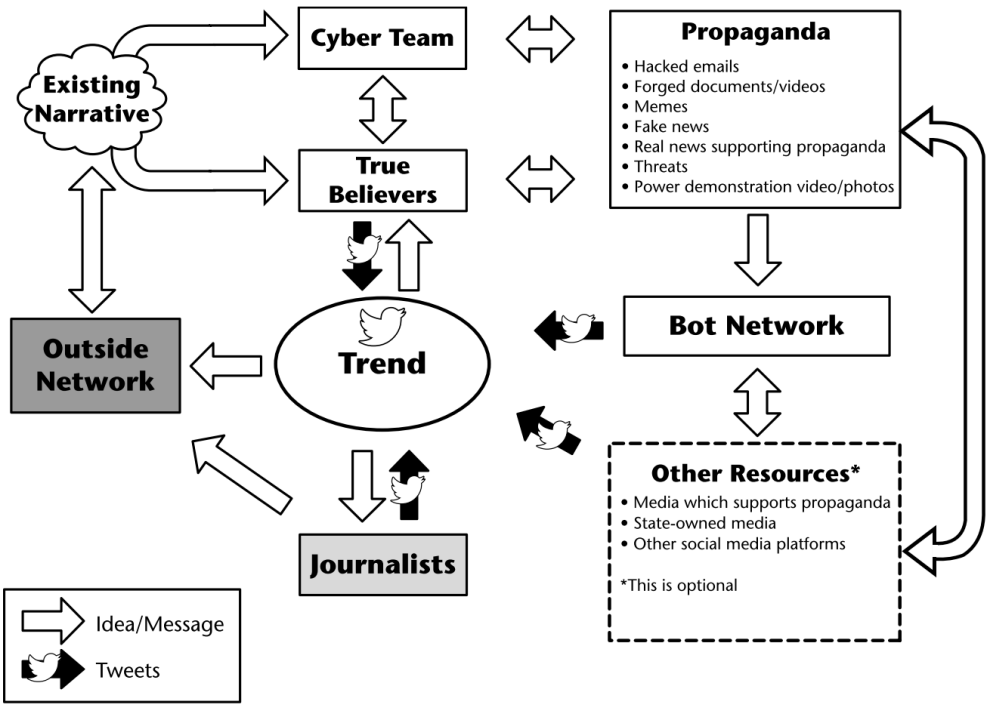

Figure 1 - Process Map of How Propaganda Spreads Via the Trend (Source: Prier, J. (2021). Commanding the Trend: Social Media as Information Warfare. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), Information Warfare in the Age of Cyber Conflict (pp. 88–113).

In sum, the cognitive processes that form human beliefs, so-called meaning-making processes, are the main target of cyber-enabled information operations on social media, given the latter's significant capability to disseminate content rapidly, easily, and globally while remaining anonymous (Bergh, 2020), therefore making social media the ideal medium through which to perform information operations in cyberspace.

2. European Cyber Regulation and Cyber Diplomacy

As cyberspace rapidly expanded, so did the opportunities it offered to private individuals and governments; however, safely operating in the digital domain requires a set of standard rules and guidelines that must apply to all actors involved. For this reason, over a short period of time the European Union (EU) has become engaged in the regulation of cyberspace activity, mainly as a way to guarantee that European businesses and citizens could enjoy the safe delivery of services and goods online. Yet, as cybercrime became more sophisticated and new kinds of cyberthreats harmed activities in the digital realm, the EU's attention began to shift from a purely internal market approach to cybersecurity to a more defence-centred policy framework, eventually leading to the development of initiatives aimed at strengthening the Union's international position against external cyberthreats through what is called cyber diplomacy. Cyber diplomacy exists in parallel with cybersecurity and cyber defence, but it is also inherently different. More specifically, while concepts related to cyberspace still lack unanimous consensus, the term 'cybersecurity' usually refers to "all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents" (ENISA, 2017), whereas 'cyber defence' has been defined as the employment of security measures to protect communication networks and common systems infrastructures against cyber-attacks (Cîrlig, 2014). Instead, the aim of cyber diplomacy is "to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace, and effective global digital governance" (Latici, 2020, p. 1) through the use of non-coercive and non-escalatory peaceful methods (Pawlak et al., 2020, p. 5), while digital diplomacy is more concerned with the development of policies regulating new technologies .

European cybersecurity witnessed a process of externalisation, which refers to the expansion of "institutionalised forms of joint representation or joint initiatives of the EU vis-à-vis external actors in the field of cybersecurity" (Miadzvetskaya & Wessel, 2022, p. 415), and its governance system is now centred around the Union's policy pillars, which

are Freedom Justice and Security (ASFJ), the Internal Market, the Common Security and Defence Policy (CSDP) (Backman, 2023, p. 87), as well as the Common Foreign and Security Policy (CFSP). Yet, it is important to mention that the legal authority to regulate on cybersecurity still lies with the Member States, with the EU having a coordinating role (Bendiek & Maat, 2019, p. 4). Despite the reluctance of Member States to devolve their competences to the Commission, the Union is expanding its role in cybersecurity governance through cyber diplomacy and is becoming an increasingly relevant cyber actor in the international arena, using its norm-setting power to enhance its digital sovereignty. In order to better understand the development of cyber regulation within the EU, which has been scarcely investigated by scholars until very recently (Backman, 2023, p. 87) this chapter will provide a concise overview of the evolution of European Cyber Regulation, followed by a section dedicated to the European Cyber Diplomacy strategy and the measures contained in the Cyber Diplomacy Toolbox, and it will conclude with a section that will look into the cyber diplomacy initiatives in which the Union is engaged, such as multilateral agreements, bilateral partnerships, and the implementation of sanctions, which have become a commonly used tool to influence behaviour in international affairs.

2.1 The Evolution of European Cyber Regulation

Like all countries deeply interconnected in today's globalized world, the Member States of the European Union have also given greater attention to the issue of cyber security and defence. However, it is crucial to remember that the EU was born as a purely economic organisation, striving to harmonize the economies of its Member States to bring peace and prosperity among them, and not as a security community like the North Atlantic Treaty Organisation (NATO) established in 1949. In fact, security and defence policies mainly remain prerogatives of the Member States, while it is within the Union's mandate to regulate the functioning of the internal market, the area in which the EU's 27 countries gave up most of their sovereignty. For this reason, it can be argued that cyberspace regulation at the European level was initially pushed by an internal market rationale: with the finalization of the internal market in 1985, the European Commission in Brussels decided to move the focus of the EU's policies and actions to the cyber domain, given the

important role played by information and communication technologies in the expanding digital market of goods and services (Bendiek & Maat, 2019, p. 5). As a result, the creation of a European digital market became the force behind the EU's development of regulations for cyberspace and cybersecurity, later leading to the launch of the EU's Digital Single Market Strategy in 2015, and eventually bringing cyber regulation in other policy domains under the Union's mandate (Bendiek & Maat, 2019, p. 4).

As the globalisation of digitalisation brought benefits for the world economy, the EU recognised that the expansion of the digital economy also entailed the emergence of threats to the correct and safe functioning of its internal market. Therefore, in order to ensure that cybersecurity regulation is enacted at the internal market level, the European Union Agency for Cybersecurity (ENISA) was established as the coordinating and governing body of European cybersecurity regulation (Bendiek & Maat, 2019, p. 9). ENISA was founded in 2004 by the *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency,* a temporary mandate that has been strengthened by additional EU Regulations (ENISA, n.d.), and its headquarters are located in Athens (Greece), with additional offices in Brussels (Belgium) and Heraklion (Greece). The main objectives of the Agency laid out in the founding regulation are four: first, "to enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems"; second, to "provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security"; third, to "develop a high level of expertise […] to stimulate broad cooperation between actors from the public and private sectors"; fourth, to "assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security" (Regulation 460/2004).

In July 2004, another European Agency was founded, the European Defence Agency (EDA) (European Defence Agency, n.d.), which regularly cooperates with other European entities working in the cyber realm, such as ENISA, Europol and the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU)

(Cyber Risk GmbH, n.d.-b). The creation of the Agency was pushed at the 2003 Thessaloniki European Council, and it was established through the formal adoption of the Joint Action by the European Council of Ministers on 12 July 2004 (Cyber Risk GmbH, n.d.-b). Located in Brussels, the role of EDA is to support and coordinate European defence projects and to provide a forum for European ministers of defence, mainly through the harmonisation of operational capabilities requirements, research and technological innovation, and training and exercises, therefore playing a key role in supporting the development of the Common Security and Defence Policy (CSDP) of the European Union (Directorate-General for Communication, n.d.). Indeed, the EDA represents one of the results of the Union's efforts to play a role in the mitigation of defence and security issues under the CSDP pillar, whose inception is linked to the signing of the Treaty of Brussels in 1948 by the United Kingdom, France and the Benelux countries (EEAS, 2021b), a project that was met with scarce political will until the signing of the Treaty of Lisbon (European Parliament, 2023a).

In fact, the Lisbon Treaty, signed at the European Council of Lisbon on 13 December 2007 and entered into force on 1st December 2009, represents a fundamental development for the Union's CSDP (European Parliament, 2023b). In practice, the Treaty amends the 'Treaty of the European Community', renaming it 'Treaty on the Functioning of the European Union' and making the 'Union' the legal successor of the 'Community', clarifying for the first time the competencies of the EU while giving the Union full legal personality. For what concerns its provisions, Article 49 (a) 1 under the Common Security and Defence Policy section states that:

> "*The common security and defence policy shall be an integral part of the common foreign and security policy. It shall provide the Union with an operational capacity drawing on civilian and military assets. The Union may use them on missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter. The performance of these tasks shall be undertaken using capabilities provided by the Member States*." (Treaty of Lisbon Amending the Treaty on European Union and the Treaty

Establishing the European Community, Signed at Lisbon, 13 December 2007, 2007)

In relation to the CSDP, the 2007 Treaty of Lisbon also includes a mutual assistance and solidarity clause, which sets out that the Union and its Member States are required to act jointly if a Member State is the victim of a terrorist attack, but also to prevent the terrorist threat and protect democratic institutions and the civilian population from terrorist attacks. Furthermore, Article 13 (a) 3 of the Treaty establishes the creation of the European External Action Service (EEAS), which functions as the diplomatic service of the European Union under the authority of the High Representative for Foreign Affairs and Security Policies, who also holds the roles of Vice President of the European Commission and of Chair of the Foreign Affairs Council.

In 2013, the High Representative, position held at the time by Catherine Ashton, proposed a Cyber Security Strategy (CSS) for the European Union, which consolidated the Union's cybersecurity approach by striving to develop a cyber defence policy framework under the Common Security and Defence Policy (Bendiek & Maat, 2019, p. 21). The Joint Communication laying out the Cyber Security Strategy, adopted in February 2013, acknowledges the importance of the cyber domain for the European society, and argues that European values must be protected both offline and online, values that include fundamental rights, democratic principles and the rule of law (European Commission, 2013, p. 2). In order to do so, the Joint Communication sets the following strategies: achieving cyber resilience through a multi-stakeholder public-private cooperation; reducing cybercrime by developing strong and effective legislation, and by improving operational capabilities and coordination at the EU level; developing cyber defence policy and capabilities under the CSDP framework; developing industrial and technological assets for cybersecurity through research and development investments; and establishing a coherent international cyberspace policy for the EU and promoting core EU values, mainly by mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy (European Commission, 2013).

In order to enact this framework, the Strategy envisions the sharing of responsibilities among national competent authorities and EU bodies as an effective way to strengthen cybersecurity. At the Network and Information Security level, the Cyber Security Strategy focuses on the role of ENISA, announcing a new Regulation to consolidate its mandate for the achievement of the cyber resilience aim, and on the work of the Computer Emergency Response Team (CERT-EU), established in 2012 with the task of guaranteeing the integrity of IT systems of the institutions, agencies and bodies of the EU. Furthermore, the document stresses the importance of European law enforcement cooperation, which includes: the European Police College (CEPOL), Eurojust, the European Union Agency for Criminal Justice Cooperation, and the European Cybercrime Centre (C3) set up in January 2013 by Europol, which is the EU's agency tasked with supporting Member States in the fight against crime, cybercrime and terrorism (Europol, 2023). The EC3 plays a fundamental role in cybercrime investigations and Member States have been organizing joint cybercrime action taskforce (J-CAT) within it, making law enforcement cooperation extremely effective in the fight against transnational cybercrime in the European digital market (Bendiek & Maat, 2019, p. 19). Finally, at the defence level, the European bodies involved with cybersecurity activities are the European External Action Service and the European Defence Agency.

The defence approach of the European Cyber Security Strategy was later included in the EU Cyber Defence Policy Framework adopted by the European Council on 28 November 2014, which lays the basis for the fight against cyberthreats by providing a framework to the earlier *European Council Conclusions on Common Security and Defence Policy (CSDP)* from December 2013 and the *Council Conclusions on CSDP* of November 2013 (Cyber Risk GmbH, n.d.-b). The December 2013 Council Conclusions represent the first time defence was discussed since the Lisbon Treaty came into effect, and its content was the result of a meeting with NATO-Secretary General (Cyber Risk GmbH, n.d.-b). Indeed, following the acknowledgement of the emergence of novel security threats, the December Conclusions of the European Council called for "an EU Cyber Defence Policy Framework in 2014, on the basis of a proposal by the High Representative, in cooperation with the Commission and the European Defence Agency" (Council of the European Union, 2013, p. 4), and it advocated for the development of "a roadmap and concrete projects

focused on training and exercises, improving civil/military cooperation on the basis of the EU Cybersecurity Strategy as well as the protection of assets in EU missions and operation", keeping in mind the fact that key capabilities for achieving these goals are under the control and management of Member States (Council of the European Union, 2013, p. 6).

As a result, the 2014 EU Cyber Defence Policy Framework, later updated in 2018, recognises cyberspace as a fifth domain of military action, crucial for the implementation of the Union's CSDP, and sets out the EU's cyber defence priorities (Council of the European Union, 2014a). First, supporting the development of Member States cyber defence capabilities related to CSDP through their cooperation with the EEAS and EDA; second, enhancing the protection of CSDP communication networks used by EU entities, with a significant role for CERT-EU as the main cyber incident response structure at the EU level and of EEAS for the development of IT security capabilities; third, promoting of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies, such as EDA, ENISA, and the EC3, as well as with the private sector; fourth, improving training, education and exercise opportunities through initiatives coordinated by EEAS together with EDA, European Security and Defence College (ESDC), and the Member States; fifth, enhancing cooperation with relevant international partners, particularly NATO, and increasing engagement under the framework of the Organisation for Security and Cooperation in European (OSCE) and the United Nations (UN).

In 2015, a *Report on the Implementation of the Cyber Defence Policy Framework* was released by the Politico-Military Group (PMG) of the Council of the EU. The Report acknowledged that since the implementation of the Cybersecurity Strategy in 2013, the European Union's Common Security and Defence Policy gave a higher level of attention to cyber defence, also due to the fact that cyber-attacks perpetrated by both state and non-state actors became increasingly common in several conflicts, like the hybrid warfare taking place in Ukraine in 2014 (Council of the European Union, 2015b). Looking at the results obtained in the cyber defence agenda, the Report notes the successful mainstreaming of cyber elements into strategic Common Security and Defence Policy

threat assessments, but also into CSDP missions and operations. At the same time, cybersecurity policy developments also took place in the EU's Area of Freedom, Security and Justice (ASFJ), more specifically for what concerns the Digital Single Market, which was presented as one of the top priorities by former President of the European Commission Jean-Claude Juncker (Bendiek & Maat, 2019, p. 17). Indeed, in 2015 the European Agenda on Security (EAS) was published by the Juncker Commission, which called for a deeper European cooperation as a way to counter cross-border threats like cybercrime, which constituted a significant threat for citizen's fundamental rights and the European economy, that was increasingly developing within the Digital Single Market (European Commission, 2015).

For what concerns the development of the regulatory approach to cybersecurity, the 2013 Cybersecurity Strategy was also accompanied by a proposal by the European Commission to the European Parliament and Council to strengthen the security of European information systems through a *Directive on a common high level of Network and Information Security (NIS) across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS* (European Commission, 2013, p. 7). This directive came into force in 2016, and it represented the first specific legislation of European cybersecurity (Vela, 2021). The NIS Directive focuses on the cooperation between Member States for the sharing of technical information between national CERTs as a way to strengthen the Union's cybersecurity, therefore creating the Computer Security Incident Response Team (CSIRT) Network at the European Union level (Directive (EU) 2016/ 1148), leading some to argue that this directive represents the first legislative cornerstone for a European cybersecurity (French National Cyber Security Agency, 2021). Furthermore, 2016 also saw the introduction of the 2016 Global Strategy for the European Union's Foreign and Security Policy by then High Representative Federica Mogherini, which stressed the importance of reinforcing the EU's capabilities in cybersecurity and strategic communications at the international level, by engaging in cyber diplomacy with relevant partners as a way to enhance the Union's resilience in the face of internal and external threats (Bendiek, 2016).

2017 saw the renewal of the Cybersecurity Strategy, which focused on expanding the EU's cyber approach to the internal market by focusing on building cyber resilience and cyber defence, reducing cybercrime, invest in technological capabilities, and produce a coherent cyberspace policy. All of these strategies seek to strengthen the EU's internal security, mainly through the development of resilience of essential services provided by the private sector, and of critical infrastructures (Bendiek & Maat, 2019, pp. 5-6). As a result, the European Commission issued the 2017 *Joint Communication on Resilience, Deterrence and Defence*, as a complementary document to the 2013 Cybersecurity Strategy (Pawlak, 2018, p. 106), with the aim of pursuing three main strategic objectives: building resilience to cyberattacks, creating effective cyber deterrence, and strengthening international cooperation on cybersecurity (European Commission, 2017). Furthermore, 2017 also witnessed an important development for European defence: in December 2017 the EU's Permanent Structure Cooperation (PESCO) was established by 25 defence ministers, with some of its projects directly linked to developing European cyber security (Bendiek, 2018, p. 4).

The EU's involvement in cybersecurity and defence further developed in more recent years through a series of key Acts and official documents, which gave increased attention to the role played by international cooperation in building an effective cybersecurity. In 2018, the European Union Cyber Defence Policy Framework was updated to expand and consolidate the EU's cyber defence structure, keeping in mind the separation of competences between the Member States and the Union's area of autonomous decision-making (Cyber Risk GmbH, n.d.-b). The Policy Framework includes six main priorities for fostering cyber defence: first, supporting the development of Member States' cyber defence capabilities; second, enhancing the protection of CSDP communication and information systems used by EU entities; third, promoting civil-military cooperation; fourth, investing in research and technology; fifth, improving education, training and exercises opportunities; sixth, enhancing cooperation with relevant international partners (Council of the European Union, 2018a).

In addition to cyber defence, the Union's attention also focused on the threat posed by the weaponization of online information, particularly as a consequence of the

disinformation activities during the 2016 presidential elections in the United States. As a result, in April 2018 the European Commission released the *Communication on Tackling Online Disinformation*, in response to the enormous of potential of social media in rapidly disseminating disinformation at a very large scale, which harms democratic institutions that are based on citizens freedom of expression (European Commission, 2018a). In order to counter these threats, the Communication published by the Commission proposed a Code of Practice on Disinformation in April 2018 (European Commission, 2022a), as well as the establishment of enhanced fact-checking capabilities and the development of education and media literacy in order to boost the resilience of the Union's democratic processes against cyberthreats (European Commission, 2018a). While the Code was signed by online platforms, tech and advertising companies, the Action Plan Against Disinformation released in December 2018 included an agreement between the Member States (European Commission, 2018c). In the same year, the Union has also made efforts to strengthen its data protection regime, by producing the "strongest privacy and security law in the world" (Council of the European Union, n.d.): adopted in 2016 and in force since May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) sets individual rights in cyberspace, establishes obligations for data controllers to implement appropriate security measures, and monitors the transfer of personal data to non-EU countries and international organisations (Council of the European Union, n.d.).

An important step towards a European wide cybersecurity framework came in 2019, with the adoption of the Cybersecurity Act through Regulation (EU) 2019/881 (European Parliament and Council of the European Union, 2019). The Cybersecurity Act strengthened ENISA, by granting a permanent mandate to the Agency and giving it additional resources and responsibilities; in particular, ENISA was given a key role in managing the European cybersecurity certification framework and in improving operational cooperation among EU member states (European Commission, 2023g). The creation of a cybersecurity certification framework at the EU level aims to enhance citizens' trust in the cyber domain (Cyber Risk GmbH, n.d.-b), while giving the Union a bigger voice in discussions around the setting of international norms for the security of ICT products (Bendiek & Maat, 2019, p. 13). Furthermore, in December 2020 the European Commission and the High Representative presented the new EU's Cybersecurity Strategy

for the Digital Decade, which aims to build cyber resilience and create safe digital technologies for citizens and businesses as a way to counter cyberthreats stemming from "geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain", like Artificial Intelligence, among others (European Commission, 2020b, p. 1).

In 2022 further actions have been taken by the Union to reinforce its cybersecurity structure. First, the NIS2 Directive (EU 2022/2555) replaced the 2016 NIS (EU 2016/1148), and it further improved the EU's cybersecurity at different levels, like creating the CyCLONe structure for cyber crisis management (French National Cyber Security Agency, 2021, p. 18), harmonizing security requirements, enhancing Member States collaboration while including different stakeholders from the societal and economic spectrum, all of this thanks to a strengthened role for ENISA (ENISA, 2023). In addition, one of the pivotal elements of European attempts at building cybersecurity has been the strengthening of cyber resilience of both the Union's institutions and those of its Member States, efforts that have materialised in the form of a proposal by the Commission for a European Cyber Resilience Act, which "aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network." (Car & Luca, 2023, p. 1). Among the most recent initiatives, the Commission also proposed the EU Cyber Solidarity Act in April 2023, which entails the creation of a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism as a way to reinforce the Union' cyber threats response activities (European Commission, 2023a).

The latest cybersecurity project for the EU is the Digital Europe Programme (DIGITAL), a first ever ambitious plan to invest €1.9 billion to build European cybersecurity capacity and improve the cybersecurity infrastructures and tools of the Union's institutions, private sector and individual citizens (European Commission, 2023b), as part of the long-term EU Multiannual Financial Framework budget for the period 2021-2027 (European Commission, 2023f). The inclusion of a digital security plan in the Union's long-term budget shows how cybersecurity will be at the top of the EU's agenda for the foreseeable future, with continued efforts to invest in the cybersecurity industry and

cybersecurity defence also included in the European Recovery Plan, given the emergence of a wider number of cyberthreats after the Covid-19 crisis moved many activities in cyberspace (Vela, 2021). Indeed, the Pandemic also demonstrated how, thanks to fast and groundbreaking technological developments, the world has transformed into an incredibly interconnected network of information systems in which borders have become almost irrelevant. Because cyberthreats do not stop at the outside border of the European Union, the Union has taken steps towards the externalisation of its cybersecurity efforts. For this reason, the next section will focus on cyber diplomacy, looking in particular at the EU's Cyber Diplomacy Toolbox as well as the Union's international cooperation activities for the creation of a global cybersecurity framework.

2.2 Cyber Diplomacy: The EU's External Approach to Cybersecurity

The European Union has always been involved in multilateral initiatives aimed at achieving a global, open and safe internet, like participating in the discussions of the United Nations Group of Governmental Experts (UNGGE) pushing for the adoption of the 2004 Budapest Convention on Cybercrime at the international level. However, UN GGE talks stopped in 2017 without having had any success in reaching a harmonisation of standards for Internet governance; instead, governments started taking different approaches, with countries like Russia forming the "Open-Ended Working Group" (Bendiek & Maat, 2019, p. 24). In turn, European countries provided a balancing force, by maintaining and developing bilateral talks with global counterparts like the United States, Canada, Japan, South Korea and others (Bendiek & Maat, 2019, p. 24). In other words, the European Union and its member states started moving from cyber defence to cyber diplomacy, a strategy seeking to de-escalate tension in the face of cyber-attacks which involves confidence-building measures (CBMs), as well as elements of "international norm building, data protection and freedom of expression, Internet Governance, and prosecution under international agreements for mutual legal assistance" (Bendiek, 2018, p. 2).

Cyber diplomacy started to appear on the policy agenda of the European Union around 2015, when the Council of the European Union released its *Council Conclusions*

on Cyber Diplomacy on 10 February 2015 (Bendiek, 2018, p. 5). The document was based on the remarks contained in the Commission's *Communication on Internet Policy and Governance* of December of 2014, which called for a sustainable Internet governance that involves all fundamental stakeholders, namely public institutions, private companies and individuals, and whose goal is to protect fundamental rights and democratic values through a single, cohesive multi-stakeholder framework (Council of the European Union, 2015a, p. 2). In turn, the Council Conclusions on Cyber Diplomacy recognized that Internet governance is "an integral part of the common and comprehensive EU approach of cyber diplomacy" (Council of the European Union, 2015a, p. 8). In particular, the Council called for the "development and implementation of a common and comprehensive EU approach for cyber diplomacy at global level", focusing on the protection of human rights and European fundamental values of democracy and rule of law while contributing to the "mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments" (Council of the European Union, 2015a, p. 4). Furthermore, the Council Conclusions stressed the "importance of cyber capacity building in third countries as a strategic building block of the evolving cyber diplomacy efforts" (Council of the European Union, 2015a, p. 9).

The Council Conclusions represent the basis for the Cyber Diplomacy Toolbox that was adopted in 2017, which was preceded by a paper on a joint EU diplomatic response to cyber operations presented by the EEAS and the European Commission on 14 March 2017. The Political and Security Committee (PSC) sent the paper for examination to the Horizontal Working Party on Cyber Issues (Cyber) (Cyber Risk GmbH, n.d.-a), a group set up in 2016 tasked with coordinating the European Council's activities on cyber issues with other parties like the European Commission, EEAS, Europol, Eurojust, FRA (European Union Agency for Fundamental Rights), EDA and ENISA (Council of the European Union, 2021). The PSC received the final text of the draft Council Conclusions on 6 June 2017, and on 19 June 2017 the European Council adopted the draft *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* ("Cyber Diplomacy Toolbox"), in which:

> "*The EU calls on the Member States, the European External Action Service (EEAS) and the Commission to give full effect to the development of a Framework for a joint EU diplomatic response to malicious cyber activities and reaffirms in this regard its commitment to continue the work on that Framework in cooperation with the Commission, EEAS and other relevant parties by putting in place implementing guidelines, including preparatory practices and communication procedures and to test them through appropriate exercises.*" (Council of the European Union, 2017a)

The Cyber Diplomacy Toolbox represents a fundamental element of the Union's approach to cybersecurity falling under the Common Foreign and Security Policy (CFSP) (Bendiek, 2018, p. 5), pillar that was shyly introduced in 1992 with the Maastricht Treaty and was later expanded with further amendments and revisions to the Treaty of the European Union (Bendiek & Maat, 2019, p. 21). Under the CFSP we find all foreign policy issues, with the exclusion of foreign trade, which is placed under the Common Commercial Policy. The European Council is the main actor operating in this Policy area, and its implementation is monitored by the High Representative and exercised by the European External Action Service (Bendiek & Maat, 2019, p. 24); yet, foreign policy still remain a policy area that is strongly protected by Member States wishing to retain their national sovereignty and authority in international affairs. Despite this reluctance to devolve responsibilities to the EU for what concerns foreign affairs, the European cyber diplomacy strategy materialised with the *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* of October 2017, under which the planned Cyber Diplomacy Toolbox was adopted (Bendiek, 2018, p. 5).

The Draft acknowledged the need for the EU to respond to malicious cyber activities that include attacks against "infrastructure, cyber-espionage, intellectual property theft, cybercrime or cyber conflict and disinformation using cyber means", which fall under the wider phenomenon of hybrid threats (Council of the European Union, 2017b, p. 2). The measures of the Framework can be employed as immediate responses to cyber incidents, as well as strategies aimed at encouraging cooperation, facilitating the mitigation of immediate and long-term threats, and influencing the behaviour of potential aggressors in

the long term (Council of the European Union, 2017b, p. 1). These measures are a kind of diplomatic, political and economic activities that act as prevention of or response to cyber-attacks that do not represent violations of international law, but still pose a threat to the security and stability of the Union and its Member States, given that such malicious cyber activities "originate from a State or non-state actor or transit through a States' territory, if that State knowingly allows its territory to be used for such activity or knowingly supports it" (Council of the European Union, 2017b, p. 5). In particular, five categories are used to differentiate between the types of measures included in the framework, which can be employed independently, sequentially or simultaneously as part of a coherent strategic approach: Preventive measures, Cooperative measures, stability measures, restrictive measures, and possible EU support to Member States' lawful responses (Council of the European Union, 2017b, p. 5). These measures are summed up in the table below.

1.	**Preventive Measures**	EU-supported Confidence Building Measures Awareness raising on EU policies EU cyber capacity building in third countries
2.	**Cooperative Measures**	Cooperation through EU-led political and thematic dialogues or through démarches by the EU Delegations
3.	**Stability Measures**	Statements by the High Representative and on behalf of the Council of the EU EU Council Conclusions Diplomatic Démarches by the EU Delegations

		Signalling through EU-led political and thematic dialogues
4.	**Restrictive Measures**	Sanctions (travel bans, arms embargo, freezing funds and economic resources)
5.	**Possible EU support to Member States' lawful responses**	Non-forcible and proportionate countermeasures Lawful use of force or an armed attack

Table 2 - Measures of the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (source: Council of the European Union. (2017). Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities)

First, the Framework includes the use of preventive measures to contrast cyber threats at the first category of activities. Under this category we find 'EU-supported Confidence Building Measures', whose goal is to enhance transparency, predictability, and stability (Council of the European Union, 2017b, p. 6). In particular, measures centred around prevention include cyber dialogues held by the EU seeking to influence the behaviour and attitude of third states and dialogue with counterparts (Bendiek, 2018, p. 6). CBMs represent an important strategy for the prevention of conflict, and the ones developed by the Organisation for Security and Co-operation in Europe (OSCE) are employed on a voluntary basis by the EU and its Member States in international and regional talks, therefore playing a significant role for the prevention and response to cyber-induced crises at the global level (Council of the European Union, 2017b, p. 6). Next, prevention is also achieved through 'Awareness raising on EU policies', which include dialogues informing other States of the EU's strategy on cybersecurity as a way to improve communication between states, and to reduce the rise of misperceptions and misunderstandings in the event of cyber-attacks that could be traced back to the territory of dialogue partners (Council of the European Union, 2017b, p. 6). Finally, prevention also takes the form of 'EU cyber capacity building in third countries'. These cyber capacity building efforts aim to further expand capabilities to investigate and prosecute cyber

criminals and to increase response capabilities in third states. Such measures include short-term elements to respond to immediate threats, like the Instrument contribution to Stability and Peace (IcSP), but also long-term mechanisms with the goal of strengthening cyber resilience and reducing cyber threats, such as the European Neighbourhood Instrument and other financing mechanisms (Council of the European Union, 2017b, p. 6).

Second, the Framework focuses on cooperative measures, which involves 'Cooperation through EU-led political and thematic dialogues or through démarches by the EU Delegations'. In practice, this mechanism is centred around the role of the European External Action Service: during an ongoing incident, the Union can send a diplomatic note through its delegations in order to signal the seriousness of the situation for the EU and its Member States to the host country's government (Council of the European Union, 2017b, p. 7). The transmission of diplomatic notes is performed under the instruction of the High Representative of the Union for Foreign Affairs and Security Policy, and it must follow the EEAS Guidelines for EU Political démarches (Council of the European Union, 2017b, p. 7). The establishment of EU-led political and thematic dialogues and the delivery of diplomatic notes by EU delegations are particularly useful in those instances in which establishing bilateral channels of communication with a particular third country is difficult, but the Union or some of its Member States still have a diplomatic dialogue (Council of the European Union, 2017b, p. 7). However, cooperative measures cannot be employed when EU delegations are recalled due to conflict (Bendiek, 2018, p. 6).

The third category of measures revolves around stability measures. One of these measures is the issuing of 'Statements by the High Representative and on behalf of the Council of the EU', which perform a signalling function for the potential aggressor, which is made aware, through the use of strategic communication, of the consequences that are likely to emerge from the perpetration of malicious cyber actions; in turn, the aim of these statements is to influence the behaviour of the aggressor and push him to refrain from conducting cyber-attacks (Council of the European Union, 2017b, p. 7). Four types of statements are set out in the EEAS Guidelines on Statements and Declarations: declarations by the High Representative on behalf of the EU; High Representative statements; Spokesperson statements; and local EU statements (Council of the European Union, 2017b,

p. 7). ‘EU Council Conclusions’ are also considered stability measures. Council conclusions, which can only be taken unanimously (Bendiek, 2018, p. 6) are used “to express a political position, to invite another EU institution to take action, or to prepare a proposal for coordinated Member States' action on a specific issue” (Council of the European Union, 2017b, p. 8). Furthermore, ‘Diplomatic démarches by the EU delegations’ or Member States that locally represent the EU can have a signalling effect without the burden of firm attribution (Council of the European Union, 2017b, p. 8). Just as in cooperative measures, stability mechanisms include ‘Signalling through EU-led political and thematic dialogues’: “The Member States / the Council can invite the EEAS and the Commission to raise a point in the relevant dialogues or exchanges with third countries and international organisations and multilateral bodies such as the UN, OSCE, NATO, WTO and G20” (Council of the European Union, 2017b, p. 8).

The fourth category of measures in the Cyber Diplomacy Framework are EU Restrictive measures: “The EU may impose restrictive measures against third countries, entities or individuals on the basis of a Council decision adopted under Article 29 TEU”, which allows the Council to adopt decisions defining matters of a geographical or thematic nature, and requires members states to conform to them, “coupled with a Council regulation setting out the necessary measures for its operation, adopted under Article 215 TFEU” (Council of the European Union, 2017b, p. 9). The imposition of restrictive measures must be performed in accordance with the guidelines on the implementation and evaluation of such measures, namely sanctions, contained in the framework of the European Common Foreign and Security, which also include travel bans, arms embargos, freezing of funds or economic resources (Council of the European Union, 2017b, p. 9). Sanctions must be targeted, either against government officials of third countries, or against state enterprises and other legal or natural entities, and they can be of two types: those decided unanimously by the Union and those whose compliance is imposed on the EU after the United Nations Security Council (UNSC) issues a resolution (Bendiek, 2018, p. 6).

Finally, the fifth category of measures concerns Possible EU Support to Member States’ lawful responses. According to the Framework, Member States, collectively or individually, can ask the Union to support them in delivering responses to malicious cyber

activities, being these responses legally sound from an intentional point of view, as well available within the CSFP (Council of the European Union, 2017b, p. 9). The responses taken by Member States as lawful measures against cyberthreats can be like the diplomatic mechanism mentioned in the previous categories or can make use of stronger individual or collective operations (Council of the European Union, 2017b, p. 9). Non-forcible, proportionate countermeasures can be taken against another State responsible for an internationally wrongful act in order to influence the given State to put an end to the malicious behaviour in cyberspace (Council of the European Union, 2017b, p. 9). In this case, Member States may call upon international law to exercise their right of individual or collective self-defence, either through Article 51 of the Charter of the United Nations, or through the mutual-assistance clause of Article 42 (7) of the Treaty of the European Union (Council of the European Union, 2017b, p. 10), which can be roughly equated to Article 5 of the NATO Treaty, or even through the solidarity clause of Article 222 of the Treaty on the Functioning of the European Union (Bendiek, 2018, pp. 6–7).

After the adoption of the 2017 Framework, further developments for European Cyber Diplomacy Toolbox took place. In 2019, the Council of the European Union adopted Council Decision (CFSP) 2019/797, and Council Regulation (EU) 2019/796 (Cyber Risk GmbH, n.d.-a). Following the Council Decision 2019/797 of 17 May (Council of the European Union, 2019a), the Council Regulation 2019/796 "establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States" (Council of the European Union, 2019b, p. 1). Article 3 (1) of the Regulation states that "All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen", which include natural or legal persons, entities or bodies that are: responsible for cyber-attacks; involved in activities in support for cyber-attacks, including planning, preparing, participating in, directing, assisting, encouraging, and facilitating them; and all those associated with the persons or entities responsible for and involved in cyber-attacks, which are defined by Article 1 (3) as "access to information systems, information system interference, data interference and data interception" (Council of the European Union, 2019b). In other words, the new regulation

strengthened the ability of the EU to impose sanctions against those actors threatening the Union and its Member States with cyber-attacks.

In the following years, European Digital Diplomacy was also given more attention, especially after the COVID-19 crisis increased the digitalisation of modern societies while making them more vulnerable to cyberattacks and the spread of disinformation in cyberspace. As a result, the Council Conclusions presented the 18 of July 2022 invited "the High Representative and the Commission, in close coordination with Member States, to ensure that Digital Diplomacy become a core component and an integral part of the EU external action, including by strengthening existing multilateral, regional and multi-stakeholder processes", and the Council also stressed the importance of the EU Digital Diplomacy for the strengthening and harmonisation of "EU external policies on digital, cyber and countering hybrid threats, including foreign information manipulation and interference" (Council of the European Union, 2022e, p. 2). In order to achieve these goals, the Council Conclusions called for the promotion of partnerships with third countries, while enhancing cooperation within the UN system, the G7, the OSCE, the OECD, the WTO, NATO, the Council of Europe and other multilateral fora (Council of the European Union, 2022c).

Finally, The Council Conclusions of 26 June 2023 represent the most recent development in the Union, and they further consolidate the EU's position on digital diplomacy and the fight against cyberthreats (Council of the European Union, 2023a). The 2023 Conclusions emerge in the context of the aggravation of the Russian invasion of Ukraine that started in 2022, as well as the rapid technological developments transforming the economy and society of the Union; therefore, the Council stressed "the need for a stronger, more strategic, coherent and effective EU policy and action in global digital affairs to confirm EU engagement and leadership" as a way to reinforce the EU's strategic independence and to protect its open economy (Council of the European Union, 2023b, p. 2). To do so, the Council lays out a set of priority actions for the development of digital diplomacy, based on the progress achieved with the implementation of the 2022 Council Conclusions mentioned above. First, the Council called on the High Representative, the European Commission, and the Member States to enhance cooperation with relevant

multilateral and stakeholder fora by improving coordination on cyber (Council of the European Union, 2023b, p. 4). Furthermore, building and fostering strategically important bilateral and regional partnerships through stronger cooperation represents another priority for the EU's approach to international digital issues, paving the way for the Union to become a leader and relevant partner in global technological development, as well as in digital governance and the setting of international standards, given that guaranteeing a cyber-secure digital public infrastructure and digital commons constitutes another priority for the Council (Council of the European Union, 2023b, p. 7). The Council also prioritised the need to strengthen cooperation in fighting foreign information manipulation and interference (FIMI), particularly disinformation disseminated by the Russia Federation as part of its hybrid campaign against Ukraine (Council of the European Union, 2023b, p. 9), an issue that will be analysed into more detail in the final section of this thesis.

2.3 The Application of the EU's Cyber and Digital Diplomacy

2.3.1 Multilateral Engagement

As part of the objectives outlined in the European Cyber Diplomacy, the Union is engaged in a series of multilateral initiatives aimed at supporting the United Nations Global Digital Compact, whose aim is to advance an "open, free, secure and human-centred digital future, one that is anchored in universal human rights and the attainment of the Sustainable Development Goals" (United Nations, 2023, p. 2). For instance, the report calls on Member States and regional organisations to follow the European GDPR for the implementation of legal protections for personal data and privacy (United Nations, 2023, p. 16). The EU also supports the work of the United Nations Secretary-General's Roadmap for Digital Cooperation, led by the Office of the Envoy on Technology (United Nations, n.d.); indeed, the European Union is one of the key constituents among the virtual participants for the Roundtable group on Global Connectivity, Digital Inclusion and Data, Digital Help Desks, Artificial Intelligence, and Digital Cooperation Architecture, whereas it is among the champions for Digital Human Rights (United Nations, 2020), demonstrating the Union's

norm-setting power as exporter of values. In sum, the EU's contribution to the UN Global Digital Compact's goal of building a free, open, secure and coherent Internet is centred around human rights and the fight against information manipulation and disinformation (Borrell, 2023), and it also focuses on the regulation of Artificial Intelligence and the protection of the Digital Commons through the establishment of transparency and accountability, much needed elements in order to achieve trusted connectivity (EEAS, 2023).

As part of its commitment to multilateralism, the European Union seeks to protect and reinforce Internet governance based on a multi-stakeholder approach aimed at avoiding the fragmentation of cyberspace. In addition, the EU recognises the fundamental role of the World Summit Forum on Information Society (WSIS), a two-phase summit initially held in Geneva in 2003 and in Tunis in 2005 (Internet Governance Forum, n.d.), in promoting digital as a key element in the achievement of the Sustainable Development Goals (SDG) of the UN 2030 Agenda (EEAS, 2023). The Union also sustains the work of the Internet Governance Forum (IGF), an independent and inclusive platform aimed at advocating for a free, open, and safe Internet that emerged as one of the major outcomes of the WSIS Tunis Agenda (Internet Governance Forum, n.d.). Furthermore, the EU also stresses the importance of the Internet Corporation for Assigned Names and Numbers (ICANN) and of the Internet Engineering Task Force (IETF) as bodies for the development of a multistakeholder model for Internet governance (EEAS, 2023).

In April 2022, together with the US and other international partners, the EU and all its Member States have endorsed a *Declaration for the future of the Internet*, which is strongly rooted in and influenced by the EU's *Declaration on Digital Rights and Principle* co-signed by the Presidents of the European Commission, the European Council and the European Parliament, therefore showing the common political will of the EU Member States in the protection of digital rights (European Commission, 2022b). Indeed, the EU is strongly committed to the promotion of human rights in cyberspace, which represents a core principle in the European Digital Agenda. In fact, the EU actively participates in UN platforms like the Human Rights Council, as well as bilateral diplomacy channels like the Human Rights Dialogues, to encourage all partner States to fight Internet shutdowns,

arbitrary or indiscriminate digital surveillance and violations of data privacy, and to safeguard human rights advocates online (EEAS, 2023). In addition to supporting the work of the office of the High Commissioner for Human Rights, the EU also actively supports several UN Resolutions concerning Human Rights & Digital issues, such as *New and emerging digital technologies and human rights*, *The promotion, protection and enjoyment of human rights on the Internet* and the *Right to privacy in the digital age* (EEAS, 2023).

2.3.2 Bilateral Engagement

Among its network of bilateral cooperation agreements, the EU is engaged in several Trade and Technology Councils, as well as bilateral Digital Partnerships. First, the EU-US Trade and Technology Council (EU-US TTC) represents the core element of transatlantic cooperation on international technology systems, as the European Union and the United States strong mutual commitments are based on shared democratic values (EEAS, 2023). After meeting for the fourth-ministerial level meeting of the TTC in Luleå, Sweden on 30-31 May 2023, the EU and the US successfully agreed on a Joint Roadmap for Trustworthy AI and risk management, cooperation in developing common standards for emerging technologies, a shared commitment in defending human rights and values, and combating foreign information manipulation and interference, and enhanced cooperation in increasing trade that is both sustainable and safer (European Commission, n.d.-a). The EU-India Trade ad Technology Council was also launched on 6 February 2023, following the announcement of 25 April 2020 by European Commission President Ursula Von der Leyen and Indian Prime Minister Narendra Modi, and this cooperation will focus on strategic issues such as trade, trusted technology and security, as well as research and innovation (European Commission, 2023d).

For what concerns Digital Partnerships, the EU is currently engaged with three like-minded partners, Japan, South Korea and Singapore, with the goal of solving the global digital divide (European Commission, 2023c). The EU-Japan Digital Partnership signed in May 2022 was the first digital partnership initiative, and it mainly focused on achieving a Secure 5G, safe and ethical applications of artificial intelligence, and the resilience of

global supply chains in the semiconductor industry, while striving for a human-centric digital transformation based on common values (EEAS, 2023). This partnership was then followed by the November 2022 EU-Republic of Korea Digital Partnership, in which the two parties agreed to centre their cooperation around semiconductors, next generation mobile networks, quantum and High-Performance Computing, Cybersecurity, Artificial Intelligence, platforms, data and skills (EEAS, 2023). The EU-Singapore Digital Partnership was launched on 1 February 2023 to further strengthen the EU's relationships with Asian countries, and it focused on the cooperation on semiconductors, trusted data flows and data innovation, digital trust, standards, digital trade facilitation, digital skills for workers, and the digital transformation of businesses and public services (EEAS, 2023). Overall, the aim of these partnerships is to foster cooperation between the Union and third countries that share the same values for the creation of a safe digital space.

In addition to bilateral partnerships, the EU has also focused on establishing initiatives fostering regional cooperation among partners and with the Union. Among these we find the EU-ASEAN initiative, adopted during the 23rd ASEAN-EU Ministerial Meeting on 1 December 2020, which is focused on fostering cooperation on Connectivity at the transport, energy, digital and human level, and stems from the strong trade relations between the EU and ASEAN (de Vega, 2022). Furthermore, the EU participated in digital cooperation as part of the *Joint Communication on Strategic Partnership* with the Gulf of May 2022, which underlines the Union's determination in supporting the Gulf's digitalisation by focusing on the digital transition, connectivity and innovation (European Commission, 2022c), and in 2018 the Commission launched the Digital Agenda for the Western Balkans, a shared commitment to invest in broadband connectivity, increasing cybersecurity trust and digitalization of industry, strengthening the digital economy and society, and boosting research and innovation (European Commission, 2018b). The EU4Digital Initiative represents the main regional programme supporting the development of the digital transformation and the harmonisation of digital markets in the Eastern Partnership's (EaP), mainly through the extension of the EU's Digital Single Market benefits to Eastern European partner countries (EU4Digital, n.d.). Additionally, the EU is engaged in fostering and supporting the digital transition through the New Agenda for the Mediterranean (European Commission, 2021), the Joint Declaration by the EU and Indo-

Pacific countries on privacy and the protection of personal data (EEAS, 2022), and in the EU-Africa Joint Vision for 2030 agreed at the 6th EU-AU Summit in February 2022 (Council of the European Union, 2022g). Another important platform for regional digital cooperation is the Digital for Development (D4D) Hub, which "promotes new international partnerships on digital transformation between the European Union and partner countries in Africa, Asia, Latin America, the Caribbean and EU Eastern Neighbourhood" (D4D Hub, n.d.), as well as the *Global Europe: Neighbourhood, Development and International Cooperation Instrument* (NDICI), with €6.38 billion allocated for geographic programmes aimed at fostering digitalisation (European Commission, n.d.-b).

Global Gateway Digital Projects are another initiative promoted by the EU to foster digital connectivity in specific countries and regions. As of 2023, the EU is engaged in flagships projects in Africa, Latin America, and the Caribbean (LAC), Asia and the Pacific, and the Western Balkans and EU Neighbourhood. The EU-Lac Digital alliance is the first intercontinental digital partnership under the Global Gateway project, with an initial budget of €145 million from Team Europe, a group consisting of the EU, its member states, the European Investment Bak and the European Bank for reconstruction and Development (EBRD) (European Commission, n.d.-c). Within this budget €50 million are allocated to strengthen digital cooperation between the EU and the LAC region (European Commission, 2023e). Furthermore, the EU-Africa Global Gateway Investment Package launched at the EU-African Summit 2022 focuses on digital transition, whereas the flagship projects will benefit the areas of the Asia-Pacific and the EU's Neighbourhood with new digital and technological infrastructure, such as new satellite connectivity and optical fibre cable, in particular for the Southern Neighbourhood and a cross-Black Sea cable to the Caucasus (EEAS, 2023). For what concerns country-level support, the Global Gateway will implement digital economic packages for infrastructure investments as part of the projects launched in Nigeria, Colombia and the Democratic Republic of Congo (EEAS, 2023). These national projects are particularly important since they come at a time in which countries like China and the Russian Federation are expanding their interests through investment projects in areas like the African continent and Latin America.

2.3.3 Sanctions

Among the five categories of measures contained in the Cyber Diplomacy Toolbox, it can be argued that restrictive measures, sanctions in particular, are the most widely used non-forcible tools to achieve some degree of deterrence in cyberspace. Indeed, as maintained by the 2017 *Joint Communication on resilience, Deterrence, and Defence,* a supporting document to the 2013 EU Cybersecurity strategy, cyber deterrence can be effective when credible measures able to influence potential aggressors are established (Pawlak, 2018, p. 106). In turn, pushed by its desire to adopt a stronger role in digital governance, the Union shifted from a softer 'naming-and-shaming' strategy, to a harder approach to malicious cyber activity (Colatin, n.d.), such as the imposition of concrete sanctions. Indeed, despite the efforts by the Commission in encouraging its Member States to openly attribute blame for cyber-attacks, public attribution still represents a serious dilemma for governments, and countries like Russia are not easily intimidated by reputational attacks (Supps, 2018). Therefore, the Council of the European Union adopted its 2019 sanctions regimes through the Council Decision (CSFP) 2019/797, as mentioned in the previous section, which introduced a legislation that allows the Union to specifically act against cyberthreats, making this development a crucial step in the consolidation of a European response to cyber-attacks (Botek, n.d.). As a result, for the first time ever, in 2020 the Council imposed restrictive measures in response to cyber-attacks, which included the attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons (OPCW), the WannaCry and NotPetya ransomware attacks, and the 'Operation Cloud Hopper' operations (Council of the European Union, 2020b).

The 2020 sanctions were imposed on the 30 of July against six individuals and three entities of Russian, Chinese and North Korean affiliation, while the restrictive measures applied include travel bans, freezing of assets and the prohibition for European individuals and entities to provide funding to said individuals and entities (Council of the European Union, 2020a). The imposition of sanctions in generally preceded by attribution of cyber-attacks, Annegret Bendiek and Matthias Schulze (2021) have analysed the technical, political, and legal steps of this process by investigating the cyber-attack that were subjected to the EU's sanctions regime of 2020. The WannaCry ransomware attack took

place on the 12 of May 2017 and while it only lasted a few days, it affected around 230,000 computers and generated damages for approximately four billion US dollars. The US and UK publicly attributed WannaCry to North Korea six months later, whereas the EU only condemned the attacks in April 2018, followed by the July 2020 targeted sanctions on the North Korean government front company Chosun Expo. Next, the NotPetya ransomware mainly targeted Ukrainian computer systems on the eve of its "Constitution Day", 27 June 2017, and it is argued to have been used as a tool for diplomatic pressure against Ukraine. In this case, political and legal attribution to Russia for the attacks was particularly hard, with sanctions imposed by the EU only in 2020, while a few Member States placed responsibility on the Russian state much earlier. For the 2016 Operation Cloud Hopper, the EU-imposed 2020 sanctions targeted two Chinese nationals and one Chinese company, while for what concerns the Wi-Fi spoofing attack against the OPCW, attribution to Russia was quite straightforward, and the European sanctions of 2020 targeted agents of the Russian military intelligence service.

However, despite the importance of targeted cyber-sanctions at the EU level, Bendiek and Schulze (2021) find that the imposition of sanctions against cyber attackers raises several issues. For instance, the process of attribution is a necessary and preliminary step for retaliation in cyberspace, yet, given that attributing cyber-attacks is considered a sovereign act, this procedure lacks coherence at the EU level, mainly due to the fact that the Union functions as a coordinating entity between the Member States' different technical and intelligence capabilities (Bendiek & Schulze, 2021, p. 5). Indeed, the attribution for the WannaCry and NotPetya attacks came years later after their deployment precisely because of the legal and technical challenges faced during attribution, including the scarce political will among EU member states to share nationally sourced sensitive information through the EU INTCEN (Bendiek & Schulze, 2021, p. 34). Furthermore, the EU and its member states heavily depend on information provided by third countries, like American IT companies and the Five Eyes intelligence alliance, composed by Australia, Canada, New Zealand, the United Kingdom, and the United States (Bendiek & Schulze, 2021, p. 34). As a result, because Member States attribute independently from each other, this fragmentation erodes the ability to retaliate against cyber-attacks credibly and legitimately through a united European front, making the imposition of sanctions a difficult process.

3. Russian Hybrid Warfare: Cyber Warfare and Information Manipulation

Ever since the Internet became the most prominent platform for communication of the 21st century, people around every corner of the world have had access to enormous amounts of information. While this development has brought many benefits to the daily lives of millions of people, the widespread reach of the digital sphere also gave new opportunities to different types of actors now entering this new and vast dimension to pursue their aims. Looking at the bright side of this phenomenon, some optimistically hoped that cyberspace and the telecommunications revolution would bring communities together to a point where waging war would gradually become a faint possibility, therefore fostering the growth of a democratic model based on freedom and rule of law around the world. Instead, cyberspace became a new place where people could operate, either to communicate or to commit digital versions of crime and other malicious activities.

In addition to cybercriminals, cyberspace has also empowered authoritarian regimes, allowing them to exploit new digital avenues to assert their control over their own populations through censorship and manipulation. Eventually, autocratic states started to export these methods abroad, making use of cyberspace activities to achieve their foreign affairs agenda. Among the main authoritarian states making use of these kinds of methods we find the Russian Federation, which represents a relevant case study of a country that uses cyberspace to achieve its agenda, both domestically and abroad, particularly through the delivery of cyber-attacks as well as information operations in the digital sphere. This chapter will start with an overview of Russian cyber capabilities and its history of information manipulation; then, it will look at the main Russian-sponsored cyber events that took place in Estonia (2007), Georgia (2008) and its meddling role in the US 2016 presidential elections. Finally, the third section will investigate Russian cyber activities in the Europe, looking in particular at the cases of Germany, the Brexit referendum of 2016 in the United Kingdom, and the leaks of personal documents of Emmanuel Macron's personal documents during the 2017 French presidential campaign.

3.1 The Russian Federation and Putin's Information Security

Like in other authoritarian countries, the government of the Russian Federation has a strong interest in securing its survival in the face of both internal and external threats. For Russia, these perceived threats mainly come Western democratic countries, especially the United States, with their attempts to infiltrate Russian culture and society in order to bring the system down from within. This fear of "foreign collusion with domestic enemies" is not new to Putin's regime, but has its origins in the inception of the Soviet Union itself (Samabaluk, 2022, p. 19). Indeed, regime sensitivity represents a point of continuity between the former USSR and today's Russian Federation, an element which has fuelled insecurity in both regimes, since the majority of Russian political officials in the early 2000s were formed and trained under the Soviet Union (Samabaluk, 2022, p. 5). As a result, post-Soviet Russia kept relying on its intelligence and secret service to control and influence its own population like the Russian governments did during the 20th century.

Even before the establishment of the Soviet Union, the Okhrana, the secret police of Tsar Nicholas II, was engaged in active operations to influence its population, for example through the publication of a false document that was supposed to represent some kind of proof of a Jewish plan for world domination, a 1903 publication called "The Protocols of the Elders of Zion" (Samabaluk, 2022, p. 3). Indeed, secret services and intelligence constituted a fundamental element of the state's operations to influence and monitor its own citizens, especially during the Soviet Union. Born in 1922, the Union of Soviet Socialist Republics made spy craft one of its key pillars for the functioning and survival of the regime, bringing security agents and officials to high levels of government. Mass repression was initially carried out by Vladimir Lenin's *Cheka*, 'Extraordinary Commission', whose role was to intimidate and silence marginalized communities that opposed the Soviet regime and were political enemies of the government (Shearer, 2006, p. 214), and its efforts were accompanied by the activities of the Committee for State Security, better known as the KGB. Internal power struggles within the KGB strongly influenced the political agenda of the Soviet regime, both directly and indirectly. After being placed under the direction of Yuri Andropov in 1967, the power of the KGB expanded enormously (Hanson, 2006, p. 299), and Andropov was later called to lead the country for

fifteen months in the 1980s, while after the collapse of the Soviet Union in 1991, Russian President Boris Yeltsin supported Yevgeny Primakov as his Prime Minister, who was previously the head of the Foreign Intelligence Service of the newly formed Russian Federation (Samabaluk, 2022, p. 4).

Vladimir Putin's rise to power represents a continuation of this strong relationship between the intelligence sector and the Russian government. Before becoming the most powerful man of Russia, Putin started his career within the intelligence services. Following his graduation in 1975, Putin started working for the KGB: he was initially assigned to foreign intelligence and was posted in the German Democratic Republic (DDR), a time during which he perfectioned the art of espionage; when he returned to Russia in 1989, Putin gradually rose to politically relevant positions thanks to his pragmatic approach and his 'doer' reputation, eventually becoming the head of the coordination of Russia's security and intelligence ministries (Herspring, 2009, pp. 152–153). Putin's turning point came on 9 August 1999 when Boris Yeltsin, after nominating and then rejecting two prime ministers coming from the Russian intelligence apparatus (Samabaluk, 2022, p. 26), appointed Putin as his prime minister as well as his designated successor, later making him acting president when Yeltsin resigned on December 31; on 26 March 2000 Putin won the presidential elections in the first round, becoming Russia's second elected president. Once in charge, influenced by its KGB background, Putin set himself to build a strong and coherent government to face the social and economic chaos that plagued post-Soviet Russia, but like his predecessors before him, his governance was based on a strategy that included a subservient society that could bend under the state's autocratic direction (Herspring, 2009, p. 156). Furthermore, his approach to foreign policy was deeply marked by his desire to rebuild Russia's status as a superpower that had to be accepted by the other great powers, but at the same time without acquiescing to the political model of Western democracies (Herspring, 2009), therefore leading him to condemn the unipolar world at the 2007 Munich Security Conference (Snegovaya, 2015, p. 9), and to advocate for a less normative, new multipolar order to contrast US hegemony in the post-Cold War international arena (Berkofsky, 2014, p. 118) and to fill Russia's international security 'gap' (Samabaluk, 2022, p. 2).

We can argue that President Putin shows a certain level of continuity in his approach to state governance, particularly when it comes to the control of society; in fact, he has shown a very aggressive approach towards domestic instability and the role of foreign sponsors in endorsing internal change (Samabaluk, 2022, p. 27), as shown by the legislation passed to restrict the work of Non-Governmental Organisations (NGOs) funded by foreign countries (Samabaluk, 2022, p. 51), which he blamed for the 'Colour Revolutions' taking place in former USSR republics (Horvath, 2011). However, differently from the Cold War era, Putin has certainly strengthened state surveillance and manipulation in ways that surpassed Soviet propaganda and repression, and this is mainly due to the technological developments of the 21st century. Thanks to the fragmented nature of the Internet, it is now easier to spread disinformation, and Russian authorities have learned how to disseminate chaos through so-called Digital Influence Operations, which encompass "digital activity most commonly employed by authoritarian regimes internationally to manipulate, censor, and degrade the integrity of the information space for strategic purposes" (Kalathil, 2020, p. 34). These operations are particularly effective in the today's world, where the deep polarization of modern societies makes the media less trustworthy in the eyes of a growing number of people, who then become vulnerable to the spread of disinformation and propaganda, particularly in cyber space (Kalathil, 2020, p. 36).

During the Cold War year, information was already at the centre of conflict, with the Soviet Union producing conspiracy theories to harm the reputation and international standing of its rivals, for instance with the circulation of false narratives against the United States that concerned the Kennedy Assassination and the AIDS epidemic of the 1980s (Samabaluk, 2022, pp. 20–21), and its importance remained prominent also during Putin's government, bringing information to the centre of its political agenda through the Information Security Doctrine of 2000, the first of its kind for Russia. This document conveys the idea of information as an incredibly dangerous weapon (Klimburg, 2014, p. 3) and argues that the "information security of the Russian Federation is understood as the state of protection of its national interests in the information sphere, determined by the totality of balanced interests of the individual, society and the state", and the national interests is composed of four elements: first, the protection of constitutional rights and freedoms, as well as traditions of patriotism and humanism, and ensuring the spiritual

renewal of Russia; second, the delivery of trustworthy information about Russian state policy to both Russian and international audiences; third, the development of modern information technologies, the domestic information industry, and the safe and effective use of domestic information resources, while also pushing Russia to "take its rightful place among the world leaders in the microelectronics and computer industries"; fourth, "the protection of information resources from unauthorized access, ensuring the security of information and telecommunication systems, both already deployed and being created on the territory of Russia" (Doctrine of Information Security of the Russian Federation, 2000).

The Doctrine also focuses on the threats to the information security of the Russian Federation, which mainly originate from the activities of "foreign political, economic, military, intelligence and information structures" and also stem from "the desire of a number of countries to dominate and infringe on Russia's interests in the global information space" (Doctrine of Information Security of the Russian Federation, 2000). The document also lists a large number of menaces to the national interest and stability of the state which include "violation of the constitutional rights and freedoms of man and citizen in the field of mass media", "the displacement of Russian news agencies, the media from the domestic information market and the increased dependence of the spiritual, economic and political spheres of Russian public life on foreign information structure", "devaluation of spiritual values, propaganda of samples of mass culture based on the cult of violence, on spiritual and moral values that contradict the values accepted in Russian society", "manipulation of information (misinformation, concealment or distortion of information)", and a wide array of "threats to the security of information and telecommunications facilities and systems", such as: illegal collection and use of information, violations of information processing technologies, introduction of non-compatible hardware and software products, development and distributions of malware, destruction and damage of means and systems for processing information, compromission of keys and means of cryptographic protection of information, the leakage of information and the "use of non-certified domestic and foreign information technologies, information security tools, informatization tools, telecommunications and communications in the creation and development of the Russian information infrastructure", among others (Doctrine of Information Security of the Russian Federation, 2000).

As it become clear from this Doctrine, Russia's conception of information security differs from the conceptualisation adopted by Western countries, which usually encompasses the "confidentiality, integrity, and availability of systems, networks, and data" (Wilde & Sherman, 2023, p. 7), as we have mentioned in the previous chapters. Instead, Russian officials see information security as the control of cyberspace activities that include Western conceptualisation of freedom of speech and freedom of opinion (Samabaluk, 2022, p. 11). Furthermore, Putin's conception of information security is strongly characterized by the paranoia triggered by the idea that foreign entities are using the information space as a weapon against the stability of the regime at home and abroad (Wilde & Sherman, 2023, p. 6). This belief was also included in other documents and policy frameworks released by the President, such as the 2000 Foreign Policy Concept's focus on the dangers posed by external information dependence, and the 2000 Military Doctrine of the Russian Federation, which mentioned the threat of foreign information warfare to domestic stability of the state (Wilde & Sherman, 2023, pp. 7–8). In sum, these documents help us to better understand Putin's vision of Russia's national interests, internal security and state power, whose protection and consolidation depend on the domination of information and communication technologies to control the domestic information landscape, therefore bringing Russian officials to gradually pay more attention to the Internet and cyberspace (Wilde & Sherman, 2023).

As the discourse on information security was mainstreamed into different policy agendas, this new narrative also triggered some institutional reforms that started in the early 2000s. Among the military and security agencies engaged in information security we find the GRITs unit of the General Staff Main Directorate (GRU); the Russian Foreign Intelligence Service (SVR), which is the successor to the KGB First Chief Directorate; the Russian military's Information Operations Troops (VIO); and the Federal Security Service (FSB), the KGB's successor (Wilde & Sherman, 2023, p. 9). All these agencies and their units are tasked with delivering psychological, disinformation and influence operations domestically as well as abroad, especially the FSB. The Russian Federal Security Service's main activities include digital information manipulation abroad, and in 2002 its cyber intelligence department was transformed into the 'Information Security Centre' (ISC), previously named Directorate of Computer and Information Security (UKIB) (Soldatov &

Borogan, 2018, p. 17). This institutional reshuffling shows how the Russian state combined cyberwarfare with information security, and for Russia its main actors in cyberspace included the ISC as well as the Federal Agency for Government Communication and Information (FAPSI), which is the Russian electronic intelligence agency that was later brought under the FSB in 2003 (Soldatov & Borogan, 2018, p. 17).

Despite these new developments in information security, Russia had been lagging behind in terms of investments in information technology and emphasis on the role of the internet; while China managed to build the 'Great Firewall' to isolate and control domestic internet, Russia's RuNet, born out of the 2008 strategies adopted by Moscow to assert its dominance of the domestic information space and to monitor its population, cannot compete in term of effectiveness and sophistication (Wilde & Sherman, 2023). The turning point in Russia's interest in the internet came in 2008, when the Arab Spring showed the threat posed by social media movements to autocratic regimes and the Russo-Georgian war of 2008, one of the colour revolutions that emerged in the former states of the Soviet Union (Soldatov & Borogan, 2018, p. 17; Wilde & Sherman, 2023, p. 12). Among the most relevant developments in terms of information security we find the internet restrictions introduced in 2012, together with the surveillance of online traffic performed by the System of Operational-Investigative Measures (SORM), the 2016 Information Security Doctrine updating the 2000 doctrine, which stressed the importance of developing information technology capacities in the context of military activities, while in 2021 the National Security Strategy included foreign tech companies as Moscow's enemies in information warfare (Wilde & Sherman, 2023).

As information security increasingly became interconnected to information and communication technologies, cyberspace rose as a prominent component of the Kremlin's foreign policy and military strategies. In fact, Russian foreign policy entails aggressive cyber elements, including denial-of-service attacks, leaking of intercepted information, trolling international media, hacking and attacking foreign critical infrastructure, and interfering in foreign institutional and social processes through disinformation and influence campaigns, making the distinction between external and internal activities increasingly blurred (Soldatov & Borogan, 2018, pp. 19–20). As a result, the Kremlin's

much sought information security is achieved through a wide array of activities, ranging from cyber-attacks to foreign information manipulation, all of which form part of Russia's "hybrid warfare" against those domestic and foreign threats that put the legitimacy of the government in danger and threaten the internal stability of the Federation (Samabaluk, 2022, p. 29). In turn, the Russian secret and military agencies have been engaged in disinformation operations as a way to exert their control at the domestic and international level, mainly "flooding the information space with false or misleading narratives designed to crowd out independent voices and expertise" (Kalathil, 2020, p. 33). In other words, Putin understood that the Internet is a double-edged sword: it can represent an information security threat to his regime while it can also be used as a weapon against internal and external enemies, and whose potential in terms of impact has been multiplied by the rise of social media (Samabaluk, 2022, p. 41).

The Russian entity that is most deeply involved in information active measures is the Internet Research Agency (IRA), established in 2013 and run by Putin's former ally Yevgeniy Prigozhin (Wilde & Sherman, 2023, p. 9), formerly known as "Putin's chef" and as leader of the para-military Wagner Group (Sevchenko, 2023), he was recently killed in a plane crash on August 23, 2023 (Kassam & Sabbagh, 2023). The IRA was initially established to influence domestic discourse inside Russia, but its activities started to move outside of the country, from the near-abroad region to Western democratic states; indeed, the IRA has been accused of meddling in the United States 2016 presidential elections, mainly through digital influence operations on social media platform like X (Twitter) (Kalathil, 2020, pp. 36–37). While the IRA has been called a 'Troll Farm', Russian-sponsored online trolling activity, defined as "the practice of malicious pontificating or harassment via social media" (Samabaluk, 2022, p. 44), started a few years before the establishment of the Agency. In 2009 the Kremlin instituted a "school of bloggers": through the employment of economically marginalized individuals to troll the regime's opponents, Moscow was able to weaponize social media, and this troll army was later deployed through the IRA at a much larger scale (Samabaluk, 2022, pp. 44–45). As it has been briefly mentioned in the first chapter, social media platforms represent the ideal environment in which to disseminate information thanks to a networking process built on connection and

engagement with viral content, which gains credibility and legitimacy as it is shared and consumed by users at exponential rates.

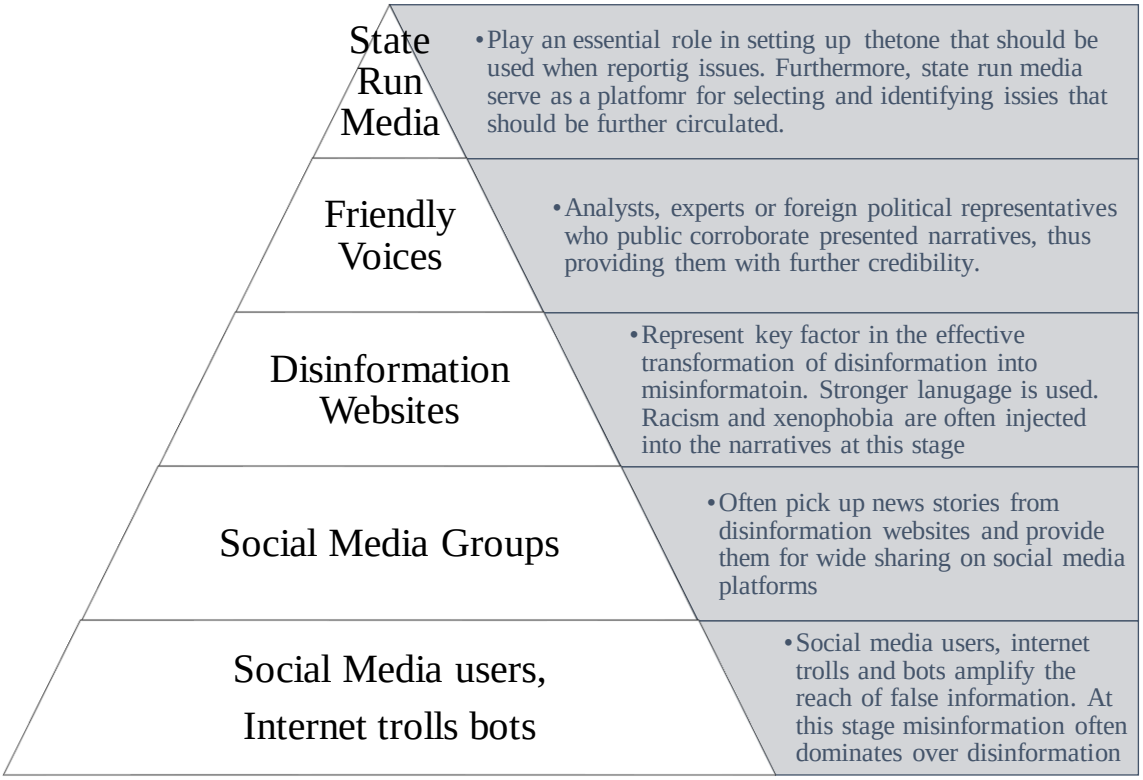

Figure 2 - Disinformation Amplification Pyramid (source : Bokša, M. (2019). RUSSIAN INFORMATION WARFARE IN CENTRAL AND EASTERN EUROPE: STRATEGIES, IMPACT, COUNTERMEASURES. https://www.jstor.org/stable/resrep21238)

In addition to trolls, since the early 2000s Russia has also become a major host of cyber criminals. After the fall of the Soviet Union, the STEM-trained professionals of the USSR (which include science, technology, engineering and mathematics experts) were left with no jobs to fill due to the lack of infrastructure in the post-Soviet regime; as a result, due to the high levels of criminality that were present during the economic hardships witnessed by 1990s Russia, these professionals turned to computer crime to make a living out of their IT knowledge and skills (Samabaluk, 2022, pp. 56–57). A prominent example of Russia's connection to cyber criminality is the Russian Business Network (RBN) established in 2006, which contributed to 60% of the world's cybercrime a year after its creation, and profited from the protection of cyber criminals until it was closed down in 2008 (Samabaluk, 2022, pp. 58–59). In order to preserve its national interest, Moscow found a way to exploit cybercrime originating from Russia that is directed at foreign

(enemy) countries: the regime tracked all cybercriminal activities and built dossiers on them, and when the state needed to employ hackers and online activists, Moscow would threaten to prosecute them if they did not comply with the state's requests, therefore, building a cyber army by enforcing the law in a way that suited Russia's interests rather than the rule of law (Samabaluk, 2022, pp. 60–61). The practice of employing cyber criminals to perform cyber operations has become a standing practice in Moscow's hybrid warfare, which was already in use during DDoS attacks on rebel Chechen websites by pro-governments hackers in the early 2000s (Samabaluk, 2022, p. 92).

The use of cyber proxies further exacerbates the attribution problem that characterises cyber activities, therefore making retaliation activities, like 'naming and shaming' and sanctions, ineffective, with the added risk of attribution to a state backfiring. In the case of Russia, whose cyber operations are carefully delivered in a way that guarantees its actors and trolls a certain degree of plausible deniability, being accused of cyber-activity it technically did not commit strengthens Putin's claims, directed mainly at domestic audiences, of being a victim of Western bullying attempts (Samabaluk, 2022, pp. 65–66). In turn, playing the victim becomes a key strategy for Russia's information warfare centred around the spread of anti-Western, particularly anti-American, sentiments at the domestic and global level. Cyber-attacks attribution is also made more difficult by the institutional competition for resources and power between military intelligence (GRU) and the security services (FSB), which have employed their Advanced Persistent Threats (APT), "Fancy Bear" (APT28) by the former and "Cozy Bear" (APT29) by the latter, to target critical infrastructure in different countries, particularly the media, telecommunication and energy sectors (Samabaluk, 2022, pp. 67–69). Indeed, Russia has also been accused of waging cyber-attacks as part of its hybrid warfare campaigns, but as the Internet expanded the potential information operations, Russia shifted its operations in the cyber realm to information operations (Libicki, 2021a, p. 697) which, unlike the short-term effects of cyber-attack, are able to transform and manipulate behaviour of the enemy in the long term (Abdyraeva, 2020, p. 21).

In fact, as Russia's cyber strategy has transformed into the dissemination of propaganda through the Internet and online platforms, the Russian government and other

Russian state institutions also started to use the Internet to communicate the official policy of the Kremlin, through Moscow's own brand of 'Digital Diplomacy'. Announced by the Ministry of Foreign Affairs (MFA) in 2012, Russia's digital diplomacy consisted in "government-sponsored dissemination of the country's political stance via social networks", and it represented the more official version of the work of Russian media agencies, like *Russia Today* (RT), on social media platforms like Twitter (now called X), therefore being referred to as "*twiplomacy*", which stands for Twitter diplomacy (Tsvetkova, 2020, p. 103). Digital diplomacy represents a case of the Kremlin employing what Jospeh Nye calls 'soft power', in order to achieve its geopolitical objectives, as supported by the increase in international media operations, made possible through significant investments on news agency like Russia Today, Moscow's main English-language broadcaster (Lexmann, 2017, pp. 42–43). Official communication channels employed in Russia's official digital diplomacy efforts, either through the government institutions own social media accounts or state-sponsored media outlets, represent a supporting element to the more clandestine cyber and information operations that Moscow has been directing behind the scenes, which will be analysed in the following section.

3.2 Russian Hybrid Warfare in Action

As mentioned above, Russia has adopted a hybrid warfare strategy as a way to achieve its national security interests abroad and, in order to protect its information security, the Kremlin's approach to cyber operations has shifted towards so called Cyber-Enabled Information Operations (CIO), which represent the combination of cyber activities with information manipulation, as illustrated in Chapter 1 of this thesis. In fact, Russia has emerged as the dominant actor in the international arena for what concerns the employment of CIO, which are described as "state level efforts to manipulate data for coercive purposes or those operations seeking to utilize compromised information to send specific messages to the adversary" (Foote et al., 2021, p. 57) and they generally take place in the context of ongoing cyber operations. Overall, Moscow's cyber activities have evolved over time, starting with the employment of cyber-attacks by proxies and outsourced hacktivists, as well as cyber-espionage operations like the *Moonlight Maze* case of state-on-state

computer intrusion (Rid & Buchanan, 2015, p. 12), and going to current foreign information manipulation and interference activities in cyberspace. In order to better understand Russia's wide approach to the use of cyber elements in its hybrid warfare operations, this section will look into a series of case studies of cyber operations that have been attributed to Russia, beginning with the cases of Estonia in 2007 and Georgia in 2008, and then moving on to the case of Russian influence operations of the 2016 US presidential elections.

3.2.1 Estonia (2007)

The cyber-attack that hit Estonia in April 2007, which has also been called 'Web War 1' or even the 'Estonian Cyberwar' of 2007, represents one of the most devastating cyber-attacks ever registered by a state. As it has been illustrated by Danny Steed in his overview of the attack, Estonia's high levels of connectivity, granting it the name of "E-stonia" (Samabaluk, 2022, p. 77), represented by the adoption of electronic means for voting, government, banking, identifications systems and taxes, made the country extremely vulnerable to malicious cyber activities (Steed, 2015, pp. 77–79). The attacks that were launched against Estonia took place over a period of three weeks and they coincided with a particular moment linked to the country's Soviet legacy. Indeed, April 2007 raised the tension between Estonia and Russia due to the plan by Estonian officials to move a Second World War memorial, celebrating Soviet Russia's victory over the Nazis in the country, from the centre of the Tallin to the city outskirts. The Kremlin, as well as Russian-speaking people in Estonia, were not pleased with this announcement, since for Russia this type of behaviour represented a threat to Russian cultural heritage items, as noted in the 2000 Information Security Doctrine (Samabaluk, 2022, p. 33).

Indeed, the bronze statue of the Unknown Soldier, as it was called by the Soviets, represented the Red Army's victory over the German occupation of the city, therefore it had a highly symbolic value; instead, Estonians referred to the Statue as the 'Unknown Rapist', symbolizing the hardship and brutality of years of Soviet rule following 1945 (Samabaluk, 2022, p. 76). An Estonian petition from 2006 had already been put forward to

destroy the memorial, but it was rejected by the then Estonian president due to the potential tensions that would emerge; however, in 2007 the new Prime Minister of Estonia started the procedure to relocate the statue on April 27, and by the 28 of April the memorial had been removed; as a result, both the Russian Government and the Russian-speaking Estonians felt attacked by this decision, and the Russian media coverage of the events further inflamed the debate (Steed, 2015). Russia's abrupt reaction was not solely caused by the decision to remove the statue, but it rather originated from Estonia's behaviour in international affairs. In fact, Estonia's Cold War years were marked by a strong aversion towards its membership in the Warsaw Pact and, following its independence, Estonia attempted to strengthen its ties with the Western world, eventually joining NATO in 2004, an event that was negatively perceived by Russia (Samabaluk, 2022, p. 77).

A series of coordinated cyber-attacks in the form of Distributed Denial of Service (DDoS) attacks were launched against Estonia's Domain Name Servers (DNS) on the night of 27 April, and the attacks increased in sophistication until a series of botnet assaults were launched on 20 April; the mechanism behind DDoS is to "crowd websites with ostensibly legitimate traffic to the point that the website temporarily collapses because it is overwhelmed with traffic", and the targets of the attacks ranged from public institutions' firewalls and servers, such as the websites of government departments, the Estonian national parliament, newspapers, broadcasters and banks (Samabaluk, 2022, p. 77). It has been calculated that approximately 85,000 computers were behind the cyber assaults that lasted for almost three weeks, and a quarter of the attacking devices were composed of bots based in the United States, where the owners of the machines were completely unaware of the attacks being launched by third parties to the other side of the world through their computers (Samabaluk, 2022, p. 78). The lack in sophistication was outweighed by the mass mobilization of internet-connected devices, therefore exploiting the scale of the assault rather than the quality. The attacks peaked on 9 May, the day Russia celebrates Victory Day of the Great Patriotic War, which is the name given to the Second World War, and the apex of the assault lasted until the 15 of May; during this period, especially on the 9th, the national bank of Estonia, Hansapank, was the among the institutions the suffered the most, as the assault made its online services unavailable for ninety minutes and for two

hours the day after (Steed, 2015, p. 78), together with the other leading bank SEB Esti Uhispank, as well as telecommunications companies (Samabaluk, 2022, p. 77).

Despite being hardly sophisticated, the cyber-attacks that hit Estonia in 2007 are an example of cyber-attacks used to achieve a political goal, without being directly connected to a national source; in fact, a 20-year-old ethnic Russian was charged for the attacks in Estonia, but Russian authorities predictably refused to support the investigations and therefore hampered the efforts to prosecute those responsible for the assault, and in some instances they proudly expressed their involvement in the attacks (Samabaluk, 2022, p. 78). This attitude supported the belief that Moscow was pursuing its political will through cyber warfare, but a lack of concrete evidence made the accusations of Russia's direction of the attacks made by Estonia's foreign minister, Urmas Paet, inconclusive, leading some to question the credibility of these allegations (Steed, 2015, p. 78). Furthermore, the literature also presents contrasting opinions for what concerns the impact of the 2007 attacks: while some argued that the attack had a minor, yet noticeable, impact with no significant long-term effects for the daily lives of Estonian citizens, others have asserted that the cyber-attacks witnessed by the former Warsaw Pact member represent "represent a new kind of war where the threat lies not in conventional armies but in a wholly asymmetric or unconventional attack deploying one or another form of IW (Information Warfare)" (Blank, 2008, as cited in Steed, 2015, p. 79). Some have even suggested that Estonia's attacks were a "dress rehearsal" for the cyberwar waged by Russia in the context of the annexation of the Crimean Peninsula (Garon, 2018, p. 5). Overall, what is noteworthy about this event is the fact that the assault was a politically motivated attack on a state's national infrastructure but without a clear attribution, given that Estonian authorities were unable to prove without a doubt Russia's involvement (Friis & Reichborn-Kjennerud, 2016, pp. 59–60).

3.2.2 Georgia (2008)

Georgia is one of the newly created states that emerged out of the dissolution of the Soviet Union, but since its inception, different ethnic identities made its borders and sovereignty

hotly contested, especially for what concerns the region of South Ossetia, which is placed on the border between Russia (where North Ossetia is) and Georgia, and the province of Abkhazia, a small region on the eastern coast of the Black Sea. Since gaining statehood in 1991, Georgia tried to become increasingly independent from Russia, and a strong wave of nationalism resulted in the so-called 'Rose Revolution' in November 2003, and three months later Mikheil Saakashvili was elected President (Samabaluk, 2022, pp. 79–80). These developments triggered a feeling of angst in Moscow, as the Kremlin watched its own periphery undergo a geopolitical transformation away from Russia's influence and towards closer ties with NATO and the West. As a result, the possibility of Georgia joining NATO, proven by the state's willingness to have a membership action plan (MAP), raised the tension in the already unstable region, eventually leading to the 2008 "five-day war" between Russia and Georgia, in which Russia supported South Ossetia and Abkhazia's independence even though Georgia considered the two regions to be inside its national borders (Kazantsev et al., 2020, p. 9). Russia decided to grant diplomatic recognition to the two ethnic regions as a reaction to the recognition that was granted to Kosovo's independence by the US, Britain and France in February 2008, but also on the grounds of its right to protect Russian nationals in those regions, which was Moscow's own version of the Western concept "Responsibility to Protect " (R2P) (Samabaluk, 2022, p. 80). Furthermore, Russia's claim on its duty to protect all ethnic Russians outside the border of the Russian Federation was also used as a justification for its intervention in Georgia (Allison, 2008, pp. 1152–1153).

Based on this duty to protect principle, Russia placed an increasing number of peacekeeping forces in the regions of Abkhazia and South Ossetia, including elite airborne forces and heavily equipped troops (Samabaluk, 2022, p. 80). In addition to military personnel, in the years that followed the election of Saakashvili, Russia consolidated its presence in the region by giving Russian passports to several people of South Ossetia, a strategy that Tbilisi, Georgia's capital city, perceived as a form of annexation of the ethnic region. Despite the alleged defensive nature of Russia's peacekeepers in South Ossetia, Georgia felt threatened by the military build-up in Ossetia, particular after the Georgian government accused Russia of moving heavy equipment and 'mercenaries' through the Roki tunnel joining North Ossetia to South Ossetia (Allison, 2008, p. 1147). The situation

worsened throughout July, as clashes emerged between Georgian troops and Ossetian separatist militias, until controlled confrontation degenerated into an open conflict on the 8 of August 2008, a war today known as the 'five-day war'. Georgian troops entered South Ossetia and launched an attack on Tskhinvali, the de facto capital of South Ossetia, and Russian peacekeeping forces on the ground responded in a swift and forceful way, managing to ward off Georgian troops from the province, while also seriously threatening the city of Tbilisi; after the end of the conflict, Russia further consolidated its relationship with the South Ossetia, thanks to the deployment of a large number of peacekeepers and the granting of millions of euros in financial aid, therefore exerting a strong political influence on South Ossetians, who saw the closer relations with Russia in a positive way (per Concordiam, 2012, p. 47).

The kinetic conflict in Georgia was paralleled by an information campaign, whose goal was to disseminate confusion around the emergence of the conflict through propaganda and the exploitation of ethnic tensions, which was made successful thanks to Russia's cyberwar operations (Samabaluk, 2022, p. 81). The cyber-attacks were delivered before, starting from the 20-July, and during physical attacks and, as in the case of Estonia in 2007, their level of sophistication was particularly low and the tools and bots used were very similar to those employed by the Russian Business Network cybercrime (Samabaluk, 2022, p. 81). The cyber warfare against Georgia followed a two-level approach: while the first approach was minimally effective and saw the defacement of public and privately owned websites, the second approach was more common and effective, and it included the delivery of DDoS and botnet attacks against both public and private networks, but mainly against the Georgian government and media systems (Steed, 2015, pp. 79–80). This "internet blockade" was put in place by Russian hacktivists and hackers, nationalistic individuals who launched cyberattacks themselves in some kind of "patriotic hacking" strategy: Russian websites like *stopgeorgia.ru* encouraged fellow hackers to launch cyber operations against Georgia by providing the targets as well as simple instructions to conduct cyber disruption for anyone who can have access to a computer (Samabaluk, 2022, p. 82). A notable example of online defacement was the vandalization of a website displaying photos of Georgian President Saakashvili portrayed as Adolf Hitler, as a way to convey the message that Georgia resembled Germany under Nazi dictatorship (Samabaluk,

2022, p. 82), an attack that used the Russian-affiliated 'Machbot' software and that was actually routed through an American IP address (Steed, 2015, p. 80). This attack marked the beginning of a larger wave of attacks that targeted the education institutions of Georgia, in order to activate the country's CERT system and divert it from other attacks carried out on more strategic targets (Steed, 2015, p. 80).

The cyberwarfare campaign launched against Georgia did not target critical infrastructure and concrete assets, like power grids and water supplies, but rather represented "low-sophistication nuisance attacks", like the defacement of Saakashvili's photos, aimed at supporting Russia's information war and propaganda operations against Georgia: on the battlefield Georgia was overtaken by Russian forces, while the country's information space was isolated due to the cyber-attacks obstructing of Internet communications with the rest of the world (Samabaluk, 2022, p. 82), and forcing the government to relocate its websites abroad to be able to operate again (Steed, 2015, p. 80). The cyber-attacks were significant not only because they jammed internet networks, but also because they disrupted Georgia's attempts to counter Russian strategic communications narrative that manipulated people's perception of the conflict (Steed, 2015, p. 81). While Moscow did not firmly deny culpability for the Estonian attacks, Russian diplomats claimed, albeit with little credibility, that the Russian Federation was not behind the cyberattacks that coincided with the country's military activity in South Ossetia, but were conducted by single individuals in the Russian territory (Samabaluk, 2022, p. 83). The 'outsourcing' of the cyber-attacks launched on Georgian websites to single individuals made the scale of the assault increase dramatically, therefore worsening the attribution problem linked to this cyber operation, which some have argued to be the first independent cyber-attack and conventional military operation to happen simultaneously (Steed, 2015, p. 80). Furthermore, Russia's information warfare continued even after the conflict ended: a Russian military official made an announcement calling for international rules against information operations, right after Russia launched such an attack on Georgia, therefore proving that Moscow did not stop pursuing its political objectives by "manipulating and potentially gaslighting the international community" (Samabaluk, 2022, p. 84).

3.2.3 US Elections (2016)

The case of the alleged Russian interference into the United States presidential elections of 2016 represents a well-known example of Russia's aggressive cyber and information strategies, whose end goal is not to hack and interfere with computer systems like the previous examples, but rather to manipulate public opinion and behaviour in target countries; in other words, the case of the US 2016 Elections shows Moscow's holistic and multi-layered approach to information warfare including cyber operations, cyber espionage, and psychological campaigns (Abdyraeva, 2020, pp. 21–22). The 2016 interference into the US presidential elections is an example of how social media cyber operations have been taking warfare, albeit in a non-traditional sense, directly to the level of citizens, namely through information operations and propaganda (Prier, 2021, p. 105). Indeed, Russia has been exploiting the growing polarization that has characterized Western societies in recent years, which find themselves to be particularly vulnerable during election seasons; as a result, Moscow has been able to exploit already present and pervasive divisions by disseminating confusions and distrust, especially towards institutions that are based on democratic values (Samabaluk, 2022, pp. 98–99). In fact, among the vulnerabilities of the US democratic system, many have pointed to the system of the US Electoral College, while others have argued that another element encouraging meddling is the prolonged campaign season of American presidential elections, which has increased the need for bigger campaign fundings, expanding in turn the time frame for disinformation to enter the national discourse (Samabaluk, 2022, p. 118).

The United States environment during the 2016 election season proved to be a particularly fertile ground for Moscow's plans of spreading chaos as a way to pit American citizens against each other. Indeed, over a period of twenty years, American society has gradually become more and more politically divided, consequently exacerbating social and political issues such as hyper-partisanship, racism and media-distrust (Thrall & Armstrong, 2021, p. 84). As a matter of fact, media professionalism in the US has been declining for decades, and journalism has gradually lost the respect of Americans; in turn, this phenomenon has led to the emergence of Fox and Fox News as a new media outlet that

caters to right and centre-right audiences, which did not find their values to be represented by traditional news outlets leaning towards leftist views (Samabaluk, 2022, p. 119). As a result, the presidential competition between former Secretary of State Hillary Clinton for the Democratic Party and business tycoon Donald Trump for the Republicans produced a highly polarized environment in which American citizens' primary push to cast their vote was to block the opposing candidate, rather than support their own (Samabaluk, 2022, p. 117).

In particular, Donald Trump played a key role in raising the social and political tension during the electoral campaign thanks to his inflammatory language and unorthodox public statements: by underlying the United States' divisive problems, attacking the democratic candidate on personal grounds, and encouraging Russian meddling, Trump opened the doors to Moscow's interference, boosting Russia's efforts in sowing distrust in every corner of the country (Thrall & Armstrong, 2021, pp. 84–85). One notable example of his explicit pro-Russian behaviour was the call he made to Moscow to hack into Hillary Clinton's email account and publish her private e-mails: "*Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing*" (Schmidt, 2018). In other words, American Intelligence investigations concluded that despite the lack of clear evidence pointing to a collusion between President Trump and the Kremlin, they were unanimous in asserting that "Russia used social media and other means in an effort to polarize the American electorate and to help Donald Trump win the election" (Thrall & Armstrong, 2021, p. 73).

In order to enact its information campaign, Moscow relied on a series of bodies and agencies that were tasked with spreading desired messages and narratives. Among these we find RT, the Russian state-controlled international TV news channel formerly known as "Russia Today", which began to broadcast English programmes in 2005 and gradually expanded its operations to different formats and platforms, such as Facebook, where it covered the 'Occupy Wall Street' movement, and YouTube, where in 2013 "it was the first self-identified news outlet to reach a total of one billion views on the website" (Samabaluk, 2022, p. 122). By bringing its activities to social media platforms, RT developed a wide echo chamber in which individuals confirm rumours by spreading and commenting upon

them, therefore spreading what they consider trusted information that is, instead, propaganda engrained in the platform's algorithms (Samabaluk, 2022, pp. 122–123). As mentioned in the first chapter of this thesis, Twitter (now X) represents the ideal medium through which information is shared and made viral, mainly thanks to its characteristically wide reach, anonymity, brevity of content, and ease of use; therefore, Twitter stands at the core of another Russian agency previously presented in this chapter, the IRA.

The Russian Internet Research Agency allegedly started its activities in 2014, according to US Federal investigators, and twenty of its Agency-controlled accounts were responsible for the vast majority of the disinformation efforts in the US campaign, among these accounts we find names of fake American organisations and grassroot movements, such as "Being Patriotic", "Heart of Texas", "Blacktivist" and "Army of Jesus" (Samabaluk, 2022, pp. 123–124), therefore showing that disinformation ran across the whole political spectrum, without discriminating between left and right. During its testimony in Congress, Google admitted that the IRA managed around 18 YouTube pro-Russian accounts that operated on an anti-democratic framework (Garon, 2018, p. 10). One example of a IRA-owned account that represented a fake US persona is the one portraying an American teenagers, Jenn Abrams, who had been quoted by RT and Sputnik (a Russian state-owned news agency) as well as several Western mainstream news outlets before the 2016 elections, such as the BBC, BET, Breitbart, Business Insider, BuzzFeed, CNN, Fox, France24, HuffPost, InfoWars, the New York Times, Sky News, USA Today, and the Washington Post; in other words, both respected media and unreliable entities referred to the IRA account, showing how fake news and propaganda made their way into established media (Samabaluk, 2022, pp. 124–125).

Since the aim is to raise feelings of fear and divide people, the IRA also engaged in the fabrication of events without any foundation, as it happened in the case of the chemical plant explosion St. Mary Parish, Louisiana, on the 14th anniversary of 9/11, and the story about white supremacists dominating the campus of the University of Missouri in Columbia; the main element of these fake news is that they exploit common narratives among targets, which differentiate insiders from outsiders and appeal to the former group, therefore increasing the visibility of such content to raise tension and outrage (Samabaluk,

2022, pp. 125–126). Overall, a Senate study found that the most targeted social group by IRA information campaigns were African Americans, as race is a divisive topic that can be exploited to build different narratives (Samabaluk, 2022, pp. 128–129).

Russia's campaign during the 2016 events is characterized by a "multi-tiered cyber approach" aimed at influencing the outcome of the elections (Garon, 2018, p. 7). The Report on Russian meddling in the 2016 US presidential elections released by the Office of Director of National Intelligence (ODNI) concluded that in addition to trolls and bots, run by Russian state agencies and state-funded media as well as third parties, engaged in overt efforts to influence and manipulate information on social media, the Kremlin complemented these overt operations with covert intelligence operations through cyber activity (Prier, 2021, p. 102), that include "theft of computer data, covert operations to plant false news and distribute political ads, and attempts to directly hack voting systems and databases" (Garon, 2018, p. 8). As Nicholas Samabaluk (2022) argues, Russian interference efforts are found on two levels: the first is "the technical aspect of cyberattacks to gain illicit access to politically compromising or embarrassing records", and the second is the "psychological avenue opened by the IRA's activities in social media" (p. 126). All these operations were built on the narrative that opposed Hillary Clinton's candidacy, therefore exploiting a group of core believers to disseminate their antagonistic propaganda (Prier, 2021, p. 102). The main operations aimed at discrediting Clinton were based on the creation of trends that could spread a particular narrative in a viral way, mainly through the use of scandals and classified materials, therefore fostering disinformation and hindering the ability of social media audiences, particularly on Twitter, to find alternative, reliable sources (Samabaluk, 2022, p. 130).

Among the most notorious campaigns based on dominating social media trends, whose goal was to harm Clinton's candidacy, we find the case of a group of social media users supporting Trump that started referring to themselves as the "Deplorables", after Hillary Clinton used this word in a speech in September 2016 to describe a part of Trump's voter base, and these Twitter users quickly became largely-followed and influential accounts, as Trump himself retweeted them (Prier, 2021, p. 102). An analysis of the "Deplorables" group found that it was a vast network mainly formed by Russian trolls and

notorious US right-wing personas and accounts, and it was able to create trends thanks to its cohesiveness; in fact, a wide network of bots is essential to "conduct cyberattacks using social media as information warfare" (Prier, 2021, p. 104). A further famous false narrative surround Clinton is the #PizzaGate hoax, a popular conspiracy theory supported by right-wing media to support the narrative that Clinton and her associates were immoral criminals running a child sex ring concealed by a pizza shop (Prier, 2021, p. 102; Samabaluk, 2022, p. 128).

The most powerful trend that put a strain on Clinton's campaign was the leak of her personal emails, and the #PodestaEmail hashtag represented "the peak of Russian command of the trend during the 2016 election" (Prier, 2021, p. 104). While both democrats' and republicans' email servers suffered hacking attacks, the Democratic candidate's emails were targeted and selected to disseminate distrust in the election process (Garon, 2018, p. 8). Despite lacking any real controversial content, Wikileaks released the stolen emails of John Podesta, Hilary Clinton's campaign chairman, and they were used to spin a common narrative among Trump supporters, i.e., discrediting established mainstream media: trending tweets distributed the emails Podesta shared with members of the media by linking them to fake news websites that supported the claim that Clinton was a corrupted politician trying to rig the presidential elections. In addition to disinformation and theft of computer data, 21 American states claimed that their "election systems were targeted by Russian hackers, according to interviews with nearly two dozen national security and state officials and election technology specialists" (Perlroth et al., 2017). Among the states that registered attacks on their electronic polling systems we find Illinois and Arizona, where the systems witnessed successful intrusions and theft of data, as well as the distribution of malware through "spear-phishing emails from a fake account to 121 state and local election jurisdictions" (Garon, 2018, p. 12).

As doubt and confusion surrounded the 2016 US presidential elections, with Trump being accused of corruption and collusion throughout his presidency, a Congressional investigation was launched to shed light on the issue of foreign interference in the American democratic processes. The investigation by Robert Mueller produced the now well-known 'Mueller Report', a two-part report of 448 pages in total that acknowledged

the presence of Russian interference into the 2016 presidential elections by attributing hacking operations and troll activities to Russia (Samabaluk, 2022, p. 135), and to the IRA in particular, which was found responsible for social media active measures through the creation of fake US online personas and organisations targeting ethnic minorities (Samabaluk, 2022, p. 129). The investigation led by Special Counsel Mueller was followed by the indictment by the grand jury of thirteen individuals and three organisations, which worked under the IRA in the performance of the trolling activities; those indicted were accused of "conspiring with each other and with persons known and unknown to defraud the U.S. by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016" (M. Schmitt, 2021, p. 188). Congress' investigations raised the issue of foreign interference in institutional processes, and as the Senate Intelligence Committee condemned the role of Facebook, Google and Twitter in one of the hearings on Russian interference, Senator Dianne Feinstein also scolded the tech giants by stating that *"what we're talking about is the beginning of cyber warfare*" (Timberg et al., 2017).

The responsibility of the Russian government in the influence operations was supported by a report produced by the US Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). For what concerns legal responsibility, the Russian GRU (General Staff Main Intelligence Directorate) was responsible for the hacking into local election systems, and the exfiltration of data from email accounts belonging to the Democratic National Committee (DNC), which were then employed by online entities like Guccifer 2.0, DCLeaks and Wikileaks; instead, for what concerns the IRA as the responsible for the trolling operations on social media, legal attribution is harder to determine given the uncertainty over the degree of control the agency received from the government (M. Schmitt, 2021, p. 187). Therefore, while legal attribution was possible in the case of the GRU, being it a state organ that acts as an instrument of the state, the IRA is considered a state-owned organ, therefore its relationship with the state is not enough to attribute the operations of the Agency to the state itself, given that the latter is not responsible for illegal actions committed by non-state actors (M. Schmitt, 2021, pp. 202–203).

3.3 Russian Hybrid Warfare in the European Union

The case of Russian meddling into the American presidential elections of 2016 raised the alarm in other democracies around the world, particularly in the European Union, which has become increasingly aware of the threat disinformation and media manipulation pose to democratic processes and institutions (Lexmann, 2017, p. 37). Indeed, the same polarization that emerged in the United States was also starting to appear in European countries following the 2008 global financial crisis, as the advent of globalisation produced winners and losers across society, consequently erasing the traditional political divide between the left and the right, while producing new anti-establishment, disaffected social groups that are brought together by their lack of trust in the liberal democratic system (Lexmann, 2017, p. 38). In turn, as it has been argued by Miriam Lexmann (2017) Russia realized the potential of divided European societies for disinformation and manipulation campaigns, aided also by fact that EU Member States assumed that the Russian federation and the EU's Eastern Neighbourhood would eventually undergo a process of democratization, a transition that failed to materialize, and by the fact that Moscow's ability to exert influence in what it calls its 'near-abroad' (or *Ruskiy Mir*) was largely neglected and overlooked (pp. 39-41).

As Russia improved its cyber capabilities and weaponized the information space, the Kremlin started targeting the European Union and its member States as a way to harm and undermine the institutions of its Western enemies (Limnell, 2018, p. 67). Indeed, Russia's aggressive behaviour towards the EU has been acknowledged by a resolution adopted by the European Parliament in 2016. The *European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI))* recognised that Moscow has made use of a wide array of instruments, such as the RT English-language channel and the Sputnik news agency, to spread disinformation and propaganda with the goal of sowing divisions among European citizens and to erode trust in the EU's democratic values by undermining the political cohesion of European institutions (European Parliament, 2016). Furthermore, the European Parliament resolution:

> "*Stresses that Russia is exploiting the absence of a legal international framework in areas such as cybersecurity and the lack of accountability in media regulation, and is turning any ambiguity in these matters in its favour; underlines that aggressive Russian activities in the cyber domain facilitate information warfare*". (European Parliament, 2016)

Indeed, there are several cases of Russian cyber-enabled information operations taking place in countries of the European Union, since officials in the Kremlin, first among them Putin, realised that the cohesion of the Union could be effortlessly challenged by employing cyber-attacks, information campaigns, and covert operations aimed at finding and exploiting the Achille's heal of European democracies (Elonheimo, 2021, p. 122). As a matter of fact, a research produced by the Alliance for Securing Democracy found that since 2004 no less than 27 countries between European and North America have been victims of cyber operations, disinformation and financial influence deployed by Moscow to interfere in domestic politics, such as the WannaCry and NotPetya cyberattacks attributed to Russia by the EU that have been briefly mentioned in Chapter 2 (Limnell, 2018, p. 68). Among the most targeted EU countries we find Germany and France, but also member states like Denmark, Italy, the Netherlands and Norway have suffered from cyber-attacks, including cyber espionage and hacking operations, coming from Moscow (Limnell, 2018, p. 69). Furthermore, Russia has been increasing its interest in targeting physical infrastructure, such as submarine telecommunications cables, which carry around 97 percent of the world's communications, including financial transfers that amount to approximately $10 trillion per day; tapping and damaging cables falls within Moscow's hybrid warfare that allows Russia to pursue its goals while steering clear of an open conflict (Limnell, 2018, pp. 69–71). Whether they target critical infrastructure or digital democracies, Russian cyber and information operations have become a daily threat to the activities of the European Union and its citizens, as it will be illustrated by the case studies analysed below.

3.3.1 Germany

Germany is among the strongest economies in Europe and for this reason it is often at the forefront of several initiatives at the EU level. Due to its important role in the Union, the German Republic has found itself at the centre of attacks, aimed at harming its cyber infrastructures, as well as information manipulation operations. In particular, in 2015 the German government was strongly supporting Ukraine's efforts against Russian forces in its eastern provinces and, in turn, Moscow unleashed a hacking attack against the websites of the German government and, most importantly, of the Bundestag, the German parliament (Samabaluk, 2022, p. 99). The attack on the German Bundestag was first detected in May 2015 and it targeted the network used by all members of the German Federal Parliament, as well as the German Chancellor: the German intelligence agency BfV (Bundesamt für Verfassungsschutz or Federal Office for the Protection of the Constitution) found that the Russian hacking group APT 28 ('Fancy Bear'), which is allegedly run by the Russian GRU, the same state agency accused of taking part in the influence operations of the 2016 US presidential elections, was the entity behind the Bundestag Hack (Cyber Law Toolkit, 2021). Russian hackers were able to infiltrate the Parliament network by sending German MPs an email resembling a UN News Bulletin that even featured a 'UN.org' address, which contained a link that installed a malware that could spread to the various networks of the Bundestag (Cyber Law Toolkit, 2021).

The attack on the emails of the German MPs that started at the beginning of 2015 allowed the hackers to access internal communications, which included confidential sensitive data like the parliamentarians' schedules and their meetings details; furthermore, what is significant about the attacks is that the group of hackers managed to sustain unauthorized access to the Parliament networks for several months until its detection in May, while also managing to infiltrate the parliamentary office of former German Chancellor Angela Merkel (Cyber Law Toolkit, 2021). The response to the attacks was to shut down the computer system of the Bundestag for four days to restore its functioning and install supplementary security mechanisms (Cyber Law Toolkit, 2021). German investigators found that a total of 16 gigabytes were stolen from the Bundestag network, and they also concluded that Dmitri Badin was involved in the hacking action, a 29-year-

old Russian hacker who was also connected to the case of interference into the American presidential elections of 2016 (Samabaluk, 2022, p. 99). German authorities issued an arrest warrant for Badin and they also imposed sanctions such as travel bans and asset freezes on Igor Kostyukov, (Lauren Cerulus, 2020) the GRU head who was charged with EU sanctions in 2019 for its role in the poisoning of Sergei Skripal, former Russian spy (Harding et al., 2018). As a response to the attacks, the EU sanctioned the hacker group 'Fancy Bear', the pseudonym used for the GRU Unit 26165 (Lauren Cerulus, 2020); the GRU is one among the bodies and individuals that have been put under a sanctions package as part of the cyber diplomacy toolbox the Union implements to "prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace." (Council of the European Union, 2020c).

Following the allegations of being behind the Bundestag Hack of 2015, Russia denied its involvement in APT activities in Germany and answered by labelling its accusers as Nazis, an accusation that ironically coincided with the rise of the far-right party AfD (Alternative for Germany) and a wave of Russian disinformation in the German media (Samabaluk, 2022, p. 100). In particular, Moscow sought to exploit and raise the tension around the presence of Muslim foreigners, whose community had grown in Germany following the humanitarian crisis triggered by the Syrian civil war (Samabaluk, 2022, p. 100), as a way to destabilize European cohesiveness and undermine the authority of Angela Markel in the eyes of German citizens (Rinke & Carrel, 2016). The most infamous case of Russian disinformation in Germany concerns the case of "Lisa F.", a 13-year-old Russian-German girl, a dual national that moved to Germany with her family in 2004, who claimed to have been kidnapped in East Berlin by migrants and held for 30 hours, and to have been sexually assaulted by "Arab" men (Rinke & Carrel, 2016; Samabaluk, 2022, p. 100).

The German investigators quickly discovered that her cell phone records indicated that she spent those hours with a male friend, therefore concluding that her statements were false; however, the event quickly became a mediatic phenomenon, as Russian trolls and media agencies realized the case represented a perfect propaganda anecdote: Russian official and social media extensively reported the case of Lisa F. and showed support to the

demonstrations that took place around Germany (Samabaluk, 2022, p. 100), like the protests of Russians in Bavaria and the demonstrations held by around 700 people in front of the Chancellor's Office with banners reading cautionary messages, like "Our children are in danger" and "Today my child, tomorrow yours" (Rinke & Carrel, 2016). The Kremlin did not need to create a false narrative to spark a reaction because the allegations were spontaneously created at the domestic level, proving that social angst around the issue of immigration was already pervasive in Germany, and providing Moscow with strong plausible deniability against accusations of spreading disinformation and information operations (Samabaluk, 2022, p. 100).

3.3.3 United Kingdom

As it has been illustrated by the German case, Russia's activities in the cyber and information space are moved by a desire to undermine the stability of the European Union by sowing divisions among its members, eventually making the system collapse, as in the case of Brexit. Voted on 23-June 2016, the membership withdrawal of the United Kingdom from the EU represented a destabilising event for Europe, with Russia hoping that it would significantly erode the unity of the Union. Indeed, Moscow did not miss the opportunity to influence the result of the Brexit referendum through a series of information campaigns on social media: a study by the University of Edinburgh found "3,000 Brexit-related Twitter posts traceable to the IRA, and other researchers tallied 150,000 Twitter accounts that abruptly pivoted attention during the run-up to the Brexit vote on that issue" (Samabaluk, 2022, p. 102). The narrative portrayed by the Russian tweets was centred around pro-Brexit arguments sustained by euro-sceptics, such as the increased levels of social unease towards the growing Muslim population in Britain, similarly to the issue present in Germany; as a result, Russian state-funded media agencies such as RT and Sputnik provided a platform to voice these concerns, as the broadcasters agencies invited figures like the staunch euro-sceptic Nigel Farage, leader of the UK Independence Party (UKIP), and also the leader of the Labour Party Jeremy Corbin, therefore showing that Moscow's allegiance is towards the political side momentarily serving Russia's interests (Samabaluk, 2022, p. 102).

This case supports the claim that democracies are most vulnerable during times of elections. In fact, Russia engaged in tampering also during Scotland's independence referendum, which some believe represents the first instance of interference in foreign elections by the Russian Federation (Samabaluk, 2022, p. 101). However, no credible investigation was conducted by the government, as it has been claimed by the UK Parliament Intelligence and Security Committee, which also produced a 47-page 'Russia Report' finding that "Moscow-based information operations, especially through social media and Russian state-funded broadcasters like Sputnik and RT—and backed up by targeted support to influential voices within UK politics—may well have been a significant factor" (Ruy, 2020). Furthermore, the report also highlighted the role of financial ties between Russian oligarch with connections to Vladimir Putin and to British political figures, therefore pointing to "potential violations of campaign financing" (Ruy, 2020).

What is most disconcerting is the fact that while the British government acknowledged the presence of Russian meddling into the 2014 Scottish Referendum and into the general elections held in December 2019, the Government failed to admit that Moscow may have interfered in the Brexit referendum, and it did not seriously investigate by producing a sort of British 'Mueller Report' that was released in the US; in fact, because putting into question the legality of the referendum would have also questioned the legitimacy of the pro-Brexit government, the latter rejected the interference accusations (Lis, 2020; Ruy, 2020). Instead, US investigations led by special counsel Robert Mueller into the allegations of Russian interference in 2016 dug deep into the issue, interviewing around 500 witnesses and issuing more than 2,800 subpoenas to uncover the truth, and produced an assessment with an unclassified summary that was made available to the public (Mackinnon, 2020). Overall, we could argue that in addition to the interference and meddling, the distrust and confusion that arise in the aftermath of questionable elections also serve the interests of the Kremlin, which benefits from increasingly divided societies and from an eroded trust in the democratic processes of European countries (Samabaluk, 2022, p. 101).

3.3.2 France

Like the case of the US in 2016, the two-round presidential election in France of 2017 was also marked by technical hacks and information operations on social media. More specifically, the target of a coordinated hacking attack exfiltrated personal data was Emmanuel Macron, the leader of the French party '*En Marche'*, whose presidential campaign suffered from the leaking of compromising information that included both stolen and falsified material (Samabaluk, 2022, p. 103). Macron was hit by rather simple phishing attacks, unlike the more sophisticated malware intrusion launched against the DNC, and forensic analysis pointed to Russian sources, given that the meta-data presented characters of the Cyrillic alphabet and it was connected to the activities of a Russian intelligence contractor (Samabaluk, 2022, pp. 103–104).

The French presidential election of 2017 saw the left-and-centre coalition party led by Macron compete against the National Front, the far-right political party headed by Marine Le Pen. While Le Pen had deep ties with Putin, being her party financed by Russian funds and having praised the Russian President herself for his Christian values as part of the European civilisation, Macron was a staunch critic of Putin's policies; unsurprisingly, the leader of the *En Marche* party became the candidate that was hit by the largest disinformation campaign launched by Russia during the presidential race, with rumours claiming that he was supported by a "very wealthy gay lobby" and that one of his staff members was involved in illegal drug activity (Samabaluk, 2022, p. 104). However, the real attack came right before the final debate that would mark the media blackout period of 44 hours that preceded the election voting day, going from May 5 to May 7 (Samabaluk, 2022, p. 104): during what came to be known as the 'Macron Leaks', Macron's team suffered a hacking attack and a combination of real emails and forged documents were released online (Vilmer, 2018, p. 1).

The leaked material sought to expose Macron's illegal off-shoring funds, and many Twitter accounts worked to emphasize the accusations through a series of hashtags, like #MacronGate and #MacronCacheCash, and Le Pen even made reference to these allegation during the presidential debate; however, the documents were quickly recognized as false

and a repeating pattern of leaks was identified: first, large dumps of fictitious hacked documents online, followed by trolls, bots and individuals galvanizing the leaks through consistent social media activity, and then Russian state-controlled media working to bring traditional media attention to the fake news narrative made viral through social media (Samabaluk, 2022, pp. 104–105). One example of this mechanism is given us by the #MacronLeaks trend, which "counted 47,000 tweets in its first three and a half hours, and in total some 9 gigabytes of exfiltrated files and 21,000 emails (including from the accounts of key Macron associates) were thrown onto Pastebin during the campaign" (Samabaluk, 2022, p. 105).

Despite the avalanche of cyber operations that hit the Macron campaign in 2017, the elections were not influenced by the disinformation campaign orchestrated by Moscow and Macron eventually won the race, all this thanks to a series of factors that were lacking in the 2016 US presidential election, therefore leading to a different outcome. Unlike the United States or the United Kingdom, one structural element that helped against the disinformation campaign launched by Moscow is the fact that the French President is elected through direct elections consisting of two rounds, which makes it more difficult for malicious actors to influence the turnout; also, France is characterized by mainstream and critical media sources, and French society is culturally equipped with a healthy dose of scepticism, as well as critical thinking (Vilmer, 2018, p. 2). Furthermore, the influence attempts failed due to their sloppiness and the fact that the disinformation material was so absurd it was considered almost unbelievable, making the whole operation look dilettantish, as Russian actors overestimated their ability to mobilize French people and online communities (Samabaluk, 2022, p. 113; Vilmer, 2018, p. 2). Moreover, the fact that fake news was spread in English did not resonate with the French voters, especially French nationalist, who tend to oppose anything they feel is being imposed by American media. In addition, timing played a crucial role in allowing the French to react against these cyber activities: on the one hand, the leaks were released right before the election media blackout, which significantly limited their ability to spread (Samabaluk, 2022, p. 105) and, on the other hand, France's government preparedness and public awareness was possible thanks to the precedents of cyberattacks in the US, UK and the Netherlands (Vilmer, 2018, p. 2),

where a Russian hacking attempt took place during a Dutch referendum on a 2016 trade agreement between the EU and Ukraine (Samabaluk, 2022, p. 107).

In addition to the attacks launched on the democratic processes and institutions of European countries, the institutions of the European Union also suffered from cyberattacks, as in the case of the European Medicine Agency (EMA) vaccine storages and the European Banking Authority (EBA), as it has been acknowledged by the 2022 *Report on foreign interference in all democratic processes in the European Union, including disinformation* released by the European Parliament (European Parliament, 2022). According to the report, the attacks suffered by the EU and its Member States are part of foreign interference tactics were aimed at eroding the stability of the Union and undermining its democratic values, through activities that include:

> "*disinformation, the suppression of information, the manipulation of social media platforms and their algorithms, terms and conditions, and advertising systems, cyberattacks, hack-and-leak operations to gain access to voter information and interfere with the legitimacy of the electoral process, threats against and the harassment of journalists, researchers, politicians and members of civil society organisations, covert donations and loans to political parties, campaigns favouring specific candidates, organisations and media outlets, fake or proxy media outlets and organisations, elite capture and co-optation, 'dirty' money, fake personas and identities, pressure to self-censor, the abusive exploitation of historical, religious and cultural narratives, pressure on educational and cultural institutions, taking control of critical infrastructure, pressuring foreign nationals living in the EU, the instrumentalisation of migrants and espionage"* (European Parliament, 2022, pp. 6–7).

All of these tactics, many of which have been applied in the case studies presented above, pose a great threat to European states that are constantly targeted by Russian cyber and information operations that form its hybrid warfare strategy against the EU. In particular, these cyber operations have been applied with greater intensity in the context of the invasion of Ukraine (Vincent & Pietralunga, 2023), and the next chapter will look into the

scope of cyber and disinformation campaigns aimed at supporting Moscow's battle in Ukraine.

4. The Invasion of Ukraine and Russia's Hybrid Warfare in Europe

The invasion of Ukraine that took place on February 24, 2022, has brought on a devastating conflict on European soil. Russian forces have deployed a hybrid campaign combining elements of kinetic, cyber and information operations, which represent "hard and soft tactics that rely on proxies and surrogates to prevent attribution, to conceal intent, and to maximize confusion and uncertainty" (Iasiello, 2017, p. 60). The cyber element has amplified other elements of warfare, such as the disruption of communication services and the damage of critical infrastructure, as well as the dissemination of disinformation and propaganda supporting Russia's narrative of the invasion, mainly through the use of social media and digital communication technologies. While the official targets of these attacks have been Ukraine and its population, cyber and information operations have also hit European societies oftentimes unaware of being targeted by Russia's hybrid campaigns.

This chapter will focus on Russian hybrid warfare, looking at the cyber and informational elements. Before discussing the recent invasion of 2022, it is useful to start with an overview of the historical relationship between Ukraine and Russia, in order to better understand the origin of today's conflict, but also to have a clearer understanding of Russia's justification of the invasion and Russian narratives employed to sustain its disinformation campaign and propaganda surrounding the invasion of Ukraine that started in 2022. Therefore, the first sections will look at the historic ties between Russia and Ukraine, briefly going from the inception of the Kievan Rus to today's Russian Federation; then, the second section will look into the Russian annexation of Crimea in 2014, which has been labelled by scholars as the origin of Russia's hybrid warfare; finally, the last section will look at the developments of the conflict in Ukraine so far, focusing on the analysis of cyber-attacks and information operations, and concluding with an investigation of the European Union's response to the attacks under the cyber diplomacy framework.

4.1 History of Russo-Ukrainian Relations

In order to understand the context surrounding Russia's invasion of Ukraine in 2022 it is necessary to first begin with an overview of the historical ties that link Ukraine and Russia. As a matter of fact, as demonstrated in *A Concise History of Russia* by Paul Bushkovitch, Russian identity and nation building history is inextricably linked to the history of Ukraine, yet the political history of these nations is quite complicated to reconstruct. The ancient land that is considered to be the original polity that gave birth to modern Russia was called Kievan Rus, where Rus stood for the people and land that lived on it and the capital was Kiev (Bushkovitch, 2012, p. 21). Today, the territory of the ancient Kievan Rus, which occupies the land going from the northern part of Novgorod and moving to the south of Kiev, comprises Belarus, northern Ukraine and the centre and north-west of European Russia, and the people of modern Belarus, Ukraine and Russia belong to the Eastern Slavs ethnic group, as their languages are derived from Kievan Rus' East Slavic language (Bushkovitch, 2012, p. 21).

The history of the Rus people is believed to originate from a Viking named Rurik and his two brothers, who arrived in Novgorod in 862 D.C. and took control of the land; however, the rule of Rurik is more legend than history, and the literature on his dynasty in Kiev is rather vague (Bushkovitch, 2012, p. 23). This ancient polity did not have the characteristics of a modern nation-state, instead, it was a conglomerate of tribes between Kiev and Novgorod that obeyed to Kiev, where a prince descending from the Rurik dynasty ruled with his army of warriors (Bushkovitch, 2012, p. 26). What is important to notice about the Rus people is that they were Orthodox Christians, and this faith greatly influenced the nature of Russian culture well into the eighteenth century (Bushkovitch, 2012, p. 29), and some argue its influence is present even to this day as President Putin has been advocating for Orthodox Christianity as a central part of Russia's identity (Laruelle, 2021).

Over time, the people of the Kievan Rus became increasingly fragmented and by 1200, apart from the region of Novgorod, the rulers of the different territories were local princely descendants of the original Rurik dynasty from Kiev, whereas the ruler of Kiev was a minor prince or even an outsider (Bushkovitch, 2012, p. 23). In other words, the

polity of the Kiev Rus slowly disintegrated, and, through this process, a new, distinct Russian language and culture developed around Novgorod and the north-east of the old land, eventually forming an area called Russia (*Rossiia*) from the fifteenth century, which was inhabited by the Russian people (Bushkovitch, 2012, p. 40). As the Russian nation and people established, the first mention of Moscow dates back to 1147, when written sources described it as a small fortress, and historians have also found that Prince Daniil of Moscow (1280-1303 circa), the grandson of the Prince of Novgorod Alexander Nevsky, secured the small land that ran across the Moscow River (Bushkovitch, 2012, p. 43).

During these centuries, the territories of the Kievan Rus, including Russia, would be conquered by Lithuania, which converted to Catholicism in the 1400s; however, the Slavic populations remained Orthodox, and these religious differences would later foster the emergence of nationalist movements of the Belorussian and Ukrainian people, similarly to the process of nation formation experienced by the Russians (Bushkovitch, 2012, p. 50). In turn, to contrast the strengthening of Lithuania, the former Kievan Rus lands worked towards becoming a centre of Orthodox Christianity, therefore building a new religious centre that would greatly influence Russia moving forward (Bushkovitch, 2012, p. 50). In addition to Lithuania, Russia came under the control of another foreign entity: in 1237 the Mongols invaded and conquered Russian territory, and during the rule of the Golden Horde, which lasted approximately two centuries, Russia strengthened its ties with the east through trade; as a result, Mongol rule over the Russians impacted modern perceptions of Russia as being an "Asiatic" nation, yet, Russian culture shows no significant signs of the Horde's heritage are left today (Bushkovitch, 2012, p. 50).

Once Russia became a unitary state at the end of the fifteenth century, it quickly found itself surrounded by strong political entities, particular in the west, where the Lithuania-Poland alliance became Russia's major rival and its first concern in terms of foreign policy (Bushkovitch, 2012, pp. 60–61). Internally, the newly formed Russian state presented a complex and vast structure, but its culture remained strongly Orthodox, and its ruler, Ivan III ('The Great') of Moscow (reign: 1462-1505), began to refer to himself as the sovereign and ruler of "All Rus" (Bushkovitch, 2012, p. 65). His grandson Ivan IV, better known as Ivan 'The Terrible' (reign: 1547-1584), was the first Russian ruler to call himself

Tsar, deriving from the name of Roman Emperor Julius Ceasar, as a way to bring himself to the same level and status of Roman and Byzantine emperors in the eyes of the Slav people (Bushkovitch, 2012, p. 70). In fact, this could be seen as an attempt at consolidating the legitimacy of Russia's authority over the Slavs that inhabited the territories of the old Kiev Rus.

After the Time of Troubles, a period of great instability and factional violence that followed the death of Ivan IV, a new dynasty of tsars came to rule over Russia, the Romanovs, until they were eventually overthrown by a popular revolt in 1917 in the context of the Bolshevik Revolution. During this period of peace, Orthodoxy was at the centre of Russia's political, religious and social issues, and a closer relationship with the Orthodox church of Kiev had a profound impact on Russian culture and society from the 1630s to the 1690s (Bushkovitch, 2012, p. 82). Once again, we can see that Russians and Ukrainians were strongly connected through the Orthodox faith, which had an enormous influence on the culture of both. Meanwhile, the Ukrainian Cossacks staged revolts in Poland, and in order to assert their independence from Polish rule, the Pereiaslav Treaty of 1654 brought the Ukrainian Hetmanate under Russian rule: under this agreement, the Cossacks maintained control over the management of the judiciary, the treasury and the army, while in Kiev and other main cities the tsar's commanders controlled the towns in which Russian garrisons were stationed, whereas the Church of Kiev, which was under the jurisdiction of the Greek patriarchate of Constantinople, agreed to have the Moscow Patriarch as its head in 1687 (Bushkovitch, 2012, p. 91). It what was only after 1667 that Kiev and today's Poltava and Chernihiv were brought under the rule of Moscow's tsar (Szporluk, 2018, p. 87); as a result, the entry of the Ukrainian Hetmanate in the Russian state had a deep impact, since it "strengthened the ties between Kiev and Moscow at a time when changes were taking place in the Russian Orthodox church" (Bushkovitch, 2012, p. 91).

Under Peter I, better known as Peter the Great (reign: 1682-1725), Russia entered into war against the Swedes, and Peter's victories brought the Baltic regions of Eastland and Livonia, under Russian rule, marking the first time Russia ruled over territories that did not have Orthodox elites; at the same time, Peter I tried to assert a stronger dominance over the Ukrainian Hetmanate, where he orchestrated the election of a pro-Russian hetman

until his death (Bushkovitch, 2012, p. 117). Meanwhile, the Ukrainian nobles retained their privileges and while Russia was composed by approximately ninety percent of Russians, Ukrainians represented the largest minority, making up five percent of the population (Bushkovitch, 2012, p. 135). Towards the end of the eighteenth century, Catherine the Great (reign: 1762-1796) further expanded the Russian territory through conquest, as Moscow felt threatened by the political and social changes taking place in Europe, especially the French Revolution of 1789 and the growing power of Russia's long-time enemy, Poland. Catherine defeated the Polish army and in 1772 partitioned the territories of the Polish-Lithuanian Commonwealth with Prussia, which acquired an area where mainly Polish people lived, whereas Russia carved up Western Ukraine, the rest of Belorussia and Lithuania: from this moment, Russia had become a multi-national empire that ruled over the territory of the medieval Kievan Rus, where the addition of 5.5 million new subjects made the Russian population decrease to 85 percent or even less (Bushkovitch, 2012, pp. 159–160).

Figure 3 - Map of the Expansion of Russia 1300-1896 (source: Encyclopaedia Britannica. (n.d.). Russian Empire – Peter I, Expansion, Reforms. In Encyclopaedia Britannica. Retrieved from https://www.britannica.com/place/Russian-Empire/The-reign-of-Peter-the-Great)

Throughout the eighteenth century and until 1905, the Ukrainians, which formed around 17 percent of the Russian population, played a counterbalancing role against the claims of the Polish national movements, Russia's major rival, while the Ukrainian national movement was a minor, slowly changing entity (Bushkovitch, 2012, p. 290). Indeed, Ukrainian nation-building was taking place in an international context that saw both Russia and Poland wanting to have the Ukrainians living in their territories to become either Russian or Polish; in other words: "The national identity of modern Ukrainians was formulated by those who, in defining Ukraine, rejected both the Russian identity and the Polish identity" (Szporluk, 2018, p. 85). The people we now refer to as Ukrainians only started to call their homeland Ukraine at the end of the nineteenth century, and other countries referred to them in different ways, with the Russian Empire calling them Little Russians, or Cossacks (Szporluk, 2018, p. 88). In fact, the creation of the Russian-nation is deeply connected to the idea of Little Russia, which could not exist as a separate identity to that of Russia:

> *"the construction of Russian national identity included the construction of a national history, built around the idea of a state distinguished by a thousand-year-long history, which connected Kiev with Moscow and the St. Petersburg of the tsars. This construct was first formulated in connection with Ukraine's becoming attached to Russia after 1654; the idea was that modern Russians had possessed a state of their own without interruption from the time of Kievan Rus to the present. The corollary of this was to disinherit the Ukrainians from any claim to historic statehood and thereby deny them any future claim to independent statehood.*" (Szporluk, 2018, p. 95)

In the 19th century, ethnic nationalism was a phenomenon taking place all over Europe, and while in the Russian part of Ukraine nationalism was limited to the intelligentsia, and did not expand until the 1905 Revolution, in Austrian Galicia (a former Austro-Hungarian region occupying today's Eastern Poland and Western Ukraine) the Ukrainian movement formed several nationalist parties, many of them positioned against the Russian tsars (Bushkovitch, 2012, p. 292). During the events of 1905, workers staged

strikes in St. Petersburg, while peasants, including in the Ukraine, seized the land and attacked the nobility (Bushkovitch, 2012, p. 314). In 1917, Ukrainian nationalists intellectuals managed to organize themselves in Kiev and together with party activists declared themselves the Ukrainian *Rada* (Council) alongside the local soviets that were being formed during the 1917 Bolshevik Revolution (Bushkovitch, 2012, p. 332). Differently from Belorussia, where the national sentiment was almost non-existent, in Ukraine the national intelligentsia was able to gather support among the peasants, but in the cities, the large Russian and Jewish populations were hard to mobilize (Bushkovitch, 2012, p. 356).

As a result, Moscow decided to face the nationalist threat by imposing the creation of a Ukrainian Communist Party by the local communist faction and proclaimed the establishment of the Ukrainian Soviet Republic in 1919, which, like the Belorussian republic, were formally independent from Moscow; in practice, however, their Communist Parties answered to the Central Committee in Moscow (Bushkovitch, 2012, pp. 356–357). During the Soviet era, the first years of the USSR saw a lot of investment in favour of the country's industrialisation, making Ukraine an important spot for the metal industry, particularly in the Donbas (Bushkovitch, 2012, p. 360), while in the 1930s, Moscow started a process of collectivization to make the production of grain more efficient; yet, this flawed policy, combined with unfavourable weather conditions, led to a period of famine that was exploited by Joesph Stalin to neutralize any resistance to farm collectivization, but also to silence the rise of nationalist voices (Bushkovitch, 2012, pp. 387–388).

The famine that hit the USSR between the end of 1932 and 1933 killed about five million people, and the Soviet state that suffered the most was the Ukrainian republic, which came to call this destructive experience *Holodomor*, an implicitly intentional hunger-related extermination that has come to represent a central event for the construction of the Ukrainian nation (Graziosi, 2005, pp. 1–2). Ukraine was not the only Soviet territory to suffer from the famine, which also hit Kazakhstan, the Northern Caucasus and the Volga basin; yet, the majority of the victims, which ranged from 3.5 to 3.8 million, were found in Ukraine, (Graziosi, 2005, pp. 5–6). Moscow saw the famine as an opportunity to use the imposition of the collectivization system as a way to crush the peasants in Ukrainian

villages, which represented the main source of opposition to the Communist government, whereas the cities were still predominantly populated by Russian, Jewish and Polish inhabitants (Graziosi, 2005, p. 8). As a result, Ukraine's national society was significantly weakened, therefore hampering Ukrainian nation-building; indeed, historians today have come to compare the victims of the 1930s famine, artificially strengthened by the Soviets, to the crimes of Nazi Germany that would later take place in Europe (Graziosi, 2005, p. 10).

Despite the atrocities committed by the Soviets in Ukraine during the Holodomor of the 1930s, the USSR exploited some elements of the Ukrainian nation-building to contribute to the building of the Soviet Union as a nation state: because of the great ethnic and cultural heterogeneity found in the newly formed Ukrainian Soviet Socialist Republic, Moscow worked hard to "Sovietize" and "Russify" the Ukrainians, whose national identity was strongly connected with Soviet identity, as well as with the Little Russians identity (Kravchenko, 2016, p. 450). In particular, Russia's westward expansion after 1939 raised the nationalist issue at the top of Moscow's agenda, especially between 1939 and 1945 when Western Ukraine, the main stronghold of Ukrainian nationalism, was annexed into the Ukrainian republic; instead, eastern Ukraine nationalist mobilisation was suppressed at an early stage, therefore leaving a strong feeling of ambiguity in relation to the national identity of the Ukrainian population, a phenomenon also experienced by other former Soviet entities like Belarus and Moldova (Yekelchyk, 2006, p. 523).

Following the end of the Second World War in 1945, the Baltics and eastern Ukraine went through a process of rapid industrial development, and traditionally agricultural areas were transformed into modern industrial complexes, mainly in areas like Lithuania, Belorussia, Western Ukraine and Moldavia; furthermore, local heads of the communist party in eastern Ukraine contributed to the process of Russification in the areas of education, the media and the urban environment, while at the western border of the country the Soviet secret services (KGB) constituted a vigilant presence ready to contain any sign of nationalist agitation (Yekelchyk, 2006, p. 540). Until 1989, local party leaders in Ukraine managed to suppress anti-Communist sentiments, but a series of events gradually added up to build a strong opposition to the Communist regime. For instance, while in Western Ukraine people started to mobilize in 1987 to restore the Greek Catholic

Church, Eastern Ukraine became the victim of one of the most notorious and devastating examples of the Soviet's regime ineffectiveness and dysfunctionality, namely the Chernobyl disaster of April 26, 1986, which became a symbolic and uniting factor against the government in Moscow (Yekelchyk, 2006, pp. 543–544).

As the authority of the Soviet central government in Moscow suffered a substantial blow during the August 1991 coup, the parliament of the Ukrainian republic, whose majority was still composed by Communists, issued a declaration of independence on August 24, and voted for its independence on December 1st 1991 through a referendum on Ukrainian independence supported by 90 percent of the population, including minority voters (Yekelchyk, 2006, p. 547). The newly formed Ukrainian state declared itself neutral as the Soviet Union dissolved, and it started a process of nationalism-building that was brought forward by Presidents Leonid Kravchuk (1991-1994), Viktor Yushchenko (2005-2010), and Petro Poroshenko (2014-2019), who have tried to link Ukrainian nationalism to its historical role of being a victim and subordinate of Soviet Russian colonialism that exploited the country's resources while attempting to Russify the social, cultural and political character of Ukrainian identity (Kravchenko, 2016, p. 453).

This nation-building process, however, differed depending on the region in which it was taking place. In western Ukraine, a strong de-Sovietization process was pushed in the public space, whereas in the east and the south, national discourse revived the Russian imperial historical heritage that preceded the Soviet regime, as the policies of the newly Russian Federation exerted a strong level of influence on its neighbour; in fact, cities in eastern and southern Ukraine replaced Soviet symbols with monuments of Russian imperial figures, with a strong support coming from the Russian Orthodox Church (Kravchenko, 2016, pp. 454-455). On the whole, the idea of Ukraine's modern national statehood was based on the state's descendance from the short-lived Ukrainian National republic (UNR) created in 1917, therefore leading the new state to acquire the UNR's symbol – the trident – and the colour of its flag – blue and yellow – as the official symbols of the post-1991 Ukrainian state (Kravchenko, 2016, pp. 455–456).

As the nation-building efforts in Ukraine tried to de-Sovietize its national identity and culture, the figure of Communist dictator Jospeh Stalin represented a controversial element in Ukrainian society, especially for what concerns the "Great Victory" in the "Great Patriotic War", the symbolic name given to the Second World War by Soviet Russia: one argument claims that, ignoring the countless victims of Soviet repression, Stalin's five year-plans were the reason behind the successful industrialisation of the USSR that eventually allowed the Soviets to defeat Nazi Germany, whereas others claim that, notwithstanding "the criminal incompetence of Stalin's government", the Soviet Union succeeded in defeating Adolf Hitler and the Nazis (Kravchenko, 2016, p. 459). Furthermore, the Holodomor, whose significance was revived by Presidents Leonid Kuchma (1994-2004) and Viktor Yushchenko, represents a symbolic event of the crimes of the Stalinist era, and it is officially considered an act of genocide against the people of Ukraine, therefore supporting the interpretation of Ukrainian Soviet domination as symbol of national martyrdom (Kravchenko, 2016, pp. 459–460).

Nonetheless, despite these nationalistic narratives, the mythology of the Great Patriotic War, also known as "Great Fatherland War", presenting the Soviets as saviours against Nazi Germany, is a predominant element in the historical memory of independent Ukraine, whose society "is still influenced by Russian politics of identity, in which historical amnesia and the glorification of Stalinism prevail" (Kravchenko, 2016, p. 464). In fact, while throughout the USSR period Russia renounced its national identity in the name of creating a Soviet identity transcending national and ethnic differences, once the Union was dissolved, the Russian Federation embarked upon its own path towards the revival of national identity and statehood; in fact, the Russian elite, first among them President Vladimir Putin, started to look back at the Russian imperial ideology of "Orthodoxy, Autocracy, and Nationality", the same one advocated by Tsar Nicholas I (reign: 1825-1855) to support the idea of Russia's religious and political uniqueness against European nationalisms (Hartley, 1992, p. 382; Kravchenko, 2016, p. 465). Most importantly, Russia's imperial national identity was also based on the ethnic union of Great Russians (Russians), Little Russians (Ukrainians) and White or Belo-Russians (Belarusians) (Szporluk, 2018, p. 105), and together, these three Slavic groups would form

the *Russki mir*, the geopolitical entity imagined by the new Russian elite to restore the power and status of the long-lost Russian Empire (Kravchenko, 2016, p. 465).

In other words, differently from former Soviet entities like the Baltic Republics of Estonia, Latvia, and Lithuania, which joined NATO and the European union in 2004, Ukraine has been unable to completely cut its ties with Russia, which has asserted its influence on the political, economic, and social spheres of the country. This ambivalence towards Moscow was reflected in the election of Ukrainian presidents, which alternated between anti-Russia and pro-Russia figures. For instance, Leonid Kravchuk pushed forward the Ukrainization of public society, while making efforts to stabilise Ukraine's relationship with Russia; however, his presidency failed to bring much needed economic reforms, therefore leading to the election of Leonid Kuchma (1994-2004): his campaign promised to reestablish economic relations with Russia and make the Russian language prominent again, while trying to maintain relations with the West; however, "Russian financial interests came to control much of Ukraine's industry and mass culture" (Yekelchyk, 2006, pp. 547–548). Despite presenting democratic institutions like competitive elections, the Ukrainian state after its independence in 1991 has been defined as a semi-democracy or competitive authoritarianism, labels that have been confirmed by the experience of the Kuchma presidency, as he attempted to influence the outcome of the 2004 elections with state resources and political pressure (Katchanovski, 2008, p. 356).

The attempt to rig the 2004 elections by President Kuchma mobilized hundreds of thousands of people peacefully protesting the interference in the election process, today known as the 'Orange Revolution' (Yekelchyk, 2006, p. 548). Scholars have described the protests as an "anti-oligarchic revolution" that opposed the corruption of the semi-authoritarian regime established under Kuchma's presidency (Katchanovski, 2008, p. 356), who attempted to turn the elections in favour of his Prime Minister Viktor Yanukovych, who was also supported by several oligarchs (Katchanovski, 2008, p. 358). Instead, the protests led to the election in January 2005 of a strong anti-corruption advocate and pro-Western candidate, Viktor Yushchenko, thanks to a peaceful revolution that carried the name of the colour (orange) used by Yushchenko and his supporters, and that followed the coloured revolutions in former Soviet republics such as Georgia, with the 'Rose revolution'

(2003) and Kyrgyzstan with the 'Tulip Revolution' (2005) (Katchanovski, 2008, p. 355). However, despite the transition towards a more democratic and pro-Western government, dualism between Russian and Western affiliations still pervaded the political institutions, parties, and values of Ukraine and deeply influenced its relationship with Russia (Katchanovski, 2008, p. 377).

In fact, Ukraine's lack of a consolidated civil society and a strongly independent media, as a result of the country's Soviet past, formed a legacy of power abuse by political leaders, even after the events of the Orange revolution; furthermore, the ethnic divisions between the eastern and western regions of Ukraine have fostered a context of chaotic political contestation, with the west being populated by a majority of pro-European Ukrainian speakers, and the east having high level of industrialization and historical ties to Russia (Way, 2008), connections that allowed Moscow to pursue its interests in the region. This divide inside Ukraine was also represented by the election of Yanukovich as Prime Minister from 2006 to 2007 during Yushchenko presidency which, as a result, was "characterized by a permanent fight for power between presidential and governmental branches of the executive" (Way, 2008, p. 262). This political division remained predominant in Ukraine, which witnessed the mobilisation of large demonstrations again in 2014, during what came to be known as the Euromaidan mass protests, and that resulted in the turbulent overthrow of Yanukovich, who had become the Ukrainian President in 2010, in February 2014. The Euromaidan protests represent the clash of pro-European factions against those that wanted to reconsolidate Ukraine's relations with Russia following President Yanukovich's sudden decision to back out form a free trade agreement with the EU and move towards closer ties with Russia instead, most probably after receiving pressures and incentives from the latter (Open Society Foundations, 2019). The protests highlighted the political and ethnic differences of the Ukrainian population, and Russia eventually stepped in to support the pro-Moscow factions in eastern Ukraine, therefore leading to the annexation of Crimea, which will be analysed in the following section.

4.2 Hybrid War in Ukraine and the 2014 Annexation of Crimea

As it has been mentioned in the previous chapters, the 2014 annexation of Crimea is linked to the rise in use of the term hybrid warfare for what concerns Russia's activities in Ukraine (Reichborn-Kjennerud & Cullen, 2016, p. 1), which includes the tactics and strategies employing the use of proxies to avoid attribution of the attacks, as well as to increase uncertainty around the real goals and intentions of the attacker (Iasiello, 2017, p. 60). Like Ukraine, Crimea is a territory that has been ruled by different peoples and regimes throughout its history: the Crimean Khanate was born from the Golden Horde in the 15th century, later becoming a vassal state under the Ottoman Turks, and was eventually conquered at the end of the 18th century, in 1783, by the Russian Empire following its victory over Ottoman Turkey, whose Islamic influence is still present today (Szporluk, 2018, p. 87). Under the USSR, the Soviets established the Crimean Autonomous Soviet Socialist Republic, but a significant part of the Crimean Tatar population died following an ethnic cleansing campaign pursued by Moscow to punish the Crimeans for their alleged collusion with the Germans during the Nazi occupation that lasted between 1941 and 1944, a campaign that was followed by the transfer of several Russian and Ukrainian migrants in the region; in 1954, during a period of de-Stalinisation, Crimea was officially reunited with the Ukrainian Republic by the new Soviet leader Nikita Khrushchev (Katchanovski, 2019, pp. 81–82; Samabaluk, 2022, pp. 24–25; Szporluk, 2018, p. 88).

As a result, the population of the Crimean peninsula is very heterogenous, and because of the different populations that moved into the region over the centuries, even after the break-up of the Soviet Union and Ukraine's independence, a census from 2001 found that the majority of the Crimean population, 58 percent, identified as ethnic Russian, whereas only 24 percent declared itself to be Ukrainian, therefore making Crimea a region with a Russian ethnic majority, the only one in Ukraine (Katchanovski, 2019, p. 82). As a matter of fact, Ukraine is divided into a predominantly Catholic and pro-European West, and an Eastern part, that is mainly Orthodox Chirstian and displays a strong social, ethnic, and linguistic Russian heritage (Samabaluk, 2022, p. 84). Like in Eastern Ukraine, Crimean people have showed pro-Russian attitudes in the political life of Ukraine, particularly after

the 2004 Orange Revolution, as the region overwhelmingly supported Viktor Yanukovich during the 2014 Euromaidan protests (Katchanovski, 2019, pp. 83-84).

At the same time, Russia's attitudes towards Ukrainian independence shifted following 2014, with the Kremlin asserting that Ukraine's accession to NATO represented an "unacceptable threat to the security of Russia", and prominent Russian figures started to advocate for the reunification of Crimea and Sevastopol, two important spots for Russia's access to the Black Sea, with the Russian Federation (Katchanovski, 2019, pp. 84–85). As Yanukovich was violently overthrown and fled to Russia, Moscow took action to support separatists in Crimea and eventually annex it to Russia, mainly by adopting the narrative that the Euromaidan was a fascist coup and that Russia had the duty to protect its ethnic Russian population from the Euromaidan 'fascists' supported by the US (Wilde & Sherman, 2023, p. 14); in fact, Putin claimed its obligation to protect the Russian ethnic minority against the Ukrainian "Other" (Kravchenko, 2016, p. 468), whose closer ties with Europe and the United States represented, according to Putin's narrative, another element of the Western powers' strategy to isolate Russia (Wilde & Sherman, 2023). In addition, intervention in Crimea was also justified by the need its national security interest by preventing its main Blacks Sea naval base from being brought under NATO jurisdiction (Katchanovski, 2019, p. 85; Samabaluk, 2022, p. 38).

The conflict in Crimea started on February 27 and February 28, when pro-Russian separatists, assisted by Russian army forces without insignia, also known as 'little green men', seized control of key Crimean institutions, such as the Parliament and other government buildings, while also taking control of Ukrainian military posts; following the coup, a controversial referendum was held on March 16 which resulted in 97 percent of Crimean voters wanting to secede from Ukraine and join Russia, whereas Ukraine and the West claimed that the referendum was illegal and illegitimate, since only a minority supported separatism in Crimea; yet, 91 percent of the population considered the referendum free and fair according to a survey held in April 2014 in the peninsula (Katchanovski, 2019, p. 86). Immediately after the referendum a deal was signed in Moscow on March 18, where Russian and Crimean leaders agreed to unite the Crimean Peninsula with Russia (Open Society Foundations, 2019). Later in April 2014, Russian-

sponsored separatist action emerged in Eastern Ukraine, mainly in the Donbass cities of Donetsk and Lugansk, where an armed conflict eventually emerged and the two cities proclaimed themselves as the Donetsk and Lugansk People's Republics (Open Society Foundations, 2019; Samabaluk, 2022, p. 85), as illustrated in the map below. This conflict, together with the activities mounting to Crimea's annexation, have been referred to by analysts and scholars as hybrid warfare, in which Russia has been employing both traditional kinetic operations as well as cyber-attacks and information campaigns, therefore engaging in a multi-dimensional conflict affecting various aspects of the targets' lives (Danyk et al., 2017, p. 9), thereby adding information, cyber, and economic, diplomatic, political and social elements to their hybrid warfare strategy (Schnaufer II, 2017, p. 19).

Figure 4 - Map of the territory annexed by Russia in March 2014 and Russia-Backed separatist-controlled (Source: Snegovaya, M. (2015). Putin's Information Warfare in Ukraine. http://www.jstor.com/stable/resrep07921.1)

One of the main goals behind the employment of hybrid warfare tactics was to erode people's trust and confidence in the authority of the Ukrainian government, mainly through information campaigns targeting Ukraine's government and authorities, such as the Ukrainian Armed Forces, as an effective way to spread chaos and destabilize the social and political spheres of the country; in order to achieve this, Russia combined cyber

operations and information warfare with unconventional forces on the ground (Danyk et al., 2017, p. 10). The Spetsnaz forces, Russia's elite soldiers working behind the line in Crimea, focused on the disruption of communications; in particular, they engaged in electronic warfare against communication systems and targeted one of Crimea's Internet Exchange Points to sever communications with other territories (Libicki, 2020, p. 700). Russia's physical attacks on Ukraine's communication and digital infrastructure, alongside with the seizure of the Internet Exchange Point, included actions such as cutting data cables, gaining control of servers, confiscating cell phones, and the rerouting of "internet traffic via Russian network nodes" (Pernik, 2018, p. 62), all of which granted Russia information superiority by interrupting communications between Crimea and the rest of Ukraine (Samabaluk, 2022, p. 85).

Furthermore, both Russian and Ukrainian employed hackers and other cyber actors to conduct noticeable, yet minor, cyber-attacks that did not reach the level of intensity of the Russian cyber-attacks on Estonia or Georgia analysed in the previous chapter (Libicki, 2021, p. 701), such as Distributed Denial of Service attacks (DDoS), the hacking of CCTV (closed-circuit television) cameras and website defacements (Abdyraeva, 2020, p. 22). Among the cyber actors supporting Russian war efforts against Ukraine's media and government we find agents such as CyberBerkut, Green Dragon and Cyber Riot Novorossiya (Abdyraeva, 2020). For instance, CyberBerkut, which was called after the riot police (Berkut) that Yanukovich unleashed against the Euromaidan protestors, is an anti-Ukrainian hacker group that engaged in the delivery of a series of DDoS attacks, the defacement of Ukrainian and NATO websites, and the interception of military documents concerning the cooperation between American and Ukrainian forces (Iasiello, 2017, p. 55).

CyberBerkut has also been linked by Canadian researchers to the Russian APT28, Fancy Bear, run by the GRU, also responsible for the attacks on the Ukrainian Central Election Committee (Samabaluk, 2022, p. 86). The attacks that hit the election digital infrastructure in April and May 2014 erased the information found in the databases and employed a malware that produced a 24-hour delay in the 2014 election results announcement on the website of the Central Election Committee (Pernik, 2018, p. 62). Moreover, cyber-attacks also included the spread of malware targeting the Android devices

of Ukrainian troops and transforming them into signals that would allow Russian forces to track and target them (Samabaluk, 2022, p. 86). These attacks, albeit with no hard proof of Russian collusion, served Moscow's strategy of using information operations to inhibit the enemy's ability to take action, as advocated by the Russian doctrine on the future of warfare developed by Valery Gerasimov, Chief of the Russian General Staff (Iasiello, 2017, p. 55; Snegovaya, 2015)

In addition to cyber activities taking place during the conflict, some have hypothesised that Ukrainian systems had been targeted and penetrated by Russian APT's in 2010, and they have been active ever since (Pernik, 2018, p. 61). One example of this was the BlackEnergy malware run by the Sandworm hacker team, which targeted critical infrastructures in Ukraine to conducted careful reconnaissance operations; in fact, BlackEnergy had been used by Russian APT hackers in the past as a cyberespionage tool, an instrument that might be employed in the early stages of sophisticated cyber-attacks (Samabaluk, 2022, p. 88). Sandworm was also responsible for the attacks on Ukraine's electrical power grid in both December 2015 and December 2016 (Samabaluk, 2022, p. 89), state-sponsored cyber-attacks that attested to Russia's high level of cyber skills sophistication (Abdyraeva, 2020, pp. 22–23).

Yet, these destabilising attacks were followed by an intense period of Russian cyber activities targeting Ukraine: President Petro Poroshenko announced that in the two months preceding the 2016 power grid attack, 6500 cyber-attacks hit more than thirty Ukrainian targets (Samabaluk, 2022, p. 89), which included critical infrastructure like the airport of Kyiv and the financial sector, such as the Treasury (Pernik, 2018, p. 61). Then, in 2017, Ukraine was further hit by NotPetya, a malware was launched by the Russian military intelligence through an accounting software, which hit the nuclear plant of Chernobyl as well as approximately 13,000 devices in different sectors of Ukraine, from public institutions and banks, to newspapers and transport infrastructure (Przetacznik & Tarpova, 2022, p. 3). The NotPetya attack "disabled 10% of computers in Ukraine and inflicted financial costs amounting to 0.5% of Ukraine's GDP", and later reached other countries as well (Pernik, 2018, p. 62): the malware spread globally and hit 65 countries, but mainly

European and American businesses, causing losses for an estimated $10 billion (Przetacznik & Tarpova, 2022, p. 3).

While these cyber-attacks on digital and critical infrastructure caused significant damage to the economy of Ukraine, what is most significant about Russia's hybrid warfare is the deployment of disinformation operations through the adoption of "complexes for conducting information-psychological activities and actions in cyber space" (Danyk et al., 2017, p. 9), which have been used as an effective way to erode trust in democratic institutions and processes. In particular, the Euromaidan protests raised high levels of angst in the Kremlin, which felt threatened by anti-Russian movements gaining strength in neighbouring Ukraine; as a result, Putin brought together cyber mercenaries and propaganda strategies, traditionally used on its domestic audiences, to spin a specific narrative portraying the Ukrainian people demonstrating in Kiev's Maidan square as 'fascists' in collusion with Western powers, who posed a threat to Russia's internal stability by interfering in its near abroad (Wilde & Sherman, 2023, p. 14). In turn, this narrative was complemented by an active disinformation campaign on the ground, aimed at discrediting Ukrainian armed forces in order to undermine their efforts in traditional kinetic operations; through the use of cyber proxies and false fronts on the Internet, Russia launched a cyber aggression in the form of disinformation spreading negative information on the Ukrainian army and government (Danyk et al., 2017, p. 13).

In practice, the spread of disinformation and false information was fostered by the use of the Internet, given that the Russian Federation hosted several Internet resources in Moscow, therefore allowing the Kremlin to oversee the flow of information in Ukraine (Danyk et al., 2017, p. 13). Social media in particular have played an important role in the presentation of Moscow's narrative of depicting Russia as a saviour coming to aid Crimean people in a crisis (Bergh, 2020, p. 110) and Russian social media companies have also blocked the activities of Ukrainians opposing Moscow on social network (Pernik, 2018, p. 62). In fact, for those conducting information operations aimed at influencing opinions and even behaviours, social media have the advantage of disinhibiting particular types of conduct that would be restricted by common civic norms, and it can also potentially affect the way individuals perceive and process new information in the future; in other words,

information campaigns have a significant impact on the way the target's domestic audience perceives an ongoing conflict, therefore allowing the attacker to weaken the support of the population for the government under attack, while also granting the aggressor the advantage of concealing its strategies and intentions through the manipulative use of technology (Danyk et al., 2017, p. 14). Furthermore, Moscow's manipulation of Russian-sponsored national media establishments in Ukraine harnessed the weaknesses of Ukraine's socio-political system, and Russian forces launched their information warfare campaign based on unreliable sources and negative narratives at the same time of the beginning of traditional warfare that took place in the Donbass region in 2014 (Danyk et al., 2017, p. 15). Overall, the result of these information campaigns through cyber aggressions was the increased level of distrust and disaffection towards state authorities, therefore mining the internal stability and cohesiveness of both the Ukrainian government and its military (Danyk et al., 2017, p. 14).

Among the entities engaged in social media information campaigns in Ukraine we find the Russian Internet Research Agency (IRA), whose agents spread news and media reports that compared pro-Russian separatist "militias" and the Ukraine army, referred to as "national guard" or "volunteer battalions", in a way that placed the two on the same level of legitimacy and moral standing, a narrative that was also employed to depict Ukraine as a mere borderland, and not a sovereign state, as well as to discredit Ukrainian efforts with additional fake news and disinformation (Samabaluk, 2022, p. 87). These disinformation campaigns often included creation of allegedly real life stories meant to manipulate the population, and one notorious example is that of Igor Krasovskiy, a medical doctor based in Odessa who spread online the story that Ukrainians were responsible for grave acts of violence and denied their victims medical assistance; however once English, German and Bulgarian translations of the violence appeared, analysts found that doctor Krasovskiy was in fact a dentist from the Caucasus, living several hundreds of miles away (Samabaluk, 2022, p. 87). Russian activity on social media through the use of bots and trolls did not stop once the annexation of Crimea was completed. Indeed, research has found that: "in early 2017 [that] trolls were being employed for about $1,000 per month to pump anti-Ukrainian propaganda into online discourse, complementing IRA's ongoing campaign of disparagement against international media and other entities whose reporting

or statements are deemed unfriendly by Kremlin decision-makers" (Samabaluk, 2022, p. 90). In fact, further investigations uncovered Russian attempts to gain access to actual Ukrainians' social media accounts in order to operate with a thicker veil of legitimacy, and this strategy has also been detected during the preparations of the 2019 Ukrainian presidential elections (Samabaluk, 2022, p. 90).

Furthermore, Russian disinformation efforts during the 2014 conflict also concerned the manipulation of real-life events, such as distortion of the circumstances surrounding the shooting down of Malaysian Airlines flight MH17 on July 17, 2014, by a Russian surface-to-air missile (SAM). After hitting the MH17 flight, a Boeing 777-200 flying from Amsterdam to Kuala Lumpur, the Russian propagandists started to share an array of absurd and contradictory claims concerning the causes and circumstances behind the MH17 incident, with the goal of raising a general feeling of confusion and doubt that hindered the development of a united response by international actors; in fact, despite having discovered that the SAM equipment had been brought by the Russian military into the Ukrainian regions where pro-Russian separatist were in control, a revelation made thanks to online crowdsourcing of evidence, Moscow responded to the allegations with a strong disinformation campaign and even threatened the individuals behind the crowdsourcing efforts (Samabaluk, 2022, p. 88). Russia's allegations ranged from blaming the airline for routing the plane over a conflict zone, to blaming Ukrainians missiles and jetfighters (Samabaluk, 2022, p. 87). Russia's strategy of intentionally creating false and contradictory narratives around the MH17 flight served the purpose of concealing the truth behind the shooting down and, as a result, the international public, Europeans in particular, failed to answer to the crisis in a more resolute and effective way than the use of sanctions (Samabaluk, 2022, p. 88).

Overall, these hybrid warfare tactics, encompassing the use of information campaigns, that have been employed by the Russian Federation in Ukraine since February 2014 in the context of the annexation of Crimea, are the result of Moscow's limited budget and relative weakness in economic and technological terms compared to other Western nations (Snegovaya, 2015, p. 9). By spreading disinformation during the 2014 conflict, Russia was able to confuse its adversaries and distract them while conducting under the

radar kinetic operations, therefore granting the Kremlin a sort of diplomatic cover for its military activities and foreign policy projects that protects it from retaliation by Western powers; in practice, Putin and his administration have engaged in a form of information warfare that translates the Soviet doctrine of reflexive control to the current international scenario (Snegovaya, 2015, p. 10). Initially conceptualized by Soviet scholar Vladimir Lefebvre, 'reflexive control' represents an expansion of information-psychological operations taken by Russia in Ukraine (Iasiello, 2017, p. 55), and it is defined by Timothy L. Thomas as:

> "*a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action*." (Thomas, 2004, as cited in Snegovaya, 2015, p. 10)

If we look at the 2014 Ukrainian conflict by applying a reflexive control framework, it can be noticed that Russian diplomatic sources and media outlets have actively worked to shape the image of the government in Kiev as an entity affiliated with Stepan Bandera, head of the 1940s pro-Nazi Organization of Ukrainian Nationalist known for its brutal methods, while "patriotic hackers" launched attacks on Ukrainian institutions, all aimed at discrediting the government and undermining its legitimacy by attributing the term 'fascist' to it (Snegovaya, 2015, pp. 12–14), a tactic adopted due to the resonance of anti-Nazi and anti-fascist propaganda among the Russian public, both at home and abroad. For what concerns cyber-enabled information warfare in Ukraine, many have argued that the use of information technologies represented an innovative strategy, as Moscow employed trolls to distort online conversations towards pro-Russian narratives, and bots to bombard online users with spam messages (Bokša, 2019, p. 6; Snegovaya, 2015, p. 14); indeed, trolls play an important role in online misinformation, as they alter the truth by creating fake content legitimising their narratives and they spread information that is left unchecked by Western media (Schnaufer II, 2017, pp. 27–28). Furthermore, Russia's activities in Ukraine resembled KGB-like active measures that comprise "disinformation, propaganda, political repression and subversion" operations, which were aimed at eroding the unity of the West and NATO, while discrediting the authority of the US as a world

power; in fact, an example of such activities included the airing by Russian television channels, in May 2015, of a documentary titled "Warsaw Pact. Declassified Pages", which allegedly revealed the involvement of the US Central Intelligence Agency (CIA) in the 1968 movements that took place in Czechoslovakia, during the events known as the Prague Spring (Snegovaya, 2015, p. 14).

Overall, as it has also been argued in the previous chapters of this thesis, social media significantly expands the scope of information warfare, while also magnifying the effects of disinformation thanks to new technological innovations that contribute to the development of computational propaganda, such as "deep fake" content (Bokša, 2019, p. 1). This type of propaganda and disinformation centred around the *Russkiy Mir* (Russian World) narrative, which targeted ethnic Russians and Russian-speaking populations abroad in order to create a sense of solidarity and compatriotism between Russian minorities in foreign countries (Bokša, 2019). As a matter of fact, this narrative was particularly fit to the case of Crimea, where at the time of the conflict more than half of its population was Russian-speaking, and therefore pro-Russian; yet, Russia's interest in Crimea went beyond patriotic feelings, since the peninsula represented "Russia's only year-round warmwater port, hosting a large portion of the Russian military—the navy's Black Sea Fleet" (Iasiello, 2017, p. 54). In short, while Russian propaganda in Crimea and eastern Ukraine was spun around a narrative of ethnic solidarity, Moscow's disinformation campaign in the West, and especially Europe, was less focused on presenting a coherent and convincing narrative, and more aimed at creating a sense of confusion and frustration stemming from contradictory and distorted information (Iasiello, 2017, p. 56).

Despite the overall success of Russia's hybrid warfare in the 2014 Ukraine conflict, as shown by the regions of Donetsk and Lugansk gaining a special status through a Ukrainian Constitutional Amendment, and the lack of an international response to the Crimean annexation thanks to Moscow's denial of interfering in Ukraine through disinformation (Snegovaya, 2015, pp. 15-18), some limitations appear. In fact, Russia's influence in Ukraine is only localised, and RT's low reputation in the West hindered Russian media's ability to shape the beliefs of Europeans about the events of 2014 (Snegovaya, 2015, p. 19). For instance, while Russian propaganda has been spread by

several German media establishments, as part the Kremlin's overall strategy to exploit "European anti-U.S. sentiment and Germany's post-WWII guilt complex towards Russia", as well as Germans' nationalism sensitivity, the German version of RT, RT Deutsch, did not establish itself as a leading television broadcaster, but limited itself to sharing content through its Internet channel (Snegovaya, 2015, p. 19). Nonetheless, it is important to not underestimate dissatisfied individuals in European societies, who might be more susceptible to the influence of Russian propaganda, serving as dangerous, but useful, "idiots" (Snegovaya, 2015, p. 21).

Following Russia's attacks on Ukraine, but also those on Georgia and Estonia, member states of the EU presented different views of the Russian Federation, as a study found that for countries like Austria, Ireland and Italy, Russia was still perceived as a trade partner; Cyprus and Greece had positive views of Moscow due to their cultural ties; trust was weakened in countries such as Belgium, Croatia, France and Malta; Denmark and Germany saw an increase in distrust; and Hungary actually developed closer ties with Russia despite Moscow's history of cyber aggressions (Samabaluk, 2022, pp. 94–95). As a result, western countries took actions to contrast Russia's disinformation campaigns and debunk the fake news pumped by the Kremlin into national and social media platforms of Western countries (Bokša, 2019, p. 11). For what concerns the initiatives taken by the EU in response to Russian involvement in the Ukrainian conflict, in which the clash between Ukrainian armed forces and Russian-sponsored separatists left more than 5000 killed between April 2014 and January 2015 (European Parliament, 2015a), the European Parliament adopted a resolution on 15 January 2015, in which it:

> "Strongly condemns Russia's aggressive and expansionist policy, which constitutes a threat to the unity and independence of Ukraine and poses a potential threat to the EU itself, including the illegal annexation of Crimea and waging an undeclared hybrid war against Ukraine, including information war, blending elements of cyber warfare, use of regular and irregular forces, propaganda, economic pressure, energy blackmail, diplomacy and political destabilisation". (European Parliament, 2015b)

Furthermore, the Resolution also called on the Commission and the Commissioner for European Neighbourhood Policy and Enlargement Negotiations to develop a "strategy to counter the Russian propaganda campaign directed towards the EU, its eastern neighbours and Russia itself, and to develop instruments that would allow the EU and its Member States to address the propaganda campaign at European and national level" (European Parliament, 2015b). As a result, in March 2015 the High Representative of the EU was tasked by the European Council (European Council, 2015) to create the *East StratCom Task Force* as part of the European External Action Service (EEAS) Strategic Communications and Information Analysis Divisions (EEAS, 2021a), whose "EUvsDisinfo" flagship project was established in 2015 to contrast Moscow's ongoing disinformation campaigns affecting the EU and Eastern Parentship countries (EUvsDisinfo, n.d.). Furthermore, the Ukrainian media NGO Media Reforms Centre established the StopFake website in 2014 to debunk Russian propaganda in the country (Bokša, 2019, p. 2011). In short, the Ukraine conflict of 2014 represented a triggering event in Europe, as the EU and its Member States gained consciousness of the scope and gravity of Russia's disinformation spreading among their own citizens.

In addition to strongly condemning Russian activities in Ukraine, EU governments, together with other Western states, imposed a regime of travel and economic sanctions against those directly involved in the annexation of Crimea, where Western companies were not allowed to operate freely following the imposition of the sanctions (Katchanovski, 2019, p. 87). In fact, the first round of sanctions came following a meeting of the Foreign Affairs Council, where the Foreign Ministries of the EU member states declared the independence referendum held in Crimea as illegal and condemned the violation of sovereignty of the Ukrainian state (Council of the European Union, 2014b). On 6 March 2014 the European Council imposed a set of "restrictive measures against 21 officials, and the persons and entities associated with them for their role in actions threatening the territorial integrity, sovereignty and independence of Ukraine" (Council of the European Union, 2014b). Since then, the EU has adopted a series of retaliatory measures against Russia over its actions in Ukraine, which include individual and economic sanctions as well as diplomatic measures, that have been extended over the years (Council of the European Union, 2023d), until the Russian invasion of Ukraine that took place in February

2022 pushed the EU to take additional measures, particularly in the face of Russian cyber and information warfare campaigns, which will be explored in the next section.

4.3 The 2022 Invasion of Ukraine: Russian Hybrid Warfare in Action

4.3.1 The Build-up to the Invasion and the Conflict in Brief

Despite the negotiation of cease fires and peace agreements, tension remained high in eastern Ukraine where the 2014 conflict emerged, particularly in the Donbass region. In fact, diplomatic discussions that began in June 2014 resulted in the signing of the 'Minsk Protocol' on 5 September 2014 by the Trilateral Contact Group formed by representatives from Ukraine, Russia and with the Chairperson-in-Office of the Organization for Security and Co-operation in Europe (OSCE) as the mediator, and on 11 and 12 February 2015 the Group signed the 'Minsk II', officially known as the Package of Measures for the Implementation of the Minsk Agreements (French Ministry for Europe and Foreign Affairs, 2022). The agreement aimed to reintegrate the contested areas held by separatists with Ukraine, and it initially helped reduce the number of victims caused by the conflict; however, neither Ukraine nor Russia were willing to respect the agreement, and political tensions continued to ignite the conflict between Russian and Ukrainian forces (French Ministry for Europe and Foreign Affairs, 2022). With the 2019 election of current Ukrainian President Volodymyr Zelenskyy, a former actor and comedian who was supported by over 73% of voters, significant progress in reducing the intensity of the conflict was made by his administration, to reduce the intensity of the conflict, which managed to implement further ceasefires measures on July 27 2020 (French Ministry for Europe and Foreign Affairs, 2022).

However, in the spring of 2021 Russia started a military build-up near the border with Ukraine, under the excuse of conducting military trainings and in November, Russia's continued massing of Russian troops was captured by satellite images, with projections estimating that Russian forces would surpass 100,000 troops (Reuters, 2022). In December,

the tension grew as Russia made demands to NATO asking the organisation to remove its troops and military armaments from Eastern Europe, while also requesting NATO to deny its membership to Ukraine, which amended its constitutions to establish "NATO membership as a strategic foreign and security policy" in February 2019 (Walker, 2023, p. 16). As Moscow expressed its dissatisfaction with Washington's response to Russian demands, the West grew anxious about the possibility of a Russian invasion of Ukraine, and warned Putin of burdensome economic sanctions if military action were to be taken against Ukraine (Reuters, 2022).

On 21 February 2022, the Russian President made a TV address in which he claimed that Russia and Ukraine are inextricably linked by their common history and that the Ukrainian government in Kyiv is a "puppet regime" manoeuvred by foreign forces: he claimed that a "genocide" is being enforced by Ukrainian forces against Russian speakers, therefore it is Russia's duty protect the population in the separatist regions and to "denazify" Ukraine (Putin, 2021). In fact, the Russian President stressed the idea that:

> "Ukrainian society was faced with the rise of far-right nationalism, which rapidly developed into aggressive Russophobia and neo-Nazism. This resulted in the participation of Ukrainian nationalists and neo-Nazis in the terrorist groups in the North Caucasus and the increasingly loud territorial claims to Russia. A role in this was played by external forces, which used a ramified network of NGOs and special services to nurture their clients in Ukraine and to bring their representatives to the seats of authority". (Putin, 2021)

Once again, Putin's anti-fascist propaganda and narrative was employed to gain support from both domestic audiences and sympathizers in Ukraine. Furthermore, Putin recognised the independence of the separatist regions of eastern Ukraine and ordered so-called 'peacekeepers' to move into this area, while on Feb 23, the eve of the invasion, separatists supported by Russia demanded Moscow's assistance in fending off Ukrainian armed forces (Reuters, 2022).

On February 24, 2022, Vladimir Putin authorized “special military operations” in Ukraine and launched a full-scale invasion by land, sea, and air, and started by striking Ukrainian cities with missiles, including Kiev, and military strongholds, with communication and transportation infrastructure, but also hospitals and residential areas, suffering substantial damages (Council on Foreign Relations, 2023). On the ground, Russian armed vehicles and troop columns marched towards Ukraine passing through Belarus to the north, towards Kharkiv from the northeast, from the annexed region of Crimea to the south, and to the east from the Donbass region (Westfall, 2023).

Figure 5 - Russian Troops advancement in March 2022 (source: BBC. (2022), Ukraine conflict: Your guide to understanding day eight. BBC News. https://www.bbc.com/news/world-europe-60606539)

Following the announcement of a reduced military activity of Russian forces in March 2022, and the withdrawal of all Russian troops from Kiev, Moscow launched a new offensive in the east of Ukraine that allowed Russia to gain control of Mariupol, a city with a strategic valence thanks to its location as a southeastern port city (Council on Foreign Relations, 2023). In fact, Russia’s attacks have been mainly focused on hitting the east and south of Ukraine, targeting port cities on the Black Sea and the Sea of Azov: Russia gained control of several Ukrainian ports, and implemented a blockade on food exports from Ukraine, therefore exacerbating the ongoing global food crisis (Council on Foreign

Relations, 2023). In addition to having significant impact on the food sector, the conflict also raised concerns over the emergence of a nuclear disaster, since in August 2022, Russian forces seized the nuclear plant of Zaporizhzhia the largest in Europe, and tensions between Ukrainians operating the plant and Russian forces made the safety of the nuclear plant precarious (Council on Foreign Relations, 2023).

Between September 2022 and the end of the year, Ukraine's counteroffensive allowed Ukrainian forces to regain control of the territories occupied by Russia, such as the city of Kherson and the area west of the Dnipro River; as a result, Moscow redirected its forces towards the Donetsk region with additional support troops in preparation for the offensive launched on February 2023 (Council on Foreign Relations, 2023). Indeed, after a stalemate period that lasted through the winter, Russia planned to acquire control of the entire Donbass region by March 2023, but only managed to seize the city of Bakhmut, a city with a small population that does not have a high strategic value. Following the destruction of the Nova Kakhovka dam, near Kherson, on June 6 2023, Ukraine engaged in a counteroffensive aimed at penetrating Russian defences in the Donetsk region (Council on Foreign Relations, 2023). At the time of writing of this thesis, September 2023, the Ukrainian counteroffensive is far from over, and the conflict is still raging on, both on the ground and in cyberspace, where both Ukraine and Russia have been launching cyber-attacks to support their kinetic campaigns; for this reason, we will now focus on the cyber-attacks witnessed during the Ukrainian Invasion until this day.

4.3.2 Russia's Cyber and Information Operations in Ukraine

Cyber-attacks have been an ongoing presence in Ukraine since the annexation of Crimea in 2014 (Council on Foreign Relations, 2023), and their intensity has been increasing during the period of time leading up to the invasion of 2022; this marked the beginning of a hybrid conflict in which military action on the ground was accompanied by a cyber campaign that started with a damaging cyber-attack against different sectors of the Ukrainian state (Microsoft, 2022, p. 2), with the most targeted being the public administration, the financial sector, the media establishment, information and

communications technologies (ICT) and transportation (Cyber Peace Institute, 2023). However, since the beginning of Russia's military operation, the cyber campaign against Ukraine has been rather limited, with the effects going from denying access to basic services, such as accessing medicines, food and aid resources, to stealing data and spreading disinformation with the employment of deep fakes; nonetheless, these attacks played a significant role in the Ukrainian conflict, which included "sending of phishing emails, distributed denial-of-service attacks, and use of data-wiper malware, backdoors, surveillance software and information stealers" (Przetacznik & Tarpova, 2022, p. 1)

Before the beginning of the invasion, in the first months of 2022, Ukraine had been targeted by a growing number of cyber aggressions. On January 13, a report from Microsoft found that Ukraine's government, numerous non-governmental organisations and IT companies were targeted by malware activity, and the next day, hackers managed to take temporary control of seventy websites of Ukrainian governmental institutions, such as the Cabinet of Ministers, the Ministry of Defence, the Ministry of Foreign Affairs, and the Ministry of Education and Science (Przetacznik & Tarpova, 2022, p. 3). A month later a strong Distributed Denial of Service attacks, allegedly launched by the Russian GRU, hit the websites of Ukraine's armed forces, the Ministry of Defence, the public radio, and Ukraine's two largest banks, Privatbank and Oschadbank, whose services were interrupted for two hours (Antoniuk, 2022). On February 23 another attack targeted the same websites, and the "HermeticWiper data-wiping malware, whose goal is to delete or destroy an entity's access to its data, was launched against 100 organisations from the financial, IT and aviation sectors" (Przetacznik & Tarpova, 2022, p. 3).

One of the most destructive cyber-attacks against Ukraine took place on the day of the invasion, an hour before it officially began (Przetacznik & Tarpova, 2022, p. 2). A cyber-attack was launched on the Viasat Inc's KA-SAT satellite system, the network responsible for providing internet access to a large part of people in Ukraine and Europe; in practice, the attack disturbed broadband internet access by disabling the modems communicating with the satellite network (CyberPeace Institute, 2022). Researchers linked the attack to the "AcidRain" malware, and in May 2022 the EU and the members of the Five Eyes group attributed the malware to the GRU, with the remarks of US Secretary of

State Antony Blinken supporting the claim that Russia's cyber-attacks aimed "to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries." (Blinken, 2022). The impact of the attacks was not limited to damages suffered by the Ukrainian miliary forces and the government in Kiev, but the attack also seriously disrupted the civilian population by denying Ukrainians access to the internet, to communicate and to retrieve information concerning the conflict; furthermore, the impact of the attack spilled over into Ukraine's European neighbours, with an energy company in Germany losing remote monitoring access of almost 6,000 wind turbines, almost 9,000 subscribers of a satellite internet service provider in France lost their internet connection, and thousands of subscribers in Europe experiencing a similar internet outage (CyberPeace Institute, 2022).

In March 2022, cyber-attacks continued, and they kept targeting government websites. As an example, the pro-Russian cyber actor active CaddyWiper malware penetrated, on March 14, the computer systems of Ukrainian governmental and financial organisations; furthermore, Ukraine also suffered from phishing attempts employed by the Russian cyber threat actor APT28 targeting UKRNet, a popular media company in Ukraine (Council on Foreign Relations, 2023), as well as phishing attempts against the armed forces and the government. Additional attacks involved the installation of surveillance software, detected on March 20; on 30 March, the user credentials of Ukrainian individuals and organisations were violated by the MarsStealer information stealer; again, in April 2022, users of government and media systems saw their credentials and sensitive information stolen by a group of hackers (Przetacznik & Tarpova, 2022, p. 2). The following month, military operations on the ground were supported by a cyber campaign launching attacks on government websites and telecommunication services, such as the cyber-attack hitting the Odesa City Council at the same time the city's residential areas were hit by a missile attack (Przetacznik & Tarpova, 2022, p. 3).

Overall, as the conflict between Russia and Ukraine raged on, and is still active today, so did Moscow's cyber campaign; yet the strategy and modality behind cyber-attacks remained quite constant. Based on an analysis of recent cyber-attacks detected in the conflict, the Cyber Peace Institute has found that the most recurring cyber aggression are DDoS attacks, which represent almost ninety percent of all cyber incidents, with the most targeted sectors being,

still, government institutions, mainly the public administration, the media, the ICT and financial sector, and transportation infrastructure (Cyber Peace Institute, 2023, p. 4). Interestingly, the analysis also found that cyber-attacks peaked in May 2023, the same month in which Russia commemorates the defeat of Nazi Germany in the Second World War, therefore bearing an almost symbolic value given the patriotic valency attributed by Russians to the victory achieved by the Soviets (Cyber Peace Institute, 2023, p. 6). The most prolific hacker group of the April-June 2023 period was the *People's Cyber Army*, responsible for almost sixty percent of detected attacks, and likely affiliated to the *KillNet* group, but uncertainty still remains around the People's Cyber Army true origin (Cyber Peace Institute, 2023).

KillNet has become a notorious pro-Kremlin hacktivist collective that self-proclaims as an "army of cyber partisans", which exploits pro-Russian media to support and spread narratives produced by the Russian government; therefore, due to its loyalty to the government in Moscow, its activities intensified with the start of the Ukrainian conflict, yet, no direct link between the collective and the Kremlin has been found (Flashpoint, 2023). In addition to conducting cyber-attacks against Russia's enemies, KillNet hacktivists are also engaged in influence operations; in fact, "One of their main objectives is to shape domestic perceptions of Russia's position in the cyber warfare landscape, while also showcasing their DDoS capabilities through media exposure and propaganda material" (Flashpoint, 2023). Therefore, KillNet represents an example of the combination of elements of cyber and information campaigns that have been employed in the hybrid conflict in Ukraine.

As a matter of fact, cyber-enabled information warfare operations have been frequently targeting the Ukrainian population as well as the armed forces, given that their conjunction with cyber-attacks and kinetic campaigns has enabled the Russian government to maximise their war efforts (Microsoft, 2022, p. 72). Indeed, as soon as the invasion on Ukrainian ground started, the Kremlin launched its narrative supporting its war efforts, and disseminated it through various Russian-sponsored media outlets, while Kremlin-sponsored groups where engaged in expanding the reach of the narrative through the Internet (Microsoft, 2022, p. 74). In particular, pro-Kremlin social media accounts are working to consolidate the narrative that the Ukraine conflict is staged, and that reports portraying the Ukrainian population in critical

conditions, as well as their death, are in fact fake news (Dale, 2022). Below, a graph illustrating the Russian Propaganda Index shows how Moscow's propaganda peaked during the Ukraine invasion of 2022, around the 2nd of March, 216% increase in propaganda activity (Microsoft, 2022, p. 79).

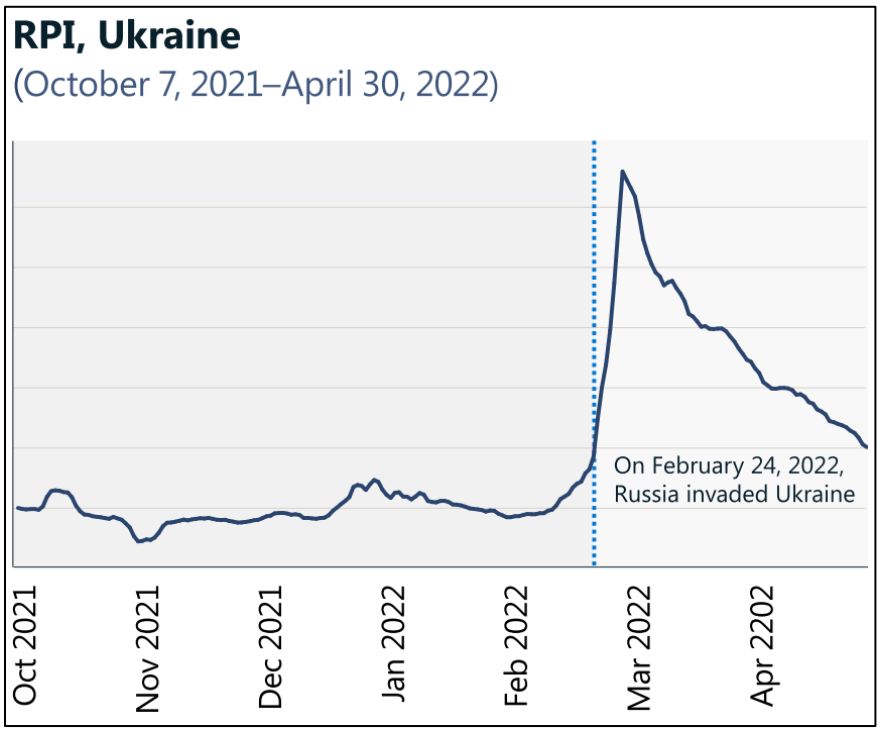

Figure 6 - Russian Propaganda Index in Ukraine (source: Microsoft. (2022). Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us)

In order to corroborate their propagandistic stories, the accounts are supported by online voices critical of what are reliable, mainstream media, in sharing false accusations of establishment media companies broadcasting photos and videos of Ukrainian "'crisis actors': happy, healthy people who are merely playing the role of terrified or deceased war victims for the cameras" (Dale, 2022). This manipulation is carried out in two steps: first, actual, but legitimate, staged footage is retrieved; second, social media users spread the false accusation that the footage is part of Ukraine's strategy to convince people that a conflict is going on, which is aided by traditional media broadcasting of such footage (Dale, 2022). Examples of fake instances of Ukrainian "crisis actors" include a video of a climate protest in Austria where people were lying on the ground in body bags, a video from a British 2013 fiction movie

portraying people running chaotically in an urban area, and footage from the 2020 TV series 'Contamin' shot in Ukraine in which fake blood is applied to an actor (Dale, 2022).

Social media is the ideal medium for the dissemination of propaganda and fake news. In fact, among the emerging threats detected in June 2023, researchers have found a campaign of phishing attacks targeting Ukrainians to access and steal their Telegram credentials; indeed, Telegram has become the ground of a recently detected pro-Russian hacktivist group, *Solntsepek*, whose Telegram channel collects and spreads disinformation concerning members of the Ukrainian military (Cyber Peace Institute, 2023, p. 5). Telegram has been one of the main platforms through which disinformation has been disseminated by pro-Russian hacktivist groups. A notorious example of forged or manipulated video footage took place in mid-March 2022, when "a false message was aired on a Ukrainian TV channel, claiming that the Ukrainian President, Volodymyr Zelenskyy, had called on the population to surrender. A complementary deep-fake video of Zelenskyy was shared on a Telegram channel" (Przetacznik & Tarpova, 2022, p. 2). A further example dates to March 2023, a year later of Zelensky's deep-fake video, and it concerns a two-minute video footage in which Ukrainian soldiers were allegedly caught attacking a Russian-speaking woman and her child; the video was even shared by the Twitter account of the Russian Embassy in the UK, notorious for its provocatory use of social media, but online open-source research quickly located the footage in the Donetsk region, occupied by Russian forces, and a pro-Russian Telegram channel was also admitted the video was an amateur's work (Khatsenkova, 2023).

However, the use of disinformation to generate confusion surrounding the conflict and erode trust in the government was not only limited to Ukraine but was also used by the Russian government to weaken support for the conflict in European populations. The most recent example of this strategy comes from late August of this year, and it concerns a case of a forged footage claiming that a man was attacked in Germany by Ukrainian refugees that had mistaken a Slovenian flag hanging outside a door the house of the victim for a Russian one, and the cover image of the video also presented the Euronews logo, a trusted European news agency (Euronews, 2023). The doctored Euronews report was first shared in Russian on Telegram pro-Russian channels and was then translated in English by the pro-Moscow Propagandist Simeon Boikov; this case further supports the propaganda strategy of using social media and reliable

media to spread fake news and disinformation, which gain legitimacy and credibility in the eyes of a malleable audience, therefore more vulnerable to influence operations.

4.3.3 The EU's Response to Russian Hybrid Warfare in Ukraine

As it has been acknowledged by the European Union Member States, the conflict in Ukraine can have spillover effects into Europe (Council of the European Union, 2022f), as Russia combines cyber and military forces to expand the reach and intensity of its hybrid campaigns (Pearson & Bing, 2022). As the analysis of the KA-SAT attack showed, Europe has also been affected by Russia's cyber campaign against Ukraine. In fact, an analysis conducted by the cyber threat analysis department of Thales, a French cybersecurity company, found that in the six months preceding April 2023, cyber-attacks launched against the European Union had increased from 9.8% to 46.6%, with countries granting most substantive support to Ukraine being the most targeted, given that Russia was behind 61% of the global recorded attacks for one year period (Vincent & Pietralunga, 2023). Furthermore, Russian propaganda activities targeting Western societies have been relentless, as it has been acknowledged by American intelligence agencies, which claim that the Russian Federal Security Service (FSB) is launching influence operations in the West to manipulate and shape public opinion, and public policy, through the creation of close relationships with influential figures in the US and Europe, which help to consolidate and spread pro-Kremlin narratives while keeping the FSB behind the curtains, therefore allowing Moscow to avoid strong attribution (Lillis, 2023). As a result, the EU has come to recognise the gravity of both cyber-attacks, disinformation campaigns, and attacks on critical infrastructure which form hybrid attacks that thrive in the context of social divisions and polarization, as it has been demonstrated also by the COVID-19 Crisis in 2020 (European Commission, 2020a).

As the conflict in Ukraine expanded to Europe, the increased level of hybrid attacks pushed the Council of the European Union to publish its *Conclusions on the Development of the European Union's Cyber Posture* of 23 May 2022, which built its conclusions on various European cyber frameworks and initiatives, including the EU Cyber Defence

Policy Framework, Cyber Diplomacy, the Joint Communication on Resilience, Deterrence and Defence, the EU External Cyber Capacity Building Guidelines, which were adopted in June 2018 (Council of the European Union, 2018b), complementary efforts to Enhance Resilience and Counter Hybrid Threats, the EU's Cybersecurity Strategy for the Digital Decade, and the EU's Strategic Compass for Security and Defence. In fact, the Conclusions acknowledge the intensification of cyber aggressions in recent years, as well as the rise of states challenging international norms in cyberspace, which is gradually becoming a contested domain, while also underlining that "Russia's military aggression against Ukraine has demonstrated that offensive cyber activities can be conducted as an integral part of hybrid strategies combining intimidation, destabilisation and economic disruption" (Council of the European Union, 2022, p. 4), therefore showing the EU's open acknowledgement of Russia's hybrid campaign that is not limited to kinetic operations on the ground.

Furthermore, the document stresses the EU's determination to being able to respond in a rapid and effective way to those malicious actors looking to disrupt and destabilise the Union's interests in cyberspace, which should be and remain open, free, global, stable and secure (Council of the European Union, 2022a, p. 5). The European Council recognizes the importance of cybersecurity as a critical element of the Union's security in the other domains, therefore stressing the need to mainstream cybersecurity awareness in all public policies of the European Union; indeed, the document calls for the improvement in cooperation efforts to counter international cybercrime between the cyber security, law enforcement and diplomatic sectors (Council of the European Union, 2022a, p. 8). For what concerns the Cyber Diplomacy Toolbox, the European Council calls on the High Representative for Foreign Affairs and Security Policy to "review the existing bilateral cyber dialogues and, if necessary, propose to start similar cooperation with additional countries or relevant international organisations" (Council of the European Union, 2022a, p. 12), and calls on the EU and its member States to sustain a multi-stakeholder approach model for the governance of cyberspace and the Internet, therefore by strengthening cooperation through the EU Foreign Policy Instrument's EU Cyber Diplomacy Initiative. (Council of the European Union, 2022a, p. 13).

Finally, for what concerns preventing, defending against and responding to cyber-attacks, the Conclusions acknowledge the geopolitical competition taking place in cyberspace, therefore, exhorting the Union "to swiftly and forcefully respond to cyberattacks, such as state-sponsored malicious cyber activities targeting the EU and its Member States and therefore needs to strengthen the EU Cyber Diplomacy Toolbox and make full use of all its instruments, including the available political, economic, diplomatic, legal and strategic communication tools to prevent, discourage, deter and respond to malicious cyber activities", since the document stresses the importance of making hostile malicious actors aware of the Union's resolve in answering cyber-attacks (Council of the European Union, 2022a, p. 16). Moreover, it acknowledges the effectiveness of EU declarations and restrictive measures implemented under the EU Cyber Diplomacy Toolbox, and stresses its intent to adopt such measures under the framework of international law and of the UN Charter (Council of the European Union, 2022a, p. 17). In addition, the document also calls for:

> "the development of gradual, targeted and sustained approaches and responses to malicious cyber activities, using the wide range of tools provided by the EU Cyber Diplomatic Toolbox, including the EU cyber sanctions regime, and envisaging additional measures. (…) Calls upon the High Representative, in cooperation with the Commission, to identify possible EU joint responses to cyberattacks, including sanctions options, across the spectrum in order to be prepared to take swift and effective action when necessary". (Council of the European Union, 2022a, p. 18)

The Council Conclusions on the Development of the European Union's Cyber Posture reiterated and stressed the importance of strengthening and implementing the tools contained in the Cyber Diplomatic Toolbox of the EU, like the use of restrictive measures, such as the imposition of cyber sanctions imposed in July 2020 against hackers from Russia, China, and North Korea that were involved in the NotPetya, CloudHopper and WannaCry attacks, followed by the sanctions imposed in October 2020 on two GRU officers responsible for the German Bundestag hack of 2015 (Laurens Cerulus, 2021). On 16 May 2022, The European Council has extended for another three years, until 18 May

2025, the framework for restrictive measures, which include a travel ban and an asset freeze, against cyber-attacks threatening the Union and its Member States (Council of the European Union, 2022b).

In fact, restrictive measures are among the actions taken by the EU in response to aggressive activities taking place in Ukraine, and they can target both individuals and entities, including those responsible of disinformation. On 2 March 2022, in response to Russia's invasion of Ukraine the European Council adopted restrictive measures that involved the interruption of the broadcasting activities of Sputnik and RT/Russia Today (including RT English, RT UK, RT Germany, RT France, and RT Spanish) in the EU, or directed at the EU, until Russian disinformation and influence operations against the Union come to an end (Council of the European Union, 2022d). Sputnik and RT have been subject to this sanctions regime because of the direct and indirect control exercised by the Kremlin on the news agencies, which are being employed as tools in Russia's military invasion of Ukraine, as well as destabilising elements in Ukraine's European neighbours (Council of the European Union, 2022d). This package of restrictive measures is complementary to the sanctions package, announced on February 27 by the High Representative, that included "a ban on the overflight of EU airspace and on access to EU airports by Russian carriers of all kinds, a ban on the transactions with the Russian Central Bank, and the SWIFT ban for certain Russian banks" (Council of the European Union, 2022d).

Furthermore, on 23 June 2023 the Council of the European Union adopted the 11th package of sanctions on Russia's war of aggression against Ukraine. This package is mainly aimed at countering Russian information warfare in Ukraine as well as fighting against the circumvention of sanctions (Council of the European Union, 2023c). The European Council included in the sanction a list of IT companies based in Russia that have been supporting the Russian intelligence apparatus with critical technologies and software, and the sanctions also targeted malicious actors "involved in disinformation, including the listing of a television and radio company linked to the Russian armed forces, media executives, propagandists and other individuals responsible for disinformation" (Council of the European Union, 2023c). More recently, on 28 July 2023, the European Council imposed restrictive measures against seven Russian

individuals and five entities which have been found to be responsible for the execution of a digital information manipulation campaign called 'Recent Reliable News' (RNN), whose goal was to forge information and spread propaganda narratives supporting Russia's invasion of Ukraine; the RNN campaign stole the identity of national media outlets, government web pages through fake websites and fake social media accounts, as part of a wider hybrid campaign launched by Russia against European Member States (Council of the European Union, 2023c).

Overall, the Russian invasion of Ukraine, justified by the Kremlin on the basis of historic and ethnic ties between the two countries, has transformed into a hybrid conflict in which traditional war efforts on the ground have been complemented by cyber operations and information operations, with the cyber element working as an amplifier of the other elements of warfare. As the war in Ukraine drags on, the effects of Russian attacks, especially cyber ones, have spilled over into European countries, which have also been targeted by Russia's hybrid warfare over the years. Consequently, the EU responded to Russia's aggression with a series of declarations and restrictive measures targeting Russian entities and individuals. Yet, the Union lacked a comprehensive and effective implementation of its cyber diplomacy policy through the instruments contained in the Cyber Diplomacy Toolbox, despite the war in Ukraine being a scenario in which cyber-attacks, albeit limited, could not be left unnoticed. For this reason, the conclusions of this work will attempt to shed some light on the (inadequate) application of the Cyber Diplomacy Toolbox in context of the war in Ukraine.

Conclusion

Before delving into the results and implications emerging from the present thesis, a brief overview of its content will be presented. The first chapter of this thesis presents a literature review on the history and transformation of cyberspace and inter-state cyber campaigns. It begins with an overview of the creation of cyberspace, and how the cyber realm has become a fifth domain of warfare, in which both state and non-state actors pursue their interests, oftentimes through malicious cyber activity. For this reason, the first chapter briefly presents the norms and standards regulating cyberspace. The second section of the chapter provides an analysis of cyber warfare and begins by placing this phenomenon into the wider context of hybrid warfare, in which traditional elements of warfare are combined with asymmetric and unconventional operations. For what concerns cyber warfare, the present analysis finds no absolute consensus on the existence of a pure and solely cyber conflict, but its strategic relevance in modern conflict is widely appreciated. Cyber warfare can be briefly described as a systematic campaign of cyber-attacks employed to pursue political and military goals that can seriously threaten the security of a state, in which cyber-attacks aim to compromise the integrity, confidentiality or availability of digital assets and information data. The section also presents an overview of various types of cyber operations, and touches upon the issue of attribution of a cyber-attack, which represents a critical, yet difficult, step in the response to cyber-attacks. The closing section focuses on an additional element of hybrid warfare, which is information warfare conducted in cyberspace, also referred to as Cyber-enabled Information Operations, in which disinformation and influence operations are disseminated and amplified through cyberspace.

The second chapter provides an overview of the evolution of cyber regulation in the European Union and of European Cyber Diplomacy. While the legal authority to regulate on cybersecurity still lies with the Member States, the role of the EU in the Union's cybersecurity has gradually expanded, stemming from the EU's desire to become a prominent cyber player in the international arena, mainly thanks to its norm-setting power. For this reason, the first section of the chapter follows the evolution of European Cyber

Regulation, while also touching upon the Union's efforts in the fight against disinformation. The second section focuses on the EU's external approach to cyber security by cyber diplomacy, which first appeared on the agenda of the Union in 2015. Cyber diplomacy aims to establish bilateral and multilateral agreements on cyber norms, lawful state and non-state behaviour in the cyber domain, and effective global digital governance, through the use of non-coercive and non-escalatory peaceful methods, and it is contained in the EU's Cyber Diplomacy Toolbox. The toolbox contains measures against malicious cyber activities that include preventive, cooperative, stability, restrictive measures and the possibility for the EU to support Member State's lawful responses. The third section investigates the application of the EU's Cyber Diplomacy Toolbox under the form of multilateral engagements, bilateral partnerships, and sanctions regime.

The third chapter of this thesis investigates the malicious activities in cyberspace of the Russian Federation, which represents one of the most active states when it comes to cyber-attacks. The first section provides a brief overview of Russian President Vladimir Putin's Information Security Doctrine (2000), which lists as threats to the state the manipulation of information and the activities threatening the security of information and telecommunication systems and facilities, which are believed to come from external agents; this section also provides a short illustration of the Russian institutions and agencies involved in cyberspace and information operations. In the second section a series of case studies shedding more light on Russian hybrid warfare in action is presented, namely the cases of Russian cyber operations in Estonia (2007), Georgia (2008), and the interference by Russian actors in the US presidential elections of 2016, while the third section focuses on hybrid operations conducted by Russia in countries of the European Union, focusing in particular on the German Bundestag Hack of 2015, the interference in the 2016 Brexit referendum in the United Kingdom, as well as on cyber and disinformation campaign launched against former French President Emmanuel Macron during the 2016 French presidential campaign. These cases provide insightful examples of Russian cyber and information operations that form its hybrid warfare strategy against the EU.

The last chapter investigates the recent conflict in Ukraine, which started with the Russian invasion on February 24, 2022, by focusing on the cyber and information

operations launched against the Ukrainian armed forces, government institutions and society. Before analysing the conflict, the first section looks at the historic and ethnic relationship between Ukraine and Russia, necessary to understand the complex relations between the two countries and the narratives employed by the Kremlin to support the invasion; in fact, the analysis illustrates how the two countries share a long and intertwined history, based on ethnic and linguistic ties. The second section investigates the 2014 Annexation of Crimea and the conflict in eastern Ukraine that took place ever since, events that are linked to the rise in use of the term hybrid warfare for what concerns Russia's activities in Ukraine. The conflict in eastern Ukraine shows how Russia employed the use of cyber-attacks, as well as information warfare, to support kinetic operations on the ground, which have also impacted neighbouring European countries. The concluding section of the fourth chapter analyses the 2022 invasion of Ukraine starting with an overview of the main developments of the conflict, so far. Then, this section focuses on the cyber operations conducted in the context of the invasion, affecting Ukraine as well as Europe, and investigates the influence campaigns launched in cyberspace, particularly on social media, by pro-Kremlin hacktivist groups, who support and boost Moscow's propaganda by manipulating information through cyber instruments. The section concludes with an overview of the EU's mixed response to Russian hybrid warfare in Ukraine.

For what concerns the role of cyber operations in the context of inter-state hybrid warfare, the analysis suggests that while cyber operations can have a substantial impact on the course of a conflict or inter-state dispute, as was the case of Estonia in 2007 and the support provided by cyber campaigns in the context of the Georgian war in 2008, the cyber-attacks launched until now in Ukraine have not significantly influenced the course of the conflict. In fact, among the main targets of Russia's cyber campaign there are Ukraine's government institutions, the public administration, the media, the ICT and financial sector, and transportation infrastructure, while, surprisingly, critical infrastructures have not been hit as strongly, contrary to what happened with the 2017 NotPetya. The level of damage cyber-attacks can inflict was consequently lower. Some cyber security experts argue that Russia's choice of targets was likely a deliberate attempt to interrupt communications between the Ukrainian people and the government in Kiev (Steer, 2022), therefore creating chaos and confusion around Russia's strategies and goals, thereby granting Moscow an informational advantage

over Ukraine and its Western allies, compared to which Russia is relatively weaker and in a position of disadvantage. In fact, the use of strong cyber-campaigns against Ukraine in the last years may have had the double result of straining Russian resources and energies (despite Moscow's strength as a cyber threat actor), while also strengthening Ukraine cyber resilience and preparedness.

In other words, as it has been suggested by Minister Laura Carpini, Head of the Cyber Policies Division at the Italian Ministry of Foreign Affairs, the much-dreaded cyber war set to take place in Ukraine never actually materialized, while kinetic warfare on the ground has remained the most important element of the conflict in Ukraine (L. Carpini, personal communication, September 11, 2023). In fact, cyber-attacks hitting Ukraine so far have been under the threshold of what is considered a full-fledged cyber war, and because many of these attacks have been performed by Russian proxies and patriotic hackers, the Russian government has avoided a strong legal attribution for the cyber operations it has most likely been coordinating behind the scenes. As a result, the low intensity of the attacks and the lack of direct involvement of Russian-state entities have granted Moscow diplomatic cover from a strong and resolute response to the cyber-attacks from the international community.

If we look at the implications of the information operations launched in the digital and cyber space in the Ukrainian conflict, Moscow has attempted to control the narrative of the conflict through disinformation by manipulating information and distorting the messages behind videos and stories shared on social media. Used in combination with cyber-attacks, information warfare can aid Russia's war efforts on the ground, by sustaining its own narrative of the ongoing conflict. Furthermore, Russian cyber and information operations have not been limited to Ukraine, but have also been targeting European countries, whose polarized and divided societies provide fertile ground for Russia's attempts at eroding public trust in European democratic institutions, thereby weakening support for Western intervention in Ukraine. Yet, Putin's efforts to control the narrative was mainly unsuccessful in both Ukraine and Western democracies (Lewis, 2022, p. 6), also thanks to newly developed fact-checking mechanisms and to the increased awareness of fake news among society and the media. Instead, Russian propaganda has consolidated its support among domestic audiences, as well

as in non-Western countries like China, Russia's current strongest ally, thereby providing the Kremlin with wide support for its aggression of Ukraine.

Furthermore, for what concerns the role of European cyber frameworks, the results that emerge from the analysis of the Ukrainian case study show that while some restrictive measures have been imposed on Russian entities responsible for the spread of disinformation and manipulation campaigns, no concrete action has been taken by the EU against the use of cyber-attacks in the context of the conflict in Ukraine; the Union only limited itself to openly condemn Russia without an official attribution, and did not impose strong restrictive measures against Russian cyber-attacks. In particular, the conflict in Ukraine did not trigger the implementation of the EU Cyber Diplomacy Toolbox, which represents the framework for a joint EU diplomatic response to malicious cyber activities, thereby employing non-escalatory measures to counter cyber threats, which could fit the cyber diplomatic issues emerging from the conflict. Among the reasons for the limited cyber diplomatic response, as it has been mentioned above, is the low level of intensity of the cyber-attacks launched so-far: in other words, the attacks, because of their limited effects, do not trigger the response reserved to cyber warfare campaigns, yet, because they are taking place within the context of an ongoing conflict, they do not fall under the peacetime norms of international state behaviour in cyberspace. This line of thought has been sustained by scholars like Dr Dennis Broeders, Professor of Global Security and Technology at Leiden University, while experts such as Mika Kerttunen, Adjunct Professor Military Strategy Finnish National Defence University, have argued that while Russia's cyber activities in Ukraine were not deterred by the EU's Cyber Diplomacy Toolbox, the framework might have deterred Russians from engaging in different, potentially more destructive cyber-attacks: however, this is something only the states involved in the conflict can know (Directions Editorial Board, 2022).

One important factor in the lack of a common and determined cyber diplomacy response by EU Member States is also represented by a phenomenon that has often hindered the EU's ability to act in a strong and cohesive way in the face of security challenges, namely, the exclusive competence of Member States to act according to national interests in area of security. As a result, the Union, through the work of the

European Commission and other European agencies, is left to play a coordinating role, thereby depending on the political will of all European countries to act upon a particular threat. For this reason, because of the political rigidity characterising top-down European security initiatives, as shown in the case of Cyber Diplomacy in Ukraine, a positive contribution to the issue of cybersecurity could emerge from the development of policies focusing on the cooperation between the private and military sector. As the former is at the forefront of cybersecurity, given that today's cyberspace is mainly managed by private tech companies that must ensure the continuity and safety of their services in the cyber realm, the military sectors of European member states could rely on the private sector's knowledge and infrastructures to strengthen the protection of national cyber systems. Tech companies are also at the centre of the fight against disinformation circulating on the Internet, especially on social media; therefore, future European cyber diplomacy efforts to counter information manipulation and influence operations should also expand the role of the private sector, especially tech giants, as relevant actor in cyber and information security. To conclude, given the constrains and limitations of the present thesis, the development of these suggestions would certainly benefit from further research, contributing, in turn, to the innovation and enhancement of European security.

Bibliography

Abdyraeva, C. (2020). *The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends*. https://www.jstor.org/stable/resrep25102.8

Allison, R. (2008). Russia Resurgent? Moscow's Campaign to "Coerce Georgia to Peace." *Internatiinal Affairs (Royal Institute of International Affairs)*, *84*(6), 1145–1171. https://www.jstor.org/stable/25144986

Antoniuk, D. (2022). *DDoS attacks hit Ukrainian government websites*. The Record. https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. *European Security*, *32*(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Bastian, N. D. (2019). Information Warfare and Its 18th and 19th Century Roots. *The Cyber Defense Review*, *4*(2), 31–38. https://doi.org/10.2307/26843890

BBC. (2022). *Ukraine conflict: Your guide to understanding day eight*. BBC News. https://www.bbc.com/news/world-europe-60606539

Bendiek, A. (2016). *The Global Strategy for the EU's Foreign and Security Policy*. https://www.swp-berlin.org/publications/products/comments/2016C38_bdk.pdf

Bendiek, A. (2018). The EU as a Force for Peace in International Cyber Diplomacy. In *SWP* (Issue April). https://www.swp-berlin.org/en/publication/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy

Bendiek, A., & Maat, E. P. (2019). *The EU 's Regulatory Approach to Cyber-security* (Issue 02). https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

Bendiek, A., & Schulze, M. (2021). *SWP Research Paper Stiftung Wissenschaft und Politik German Institute for International and Security Affairs Attribution: A Major Challenge for EU Cyber Sanctions*. https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf

Bergh, A. (2020). Understanding Influence Operations in Social Media. *Journal of Information Warfare*, *19*(4), 110–131. https://doi.org/10.2307/27033648

Berkofsky, A. (2014). Russia and China: The Past and Present of a Rocky Relationship. *Il Politico*, *79*(3), 108–123.

Bindt, P., Faesen, L., Farnham, N., Frinking, E., Klimburg, A., Rõõs, H., & Rademaker, M. (2017). *Cyber as a Domain*.

Blinken, A. J. (2022). *Press Statement: Attribution of Russia's Malicious Cyber Activity Against Ukraine*. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Bokša, M. (2019). *RUSSIAN INFORMATION WARFARE IN CENTRAL AND EASTERN EUROPE: STRATEGIES, IMPACT, COUNTERMEASURES*. https://www.jstor.org/stable/resrep21238

Borrell, J. (2023). *Europe's Contribution to the UN Global Digital Compact*. EEAS. https://www.eeas.europa.eu/eeas/europe's-contribution-un-global-digital-compact_en

Botek, A. (n.d.). *European Union establishes a sanction regime for cyber-attacks*. NATO CCDCOE. https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/

Bushkovitch, P. (2012). *A Concise History of Russia*. Cambridge University Press.

Car, P., & Luca, S. De. (2023). *EU cyber-resilience act* (Issue May).

Cerulus, Lauren. (2020). *EU sanctions Russian hackers for 2015 Bundestag breach*. POLITICO. https://www.politico.eu/article/eu-sanctions-russias-fancy-bear-hackers-for-2015-bundestag-breach/

Cerulus, Laurens. (2021). *EU countries extend sanctions against Russian, Chinese hackers*. POLITICO. https://www.politico.eu/article/eu-council-cyber-sanctions-russia-china-hackers/

Chernenko, E., Demidov, O., & Lukyanov, F. (2018). *International Cooperation in Cybersecurity and Adapting Cyber Norms*. https://about.jstor.org/terms

Cîrlig, C.-C. (2014). *Cyber defence in the EU: Preparing for cyber warfare?* https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Colatin, S. D. T. (n.d.). *Si vis cyber pacem, para sanctiones: The EU Cyber Diplomacy Toolbox in action*. NATO CCDCOE. https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/

Council of the European Union. (n.d.). *The general data protection regulation*. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The GDPR establishes the general,data processing operations they perform

Council of the European Union. (2013). *Conclusions of the European Council of 19/20 December 2013 (CO EUR 15 CONCL 8)*. https://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/en/pdf

Council of the European Union. (2014a). *EU Cyber Defence Policy Framework adopted by the Council on 18 november 2014 (15585/14)*. https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf

Council of the European Union. (2014b). *Foreign Affairs Council, 17/03/2014 - Council condemns the illegal referendum in Crimea*. https://www.consilium.europa.eu/en/meetings/fac/2014/03/17/

Council of the European Union. (2015a). Council Conclusions on Cyber Diplomacy. In *Official Journal of the European Union* (pp. 1–13). http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the European Union. (2015b). *Six Monthly Report on the Implementation of the Cyber Defence Policy Framework of 10 November 2015*. https://data.consilium.europa.eu/doc/document/ST-13801-2015-INIT/en/pdf

Council of the European Union. (2017a). *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox)*. https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

Council of the European Union. (2017b). *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*. https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Council of the European Union. (2018a). *EU Cyber Defence Policy Framework Adopted by the Council on 19 November 2018 (2018 update) (14413/18)*. https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf#:~:text=The CDP 2018 identifies cyber,%3B education%2C training%2C exercises and

Council of the European Union. (2018b). *EU External Cyber Capacity Building Guidelines - Council conclusions (26 June 2018)*. https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

Council of the European Union. (2019a). Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. In *Official Journal of the European Union: Vol. L 129* (Issue I, pp. 13–19). https://www.dropbox.com/preview/IPEEA%0AInternship%0ASS2021%3A%0AResearch%0AGroups/Project%0A1%3A%0ACyberdiplomacy%0Aand%0AChina/1.%0AEU%0AOfficial%0ADocuments/Council%0ADecision_2019_restrictive%0Ameasure.pdf?role=personal

Council of the European Union. (2019b). *Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC

Council of the European Union. (2020a). *Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

Council of the European Union. (2020b). *EU imposes the first ever sanctions against cyber-attacks*. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

Council of the European Union. (2020c). *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack*. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

Council of the European Union. (2021). *Horizontal Working Party on Cyber Issues (Cyber)*. https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues/

Council of the European Union. (2022a). *Council conclusions on the development of the European Union's cyber posture, 23 May 2022*. https://www.consilium.europa.eu/media/56358/st09364-en22.pdf

Council of the European Union. (2022b). *Cyber-attacks: Council extends sanctions regime until 18 May 2025 - Press Release*. https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/

Council of the European Union. (2022c). *EU digital diplomacy: Council agrees a more concerted European approach to the challenges posed by new digitial technologies*. https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+digital+di

Council of the European Union. (2022d). *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU - Press Release*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/

Council of the European Union. (2022e). *European Council Conclusions on EU Digital Diplomacy of 18 July 2022 (11406/22)*. https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf

Council of the European Union. (2022f). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Press Release*. https://www.consilium.europa.eu/en/press/press-

releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Council of the European Union. (2022g). *Sixth European Union - African Union Summit: A Joint Vision for 2030*. https://www.consilium.europa.eu/en/press/press-releases/2022/02/18/sixth-european-union-african-union-summit-a-joint-vision-for-2030/

Council of the European Union. (2023a). *Digital diplomacy: Council sets out priority actions for stronger EU action in global digital affairs*. https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/digital-diplomacy-council-sets-out-priority-actions-for-stronger-eu-action-in-global-digital-affairs/

Council of the European Union. (2023b). *European Council Conclusions of 26 June 2023 on EU Digital Diplomacy (11088/23)*. https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf

Council of the European Union. (2023c). *Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities*. https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/

Council of the European Union. (2023d). *Timeline - EU restrictive measures against Russia over Ukraine - Consilium*. https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/

Council on Foreign Relations. (2023). *War in Ukraine*. Global Conflict Tracker. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

Cyber Law Toolkit. (2021). *Bundestag Hack (2015)*.

Cyber Peace Institute. (2023). *Cyber Dimensions of the Armed Conflict in Ukraine*. https://cyberpeaceinstitute.org/wp-content/uploads/2023/09/Ukraine-Report-Q2_4.09.pdf

Cyber Risk GmbH. (n.d.-a). *Cyber Diplomacy Toolbox*. https://www.cyber-diplomacy-toolbox.com/

Cyber Risk GmbH. (n.d.-b). *European Cyber Defence Policy*. Retrieved July 28, 2023, from https://www.european-cyber-defence-policy.com/

CyberPeace Institute. (2022). *Case Study: Viasat Attack*. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

D4D Hub. (n.d.). *Digital for Development (D4D) Hub*. https://d4dhub.eu/

Dale, D. (2022). *Fact check: Pro-Russia social media accounts spread false claims that old videos show Ukrainian 'crisis actors.'* CNN Politics. https://edition.cnn.com/2022/03/10/politics/fact-check-ukraine-not-actually-crisis-actor-fakes/index.html

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*, *16*(2), 5–24. https://doi.org/10.2307/26326478

de Vega, E. J. A. (2022). *The EU-ASEAN digital connectivity partnership in a post-pandemic world*. Friends of Europe. https://www.friendsofeurope.org/insights/the-eu-asean-digital-connectivity-partnership-in-a-post-pandemic-world/

Department of Defense. (2006). *JP 3-13 (R) - Information Operations*. https://irp.fas.org/doddir/dod/jp3_12r.pdf

Department of Defense. (2013). *JP 3-12 (R) - Cyberspace Operations*. https://irp.fas.org/doddir/dod/jp3_12r.pdf

Directions Editorial Board. (2022). *Is War in Ukraine the End of Cyber Diplomacy?* Directions. https://directionsblog.eu/is-war-in-ukraine-the-end-of-cyber-diplomacy/

Directive (EU) 2016/ 1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Pub. L. No. 2016/1148 (2016). http://data.europa.eu/eli/reg/2021/694/oj

Directorate-General for Communication. (n.d.). *Common Foreign and Security Policy Agenda - European Defence Agency (EDA)*. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-defence-agency-eda_en

Dixon, S. (2023). *Biggest social media platforms 2023*. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

EEAS. (2021a). *Countering Disinformation: Questions and Answers about the East StratCom Task Force*. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11243

EEAS. (2021b). *The shaping of a Common Security and Defence Policy*. https://www.eeas.europa.eu/eeas/shaping-common-security-and-defence-policy_en

EEAS. (2022). *Joint Declaration on privacy and the protection of personal data*. https://www.eeas.europa.eu/eeas/joint-declaration-privacy-and-protection-personal-data_en

EEAS. (2023). *Digital Diplomacy*. https://www.eeas.europa.eu/eeas/digital-diplomacy_en

Elonheimo, T. (2021). Comprehensive Security Approach in Response to Russian Hybrid Warfare. *Quarterly*, *15*(3), 113–137. https://doi.org/10.2307/48618299

Encyclopaedia Britannica. (n.d.). Russian Empire - Peter I, Expansion, Reforms. In *Encyclopaedia Britannica*. Retrieved September 16, 2023, from https://www.britannica.com/place/Russian-Empire/The-reign-of-Peter-the-Great

ENISA. (n.d.). *ENISA Mandate and Regulatory Framework*. Retrieved July 28, 2023, from https://www.enisa.europa.eu/about-enisa/regulatory-framework

ENISA. (2017). *ENISA overview of cybersecurity and related terminology*. www.enisa.europa.eu

ENISA. (2022a). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA. (2022b). *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity- Threat Landscape*. https://doi.org/10.2824/7501

ENISA. (2023). *NIS Directive*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

EU4Digital. (n.d.). *The EU4Digital Initiative*. https://eufordigital.eu/discover-eu/the-eu4digital-initiative/

Euronews. (2023). *Don't fall for this doctored Euronews report spread by pro-Kremlin channels*. Euronews. https://www.euronews.com/2023/08/29/dont-fall-for-this-doctored-euronews-report-spread-by-pro-kremlin-channels

European Commission. (n.d.-a). *EU-US Trade and Technology Council*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

European Commission. (n.d.-b). *Global Europe: Neighbourhood, Development and International Cooperation Instrument*. https://international-partnerships.ec.europa.eu/funding-and-technical-assistance/funding-instruments/global-europe-neighbourhood-development-and-international-cooperation-instrument_en

European Commission. (n.d.-c). *Team Europe Initiatives*. https://international-partnerships.ec.europa.eu/policies/team-europe-initiatives_en

European Commission. (2013). *Joint Communication JOIN (2013) 1 final of the Commission and the High Representative of 7 Febraury 2012 on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001

European Commission. (2015). *Communication COM(2015) 185 final from the Commission of 28 Aprile 2015 on The European Agenda on Security*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185

European Commission. (2017). *Joint Communication JOIN (2017) 450 final from the Commission and the High Representative of 13 Septmber 2017 on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. https://www.europeanpapers.eu/sites/default/files/EP_Style_Guide.pdf

European Commission. (2018a). *Communication COM(2018) 236 final from the Commission of 26 April 2018 on the EU Tackling online disinformation: a European Approach* (p. 17). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

European Commission. (2018b). *European Commission launches Digital Agenda for the Western Balkans*. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4242

European Commission. (2018c). *Joint communication JOIN (2018) 36 final from the Commission and the High Representative of 5 December 2018 on an the Action Plan against Disinformation* (p. 13). https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

European Commission. (2020a). *Communication from the European Commission on te EU Security Union Strategy*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605

European Commission. (2020b). *Joint Communication JOIN(2020) 18 finalt from the Commission and the High Representative of 16 December 2020 on The EU's Cybersecurity Strategy for the Digital Decade*. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

European Commission. (2021). *Joint communication JOIN (2021) 2 final from the Commission and the High Representative of 9 February 2021 on the Renewed partnership with the Southern Neighbourhood: A new Agenda for the Mediterranean* (pp. 1–24). https://www.eeas.europa.eu/sites/default/files/joint_communication_renewed_partnership_southern_neighbourhood.pdf

European Commission. (2022a). *2018 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

European Commission. (2022b). *EU and international partners put forward a Declaration for the Future of the Internet*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695

European Commission. (2022c). *Joint Communication JOIN (2022) 13 final from the Commission and the High Representative of 18 May 2022 on A strategic partnership*

with the Gulf (pp. 1–23). https://www.eeas.europa.eu/eeas/joint-communication-“strategic-partnership-gulf”_en

European Commission. (2023a). *COM (2023) 209: Proposal for a Regulation of the European Parliament and of the Council of 18 April 2023 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents of*. https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2023)209&lang=en

European Commission. (2023b). *Cybersecurity Policies*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commission. (2023c). *Digital Partnerships*. https://digital-strategy.ec.europa.eu/en/policies/partnerships

European Commission. (2023d). *EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_596

European Commission. (2023e). *Global Gateway: EU, Latin America and Caribbean partners launch in Colombia the EU-LAC Digital Alliance*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1598

European Commission. (2023f). *The Digital Europe Programme*. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Commission. (2023g). *The EU Cybersecurity Act*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Council. (2015). *Conclusions - European Council meeting (19 and 20 March 2015)*. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Defence Agency. (n.d.). *Our History*. Retrieved July 28, 2023, from https://eda.europa.eu/our-history/our-history.html

European Parliament. (2015a). *EU reaction to Russia-Ukraine conflict*. https://epthinktank.eu/2015/02/05/eu-reaction-to-russia-ukraine-conflict/

European Parliament. (2015b). *European Parliament resolution of 15 January 2015 on the situation in Ukraine (2014/2965(RSP))*. https://www.europarl.europa.eu/doceo/document/TA-8-2015-0011_EN.pdf

European Parliament. (2016). *European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI))*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016IP0441

European Parliament. (2022). *Report on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)) Special*. https://doi.org/10.1080/00344897208656356

European Parliament. (2023a). *Common Security and Defence Policy*. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy

European Parliament. (2023b). *The Treaty of Lisbon*. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon

European Parliament and Council of the European Union. (2019). REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Europol. (2023). *European Cybercrime Centre - EC3*. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

EUvsDisinfo. (n.d.). *About EUvsDisinfo*. Retrieved September 8, 2023, from https://euvsdisinfo.eu/about/

Even, S., & Siman-Tov, D. (2012). *Cyberspace and the Security Field: A Conceptual Framework*. http://www.jstor.com/stable/resrep08940.4

Flashpoint. (2023). *Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective*. Flashpoint. https://flashpoint.io/blog/killnet/

Foote, C., Maness, R. C., Jensen, B., & Valeriano, B. (2021). Cyber Conflict at the Intersection Of Information Operations: Cyber Enabled Information Operations, 2000-2016. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 54–69). Routledge. https://doi.org/10.4324/9780429470509

French Ministry for Europe and Foreign Affairs. (2022). *Understanding the situation in Ukraine since 2014*. France Diplomacy. https://www.diplomatie.gouv.fr/en/country-files/ukraine/situation-in-ukraine-what-is/understanding-the-situation-in-ukraine-since-2014/

French National Cyber Security Agency. (2021). European Cyber Security: History of a Cultural Transformation. *Papiers Numériques*. www.ssi.gouv.fr

Friis, K., & Reichborn-Kjennerud, E. (2016). From cyber threats to cyber risks. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space - Theoretical, Strategic and Legal Pespectives* (pp. 53–74). Routledge. https://doi.org/10.4324/9781315669878

Garon, J. M. (2018). Cyber-World War III Origins. *Source: Journal of Law & Cyber Warfare*, *7*(1), 1–60. https://www.jstor.org/stable/26777962?seq=1&cid=pdf-reference#references_tab_contents

Gibbs, S. (2014, October 27). Elon Musk: artificial intelligence is our biggest existential threat. *The Guardian*. https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat

Goldfarb, A., & Lindsay, J. R. (2022). Prediction and Judgement: Why Artificial Intelligence Increases the Importance of Humans in War. *International Security*, *46*(3), 7–50. https://doi.org/10.1080/03071847.2019

Gomez, M. A. (2021). Cyber-enabled Information Warfare and Influence Operations: A Revolution in technique? In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 132–146). Routledge. https://doi.org/10.4324/9780429470509

Graziosi, A. (2005). The Soviet 1931-1933 famines and the Ukrainian Holodomor: Is a new interpretation possible, what would its consequences be? *Cahiers Du Monde Russe*, *46*(3). https://doi.org/10.4000/monderusse.2818

Guyonneau, R., & Le Dez, A. (2019). Artificial Intelligence in Digital Warfare. *Source: The Cyber Defense Review*, *4*(2), 103–116. https://doi.org/10.2307/26843895

Hanson, S. E. (2006). The Brezhnev Era. In Ronald Grigor Suny (Ed.), *The Cambridge History of Russia* (pp. 292–315).

Harding, L., Morris, S., & Bannock, C. (2018). *Former Russian spy critically ill in UK "after exposure to substance."* The Guardian. https://www.theguardian.com/world/2018/mar/05/salisbury-incident-critically-ill-man-is-former-russian-spy-sergei-skripal

Hartley, J. M. (1992). Is Russia part of Europe ? Russian perspections of Europe in the reign of Alexander I. *Cahiers Du Monde Russe et Soviétique*, *33*(4), 369–385. https://doi.org/10.3406/cmr.1992.2325

Herspring, D. R. (2009). Vladimir Putin: His Continuing Legacy. *Social Research*, *76*(1), 151–174. https://www.jstor.org/stable/40972142

Hodges, D., & Creese, S. (2015). Understanding cyber-attacks. In J. A. Green (Ed.), *Cyber Warfare - A Multidisciplinary Analysis* (pp. 33–60). Routledge. https://doi.org/10.4324/9781315761565

Horvath, R. (2011). Putin's "Preventive Counter-Revolution": Post-Soviet Authoritarianism and the Spectre of Velvet Revolution. *Europe - Asia Studies*, *63*(1), 1–25. https://doi.org/10.1080/09668136.2011.534299

Hutchinson, W., & Warren, M. (2001). Principles of Information Warfare. *Source: Journal*

of Information Warfare, *1*(1), 1–6. https://doi.org/10.2307/26485918

Iasiello, E. J. (2017). Russia's Improved Information Operations: From Georgia to Crime. *Parameters*, *47*(2). https://doi.org/10.55540/0031-1723.2931

Internet Governance Forum. (n.d.). *WSIS+20 and IGF+20 Review by the UN General Assembly (2025)*. https://www.intgovforum.org/en/content/wsis20-and-igf20-review-by-the-un-general-assembly-2025

ITU. (2010). *ITU Toolkit for Cybercrime Legislation*. https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf

Johnson, J. S. (2020). Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Qarterly*, *14*(1), 16–39. https://doi.org/10.2307/26891882

Kalathil, S. (2020). The Evolution of Authoritarian Digital Influence: Grappling with the New Normal. *PRISM*, *9*(1), 32–51. https://doi.org/10.2307/26940158

Kassam, A., & Sabbagh, D. (2023). *Yevgeny Prigozhin confirmed dead after plane crash, Russian investigators say*. The Guardian. https://www.theguardian.com/world/2023/aug/27/wagner-boss-yevgeny-prigozhin-killed-in-plane-crash-russia-investigative-committee-confirms

Katchanovski, I. (2008). The Orange Evolution? The "Orange Revolution" and political changes in Ukraine. *Post-Soviet Affairs*, *24*(4), 351–382. https://doi.org/10.2747/1060-586X.24.4.351

Katchanovski, I. (2019). Ukraine and Russia People, Politics, Propaganda and Perspectives. *Ukraine and Russia*, 287. http://ssrn.com/abstract=273136

Kazantsev, A. A., Rutland, P., Medvedeva, S. M., & Safranchuk, I. A. (2020). Russia's policy in the "frozen conflicts" of the post-Soviet space: from ethno-politics to geopolitics. *Caucasus Survey*, *8*(2), 142–162. https://doi.org/10.1080/23761199.2020.1728499

Khatsenkova, S. (2023). *Pro-Kremlin groups caught staging video of Ukrainian soldiers attacking woman and baby*. Euronews. https://www.euronews.com/2023/03/30/pro-kremlin-groups-caught-staging-video-of-ukrainian-soldiers-attacking-woman-and-baby

Klimburg, A. (2014). Roots Unknown – Cyberconflict Past, Present & Future. *Sicherheit Und Frieden (S+F) / Security and Peace*, *32*(1), 1–8. https://about.jstor.org/terms

Kravchenko, V. (2016). Fighting Soviet Myths: The Ukrainian Experience. *Harvard Ukrainian Studies*, *34*(1), 447–484. http://www.jstor.org/stable/44364503

Laruelle, M. (2021). *Is Russia Fascist? Unraveling Propaganda East and West*. Cornell

University Press.

Latici, T. (2020). *Understanding the EU's approach to cyber diplomacy and cyber defence* (Issue May). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

Lewis, J. A. (2022). Cyber War and Ukraine. *Center for Strategic & International Studies*, 1–14. https://www.csis.org/analysis/cyber-war-and-ukraine

Lexmann, M. (2017). The European Union and Russia: mirror-like asymmetry in hybrid conflict. *International Issues & Slovak Foreign Policy Affairs*, *26*(3–4), 35–55. https://doi.org/10.2307/26592057

Liaropoulos, A. (2016). Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics. *Source: Journal of Information Warfare*, *15*(4), 14–26. https://doi.org/10.2307/26487548

Libicki, M. C. (2020). Cyberwar is What States Make of It. *The Cyber Defense Review*, *5*(2), 77–87. https://www.jstor.org/stable/10.2307/26923524

Libicki, M. C. (2021a). *Cyberspace in Peace and War* (Second Edi). Naval Institute Press.

Libicki, M. C. (2021b). The Convergence of Information Warfare. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 15–26). Routledge. https://doi.org/10.4324/9780429470509

Lillis, K. B. (2023). *Newly declassified US intel claims Russia is laundering propaganda through unwitting Westerners*. CNN Politics. https://edition.cnn.com/2023/08/25/politics/us-intel-russia-propaganda/index.html

Limnell, J. (2018). Russian cyber activities in the EU. *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, 65–73. https://www.jstor.org/stable/pdf/resrep21140.10.pdf

Lis, J. (2020). *Was there Russian meddling in the Brexit referendum? The Tories just didn't care*. The Guardian. https://www.theguardian.com/commentisfree/2020/jul/21/russian-meddling-brexit-referendum-tories-russia-report-government

Mackinnon, A. (2020). *4 Takeaways From the British Report on Russian Election Interference*. Foreign Policy. https://foreignpolicy.com/2020/07/21/britain-report-russian-interference-brexit/

Metz, C., & Schmidt, G. (2023, March 29). Elon Musk and Others Call for Pause on A.I., Citing 'Risks to Society.' *The New York Times*. https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html

Miadzvetskaya, Y., & Wessel, R. A. (2022). The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox. *European Papers - A Journal on Law and Integration*, *7*(1), 413–438. https://doi.org/10.15166/2499-8249/570

Microsoft. (2022). *Microsoft Digital Defense Report 2022*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Muller, L. P. (2016). How to Govern Cybersecurity? The Limits of the multi-stakeholder approach and the need to rethink public-private cooperation. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space - Theoretical, Strategic and Legal Pespectives* (pp. 159–175). Routledge. https://doi.org/10.4324/9781315669878

Ning, H. (2022). *A Brief History of Cyberspace* (First Edit). CRC Press. https://doi.org/10.1201/9781003257387

Nissen, T. E. (2016). Cyber Warfare by Social Network Media. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space - Theoretical, Strategic and Legal Pespectives* (pp. 176–201). Routledge. https://doi.org/10.4324/9781315669878

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 54–71. https://doi.org/10.1162/ISEC

Nye Jr, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *Journal of Cyber Policy*, *41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Open Society Foundations. (2019). *Understanding Ukraine's Euromaidan Protests*. https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests

Ortiz-Espina, E. (2019). *The rise of social media*. Our World In Data. https://ourworldindata.org/rise-of-social-media

Pasquazzi, S., & Savarino, A. (2023). Cyber-attacks , geopolitica e settore energetico. *Rivista Scientifica "Europea," 1*, 1-28, (forthcoming).

Pawlak, P. (2018). Protecting and defending Europe's cyberspace. In *Hacks, Leaks and Disruptions: Russia Cyber Strategies*. https://ec.europa.eu/digital-single-market/en/news/special-eurobarometer-europeans-attitudes-towards-cyber-security

Pawlak, P., Kerttunen, M., & Tikk, E. (2020). CYBER CONFLICT UNCODED - The EU and conflict prevention in cyberspace. *European Union Institute for Security Studies (EUISS)*. https://about.jstor.org/terms

Pearson, J., & Bing, C. (2022). *The cyber war between Ukraine and Russia: An overview*. Reuters. https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

per Concordiam. (2012). Post-Soviet "Frozen Conflicts." *Per Concordiam*, 42–47. http://cria-online.org/Journal/6/Done_Kapitonenko_Resolving Conflicts.pdf

Perlroth, N., Wines, M., & Rosenberg, M. (2017). *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*. New York Times. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html

Pernik, P. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. *Chaillot Paper*, *148*, 53–64.

Petrosyan, A. (2023). *Internet and social media users in the world 2023*. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Prier, J. (2021). Commanding the Trend: Social Media as Information Warfare. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 88–113). Routledge. https://doi.org/10.4324/9780429470509

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*.

Puddephat, A. (2020). Governing the internet: The makings of an EU model. In C. Hobbs (Ed.), *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry* (pp. 13–24). European Council on Foreign Relations. https://www.jstor.org/stable/c6f91626-0239-3af2-a9a6-ffb981b98872?seq=4

Putin, V. (2021). *Address by the President of the Russian Federation*. President of Russia. http://en.kremlin.ru/events/president/news/67828

Pytlak, A., & Mitchell, G. E. (2016). Power, Rivalry and Cyber Conflict: An Empirical Analysis. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space - Theoretical, Strategic and Legal Pespectives* (pp. 97–117). Routledge. https://doi.org/10.4324/9781315669878

Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is Hybrid Warfare?* https://about.jstor.org/terms

Reuters. (2022). *Timeline: The events leading up to Russia's invasion of Ukraine*. Reuters. https://www.reuters.com/world/europe/events-leading-up-russias-invasion-ukraine-2022-02-28/

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*, 4–37. https://doi.org/10.1080/01402390.2014.977382

Ringhof, J., & Torreblanca, I. (2022). *THE GEOPOLITICS OF TECHNOLOGY: HOW THE EU CAN BECOME A GLOBAL PLAYER*. https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/

Rinke, A., & Carrel, P. (2016). *German-Russian ties feel Cold War-style chill over rape case*. Reuters. https://www.reuters.com/article/us-germany-russia-

idUSKCN0VA31O

Rowe, N. C. (2015). The Attribution of Cyber Warfare. In J. A. Green (Ed.), *Cyber Warfare - A Multidisciplinary Analysis* (pp. 61–72). Routledge. https://doi.org/10.4324/9781315761565

Rühle, M. (2016). Preface. In J. R. Karsten Friis (Ed.), *Conflict in Cyber Space - Theoretical, Strategic and Legal Pespectives* (pp. 15–20). Routledge. https://doi.org/10.4324/9781315669878

Doctrine of information security of the Russian Federation, 1 (2000).

Ruy, D. (2020). *Did Russia Influence Brexit?* Center for Strategic and International Studies. https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

Samabaluk, N. M. (2022). *Weaponizing Cyberspace: Inside Russia's Hostile Activities*. Praeger Security International.

Schmidt, M. S. (2018). *Trump Invited the Russians to Hack Clinton. Were They Listening? - The New York Times*. New York Times. https://www.nytimes.com/2018/07/13/us/politics/trump-russia-clinton-emails.html

Schmitt, M. (2021). Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 186–214). Routledge. https://doi.org/10.4324/9780429470509

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1080/09668136.2014.897423

Schnaufer II, T. A. (2017). Redefining Hybrid Warfare: Russia's Non-Linear War against the West. *Journal of Strategic Security*, *10*(1), 17–31. https://doi.org/10.2307/26466892

Sevchenko, V. (2023). *Yevgeny Prigozhin: From Putin's chef to rebel in chief*. BBC. https://www.bbc.com/news/world-europe-64976080

Shearer, R. D. (2006). Stalinism, 1928–1940. In Ronald Grigor Suny (Ed.), *The Cambridge History of Russia* (pp. 192–216). Cambridge University Press.

Siers, R. (2018). Cybersecurity. In P. D. Williams & M. McDonald (Eds.), *Security Studies: An Introduction* (Third Edit). Routledge.

Siman, B. (2022). Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations. *Security Policy Brief*, *155*(February). http://www.jstor.org/stable/resrep39418

Smith, T. E. (2013). National Military Intelligence Foundation Cyber Warfare: A Misrepresentation of the True Cyber Threat. *American Intelligence Journal*, *31*(1), 82–85. https://doi.org/10.2307/26202046

Snegovaya, M. (2015). *Putin's Information Warfare in Ukraine*. http://www.jstor.com/stable/resrep07921.1

Soldatov, A., & Borogan, I. (2018). Russia's approach to cyber: the best defence is a good offence. *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, *148*, 15–23.

Steed, D. (2015). The Strategic Implications of Cyber Warfare. In J. A. Green (Ed.), *Cyber Warfare - A Multidisciplinary Analysis* (pp. 73–95). Routledge. https://doi.org/10.4324/9781315761565

Steer, G. (2022). *Russia's cyber war that wasn't*. Financial Times. https://www.ft.com/content/1315165d-3986-4671-972f-c1ce04104560

Stiennon, R. (2015). A Short History of Cyberwarfare. In J. A. Green (Ed.), *Cyber Warfare - A Multidisciplinary Analysis* (pp. 7–32). Routledge. https://doi.org/10.4324/9781315761565

Sulleyman, A. (2017, July 17). Elon Musk: AI is a 'fundamental existential risk for human civilisation' and creators must slow down. *The Independent*. https://www.independent.co.uk/tech/elon-musk-ai-human-civilisation-existential-risk-artificial-intelligence-creator-slow-down-tesla-a7845491.html

Supps, C. (2018). *Commission urges EU countries to publicly blame states behind cyber attacks*. EURACTIV. https://www.euractiv.com/section/defence-and-security/news/commission-urges-eu-countries-to-publicly-blame-states-behind-cyber-attacks/

Sweijs, T. (2018). *Intelligence and Its Future Impact on Security*. http://www.jstor.com/stable/resrep19348

Szporluk, R. (2018). Ukraine: From an imperial periphery to a Sovereign State. *A New Europe for the Old?*, *126*(3), 85–120. https://doi.org/10.4324/9781351308809-5

Thrall, A. T., & Armstrong, A. (2021). Bear market? Grizzly steppe and the American marketplace of ideas A. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information Warfare in the Age of Cyber Conflict* (pp. 73–87). Routledge. https://doi.org/10.4324/9780429470509

Timberg, C., Shaban, H., & Dwoskin, E. (2017). *Fiery exchanges on Capitol Hill as lawmakers scold Facebook, Google and Twitter*. The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2017/11/01/fiery-exchanges-on-capitol-hill-as-lawmakers-scold-facebook-google-and-twitter/

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the

European Community, signed at Lisbon, 13 December 2007, Pub. L. No. 2007/C 306/01 (2007). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

Tsvetkova, N. (2020). Russian Digital Diplomacy: A Rising Cyber Soft Power? In A. A. Velikaya & G. Simons (Eds.), *Russia's Public Diplomacy* (pp. 103–117). https://doi.org/10.1007/978-3-030-12874-6_6

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da, (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

United Nations. (n.d.). *SECRETARY-GENERAL'S ROADMAP FOR DIGITAL COOPERATION*. https://www.un.org/en/content/digital-cooperation-roadmap/

United Nations. (2020). Roadmap for Digital Cooperation. In *Report of the Secretary-General* (Issue June). https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

United Nations. (2023). *A Global Digital Compact - an Open, Free and Secure Digital Future for All* (No. 5). https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf

Unver, H. A. (2017). Digital Challenges to Democracy: Politics of Automation, Attention and Engagement. *Journal of International Affairs*, *71*, 127–146. https://doi.org/10.2307/26494368

van der Meer, S. (2018). *State-level responses to massive cyber-attacks: a policy toolbox*. http://www.jstor.com/stable/resrep21308

Vela, J. (2021). *The Development of the EU Cyber Security Strategy and its Importance*. FINABEL. https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/

Vilmer, J.-B. J. (2018). Successfully Countering Russian Electoral Interference: 15 lessons learned from the Macron leaks. *CSIS Briefs*, 1–6. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference%0Ahttp://lib.ugent.be/catalog/ebk01:5360000000032732

Vincent, E., & Pietralunga, C. (2023). *Cyberattacks on the rise in Europe amidst the war in Ukraine*. Le Monde. https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html

Walker, N. (2023). Conflict in Ukraine: A timeline (2014 - present). *House of Commons Library*, *February 2022*, 1–96. https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf

Way, L. A. (2008). Between National Division and Rapacious Individualism Ukraine before and after the Orange Revolution. *Brown Journal of World Affairs*, *xiv*(2), 253–264.

Westfall, S. (2023). *A Russia-Ukraine timeline: Key moments, from attacks on Kyiv to counteroffensive*. The Washington Post. https://www.washingtonpost.com/world/2023/06/09/russia-ukraine-war-timeline-counteroffensive/

Wilde, G., & Sherman, J. (2023). *No Water's Edge: Russia's Information War and Regime Security*. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644

Yasin, B. M. (2020). *Hybrid Warfare: Countering the Impending Threats*. https://www.jstor.org/stable/resrep29111.5

Yekelchyk, S. (2006). The western republics: Ukraine, Belarus, Moldova and the Baltics. In Ronald Grigory Suny (Ed.), *The Cambridge History of Russia*. Cambridge University Press.