RUSSIAN INFORMATION AND INFLUENCE OPERATIONS

Putin’s regime survival tools

OPERATIONS D’INFORMATION ET D’INFLUENCE DE LA RUSSIE

Des outils au service de la survie du régime de Poutine

A Thesis Submitted to the Division of Graduate Studies of
the Royal Military College of Canada
by

BENOÎT MORIN

In Partial Fulfillment of the Requirements for the Degree
of Master in War Studies

Abstract

This paper examines Russia’s use of active measures and reflexive control type of methods carried out in the cyberspace as governance tools to ensure Putin’s regime survival. This paper applies an International Relation theoretical framework based on a structuralist epistemology and a constructivist ontology. This approach highlights Russia’s domestic considerations such as the nature of Putin’s regime and Russia’s national identity, as main driving factors for Putin’s regime use of information and influence operations against Western democracies. Indeed, Putin’s centralized and personified governance model overemphasis Putin’s inputs into the Russian state decision-making, meaning that Putin’s background, experience and vision of Russia play a significant role in Russia’s national and defence security doctrines, which emphasis perceived domestic and foreign threats directed to destabilizing and weakening Putin’s grips onto power. To ensure Putin’s regime longevity, Russia launched a total information war against the West, which includes cyber operations to achieve information supremacy in the information space and convince Russian society that they are better off with him in power. To achieve this informational goal, Russia’s cyber threat actors are carrying out information and influence operations in the cyberspace to: 1) Portray Russia as a besieged fortress, by creating a narrative bubble claiming that Russians and Russian society are constantly under threat from Western militaries and its malicious influence; 2) Amplify positive narratives on Russia and his regime, while at the same time suppressing and delegitimizing negative ones; and 3) Weakening Western soft power by exposing, distorting and amplifying Western societal tensions and issues. Based on a discursive approach, this paper contributes to the body of literature framing Russia’s cyber operations as a sub-component of information warfare.

Résumé

Cette recherche examine l’utilisation par la Russie de mesure active et de contrôle réflexif dans le cyberespace comme outils de gouvernance pour assurer la survie du régime de Poutine. Cette recherche s’inscrit dans le corpus théorique des Relations internationales et utilise un cadre analytique formé d’une épistémologie structuraliste et une ontologie constructiviste. Cette approche met en lumière les facteurs domestiques de la Russie tels que la nature du régime de Poutine et l’identité nationale russe comme déterminant des opérations d’information et d’influence à l’encontre des démocraties occidentales. En effet, la nature centralisée et personnifiée du système de gouvernance de Poutine engendre une surreprésentation de Poutine dans le processus décisionnel de l’État russe. Ainsi, le parcours passé et les expériences de Poutine ont joué un rôle déterminant dans le développement des doctrines russes de sécurité nationale et de défense nationale, expliquant la surreprésentation des menaces domestiques et extérieures perçues comme pouvant déstabiliser et affaiblir le pouvoir de Poutine. Dans le but d’assurer la longévité du régime de Poutine, la Russie a déclenché une guerre informationnelle totale à l’encontre de l’Occident, incluant des opérations cybernétiques pour atteindre une suprématie dans l’espace informationnel russe dans le but de convaincre la société qu’elle est mieux avec Poutine au pouvoir. Pour atteindre cet objectif informationnel, les cyberacteurs russes montent des opérations d’information et d’influence dans le cyberespace pour : 1) dépeindre la Russie comme une forteresse assiégée en créant une bulle narrative dans laquelle la société russe et les Russes seraient constamment sous la menace militaire occidentale et de son influence malicieuse; 2) amplifier les narratives positives à l’égard de la Russie et du régime de Poutine, tout en supprimant et délégitimant les narratives négatives; 3) affaiblir le *soft power* occidental en exposant, en distordant et en amplifiant ses tensions et problème sociétaux. En se reposant sur une approche discursive, cette recherche contribue au corpus de littérature qui encadre les opérations cybernétiques de la Russie comme étant une sous-composante de la guerre d’information.

Table of Contents

1 - INTRODUCTION

In the late 2000s, the world witnessed a digital revolution driven by the wide spread of affordable and portable connected devices (e.g., smart phones, tablets, etc.), which increased access to internet, social media platforms, and the digitalization of public and private services. This new digital context characterized by a fast-paced information technology (IT) development and government dependencies on them, enhanced interconnectedness of IT infrastructure worldwide, the almost instantaneous sharing and production of information created a well-suited environment for the use of old active measures and reflexive control methods in the "cyberspace."[1] Today, "cyber threat actors"[2] have more than ever the ability to disrupt, manipulate and destabilize adversaries' political institutions, economies and societies.

Western governments and societies proved to be particularly vulnerable to this new technological context due to their digital dependency and the way the liberal democratic system is built. Indeed, as Western societies are becoming more and more digital dependent, in the sense that their economy and governance model are relying ever more on IT systems and digital services, they also become more vulnerable to state-sponsored cyber threat actors. (Rid, 2020, pp. 7-8) Highlighting this new context, the Canadian Center for Cyber Security (CCCS)[3] recognized that internet-connected devices and applications are providing great benefits to individuals and institutions, but the more digitalized our societies become, the more cyber threat actors will have opportunities to conduct malicious cyber activities to access information and disrupt operations. (CCCS, 2021, p. 2)

[1] Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructure including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (NIST, Glossary: https://csrc.nist.gov/glossary/term/cyberspace#:~:text=A%20global%20domain%20within%20the,and%20embedded%20processors%20and%20controllers.)

[2] CCCS defines cyber threat actors as: "states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks." (CCCS, An Introduction to the Cyber Threat Environment : https://www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf)

[3] CCCS is the public facing entity of the Communications Security Establishment of Canada, which serves as lead technical authority for IT security for the Government of Canada, and also as the lead signal intelligence agency in Canada.

The nature of Western liberal democratic societies, built upon fostering free speech, transparency, the unrestricted exchange of ideas and political competition, as well as their increasing dependency on digital technology and services expose them to foreign propaganda, disinformation and political manipulation. Based on the Communications Security Establishment of Canada (CSE) environmental scan in Canada, 94% of Canadian adults use the internet, of which 94% had at least one social media account. (CSE, 2021, p. 10) Of those having at least one social media account, 83% had a Facebook account, of which 77% used Facebook on a daily basis. (CSE, 2021, p. 10) This overgrowing intertwinement between information technology and society is not only revolutionizing the way we communicate with each other, it is also abolishing the traditional distinction between producer and consumer of information. (Marangé and Quessard, 2021, p. 51) Social media and streaming platforms enable horizontal creation, consumption and sharing of information bypassing traditional and more centralized information channels, such as radio and TV stations, thus creating direct channels of communication to reach the population of rival countries. (Marangé and Quessard, 2021, p. 269) Through the cyberspace, malicious governments can gather massive amounts of information on foreign populations, specific social groups or individuals and directly reach them with tailored information that plays on preconceived bias and emotions (Bagge, 2019, p. 53) exacerbating existing grievances and social tensions. (OTAN, 2018, p. 6) With the interconnected nature of the internet and information being created, shared and consumed almost instantly on social media platforms, societies and governments have never been as much exposed and permeable to unrestricted foreign interference operations. This new international technological context may affect liberal democracies the most, but authoritarian regimes such as Russia are not immune either.

Like Soviet Union type of control over Russia's information space, shortly after Vladimir Putin became president, he adopted by presidential decree the *Doctrine of Information Security of the Russian Federation* in 2000, in which the affirmed objective is to control and extend the state national sovereignty over Russia's information space to protect Russians against foreign information threats. (Marangé and Quessard, 2021, pp. 116-117) Five years later, *Russia Today* (today known as RT) was created in reaction to the Orange

Revolution in Ukraine in 2004 and in 2014 the Kremlin purchased *Ria Novostia*, renamed it *Rossia Segodnia* and created its international branch *Sputnik*. (Marangé and Quessard, 2021, p. 126) Russian elites and military strategists are aware of the risks produced by this new technological context. For instance, the 2010 Military Doctrine of the Russian Federation states:

> At the same time, the need for adoption of such measures [Information warfare capabilities] on a priority basis in the current context is due to but not limited to the fact that hundreds of millions of people are involved in a single global information space formed by the Internet, electronic mass media and mobile communication systems. (Bagge, 2019, p. 125)

In addition, the then Chief of the General Staff Valery Gerasimov stated in 2019 during a conference that:

> […] without having clearly defined national borders, [the information space] provides the possibility of remote, covert influence not only on critical information infrastructure, but also on the country's population, directly affecting the state's national security (Lilly and Cheravitch, 2020, p. 134)

Although the willingness of Putin's regime to influence Russia's information's space go as far back as Putin's first mandate, Russia stance against the West changed drastically when Putin came back to power in 2012. The popular protests in Russia in 2011-2012, also called November movements were perceived by Russian elites and military strategists as a continuity of a Western political destabilization strategy that started in 2010 under the cover of the Arab Spring movements that toppled long established Arab dictators in Tunisia, Libya, Egypt, and Syria. (Rashid et al., 2021, p. 661) These events sent a loud and clear warning to the Kremlin that it needed to do more to control and influence Russian information space against perceived Western information operations. Similar to Soviet elites before them, Russian elites are claiming that Russia is facing ongoing existential internal and external threats that challenge its security in the information space and they perceive the free flow of information enabled by the internet as both a threat and an opportunity. (Connell and Vogler, 2017, p. i) The Kremlin's traditional ways of influencing Russia's information space including restricting access to media for oppositional speech and state-controlled media were not enough anymore as Russians can easily have access to alternative sources of information and post alternative narratives online.

However, contrary to China, Russia does not have a national internet that is cut off from the worldwide internet yet[4]. As the Kremlin cannot exert total state control over Russia's information space, Putin's regime decided to create a state controlled or influenced information ecosystem strong enough to compete with and crowd out alternative sources of information accessible to Russian society. As the Kremlin lost its monopoly in the Russian information space, it is not enough anymore to affirm that Western values are dangerous and disruptive for Russian's society, or that Russia is under constant threat from the North Atlantic Treaty Organisation (NATO) and the United States (U.S.). Although these discursive thematic elements have been at the core of Putin's national narrative since he was appointed Prime Minister in 1999, Russia political and diplomatic stance toward the West changed during the 2000s and reached a breaking point when Putin was elected president for the third time in 2012. (Rid, 2020, p. 7) Indeed, Putin's discourse at the 2007 Munich Summit was marked by an aggressive rhetoric against the U.S. and NATO's intervention in Kosovo, but it is really in 2012 that Putin's narrative has taken a significantly more critical and aggressive stance against the West and its influence around the world.

Putin is using skills and methods learned as a KGB case officer, and tries to subvert, corrupt, destabilize and manipulate Western societies so they can be perceived the way Putin is describing them to Russians. (Belton, 2020, p. 445) To achieve that, Putin's regime is using the full extent of Soviet era inspired active measures and reflexive control operations, including the "use of economic, political, diplomatic, religious, legal, security, cyber and military instruments." (Bertelsen, 2021, p. 216) Putin leveraged and weaponized every sector of the Russian state and society from elaborating financial schemes to corrupt Western companies, funding far-right and far-left political parties across Europe and launching an information war against the West. (Belton, 2020, p. 446) As Russia's active measures and reflexive control operations have

[4] Although Russia passed a series of amendments to existing information and internet-related laws in 2019 with the intention to create Russia's Sovereign Internet design to replicate what China and North Korea did in the early 2000s, it will take time to redesign IT infrastructure in Russia due to the potential economic impact of doing so, as Russian financial institutions and companies are well connected and integrated into the international internet network. (Marangé and Quessard, p. 63) The amendments aim realizing three main objectives: 1) "the compulsory installation of technical equipment for counteracting threats"; 2) "Centralized management of telecommunication networks in case of a threat and a control mechanism for connection lines crossing the border of Russia"; 3) "The implementation of a Russian national Domain Name System (DNS)" (DGAP, 2020, p. 2)

been extensively studied in the West as a general topic, this paper will focus on active measures and reflexive control operations carried out in the cyberspace, as a sub element of Russia's information warfare against Western democracies. (Blank, 2017, p. 83)

In the context of information warfare, Putin has adapted old Soviet-style active measures and reflexive control methods to the new technological context to achieve information superiority in the information space to support its regime core political objective – regime survival. In this paper, the concept of information superiority is defined as the discursive domination of specific state-sponsored narratives in the information space, while countering and mitigating alternative and opposite narratives. This definition is different from Western military understanding of the concept, which focuses on a "network-centric" approach seeking to establish uninterrupted flow of information between units, weapon systems and command centres to increase coordination of arms, situational awareness, and lethality on the battlefield. (Gallant, 2021, p. 55)

Putin's regime has a holistic understanding of information warfare, which encompasses traditional information-based reflexive control operations, such as propaganda and disinformation targeting traditional media and social media, and cyber-based active measures operations, such as cyber-attacks targeting IT infrastructure. (Bertelsen, 2021, pp. 168-178) In addition, contrary to the predominant Western understanding of cyber security and information security[5] as two different domains, Russia's National Security and Defence doctrines combine both in the concept of information security. In the same way, from Russia's perspective cyber warfare is a sub-component of information warfare. In that context, this research is conceptually framing cyber security and Russia's cyber operations within the domain of information warfare, as they are about operations targeting information (adversarial data and information systems), for information (carries discursive power) and carried out with information (malicious code). (Marangé and Quessard, 2021, p. 49) In mobilizing and leveraging the Russian state capabilities and resources to fight

[5] Information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." https://csrc.nist.gov/glossary/term/information_security

alternative narratives about Russia in the information space, Putin has engaged Russia in an ongoing information war against Western democracies.

Why Studying Russia's Information Warfare in the Cyberspace is Important?

Since its cyber-attacks against the Estonian government in 2007, Russia's cyber activities seemed to have increased drastically both in terms of frequency and scope over the last decade and a half. (Valeriano et al., 2018, p. 110) For instance, Russia, with the help of nationalist hacktivist groups, believed to have ties to Russia's Federal Security Agency (FSB), carried out a Distributed Denial of Service (DDoS) attack against the Estonian government in 2007. The attacks followed the Estonian government's announcement of the removal of a statue dedicated to the sacrifice of millions of Union of Soviet Socialist Republics (USSR) soldiers during the Great Patriotic War (Russian term for the Second World War). The following year, similar attacks targeting the Georgian government were carried out in parallel to Russia's ground and air counteroffensive against Georgian troops in Abkhazia and South Ossetia. In 2013-14, during the Euromaidan demonstrations in Ukraine and the subsequent military conflict against pro-Russian separatist groups, Russia with the support from Russian Hacktivist groups, such as CyberBerkut, believed to have ties to Russia's military intelligence (GRU), carried out multiple cyber-attacks against Ukraine. (Greenberg, 2019, p. 225) Russia targeted Ukrainian opposition members, members of parliament, Ukraine's National Strategic infrastructure, including power grids, and Ukraine Central Election Commission (CEC) during the presidential election in 2014. (Jasper, 2020, pp. 55-56) In 2015, the French Television channel TV5 was hacked, and scheduled broadcasting was shut down for hours by what is believed to be Russian hackers working for the GRU passing themselves for Islamic state's hackers. (Rid, 2020, p. 370) In 2016, the Democratic National Committee (DNC) servers were hacked and thousands of emails and document pages pertaining to DNC senior officials such as John Podesta and Hillary Clinton herself were leaked on the WikiLeaks website, marking a sharp drop in Hillary's vote intention polls. (Rid, 2020, p. 387) Forensic evidence pointed to both the GRU and Russia's Foreign Intelligence Agency (SVR). (Jasper, 2020, p. 79) In 2017, the political party of Emmanuel Macron then presidential candidate was hacked, and 9 gigabytes of personal data was leaked by Russian hacktivist groups known as Pawn Storm or APT28. (Jasper, 2020, p. 122) The same year, Ukraine along with hundreds of thousands of other computers worldwide, were hit by a cyber-attack disguised as a ransomware called NotPetya, which was later linked to the GRU by U.S. intelligence agencies and private forensic experts. (Bendiek and Matthias, 2021, p. 25)

Cyber-attacks attributed to Russia against countries located in Russia's "Near Abroad,"[6] such as Estonia, Georgia, Ukraine, and against Western countries, such as France, Germany, Canada and the U.S. are highlighting a new international security context. This new context is characterized by societies increasing dependency on digital technology and infrastructure, and digital services, and a highly interconnected information network enabling the instant creation, sharing and consumption of information bypassing traditional channels of communication. Furthermore, Western media and cyber "forensic analysts usually focus on the origins and vectors of cyber-attacks, the techniques and tools used, their impact, and how their effects can be defended against or mitigated." (Connell and Vogler, 2017, p. 1) However, strategic questions, such as why state sponsored cyber threat actors are conducting cyber-attacks, their intentions, and how risks and escalations in cyberspace is perceived by them are often overlooked or brushed superficially. (Connell and Vogler, 2017, p. 1) In this context, Western governments and cyber security experts tend to apply a mirror image to state-sponsored cyber threat actors, such as Russia. Accordingly, they tend to make assumptions about Russia's motivations, intentions, and risk calculus based on Western thinking and governance models about the cyber space. (Connell and Vogler, 2017, p. 1) It may be hard for Western policymakers and cyber experts to understand that some countries, such as Russia are actively investing in information warfare capabilities, including in the cyberspace to destabilize societies in an ongoing fashion to achieve information supremacy and ensuring regime survival at home.

[6] The concept of Near Abroad was developed right after the collapse of the USSR and designate a zone where Russia has perceived privilege interests in Ex-Soviet Republics, as a result of historical and cultural ties and significant Russophone populations. (Spechler and Spechler, 2019, p. 1) Important to note that Baltic states are usually not amongst the Near Abroad countries.

Furthermore, Russia's "hybrid warfare" methods as multiplicator of traditional military capabilities during conflicts amongst states have been thoroughly examined in the West. (Marangé and Quessard, 2020; CCCS, 2021; Lilly and Cheravitch, 2020; OTAN, 2018; Duncan, 2017; Valeriano et al., 2018; Bertelsen, 2021; Jasper, 2020; Medvedev, 2015; Rid, 2021; Greenberg, 2019; Connell and Vogler, 2017) Indeed, the publication in 2013 of the then Chief of the General Staff Valery Gerasimov's article entitled "*The Value of Science is in the Foresight*" in the *Voyenno-Promyshlennyy Kurier* journal layout his vision of the 21st century security environment where modern warfare encompasses military and non-military capabilities. (Duncan, 2017, p. 6) The article became the subject of intense debate in the West, especially after Russia's involvement in the Ukrainian conflict and the annexation of Crimea in 2014. Some scholars in the West saw in Gerasimov's article the blueprint of Russia's new strategic and tactical approach to war and Russian intervention in Ukraine as the implementation of the hybrid warfare model. (Duncan, 2017, p. 6) On the other hand others argued that Gerasimov's article only summarized and adapted old Soviet Cold war era doctrines to today's security context. (Duncan, 2017, p. 9) Without taking part in this debate, it seems clear that Russia has militarized unconventional information capabilities to support its conventional forces amid interstate conflicts. However, not much attention has been devoted to understanding why and how Russia has developed these capabilities. After all, as it will be demonstrated in this paper, Russia had published doctrines laying down the foundations of information warfare in the cyber space as early as 2000, which correspond with Putin's election as president of Russia. (Carman, 2002, p. 352) In addition, in examining Russian information security doctrines, it becomes clear that the conceptual and doctrinal underpinnings of Russia's information warfare extend far beyond the realm of military conflicts and operations. As such, the first chapter of this paper will examine historical and political underpinnings framing Russia's understanding of information warfare as a holistic concept, in which Putin's core political considerations are embedded. The theoretical framework of this paper applies a structuralist epistemology and a constructivist ontology, which enable an approach tailored to Russia's historical and political context, and Putin's governance model. This theoretical framework also enables a multidisciplinary understanding of Russia's information warfare consolidating the military and socio-political perspectives.

This paper proposes that Russia’s information warfare in the cyberspace has been primarily developed to ensure Putin’s regime survival and then applied to the military realm through a militarization process of Russia’s information warfare capabilities overtime. To achieve regime survival, Putin’s regime is carrying out information and influence operations in the cyberspace to support three main objectives: 1) Portraying Russia as a besieged fortress, by creating a narrative bubble claiming that Russians and Russian society are constantly under threat from Western militaries and its malicious influence; (Herd, 2022, p. 155) 2) Amplifying positive narratives on Russia and his regime, while at the same time suppressing and delegitimizing negative ones; (Marangé and Quessard, 2021, pp. 121-122) 3) Weakening Western soft power by exposing, distorting and amplifying Western societal tensions and issues. (Marangé and Quessard, 2021, p. 135) These three main objectives aimed to influence Russians’ perceived reality into accepting Putin’s regime willingly, hence increasing his regime survival’s probability. Russia’s information warfare doctrine and capabilities will be discussed in detailed in the second chapter.

Tying Russia’s use of information and influence operations to Putin’s regime survival goal, instead of being solely pragmatic short-term supports to traditional military capabilities employed on specific theatres of operation, these concepts become common characteristics of the Western-Russian relationship. If the core objective of Russia’s information warfare against the West is to ensure Putin’s regime survival, Russian operations will not stop even if important issues and grievances are resolved between the West and Russia (e.g., over Ukraine). Russia’s information warfare against the West will continue as long as Putin’s regime benefits from propagating a narrative of military and political rivalry with the West. The intensity and frequency of these operations may well vary according to Putin’s changing perception of how well he is holding his grip on Russian society, instead of positive diplomatic outcomes from Russia’s relations with the West. This conceptual shift may inform new ways to react to Russia’s information and influence operations in the cyberspace and inform escalation risk calculus.

Theoretical Approach Structuralist-Constructivism

From an International Relations (IR) perspective, governments are the main actors on the international stage as they hold most of the legislative, and military powers. From the Structuralist and Constructivism perspectives, international and domestic considerations such as the nature or the type of regime in place in a country and its national identity[7] are crucial to understand the states' action on the international stage. (Waltz, 2001, p. 81; Macleod and O'Meara, 2010, p. 250) Classical IR structuralist School of thoughts, including neoclassical realism developed by Kenneth N. Waltz and republican liberalism, firstly proposed by Emmanuel Kant are also taking structural and domestic factors into considerations. However, their paradigm framework does not take into consideration the "intersubjective"[8] effects of information underpinning social understanding of world events and how it informs countries' national identity. It is not to say that these are not relevant approaches, but as information operations and influence operations are discursive in nature, it is important to take under consideration how information is produced, promulgated, consumed and how it can affect targeted societies social and political structures. Therefore, these traditional IR approaches are too limited to study Russia's information and influence operation in the cyberspace.

National identities, along with individual "past experiences, education, cultural values, perceived [political] role requirements" (Heuer, 1999, p. 7) are acting as a filter through which information is processed by individuals, influencing the decision maker's understanding of world events and framing their mindset. Indeed, national identities influence a government's decision-making process by attributing different sets of meanings and values to events and challenges influencing the prioritization of issues and certain governance aspects, including centralization/decentralization, vertical hierarchy, transparency, diversity of opinions, etc. For instance, in a country where the state embodied a national identity underpinned by

[7] National identity is "[…] a discursive process (intersubjective) between the state (structure) and the population (agents), where a consensus is reached on a more or less vaguely define and stable set understandings and significations (values, cultural traits, historical underpinnings) differentiating it from other (or foreign) identities." (Macleod and O'Meara, 2010, p. 267)

[8] Intersubjectivity is the process through which collective understanding is created as a result of shared social interaction amongst individuals, groups, organizations and governments. (Macleod and O'Meara, 2010, p. 267)

inspired liberal democratic philosophy and values, civil society, market forces, election cycles maybe themes weighting more in the decision-making process of the government than its leaders' personality, past experiences or considerations about mitigating political competition, and regime survival. A national identity is formed by the intersubjective dynamism between, the state and the population through discursive actions promoting and contesting the dominant narrative about national identity. (Macleod and O'Meara, 2010, p. 250) This ongoing competition between different and sometimes contradictory narratives on what it means to be a citizen of a country (e.g., Russians) end-up creating a dominant national picture or collective understanding more or less well define encompassing the core values and national interests of a country. However, it is important to note that national identities are not fixed, they change and evolve as per the state (structure) and population (agents) shared understanding of their common identity, role and place in the world and their actions and reactions to world events and narratives. (Macleod and O'Meara, 2010, p. 249) No society is homogenized, there is always alternative and counter narratives advocating for different understandings of events or what it means to be a citizen of a country, which over time influence and change the collective understanding of the national identity. As a discursive process, national identity is formed, contested, legitimized and evolved primarily in the information space of countries.

Governments play an important role in shaping the national identity of their country by their ability to influence the information space, due to their communication resources and their authoritative power of declaring what the official (or right) interpretation of an event is or their ability to embody and speak on behalf of segments of the population. In that context, the nature of the regime in power can have a significant effect on the development of national identity. For instance, liberal democratic governments (structure) are well equipped to channel counter narratives and societal impulses and pressures to change the national identity, as the democratic structure allows for political changes through institutionalized political and legal mechanisms such as elections. This allows democratic states to adapt and change overtime reflecting societal impulses and pressures redefining the national identity and states' objectives and goals. However, autocratic systems such as Russia, are more rigid and inflexible, because the nature of their system does not allow for political changes (or allow for top-down limited changes) reflecting emergent alternative and counter narratives about the national identity in the information space. In that context, Putin needed to find other ways to channel these social impulses and pressures developing overtime into a national identity that reinforce his rule over Russia, while delegitimizing and suppressing alternative and counter narratives advocating for political changes. Although Russia's political system seems somewhat democratic on paper, since Putin became president in 2000, his regime eroded and co-opted Russia's democratic foundations into a "managed democracy."[9] (McFaul, 2021) The autocratic nature of Putin's regime and governance model means that Putin's individual mindset must be overrepresented in the government decision-making process, thus heavily influencing Russia's government vision of Russia's national identity. (Stent, 2020, p. 41) Therefore, even in Russia, the nature of the regime does not preclude social changes from happening; however, it does change the weight and role of the government and of Putin in the intersubjective process creating the dominant national identity in the information space.

Putin's Regime Survival Methods

To ensure regime survival in this context, Putin employs a mix of persecution and persuasion methods domestically while using a mix of hard power and soft power abroad. Persecution at home is achieved via the use of force enabled by the establishment of a police state. Internationally, hard power is exercised via the show of conventional military might (e.g., armed forces modernization and foreign military interventions). On the other hand, this paper defines "persuasion" as the use of tailored narratives aimed at influencing Russia's national identity and boosting both domestic support for his regime and soft power abroad. Persecution and hard power projection are coercion-based mechanisms, while persuasion and soft power projection are discursive-based mechanisms. Persecution uses force to physically coerce Russian society into accepting Putin's regime, while persuasion aims at creating a perceived social reality (national

[9] The concept of Managed Democracy was first introduced in a speech of Vladislav Surkov to a conference of United Russia by Vladislav Surkov in 2001. Surkov known to be a figured well respected by Putin described his vision of a managed democracy in Russia as "a centralized political system, dominated by a single political party, which would manage the operation of democratic institutions to ensure the well-being and prosperity of society." (Spechler and Spechler, 2019, p. 8)

identity) where Putin’s regime is accepted willingly and even needed by Russian society. As autocratic regimes are not based on democratic principles (popular legitimacy, political competition, rule of law, etc.) the balance between the use of persecution and persuasion is critical for their longevity. The more successful Putin’s regime is in persuading Russians at home and people abroad that they are better off with him, the less he must coerce Russian society into accepting his reign. Active measures and reflexive control operations in the cyberspace are tools in Putin’s toolbox to maintain military dominance in a given theatre, and also more broadly to maintain informational supremacy in Russia’s information space. (Valeriano et al., 2018, p. 115) To achieve that, Putin is trying to influence Russians perceived reality by using old KGB active measures and reflexive control type of operations to influence narratives about Russia in the national and international information space. Active measures are defined in this paper as:

> a form of political warfare conducted by Soviet intelligence and security services to influence the course of world events. Active measures ranged from media manipulations to special actions involving various degrees of violence and included disinformation, propaganda, counterfeiting official documents, assassinations, and political repression. (Duncan, 2017, p. 11)

Reflexive control is defined in this paper as:

> a means of conveying to a partner or an opponent specifically prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action. (Duncan, 2017, p. 12)

Active measures and reflexive control are wide-encompassing concepts that can include a large array of operation types carried out through the internet and human assets. As this paper focuses on operations carried out through the cyberspace exclusively, this paper uses the concept of information operations and influence operations respectively to designate active measures and reflexive control operations carried out in the cyberspace. Information and influence operations are not new concepts in Russia, as they found their roots in the concepts of active measures and reflexive control going back as far as Imperial Russia and its secret police *Okhrana*. (Valeriano et al., 2018) Putin as a former KGB case officer stationed in Dresden in East Germany, which was one of the main centres for the development of active measures and information operations during the cold war, must understand very well the power of information and what active measures can achieve in terms of regime survival. (Rid, 2021) Although from old Russian concepts, active measures and reflexive control type operations are re-emerging in Russia's foreign policy toolbox as a result of the new technological context characterized by our societies becoming increasingly information based. (Seaboyer, 2018, p. 3) Just like traditional active measures using human assets, cyber-attacks are not only about damaging IT infrastructure, as they can be leveraged for their discursive power in influencing both the behaviour of the targeted organization and the perception of others about the organization victim of a cyber-attack and the country's ability to prevent them. The third chapter will demonstrate the discursive power and impact of Russia's cyber-attacks in Ukraine since 2014.

In this paper, information operations will include IT infrastructure infiltration (e.g., spyware, ransomware), damages to IT infrastructure and defacement of websites. Influence operations will include data leaks, weaponization of social media, and co-opting hacktivist brands such as WikiLeaks and Anonymous.

Research Main Limitations

It is important to note that this research is based solely on unclassified open-source information and on French and English translations of original Russian documents included in the referenced sources. Therefore, the reliance on second-hand materials in French and in English constitutes the main limitation of this research in terms of translation accuracy and possibility of authors' narrow selection of original materials in Russian. Future research on the subject would benefit greatly from including Russian-language literature.

2 - PUTIN'S BACKGROUND AND GOVERNANCE MODEL (PUTINISM)

Due to his central position within Russia's governance structure (Stent, 2020, p. 346), understanding Putin as an individual before he becomes president of the Russian Federation in 2000 is crucial to understand Russia's governance model and its actions domestically and internationally. However, personal information on Putin's past is scarce and many available sources are believed to be unreliable as they are often based on rumours and/or do not have sufficient distance from their subject of research to be considered objective. (Hill and Gaddy, 2015, p. 6) Albeit his secretive past the grand lines are publicly available and can help us brush a broad picture of the man.

Putin grew up in Leningrad (St. Petersburg) and he graduated with a law degree from the Leningrad State University in 1975 and was immediately recruited in the KGB (*Komitet Gosudarstvennoy Bezopasnosti*) as a case officer and attained the rank of lieutenant colonel. (Hill and Gaddy, 2015, p. 7) He was posted to Dresden in East Germany in 1985 and came back to Leningrad in 1990, just as the USSR was on the verge of collapsing. (Herd, 2022, p. 12) Back in Leningrad, Putin worked with his former law professor Anatoly Sobchak and supported his successful electoral campaign to become the first democratically elected mayor of St-Petersburg in 1991. (Belton, 2020, p. 47) Shortly after having been appointed as deputy mayor of St. Petersburg, Putin resigned from the KGB in August 1991. (Gessen, 2014, p. 95) In 1996, after Mayor Sobchak's electoral defeat, Putin moved to Moscow to work in the Kremlin and a year later he was elevated to the position of deputy chief of the Presidential staff. (Belton, 2020, p. 110) In 1998, Putin became the head of the Russian Federal Security Service (FSB), which is the main successor of the KGB and a year later, he was appointed deputy prime minister. Shortly after, he was chosen as prime minister of the Russian Federation by President Boris Yeltsin. (McFaul, 2021, p.17) Two days before Boris Yeltsin's resignation announcement, Putin published a text of 5000 words entitled *Russia and the Threshold of the New Millennium* (Millennium Message), laying out Putin's vision and overall plan for Russia. (Hill and Gaddy, 2015, p. 56) Finally, Putin became acting president on December 31, 1999, and was officially elected president in March 2000. Although it is nearly impossible to know exactly what Putin's personality and thoughts were back then, and how they have influenced his governance style once he became president, we can analyze the overall historical periods and events, in which Putin found himself during the 1980s and 1990s and, accordingly to constructivist approaches infer plausible impacts these events may have had on Putin. Indeed, as any individual, Putin's vision and understanding of the world is based on a mindset formed and shaped from experiences, socialization, education, values and perceived role requirements. (Heuer, 1999, p. 7)

The two following experiences have been selected for this study – Putin's experience in Dresden, East Germany as a KGB case officer between 1985 and 1990 and his early political career experience as deputy Mayor of the first democratically elected mayor of St-Petersburg Anatoly Sobchak between 1991 and 1996. These two particular periods of Putin's life were selected based on sources availability and their historic significance. In Dresden, Putin witnessed the unexpected collapse of an autocratic regime that was believed at the time to be the most stable and Stalinist of the Soviet satellite countries. (Herd, 2022, p. 12.) In St. Petersburg, Putin not only witnessed the chaos unleashed by the liberal democratic transition in Russia, but he was also an active actor in this new system, which almost cost him to be charged with corruption and abuse of power. (Gessen, 2014, p. 123) Due to their historical significance and chaotic nature, these two experiences have a high potential to be amongst the events that constitute the bedrock of Putin's mindset and vision of Russia as it will be expressed in his Millennium Message before he becomes president, and during his presidency under the form of Russia's national identity narrative promulgated by the Kremlin.

Dresden 1985-1990

While Mikhail Gorbachev was pushing the USSR on the path of *perestroika* and *glasnost*, Putin was in Dresden and witnessed the inherent tensions created by the attempt to reform a complex authoritarian system without losing control. (Hill and Gaddy, 2015, p. 113) As a result of the German Democratic Republic (GDR) communist elites' refusal to follow and adopt Gorbachev's reform of *perestroika and glasnost*, popular pressures and resentment against the Communist regime was increasing quickly (Hill and Gaddy, 2015, p. 145) In addition to popular unrest, East Germany went through a severe economic crisis that aggravated the situation significantly. Putin witnessed in Dresden monumental political and economic failure due to blind ideological resistance to reforms. Notwithstanding all the geographical and economic advantages of the GDR, including access to important ports, educated labour force, proximity with Western markets, its economy spiralled down in the early 1980s following a significant drop in global oil prices. (Hill and Gaddy, 2015, p. 146) In urgent "need for hard currency, the GDR was forced to cannibalize its entire economy by exporting whatever it could to the rest of Europe often at a loss." (Hill and Gaddy, 2015, p. 146) East Germany in the 1980s was a classic case of reform dilemma, which can be understood as:

> a crisis emerge, leading to experiments in reform that tend to fail, leading to protest and popular dissatisfaction, which the authorities react to by backing away from reform and trying to buy off the population with consumer goods, stability and jobs. (Hill and Gaddy, 2015, p. 146)

This led to economic stagnation and a new crisis emerged with the need for new reform, and so on. (Hill and Gaddy, 2015, p. 147) The lack of flexibility and pragmatism of the GDR political system and its leader's obsession with control, led East Germany into an uncontrollable socio-economic turmoil. Putin noted in his official biography *Ot pervogo litsa* published in 2000:

> […] the GDR in many respects was an eye-opener for me. I thought that I was going to an East European country, to the centre of Europe. Outside it was already the end of the 1980s, but in dealing with the people who worked for the MGB (Ministry of State Security, or *Stasi*), I realized that they themselves and the GDR were in a situation which we had gone through many years ago already in the Soviet Unions. It was a harsh totalitarian country, similar to our model, but 30 years earlier. And the tragedy is that many people sincerely believed in all those communist ideals. (Nataliya et al., 2000, p. 70)

At the end of his assignment in Dresden and after the fall of the Berlin Wall, a crowd of East German protesters gathered in front of the *Stasi* building where Putin worked and later stormed the building. (Gessen, 2014, p. 68) Later Putin stated that he confronted the crowd slowing them down until the military came and dispersed the protesters. (Gessen, 2014, p. 68) Although it is impossible to know if that is true, he told the biographers, "I accept the Germans' crashing their own Ministry of State Security headquarters, but we were not their internal affairs." (Gessen, 2014, p. 68) Soviet military took several hours to come and dispersed the crowd as per Putin's own account, the Soviet military commander told him on the phone, "we cannot do anything without orders from Moscow. And Moscow is silent." (Belton, 2020, p. 43) Putin seems to have realized then that the Soviet Union model was about to collapse. Putin will later tell a journalist that "I got the feeling then that the country no longer existed. It was clear the Union was ailing. And it had a terminal disease without a cure – a paralysis of power. (Belton, 2020, p. 43)

Amid the chaos unfolding in East Germany, several groups of high-ranking KGB and *Stasi* (East German equivalent of KGB) officers were preparing to the eventual collapse of the Soviet Union. Some started designing financial scheme using KGB and *Stasi* front companies in the West to ensure uninterrupted flow of hard currency to support KGB foreign operative networks. (Belton, 2020, pp. 32-33) Other groups of officers elaborated plans to take power in East Germany in case of collapse of the Communist Party. (Belton, 2020, pp. 33-34) Although, several sources' points to Putin's involvement in these schemes, it is virtually impossible to empirically confirm Putin's direct participation. Nonetheless, it shows a particularly strong cultural and identity trait amongst the people working in the Soviet security and intelligence agencies – survival.

Later, Putin would experience similar outcomes in Russia. However, from Putin's perspective the cause of the USSR and subsequently the Russian Federation socio-economic crisis would be the opposite – too many liberal reforms that weakened and paralyzed the state. (Herd, 2022, p. 12)

St. Petersburg 1991-1996

Putin was transferred back to Leningrad (St. Petersburg) in 1991 to work with his former professor Sobchak. (Gessen, 2014, p. 95) The reason for his transfer may have been Putin's experience in living abroad and his knowledge of international trade law, as the KGB had been instructed to act as a middleman between foreign companies wishing to establish themselves in USSR and supporting Soviet corporations that wanted to enter foreign markets. (Hill and Gaddy, 2015, p. 148) After the election of Sobchak as the first democratically elected mayor of St. Petersburg in 1991, Putin was appointed deputy mayor and chairman of the Committee for External Relations. (Belton, 2020, p. 47)

During his time as deputy mayor, Putin not only witness the economic and political chaos of Post-Soviet Russia exemplified by food shortages in major Russian cities, including St. Petersburg, but he was also involved in a major scandal that could have cost him his position and he could have been potentially arrested. After the collapse of the USSR centralized economy, Russia's economy collapsed as most of its trade and industrial structures were designed to address USSR centralized economic demands. (Tsygankov, 2019, p. 84) Russia's Gross Domestic Product (GDP) contracted by more than 40% between 1991 and 1994 and the country went through a hyperinflation period with catastrophic consequences. (Tsygankov, 2019, p. 84) For instance, Russia's biggest cities like St. Petersburg and Moscow were not able to purchase food products on Russia's domestic markets, creating food shortages and famine in big cities. (Hill and Gaddy, 2015, p. 155) In that context, Putin used barter type deals to import food products from foreign countries like Germany and others to address the situation in St. Petersburg. However, Putin failed as only a fraction of the food promised in the deals made it to St. Petersburg. (Belton, 2020, p. 89) Following this dramatic event and Putin perceived failure to address the situation, the St. Petersburg city council committee in charge of securing food supplies during the crisis of 1991, launched an investigation targeting Putin and the deals he made on behalf of the mayor's office in 1991. (Gessen, 2014, p. 123) The committee found that the dozens of contracts totalizing $94 million made by Putin were overtly illegal (Belton, 2020, p. 91) The committee wrote a report to the mayor Sobchak, accusing Putin of corruption and abuse of power and recommending the mayor to submit the report to the prosecutor's office in Moscow, but Sobchak ignored the report entirely, hence protecting Putin from prosecutions. (Gessen, 2014, p. 123) People involved in Putin's oil-for-food scheme later said that the main aim was not to secure food supply, but to ensure the influx of hard currency to pay for the city's public debts and maintenance of critical infrastructure. (Belton, 2020, pp. 92-93) However, considering the significant amount of money that was never accounted for, and the spectacular enrichment of Putin and the people close to him during this period (Belton, 2020, p. 94) suggest that neither moral imperatives to feed Russian citizens nor the crucial need to maintain public infrastructure were the main goals.

Putin would often refer to this time as a time of chaos enabled by a weak and powerless federal state unable to take actions to address the economic and social issues. The general population was exhausted after almost a decade of successive economic and political crises, and the sentiment that something needed to be done to stop the dismemberment of the state grew significantly amongst political elites. (Belton, 2020, p. 167) For instance, in the late 1990s the sentiment of political urgency was so strong amongst Russian politicians that virtually all political parties and groups from left to right "felt that the post-Soviet dismantling of the state had gone too far and advocated the restoration of Russian state power." (McFaul, 2021, p. 16)) Even some economists around Yegor Gaidar, who was heading the liberalization of the Soviet-style economy (the shock therapy) in 1992-93, were advocating for a stronger state and slowing down economic reforms. (Hill and Gaddy, 2015, p. 38) The sentiment that Yeltsin was unfit to rule Russia and that Russia was about to descent into chaos due to these liberal and democratic reforms were particularly dominant in old Soviet elite and KGB circles. They viewed Yeltsin's overture to democracy with disgust, and they believed that his "appealed to Russia's regions to take as much freedom as they could swallow" was a Western undercover plot to dismember the Soviet empire. (Belton, 2020, p. 117) Although these sentiments seemed to have been popular in social circles Putin was part of, it is hard to know for sure whether Putin was personally convinced that liberal democracies and liberal capitalism were not suited for Russia, or whether he took advantage of these sentiments to justify his grip on power. In any case, Putin would create a national narrative that refers to this period as a "Time of Troubles" and a period of chaos that was created mainly by Russian elites attempt to emulate in Russia Western principles and values. (Herd, 2022, p. 58) Indeed, conform to the predominant sentiment existing in the old Soviet elite and KGB circles Putin's national narrative portrays the 1990s as empirical proof that Western liberal values and democratic principles were weakening the Russian state's ability to function and therefore almost led to the collapse of the Russian state. In this narrative, Putin embodied the role of a strong and efficient manager that was able to strengthen the state, managed inner fighting amongst traditional political elites and the newly created oligarch class, thus bringing stability back to Russia and essentially saved the state from inevitable collapse. (Herd, 2022, p. 59)

The core ideas forming Putin's national narrative since he became president of the Russian Federation can be found in the treatise he wrote and published online before becoming president in 1999 entitled *Russia and the Threshold of the New Millennium* (Millennium Message). Putin's vision aligns closely with the philosophy of the tsar's loyalists that have left Russia amid the Bolshevik revolution of 1917, which are known in Russia as the White émigrés. Once in exile across Europe, the White émigrés started developing a national vision for a post-Soviet Russia. This group envisioned Russia as a great power distinct from the West, a Eurasian civilization fated to counter Western powers. (Belton, 2020, 259)

Putin's narrative first core idea is the importance of a strong Russian state able to ensure Russia's sovereignty in all spheres of activities and, economic and political stability. Putin describes himself in his Millennium Message as a *gosudarstvennik* or statist, which as a specific meaning in Russian, as it does not refer to traditional politicians or policymakers, but rather to a builder of the state or a self-selected permanent servant of the state who believes only in the state itself. (Putin, 1999, p. 6) This self-identification as a statist is aligned with the institutional culture cultivated in the KGB. In Russia, people who have worked or are working for Security and Defense Departments, also called *silovyye struktury* (power structure), are known as *siloviki*. (Hill and Gaddy, 2015, p. 41) *Siloviki* enjoyed a specific reputation in Russia of being ultimate Russian patriots and proponents of a strong state. (Belton, 2020, p. 117) They also cultivate the myth of importance in defending Russian land against constant foreign and domestic threats, reaching back to the tsarist secret police the *Okrana* (Stepanov, 1999, p. 6) and later under Vladimir Lenin – the Chekist. (Kari and Pynnöniemi, 2019, p. 18) In addition, Putin's Millennium Message emphasis a Russian definition of the state, which differs from Western understandings. In the West, we understand the role of the state as a protector of individual rights and facilitator of the socio-economic life of its citizens. Putin's narrative supports the idea that "while Mother Russia must be protected, she does not necessarily protect her own citizens. The Russian state is primary. […] The individual and society are and must be subordinate to the state and its interests." (Hill and Gaddy, 2015, p. 40) This idea that everything is subordinated to the interest of the state, is an important element, as it highlights the utilitarian approach of Putin to leverage all sectors of Russian society including, politics, economy, financial, natural resources and information to achieve his regime objectives. Putin's understanding of the state is made very clear in the Millennium Message. He wrote:

> For us, the state and its institutions and structures have always played an exceptionally important role in the life of the country and the people. For Russians, a strong state is not an anomaly to fight against. Quite the contrary, it is the source and guarantor of order, the initiator and the main driving force of any change. […] Society desires the restoration of the guiding and regulating role of the state. (Putin, 1999, p. 7)

The second core idea is that Russia is a besieged fortress, and its unity is compromised by foreign originated values and ideologies. Putin stressed that throughout history, the Russian state lost its status when Russians were divided and embraced foreign values and ideologies. Putin wrote in the Millennium Message: "Since the fall of communism, Russians had embraced personal rights and freedoms, freedom of personal expression, freedom to travel abroad. These universal values were fine, but they were not Russian." (Hill and Gaddy, 2015, p. 39) Putin affirms also in his Millennium Message that Russian society has been historically collectivist and not individualist, meaning that Russians need a strong and paternalistic state able to support and drive socio-economic development. (Putin, 1999, p. 7) Putin advocates for a return to the traditional values that makes what he called "the Russian Idea," which are patriotism, collectivism, solidarity, *derzhavnost* (the belief that Russia is destined to be a great power). (Putin, 1999, p. 7) Although, Putin stated a few times that he did not aspire to re-establish an authoritarian state in Russia and that democracy was here to stay (Putin, 1999, p. 6) his emphasis on social and political stability was a clue of his intention to establish a managed democracy. Putin portrayed political competition as an engine for chaos and the creation of extremist sentiments that would jeopardize the unification of Russian society behind his "Russian Idea" and he also openly advised political parties and movements to fall in line with his vision. Putin wrote:

> I suppose that the new Russian idea will come about as an alloy or an organic unification of universal general humanitarian values with traditional Russian values which have stood the test of the times, including the test of the turbulent 20th century. This vitally important process must not be accelerated, discontinued and destroyed. It is important to prevent that the first shoots of civil

> accord be crushed underfoot in the heat of political campaigns, of some or other elections. […] The overwhelming majority of Russians said No to radicalism, extremism and the opposition with a revolutionary tint. […] Serious politicians whose parties and movements are represented in the new State Duma, are advised to draw conclusions from this fact. I am positive that the feeling of responsibility for the destinies of the nation will have the upper hand, and Russian parties, organizations and movements and their leaders will not sacrifice the common interests of and prospects in store for Russia, which call for a unified effort of all healthy forces, to the narrow partisan and time-serving considerations. (Putin, 1999, p. 8)

In addition, following the 2004 Orange revolution in Ukraine, Putin established a mass youth movement called *Nashi* which are loyal to the state and to Putin himself. (Spechler and Spechler, 2019, p. 8) The *Nashi* is designed as a counter movement to the colour revolution movements, as they are in charged of organizing counter protests to democratic demonstrations, and even identify and intimidate protesters in the streets. (Spechler and Spechler, 2019, p. 8) The creation of such a youth movement was also part of Surkov's concept of "managed democracy". The *Nashi* is used in Putin's narrative to give the impression that he and his government enjoys wide support from Russia's youth, which is not the case. Recent surveys of Putin's popularity made in 2021 shows a strong correlation between age and rate of approval of Putin as president, with younger generations having significantly higher rates of disapproval than older generations. (Statista, 2021)

The third core idea is that Russia is destined to be a great power and therefore should be treated as one on the international stage. Putin wrote in his Millennium Message that:

> Russia was and will remain a great power. It is preconditioned by the inseparable characteristics of its geopolitical, economic and cultural existence. They determined the mentality of Russians and the policy of the government throughout the history of Russia, and they cannot but do so at present. (Putin, 1999, p. 7)

In 2000, at the beginning of his first mandate as president of Russia, to a journalist question about his ability to reinstitute Russia as a great power, Putin responded that Russia is not claiming a great power status, as it is a great power by virtue of its huge potential, its history, and its culture. (Herd, 2022, p. 30) This idea is based upon a sense of historical and geopolitical continuity between the Russian Federation, the Soviet Union and the former Russian Empire, and encompasses key concepts, including keeping Russia's sovereign autonomy by limiting Russia reliance on other states; Russia as a civilizational power distinct from Western civilization (Tsygankov, 2019, p. 97); and also, the concept of the Russia's Near Abroad. The Near Abroad is a Russian foreign policy concept describing Russia's special relation and interest with former-Soviet republics, excluding the Baltic states. (Spechler and Spechler, 2019, p. 2) The concept of Near Abroad encompasses two main ideas in Russia's foreign policy. First, the Near Abroad region is understood as a zone of privileged interests for Russia, resembling the U.S. Monroe Doctrine toward South American countries in the 19th century. (Stent, 2020, p. 145) Second, the Near Abroad region is also understood as a strategic space acting as a buffer zone between Russia and Western countries, which implies that Russia does not recognize these former Soviet republics as fully sovereign nor independent from Russia. (Stent, 2020, p. 145) Putin narratives signals that as a great power, Russia has the right to cultivate special interests in Near Abroad countries and that due to historical ties, these countries should be under Russia's tutelage and influence. (Spechler and Spechler, 2019, p. 2)

These three core elements of Putin's vision of Russia seemed to have informed his governance model and his narrative about Russia's national identity. Putin needed to establish a governance model that reflects his vision of Russia in order to ensure the control over the Russian government and developed the institutional capabilities needed to influence Russia's information space into supporting his national identity narrative, putting himself at the centre of Russia's government governance model.

Putin's Governance Model – Putinism

Understanding Putin's experiences as a KGB case officer in Dresden and his early political career as deputy mayor of St. Petersburg is key to understanding Putin's system of governance, also known in the Western literature as Putinism. The common denominator connecting Putin's experiences, as described above is the threat of state collapse and by extension the collapse of his regime. (Belton, 2020, p. 348) In that context, Putin established a governance model, which encompasses three core conceptual foundational blocs aggregating lessons learned from his past and reflecting his vision of the Russian context, such as *vertikal vlasti* (vertical of power), *pravovoye gosudarstvo* (law-abiding state), and *gosudarstvennik* (state builder).

Vertical of Power (*Vertikal Vlasti*)

To ensure the cohesion of the Russian state and avoiding state paralysis that marked Russia's 1990s political context, Putin started restructuring the federal government and established a strong vertical of power right at the beginning of his presidency in 2000. (Gessen, 2014, p. 181) This vision is marked by a personalized and centralized governance structure where everyone is accountable to the man at the top. (Herd, 2022, p. 111) In that system, Putin is the ultimate authority and no holders of political or economic power can openly defy and contradict Putin. (Fish et al., 2017, p. 68) The personalized nature of Putinism has propagated an image of Putin as the ultimate pragmatic problem fixer of Russia. (Belton, 2020, p. 395) Nourishing this image of Russia's problem fixer, on numerous occasions, usually highly covered by the media, Putin goes himself to remote cities to address population grievances and publicly punish state officials. One of the best-documented incidents is in 2009, when Putin flew to the small city of Pikalyovo, near St. Petersburg to dress down the owner of a cement factory the oligarch Oleg Deripaska for having laid off hundreds of residents due to the economic downturn amid the international financial crisis of 2008-09. (Hill and Gaddy, 2015, p. 123) These staged public interventions reinforced Putin's image as Russia's ultimate authority and problem fixer, not too differently from the old Russian idea of the good tsar that was cultivated during Russia's imperial era. (Hill and Gaddy, 2015, p. 123) Since Putin is at the centre of his system of governance, he cannot always be personally handling every little issue that emerges. Putin is the "strategic planner laying out strategic objectives and goals, while expecting the Russian government to run by itself on autopilot mode, or as Putin regularly expressed like a Swiss watch." (Hill and Gaddy, 2015, p. 195) In that respect, Putin has developed a system formed with varying levels of concentric circles, with at its centre himself and his inner circle. (Ledeneva, 2013, p. 73) The closest comparison in Canada would be the Prime Minister Privy Council, however, places in Putin's inner circle are not in function of any specific position within the Russian government. Places in Putin's inner circle are solely based on the level of connection, personal proximity and loyalty to Putin. (Herd, 2022, p. 123) Only Putin can lay out state's goals and objectives and assign responsibility to lower layers of officials to attend these goals. (Fish et al., 2017, p.

68) This centralized and personalized system of governance implies that formal hierarchy amongst institutions, positions and organizational charts are not important, as appointment opportunities are based on loyalty and personal relationships to Putin. (Ledeneva, 2013, p. 80) The position in the inner circle and outer concentric circles of the government are made important by the individuals who hold them, not the other way around. (Herd, 2022, p. 123) The personalization of power in the Russian government was highlighted during the presidency of Dmitry Medvedev between 2008 and 2012, as it is believed that Putin although occupying the position of prime minister was still largely in charge of the government. (Gessen, 2014, p. 264) Indeed, it is believed that Medvedev was chosen by Putin as a front to show that Russia was still a democratic state, and that Putin was respecting Russia's 1993 constitution, which limited the number of presidential mandates for any president at two terms. (Ledeneva, 2013, p. 94)

Contrarily to some scholars' claim that Putin inherited this governance model from the Yeltsin era, usually pointing at the 1993 constitution that attributed significant powers to the presidency, Putin created the current governance model. (Fish et al., 2017, p. 68) The Yeltsin era was filled with corruption and tax evasion schemes that enabled the creation of an oligarchic class that controlled by the early 2000s more than 50% of the Russian economy (Belton, 2020, p. 192), but the foundation for a liberal democracy was established. Although the 1993 constitution clearly favored a strong presidency, it also provided division of powers between the executive, the legislative and the legal branch, while also delegating significant powers to provincial government authorities, especially in the realms of budgeting and law enforcement. (Fish et al., 2017, p. 68) The Russian parliament (*Duma*) and the Senate were bodies hosting intense debates often critical of the government; regional governors were elected; and the media was largely free from state interference. (Belton, 2020, p. 167) Since his arrival to power, Putin spent tremendous efforts in strengthening the federal government and to centralized power within his own hand. Putin started to appoint regional security-service personnel himself, sent federal inspectors to audit on an ongoing basis regional officials and offices and established federal institutions at the provincial level to monitor compliance and alignment with Moscow's decisions. (Fish et al., 2017, p. 69) Putin used every opportunity to centralize power at the federal level. For instance, following the 2004 terrorist attack against a school in Beslan in the North Caucasus, where hundreds of teachers and children taken hostage by Chechen terrorists perished during the final assault of federal forces to put an end to the stand-off. Putin used this tragedy to end the elections of crucial position across the Russian Federation, including for the governor's office in September 2004 and decided to appoint them instead. (Belton, 2020, p. 267)

The next level circle outside Putin's inner circle is constituted by the most important Russian oligarchs, mainly from the natural resources sector. His experience in Dresden and his bad experience dealing with private corporations back in St. Petersburg, might have taught him two things. 1) The state should remain in control of Russia's strategic resources, as in times of crisis private sector's businessman cannot be trusted. 2) Although the free market and capitalism proved to be superior management model for the economy than Soviet planned economy, the Russian strategic resources should actively support the state's objectives as nothing is above or equal to the state. (Belton, 2020, p. 259) Leveraging a complex scheme involving Russian banks loyal to his regime, security forces and Russia's federal court system, Putin successfully placed loyal allies, mainly *siloviki* at the head of the most important private and public companies operating in strategic sectors for Putin's regime survival, including in the natural resources, financial/banking and the media. (Belton, 2020, p. 275) By doing so, Putin removed most of the Yeltsin era oligarchs, which he despised for their liberal inclinations and often opposition to the state, took their businesses and gave them to loyal *siloviki* sharing the same vision as him. (Stent, 2020, p. 355) For instance, Mikhail Khodorkovsky, a billionaire at the head of *Yukos*, a major Russian oil company in the 2000s seen as an example of Russia's and Western economic integration was prosecuted for breaking taxation laws, that were retroactively applied to his company. Although, he might have broken Russian federation laws, the real motivation for his trial and imprisonment in 2007 seemed to be due to his personal ties with the West and to his funding of opposition political parties. (Belton, 2020, pp. 235-238) Another example of the *siloviki* takeover of Russia's most important sector, including the media is Boris Berezovsky, which was the owner of an important Russian television channel media called *ORT* which was overtly critic of Putin's rule. Berezovsky was charged with embezzlement of fund from *Aeroflot* the Russian state airline he partly owned and left to exile in 2001. (Belton, 2020, p. 206) Similar to other Russian businessman active in the 1990s, he might have broken the law, however the fact that he started to be targeted by Russian law enforcement shortly after his television channel started criticizing Putin's government shed light on a broader pattern of Russian law enforcement targeting and cracking down on oligarchs critical of Putin. (Stent, 2020, p. 355)

Due to the nature of Putin's governance system based on concentric circles, Putin is ruling in an isolated bubble from the Russian population (Gessen, 2014, p. 302), and therefore he relies on transmission belts institutions to gather critical information such as the level of popular approval or resentment and the level of cynicism against his regime. One of these institutionalized transmission belts is the *Duma*, especially the main political party United Russia (UR), which serves as a conveyor of information between Russian society and formal state structures so they can reach Putin's inner circles. (Hill and Gaddy, 2015, p. 220) Gleb Pavlovky, former key advisor to Putin regarding the management of Russian public opinion between 1999 and 2012 stated during an interview with The Guardian in 2012 that UR was like "a telephone system, transmitting signals from the Kremlin to the bottom through the regional apparatus." (The Guardian, 2012) Another example of transmission belts is the hot line used during his annual end-of-year show where Putin addresses callers' question. The questions are filtered in advance to ensure no unexpected questions or criticisms would happen during live broadcasting and all questions and calls are recorded and used for intelligence purposes to sense the population mood. (Hill and Gaddy, 2015, p. 272)

Law-abiding state *(Pravovoye Gosudarstvo)*

Another crucial element of Putin's system of governance is the empowerment and strengthening of Russia's federal court system so it could serve the state's national interests. Indeed, one of the main critics of the Yeltsin era was the weakness and contradiction of the Russian legal system and laws. As experienced by Putin in St. Petersburg, in the 1990s it was virtually impossible to do anything without breaking the law, as nothing was being accomplished via official and formal channels. The chaos was such that even Yeltsin started in the middle of the 1990s to rule by presidential decrees, bypassing the *Duma* and striking bilateral deals with Russia's regional level of government. (Belton, 2020, p. 192) To implement his vertical of power idea, Putin needed to centralized Russia's judicial power at the federal level. Putin's first effort was to consolidate Russia's judicial basis by strengthening the 1993 constitution (which his close friend, former law professor and boss in St. Petersburg Anatoly Sobchak helped draft) and elevating the federal Central Agencies such as the presidency, and the federal court. (Hill and Gaddy, 2015, p. 196) Political interference is also one of the main characteristics of Putin legal model (Ledeneva, 2013, p. 160), as according to his national narrative, every aspect of the Russian government and society must support the state national interests. For instance, according to the report entitled *The judicial system in Russia: its present state and issues* published by the Centre for Political Technologies based in Moscow in 2009: "the main problem is not corruption, levels of which do not exceed those afflicting society as a whole. Rather, the principal cause for concern is the degree to which the courts are susceptible to administrative pressure by government officials and court chairmen and chairwomen, in charge of pursuing informal agendas and communicating informal commands." (Ledeneva, 2013, p. 151) A strong federal court system firmly under political control is important for Putin as it enables Russian's bureaucracy to run like a "Swiss watch." In addition to clarify institutions' role and responsibility, Russian legal system also "act as a kind of release valve for pressure building up in the lower level of the system." (Hill and Gaddy, 2015, p. 196) Under the cover of judicial legitimacy, Putin repeatedly insisted that electoral complaints be handled in court, instead of protesting in the streets. (Hill and Gaddy, 2015, p. 196)

State Builder (*Gosudarstvennik)*

The idea of Putin as a state builder and not only as a usual president is crucial to distance us from Western perspectives and assess Putin's regime with Russian lenses. Putin is actively linking his political position as president of the Russian Federation to the survival of Russia as a sovereign country. (Shiraev and Khudoley, 2019, p. 92) This specific identity mainly cultivated in power structure such as the KGB, was infused throughout the system, as Putin assigned a wide number of former KGB and FSB officers at key positions. (Herd, 2022, p. 116) For instance, Sergei Ivanov a former lieutenant general in the KGB and in the FSB was appointed secretary of the Security Council of Russia in November 1999, effectively replacing Putin as he was appointed prime minister by Yeltsin. Later Ivanov became the defence minister in March 2001, shortly after he was appointed as the chief of staff of the presidential administration of Russia in 2011 until 2016. (Belton, 2020, p. 183) Viktor Cherkesov, the former head of the KGB directorate in St. Petersburg, became the presidential envoy to the Russian Northwest Federal District covering St. Petersburg in 2001. (Hill and Gaddy, 2015, p. 41) Nikolai Patrushev was director of the FSB from 1999 to 2008, and then secretary of the Russian Security Council. (Belton, 2020, p. 181) In an interview in *Spetsnaz Rossii* in 2001, a journal close to Russian intelligence services, retired KGB General Nikolai Leonov responded to a question about the unusually high number of ex-KGB/FSB officials at the top of the government, he said:

> First of all, the demand today is precisely for such tough, pragmatically thinking politicians. They are in command of operative information. But at the same time, they are patriots and proponents of a strong state grounded in centuries-old tradition. History recruited them to carry out special operation for the resurrection of our Great Power, because there has to be a balance in the world, and without a strong Russia the geopolitical turbulence will begin. […] What is a KGB officer? He is, above all, a servant of the state. […] Experience, loyalty to the state and an iron will – where else are you going to find cadres? […] The only people that can bring order to the state are state-people (*gosudarstvennyye lyudi*). (Hill and Gaddy, 2015, p. 41)

In Dresden, Putin witnessed the collapse of an authoritarian regime due to its extreme inflexibility, lack of pragmatism, and ideological obsession. In St. Petersburg, Putin witnessed the collapse of first the Soviet Union, then the near collapse of the Russian Federation in less than ten years, due to, as Putin perceives it, Russia's attempt to emulate the Western liberal democratic system and values. (Stent, 2020, p. 41) This experience combined with his 15 years as a KGB agent, where statist views were predominant, Putin might have concluded that a balance between reforms (mainly economic) and state's strength must be stroked to ensure his regime survival. Contrary to USSR state Soviet ideology, capitalism and a strong Russian state are not exclusive for Putin. As Putin stated himself, "communism vividly demonstrated its inaptitude for sound self-development, dooming our country to steadily lag behind economically advanced countries. It was a road to a blind alley, far away from the mainstream of civilization." (Belton, 2020, p. 259) For Putin, the Russian economy is to be harnessed as a weapon to restore the power of the Russian state. (Belton, 2020, p. 190) Therefore, stronger is Russian economy, more powerful is the state. A strong emphasis on economic reforms and economic growth were characteristic to Putin's first and second mandate. Although, Putin continued to strengthen his vertical of power and cracked down on Russian media, he instituted liberal market type reforms to bolster foreign investments in Russia and market integration with the West. (Stent, 2020, p. 97) However, by 2012, Russia's economy was showing signs of structural stagnation and more than 50% of Russia's GDP was in the hand of the Putin regime's members. (Belton, 2020, p. 275) At the same time, something seemed to have changed in Russia with Putin's return to the presidency and the 2011 and 2012 protests in Russia, also called the December movements.

Over the course of the 2010s, Putin and the Kremlin in general started to be more openly critical of Western countries, especially of the U.S. going as far as affirming that liberal democratic values were by definition anti-Russians." (Shiraev and Khudoley, 2019, p. 92) For instance, at the Valdai Club in 2013, Putin asserted that:

> The Euro-Atlantic countries are actually rejecting their roots, including the Christian values that constitute the basis of Western civilization. They are denying moral principles and all traditional identities: national, cultural, religious and even sexual […] Holidays are abolished or even called something different; their essence is hidden away, as is their moral foundation. And people are aggressively trying to export this model all over the world. I am convinced that this opens a direct path to degradation and primitivism, resulting in a profound demographic and moral crisis. (Herd, 2022, p. 97)

The December movements demonstrated two important elements. Firstly, it highlighted long-term changes and evolution of Russian society creating a gradual growth of societal pressures on the Russian government for changes, notwithstanding Kremlin's past efforts to prevent alternative narratives. (Robertson, 2013, p. 13) Secondly, the protests demonstrated the inability or unwillingness of Putin to effectively understand and address these changes. In 2011-2012, the Kremlin repressed in violence the protesters and arrested figure opposition groups such as the anarchist and atheist punk music group the Pussy Riots after they had performed in Moscow's Cathedral of Christ the Saviour. (Gessen, 2014, p. 294) Putin went after other opposition figures too, including Alexei Navalny known for his anti-corruption investigations and somewhat broad popular support and leftist opposition leaders, such as Sergei Udaltsov and Leonid

Razvozzhayev. (Hill and Gaddy, 2015, p. 249) Russian elites close to Putin were not protected either. For instance, Putin went after his close friend and mentor Anatoly Sobchak's daughter Ksenia Sobchak, as she emerged as a supporter of the 2011-2012 protests, speaking publicly at rallies and vocally expressed her dislike of the political system. (Hill and Gaddy, 2015, p. 249) Ksenia's home was raided by Russian law enforcers and "seized an estimated 1 million Euros and USD 500,000 and she was threatened with prosecution for tax evasion." (Hill and Gaddy, 2015, p. 250) Putin did not only use force to crash protests, but he also discursively framed them as non-Russian outsiders acting as a fifth column for the benefits of the West. For instance, he portrayed protesters' concerns as illegitimate and often stated that protesters were from a fringe minority segment of the population, calling them non-Russian and foreign agents. (Herd, 2022, p. 98) In a political rally in February 2012, Putin told the crowd that "we will not allow anyone to force their will upon us, because we have our own will […] We are a victorious people! It is in our genetic code. It is transferred from generation to generation, and we will have victory!" (Belton, 2020, p. 373) In addition, since 2011, at least 13 journalists have been killed or are missing and 17 have been jailed. (Committee to Protect Journalists) For Putin, the 2011-2012 protests in Russia were just part of a long sequence of events that started with the Arab revolutions that toppled Zine El Abidine Ben Ali in Tunisia, Muammar Qaddafi in Libya, and Hosni Mubarak in Egypt in 2011. (Shiraev and Khudoley, 2019, p. 92) The fact that the West seemed to embrace the democratic revolutions against long established authoritarian regimes in Northern Africa, and Western press continually drawing linkages between earlier colour revolutions in countries in Russia's Near Abroad, the Arab Spring, and the 2011-12 protests probably encouraged Putin's understanding of the events. (Hill and Gaddy, 2015, p. 245) For instance, following Putin's presidential victory, a U.S. republican senator tweeted, "Dear Vlad, the Arab Spring is coming to a neighbourhood near you." (Belton, 2020, p. 374) These manifestations and the way Putin choose to handle them indicates that his regime is facing a real and growing problem inherent to autocratic regimes – the need to reaffirm its usefulness to new generations of people and changing socio-political contexts.

This changing socio-political context in Russia and the inability or unwillingness of Putin to adapt his narrative and connect with new generations of Russians are creating a real threat to his regime, as it is creating disgruntlement in large part of the Russia society, which allows Western soft power to penetrate deeply into Russia (Bagge, 2019). Indeed, by proving inflexible on democratic reforms and unable to address younger generations' aspirations and grievances, Putin's regime is creating social tensions and pressures that are not channelled into Russian state's representative institutions, such as the *Duma*. Confronted to the situation, instead of addressing these popular grievances by implementing reforms that would address mounting social pressure for change, but inevitably diminish Putin regime's grip on power, he decided to double down on persecution of the oppositions and critics and ratcheted up information and influence operations to demonize and use the West as a scapegoat. (Stent, 2020, p. 309) This inflexibility from Putin's regime is creating a governance structure that is less and less aligned with Russia's social changes and evolution, which enhanced tensions between the state and Russia's society. Disgruntled Russians will be more receptive to Western soft power that aligns with their vision of political freedom. Therefore, as it will be demonstrated in the next chapter, Western's soft power and influence in Russia are seen as a survival threat by Russian political elites. They fear that Russian society's exposure to Western higher standards of living, liberal values and democracy would bolster domestic critics of Putin's regime and support an alternative national narrative advocating for a change of regime. Accordingly, Putin claims that Western states' soft power in Russia is the result of information and influence operations. (Bertelsen, 2021, p. 28) For Putin, any form of political protests arises at least in part because of information operations against Russia. (Giles and Akimenko, 2020, p. 71) Due to his experience, witnessing the collapse of two Soviet states, combined with his KGB experience and education, Putin understands the power and the critical role of information in keeping authoritarian regimes alive. Persecution alone does not alleviate Western's influence in Russia, only by persuading Russians that they are better off with him and his regime, instead of regime change that would from a *siloviki's* perspective bring the collapse of the state and chaos in Russia. Furthermore, to keep his system together, Putin intensified his regime information warfare efforts at home and abroad to achieve information supremacy in Russia’s information space and seeking information superiority in the international information space.

3 - RUSSIA’S INFORMATION AND INFLUENCE CAPABILITIES AS AN ECOSYSTEM

As discussed in the first chapter, Putin established a system of governance (Putinism) which enables him to control the Russian government and set the state objectives according to Putin’s regime main goal – ensuring its survival. Just like in any organizational structure of this size, Putin’s vision must be institutionalized to steer Russia’s government bodies toward accomplishing his goal. To achieve that, Putin has embedded core elements of his national narrative within Russia’s foundational national security and defence doctrine documents. This has a high discursive power in Russia, as national security and national defence departments also known as power structures benefit from a particularly high level of authority and historical prestige in Russian society. In reviewing official national security and defence documents, Putin’s vision as described in his Millennium Message and his objectives becomes clear. 1) Portraying Russia as a besieged fortress, consisting in creating a narrative bubble in Russia, where it appears as if Russians and their society are constantly under threat from Western military and its malicious influence; (Herd, 2022, p. 155) 2) Amplifying positive narratives on Russia and its regime, while at the same time suppressing and delegitimizing negative ones; (Marangé and Quessard, 2021, pp. 121-122) 3) Weakening Western soft power by exposing, distorting and amplifying Western societal tensions and issues. (Marangé and Quessard, 2021, p. 135)

It is important to note that Russia’s official doctrine documents are using the concept of “information sphere” and “information war,” which has broader meanings than the concepts of “information space” and “cyber war” used in the West. From Russia’s perspective, the information domain, like other domains of activity falls under the sovereignty of the state. (Belton, 2020, p. 198) Conceptually, the “information sphere” is closely tied to nation-state defining characteristics, including sovereignty and borders. (Lilly and Cheravitch, 2020, p. 134) Accordingly, Russia’s doctrines consider the information domain as a theatre of conflict and competition amongst states (Marangé and Quessard, 2021, p. 122) which is formed by well delimited national “information spheres” interacting with each other’s, without overlapping. This perspective is consistent with authoritative regimes institutional suspicions about uncontrolled and free flow of information that could foster critics against their regime. In that context, Russia is defending what it perceives as Russia's national information space against foreign informational interference and intrusion. (Marangé and Quessard, 2021, p. 124) In the West, the concept of information space does not include national sovereignty nor any border considerations. The information space is not clearly delimited, and it is understood as being permeable to the information produced in other countries. Although some countries may be exposed more than others to information sources coming from certain countries, the origin and type of the information consumed in a certain country are driven more by free market type of considerations and mechanism than state's national interests and sovereignty considerations. For instance, in Canada the information produced domestically, from the U.S. or more largely from the West may be more predominant than information produced in Asia, due to general language affinities, and cultural proximities to our southern neighbour. However, the Canadian government does not seek to shield Canadians from Asian information sources. Russia regulates all types of information to reduce transparency, free speech and to ensure they conform to Russia's national interests and Putin's narrative. (Bertelsen, 2021, p. 18) It is not to say that Russia is preventing all information produced in the West to enter Russia's national information space, as it would mean cutting Russia from the worldwide internet infrastructure, which would be technically unrealistic and economically unsuitable. (Marangé and Quessard, 2021, p. 76) However, Russia clearly signalled its intention to regulate the flow of information crossing its border as much as it can, in the same way any sovereign country regulates the flow of people or goods going through its border crossings. (Doctrine on Information Security of the Russian Federation, 2016) (see figure 1) This particular understanding of the information domain led to significant national interests and strategic considerations, which differ greatly from the West. For instance, while Western countries are regulating media operating on their soil to ensure transparency, good journalism practices, free speech, and preventing hateful speeches, Putin's regime made it clear since the beginning that Russia's information space most reflects the regime's national narrative and support the state's national interest. (Belton, 2020, p. 198) In that sense, Russia's information space is understood by Putin as a strategic resource at the service of Putin's regime's strategic objectives and therefore must be protected at all costs. (Doctrine on Information Security of the

Russian Federation, 2016) The strategic implications of Russian particular understanding of information space will be discussed further below in this chapter.

The concept of "information sphere" not only contains traditional information sharing considerations, but also human and societal considerations, such as how the information is created, shared, regulated, and consumed. The *Doctrine of information security of the Russian Federation* published in 2016 defines information sphere as:

> a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere. (Doctrine on Information Security of the Russian Federation, 2016)

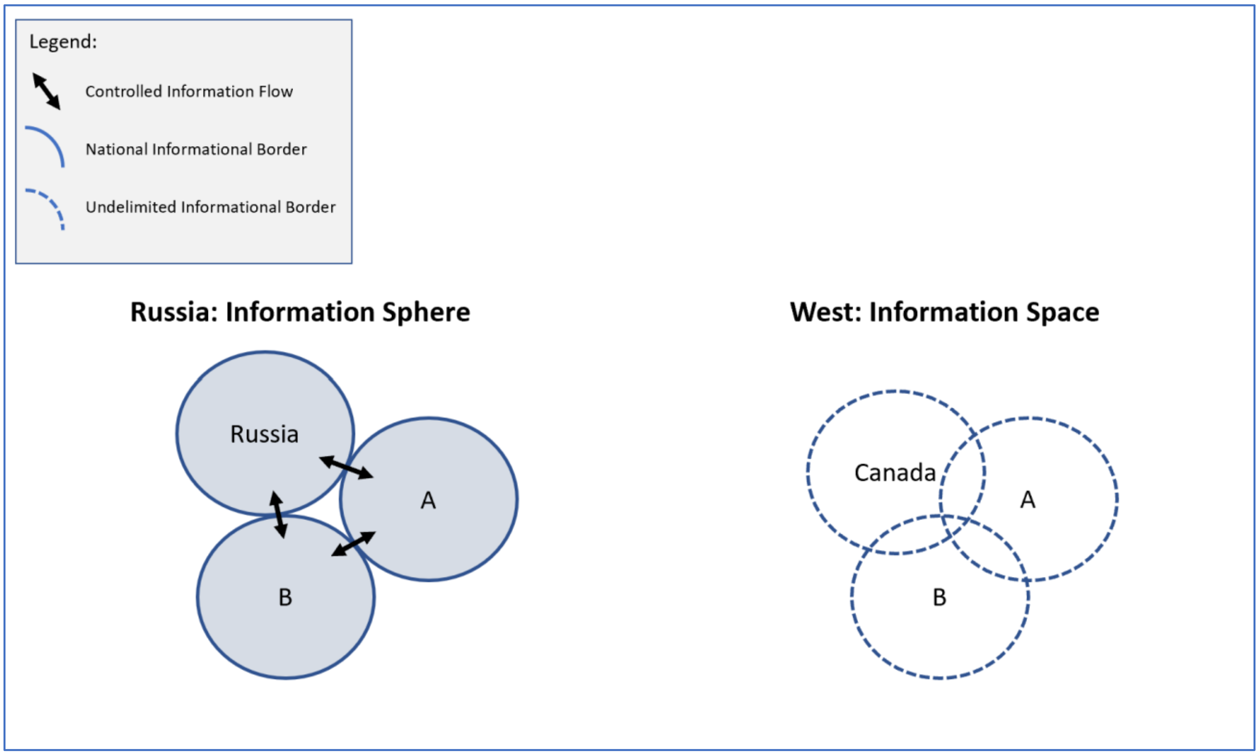
In that context, for Russia the information space is not only the aggregation of networks and platforms where information is exchanged, but it is also a system regulating social interactions. Therefore, Russian understanding of the information space aligns with the Structuralist-Constructivism perspectives about discursive structures framing and influencing social agents living in it. Indeed, the national information space allows individuals, groups, and organizations to participate in the creation and evolution of a cohesive "imagined community" advocating for certain values and understandings of past and current events that are simultaneously shaping their perceived social reality. (Carman, 2002, p. 362) While Western governments tend to adapt themselves to the ever-changing national discursive structure through their democratic institutions, which are permeable to social changes and pressures, Russia is seeking the opposite. Putin's regime understanding of the information space highlights that the Kremlin seeks to monopolize discursive mechanisms to influence the discursive structures in Russia in order to align the information space with the state national interests and projected social reality. (Herd, 2022, p. 83)

In addition, it is important to note that the Russian understanding of the information space does not differentiate between traditional platform of information such as television, radio and paper-based media and newer ones that are digital and internet-based. This all-encompassing understanding of the information domain is important as it also applies to the way Russian performed information and influence operations in the cyberspace. As discussed in the introduction, unlike Western countries, Russia does not differentiate between cyber security and information security, in the same way it does not differentiate between cyber war and information war. Information and influence operations carried out in the cyberspace are part of Russia's overall active measures and reflexive control toolbox to achieve political objectives (Marangé and Quessard, 2021, p. 130) including ensuring the survival of Putin's regime.

Underpinned by the all-encompassing understanding of information space, Russia's information warfare uses "all the means and methods of impacting information, information-psychological, and information-technological objects and information resources to achieve the objective of the attacking side." (Brangetto and Veenendaal, 2016, p. 119) This holistic understanding of information warfare is important as it encompasses the three types of operational considerations underpinning Russia's information and influence operations in the cyberspace, namely: 1) content of information; 2) technical (malicious code); and 3) cybernetic (the interface between human and digital systems). (Lilly and Cheravitch, 2020, p. 135) In addition, assessing Russia's official doctrine documents provide a good understanding of what Putin's regime wants Russian organizations and civil society to believe and the tool Russia is using to influence the Russian information space to manipulate perceived social reality in Russia. Official security and defence doctrines carry significant discursive power, as they established what the main source of threats to Russia's security and who the main adversary is. In that context, knowing whether Putin and his regime really believe what it is stated in the doctrines is of little importance for this paper as it focuses on the Russian state discursive power and capacity to push Putin's national narrative and influence Russia's information space.

This section will review three of the main doctrinal documents of the Russian Federation and highlight the doctrinal and strategic underpinnings of Russia's information warfare in the cyberspace against Western democracies. Secondly, this section will identify two main institutional cyber threat actors and two types of civilian cyber threat actors carrying out information and influence operations in the cyberspace against Western democracies.

Figure 1: Information Sphere vs. Information Space


Legend:
Controlled Information Flow
National Informational Border
Undelimited Informational Border
Russia: Information Sphere
Russia
A
B
West: Information Space
Canada
A
B

Russia's Information Warfare Doctrines

Russia's information warfare is rooted in four main doctrinal documents: The *Information Security Doctrine of the Russian Federation (2000);* The *Doctrine of Information Security of the Russian Federation (2016);* The *Military Doctrine of the Russian Federation (2010)* published along with another document entitled *Conceptual views Regarding the Activities of the Armed Forces of the Russian Federation in Information*; and the *Military Doctrine of the Russian Federation (2015).* However, only the *Information Security Doctrine of the Russian Federation (2000), Information Security Doctrine of the Russian Federation (2016)* and the *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information (2010*) have been selected for this paper. They are Russia's foundational information warfare doctrines and the current iteration of the Military Doctrine is aligned with the previous version and do not constitute a paradigmatic shift from the previous one, without providing new doctrinal underpinnings. (Lilly and Cheravitch, 2020, p. 135)

The Doctrine of Information Security of the Russian Federation (2000 and 2016)

The *Information Security Doctrine of the Russian Federation* (2000 and 2016) are focusing primarily on domestic threats and objectives as it is a national security document. Analyzing the threats identified in these two documents is of great importance as they will reveal Putin's regime perceived threats to support Putin's national narrative. As the documents are identifying a large number of threats, only the more pertinent to this paper have been retained:

> The threat to the information security of the Russian Federation is a combination of actions and factors creating a **risk of damaging the national interests in the information sphere**. [This threat underscore Putin's specific understanding of the information space as a strategic resource supporting the state's interests and objectives.] (Doctrine on Information Security of the Russian Federation, 2016)
>
> The information security of the Russian Federation is the state of protection of the individual, society and the **state against internal and external information threats**, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, **the sovereignty, the territorial integrity** and sustainable socio-economic development of the Russian Federation, **as well as defence and security of the state.** [The choice of words is important as they highlight Russia's specific understanding of the information space as being part of nation states' attributes.] (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Illegal use of special means of influence [active measures and reflexive control methods] on individual, group and public consciousness** (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Intelligence services of certain states are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation** in various regions across the world, **undermining sovereignty and violating the territorial integrity of other states.** [This threat highlights Russia's narrative about Western information operations to create rebellion and revolutions.] (Doctrine on Information Security of the Russian Federation, 2016)
>
> Information security in the sphere of **state and social security** is characterized by a continued increase in the complexity, scope, and coordination of computer attacks on objects of critical information infrastructure, enhanced intelligence activities of foreign states against the Russian Federation, **as well as growing risk that information technologies will be used to infringe on the sovereignty, territorial integrity, or political and social stability of the Russian Federation**. [Russia recognizes the threats created by the new international technological context.] (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Development by a number of states of information war concepts that provide for creating means for dangerous attack on the information spheres of other countries of the world.** [This threat supports Putin's narrative about the West waging an information war against Russia.] (Doctrine on Information Security of the Russian Federation, 2000)
>
> **The immaturity of civil society institutions, and insufficient state control** over the development of the Russian information market [e.g., media, telecommunications, internet providers, etc.]. (Doctrine on Information Security of the Russian Federation, 2000)

> Ousting of Russian news agencies and media from the national information market [e.g., telecommunication, internet and media industries], and **an increase in dependence of the spiritual, economic and political areas of public life in Russia on foreign** [mainly Western] information entities. (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Insufficient legal governance of relations in the area of the rights of different political forces to use the media for the advocacy of their ideas.** [This threat highlights the concept of Managed Democracy put in place by Putin, in which the state restricts access of Russian opposition political parties to media platforms.] (Doctrine on Information Security of the Russian Federation, 2000)
>
> **The spread of disinformation about the policy of the Russian Federation**, the activities of the Federal bodies of state authority **and events occurring in the country and abroad**. [This threat highlights that there is no limit to the scope and reach of information operation.] (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Depreciation of spiritual values**, propaganda of specimens [models] of mass culture based on the cult of violence, and on **moral value contrary to the values adopted in Russian society, [such as decadent Western values]**. (Doctrine on Information Security of the Russian Federation, 2000)
>
> **The inability of contemporary Russian civil society** to ensure the formation in the growing generation, and **maintenance in society, of socially required moral values** patriotism and civic responsibility for the destiny of the country. [This threat highlights Putin's national narrative trait of the need for a strong Russian state able to protect Russia's true values.] (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Foreign special services' use of media operating within Russian Federation [highlight the idea of fifth column[10] elements hiding in Russia]** to inflict damage to the nation's security and defence capability and to spread disinformation. (Doctrine on Information Security of the Russian Federation, 2000)
>
> Possible information and propaganda activities **undermining the prestige of the Russian Armed Forces and their combat readiness**. [This threat is linked to the idea of Russia as a great power.]" (Doctrine on Information Security of the Russian Federation, 2000)

These threats highlight Putin's awareness and worries since 2000 of the potential risks posed by Russia's uncontrolled information space, which could be leveraged by internal and external adversaries through informational operations to influence Russian "collective consciousness." It also highlights Russia's specific understanding of the information space, as it uses concepts, such as "national interests," "state security," "sovereignty," and "territorial integrity," associated with the modern understanding of nation states. Although these are not military doctrines, but rather civil doctrines of information security, they do not make a distinction between military and civil affairs. This doctrinal approach is also consistent with Russia's particular understanding of the state. As discussed in the previous chapter, the Russian state is

[10] Fifth column is a group sympathizers or supporters of an enemy, hiding within a country and engaging in activities detrimental to the state's and country stability.

primary and all other considerations and sector of activity in Russia must be subordinated to the state and support the state's interests as defined by the president. (Herd, 2022, p. 69) As all domain in Russia must support the state's interests, any perceived attack on any of them, including the information space constitutes an attack against the state. This holistic approach to information security also supports the idea that Russia is a besieged fortress in all sectors of activity, which is one of the core discursive elements of Putin's national narrative. (Herd, 2022, p. 65)

In addition, these perceived threats reveal Putin's main objective of controlling and influencing the Russian information space, based on conservative values and the idea of "managed democracy" entrenched in the national narrative described by Putin the Millennium message. These perceived threats are reinforcing Putin's national narrative, in which, only a strong state with strong institutions can protect Russian society from itself and from foreign liberal influences and values that are not Russians, and thus are potentially destructive for Russian society. (Herd, 2022, p. 141) In this narrative, which has its root in White émigré's monarchic philosophy, the Russian state is portrayed in an assumed paternalistic way, as the only moderator able to calm Russian political, social and ideological extremism, while also being the guardian of Russia's true national identity and Russian values. (Belton, 2020, pp. 348-349) In fact, Putin is protecting his regime against revolutionary ideas that would topple down his regime, while also enforcing a specific national identity narrative rejecting Western democratic and liberal values to mitigate Western soft power in Russia. (Stent, 2020, p. 46) Finally, the last perceived threat regarding Russia's Armed Forces is linked to the idea that Russia is destined to be a great power. This is important because, as discussed in the previous chapter, the nature of Putin's regime has blurred the line between the Russian state and Putin himself. Therefore, attacking Russia's military power is attacking the main indicator upon which Russia's great power status is measured against, which undermines the state's prestige and by extension, Putin's authority and his regime legitimacy to rule Russia. (Herd, 2022, p. 162)

The doctrines also establish objectives to mitigate these perceived threats, which aimed at creating the Russian state's capabilities to influence Russian information space:

> **The structure of the information security system is determined by the President of the Russian Federation**. (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Developing the theoretical and practical foundations of national information security** assurance with regard for the current geopolitical situation, Russia's political and socioeconomic development conditions and the **reality of the use of the information weapon**. (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Elaborating civilized forms and methods for public control over the formation in society of spiritual values meeting the national interests of the country and over the education of patriotism and civic responsibility for its destiny.** (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Strengthening the vertical management system and centralizing information security forces** at the federal, inter-regional, regional and municipal levels, as well as at the level of informatization objects, and operators of information systems and communication networks. (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Developing the infrastructure of Russia's unified information sphere**, countering information war threats in a comprehensive way. (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Neutralizing the information impact intended to erode Russia's traditional moral and spiritual values** (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Development of special legal and institutional mechanisms for preventing illegal informational and psychological influences on the mass consciousness of society […]** along with similar mechanisms to ensure preservation of the cultural and historical values of the peoples and nationalities of the Russian Federation and **rational utilization of the information resources amassed by society that constitute national property. [This underscore Russia's understanding of the information space as the state strategic resource.]** (Doctrine on Information Security of the Russian Federation, 2000)
>
> **Maintaining a balance between citizens' demand for the free exchange of information and restrictions related to national security, including in information sphere**. [This objective highlight Putin's lessons learned from his time in Dresden and St Petersburg on how to ensure regime longevity.] (Doctrine on Information Security of the Russian Federation, 2016)
>
> **Securing the international exchange of information, including information flows** via national telecommunication and communication channels. (Doctrine on Information Security of the Russian Federation, 2016)

These objectives are confirming Russia's broad and multifaceted understanding of information warfare, while expressing the need to give the state and the president the legal power to tighten their grip on the Russia national information space and to develop states "methods of social control" to influence Russian perceived social reality. These objectives enable the Russian state and by extension Putin to establish what the truth is, while silencing counter or alternative narratives perceived to weaken his grip onto power. (Herd, 2020, p. 83) Also, "developing the infrastructure of Russia's unified information space" and "securing the international exchange of information” seems to be referencing a “Russian internet” following other authoritarian states' path to extend their sovereignty firmly over a carved-out section of the World Wide Web. This aligns with Russia’s understanding of information space based on national state attributes, including sovereignty and borders.

> Improvement of the ways and means of **providing strategic and operational camouflage and conducting intelligence and electronic countermeasures**, along with the betterment of methods and tools for **actively countering propaganda, information and psychological operations** by a likely adversary. (Doctrine on Information Security of the Russian Federation, 2000)

Although this objective is using defensive terms, it effectively allows and commands offensive foreign operations. (Bagge, 2019, p. 94) Indeed, in line with Soviet tradition of portraying Russia as a besieged fortress, Russian elites and strategic thinkers already considered Russia to be under constant threat and even under attacks from the West in the information space (Lilly and Cheravitch, 2020, p. 134) which means that the conditions of engagement in the information space are already met. The notion that Russia is already engaged in an information war against the West seems to be well established in Russian National Security literature and amongst Russian political elites. (Connell and Vogler, 2017, p. i) Several academics working on the topic of information warfare in Russia are using the term “*informatsionnoe protivoborstvo”* meaning information counter-struggle, which highlights that Russia is effectively under attack in the information space. (Pynnöniemi, 2019, p. 216)

In addition, Igor Panarin, a Russian scholar and expert on Russian information warfare and former KGB agent and recently appointed Dean of the Diplomatic Academy of the Foreign Ministry of the Russian Federation, published two books respectively entitled *The First Global Information War: The Collapse of the USSR* (2010) and *Information War, PR, and World Politics* (2014). (Bertelsen, 2021, pp. 38-39) The first book published in 2010 affirms that the information war that ended only with the collapse of the Soviet Union was initiated by the West in 1943. (Bertelsen, 2021, p. 38) In his second book published in 2014 Panarin affirms that Russia is currently engaged in a second information war initiated by the West in the 1990s and the author described the colour revolutions in the Near Abroad and the Arab Spring as the results of Western information operations. (Marangé and Quessard, 2021, p. 123) As Russian political elites, scholars and military strategists are claiming that Russia is already engaged in an information war against the West, the defensive wording of the Doctrine may be interpreted by “information soldiers” as rules of engagement that have already been met, thus authorizing the launch of information operations against the West.

As the Information Security doctrines of the Russian Federation consider Russian information space exposure to foreign information and influence operations as a national security threat, the doctrines indicate that Russian strategists understand Russia’s information space as a strategic resource. As such, according to Putin’s national narrative, the Russian information space must be protected and leveraged to support the state’s national interests, just like any other strategic resource critical to the good functioning of the Russian state. From a defence and military perspective, as the information space is considered to be a strategic resource to be protected, information space of other countries also become high-value targets for Russian Defense and Security agencies. (Marangé and Quessard, 2021, p. 135)

The perceived threats identified in the document are institutionalizing Putin’s national narrative’s main elements, as described in the Millennium Message: 1) Russia is not like Western liberal civilizations; therefore, liberal values, such as free speech, liberal democracy, and individualism are considered non-Russian and even destructive for Russian society; 2) Let to themselves with too much political and ideological freedom, Russian civil society endangers itself and thus Russians need a strong state to moderate political and ideological extremism inherent to Russian society; and 3) Russia is a besieged fortress, as its society is constantly under threat and even assaulted by Western powers information war, trying to dismantle Russia and the state or by extension Putin’s regime. This institutionalization of Putin’s narrative generates a lot of discursive power, as it gives the Russian state the power to decide what the truth is in the Russian information space, while delegitimizing counter or alternative narratives in Russia. (Herd, 2022, p. 83) For instance, politically and legally speaking, since the publication of the first Information Security doctrine in 2000 at the beginning of Putin’s presidency, Russians expressing alternative opinions and ideas about what is and what should be Russia is potentially illegal as they can be considered as threats to Russia’s national security. Finally, it is interesting to note that there is no paradigmatic distinction made between peacetime/wartime and friend/foe in the mind of Russian strategists. (Pynnöniemi, 2019, p. 219) This reinforces the idea that Russia is in a constant state of war in the information space, and that the decision-making process of launching information operations is not influenced by the state of Russia's diplomatic relations with the West. (Gilles and Akimenko, 2020, p. 69)

The Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information (2010)

The Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information was published shortly after the publication in 2010 of the *Military Doctrine of the Russian Federation*. As the previous doctrines studied were focusing mainly on internal oriented threats and objectives, the Conceptual Views are externally oriented. The document is of great importance to understand Russian military action in the information space, as it is the first doctrinal document to specifically state that information space constitutes another operational domain, which predates by six years NATO's declaration of cyberspace as a functional domain at the Warsaw Summit. (Bagge, 2019, p. 122)

In the Conceptual Views Russia defines information warfare (*informatsionnaya vojna)* as:

> the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force. (Lilly and Cheravitch, 2020, p. 133)

Once again, this official definition highlights the broad and holistic understanding of information warfare, as it is not limited to IT infrastructure or damaging systems, but it is also about "a massive psychological manipulation of the population" and "coercion of the state to take decisions" benefiting Russia. In addition, the Military Doctrine of the Russian Federation (2010) mentioned the need for the decentralization of the command structure for carrying out information and influence operations:

> Commanders and staff at all levels are directly involved in the organization of the information space activity in peacetime, in wartime, in the preparation and execution phases of operations. Each of

> these command structures, with regard to their functions and authority, plans the subordinate troop activities linked by a single concept of action in the information space. (Bagge, 2019, p. 126)

The decentralization of the command structure regarding information and influence operations reflects Russia's particular understanding of information warfare as different from other forms of warfare. Giving the authority to launch information and influence operations at the lowest command structure levels in peacetime and war times alike indicates a normalization of these types of operations. This normalization implies that information and influence operations are not short-term and operational means exclusive to traditional military considerations. The normalized status of such operations reinforces the idea that Russia information warfare is more a governance tool serving Putin's political objectives than a military tool mapping back to the National defence and security paradigm.

In that context, Russia's military forces and assets are not only expected to defend against military attacks, but also political ones, blending military and non-military means of influence and might. (Bagge, 2019, p. 126) This doctrinal approach not only authorizes the use of military assets, including Russia's military Main Intelligence Directorate (GRU) to counter political, non-military threats in the civilian global information space, it encourages it. (Gilles and Akimenko, 2020, p. 70)

Three main paradigmatic elements informing Russia's understanding of information warfare can be extracted from these three doctrinal documents:

1) <u>New Technological Context</u>: Today governments (including Russia) decision-making processes are reliant on modern information technologies and on the undisrupted flow of information. These technologies allow governments to gather process and analyze vast amount of data crucial for their decision-making process, and to communicate efficiently with other governmental bodies and the civil society. (Bagge, 2019, p. 41) This context of digital dependency created inherent vulnerabilities that can be exploited by cyber threats actors. (CCCS, 2021, p. 2)

2) <u>Russian Perceived Social Reality can be influenced</u>: As stated, in the 2020 Russian Constitution, the president of the Russian Federation as the duty to determine, define and defend historical truth. (Herd, 2022,

p. 83) As such, combine with the 2016 Doctrine on information security, which provides the president with the responsibility to design and establish the structure of information security systems in Russia (Doctrine on Information Security of the Russian Federation, 2016) the Russian state acquired the monopoly on developing and setting the narratives around historical and social events. However, due to the modern technological context the Russian state must compete with and mitigate alternative sources of national narratives in Russia's information space to influence Russian perceived social reality. Information operations and influence operations are tools to achieve information supremacy in Russia's information space, then influence it by exploiting the technical and human designed vulnerabilities created by the new technological context, thus the manipulation of Russian society. Here, information space is being given Nation State attributes and is considered as a national strategic resource, that can be leveraged by the State and must be defended by civilian and military means alike. (Kari and Pynnöniemi, 2019, p. 18)

3) The interconnection between human and IT/Digital systems: In Russia, the interconnection between human and IT/Digital systems is called cybernetics (*Kybernetika*). In "Slavic languages *Kybernetika*, consist of technological/digital and cognitive perceptional components." (Bagge, 2019, p. 45) Contrary to cyber focused on IT/Digital infrastructure and systems, cybernetics is a discipline that explores the interface between human and IT/digital systems and how it shapes individuals, groups, and organizations decision-making process in a complex environment made of systems. (Bagge, 2019, p. 45) A somewhat equivalent Western Cyber security concept would be "social engineering," although it has a narrower meaning, as it mainly means identifying and taking advantage of human errors for specific hacking purposes. Russia's cybernetic concept goes as far as studying how people's consumption of digital content affect their decision-making process on a daily basis and how it can be leveraged to manipulate governments and entire populations.

Russia Main Cyber Threat Actors

Based on an exhaustive literature review addressing Russia's information and influence operations, four main Russian cyber threat actors have been identified for this paper. (Bertelsen, 2021; Valeriano et al., 2018; Marangé and Quessard; Rid, 2020; Polyakova and Boyer, 2018; Connell and Vogler, 2017; OTAN, 2018; Sanger and Frenkel, 2018; Satter, 2018) Two are governmental cyber threat actors – Russia's Federal Security Service (FSB) and GRU, and two are officially non-governmental cyber threat actors – Troll farms and Russian Hacktivists. These four actors form the main pillars of Russia's information warfare ecosystem and often work in symbiosis, although they are not always well coordinated. The Russia's SVR is also sometimes identified as a main actor in the literature, especially in papers studying Russia's meddling in the 2016 U.S. election. However, the SVR was not retained for this paper due to the very limited available information and details on the organization and its potential role in carrying out information and influence operations.

As the FSB and GRU are secretive intelligence organizations accurate open-source information on them and their activities are limited, which makes it hard to establish its official role and responsibility within Russia's information warfare ecosystem. However, based on the testimonies of security agency's officials that left Russia and seek protection in the West; investigative journalists' work, digital forensic report of the cyber incidents in Ukraine, the institutions' history and culture, we can brush a broad and high-level picture of these actors' role in Russia's information warfare ecosystem. As mentioned earlier the FSB and the Defense Ministry, which host the GRU, are viewed in Russia as central elements in the state apparatus, infused with a dedicated institutional identity called "power structure". For centuries, they have cultivated a distinct institutional culture characterized as being the ultimate Russian patriots and having a critical role in Russia's political affairs. (Hill and Gaddy, 2015, p. 41) Their important role in the Russian state apparatus makes them crucial lead security agencies in Russia's information warfare ecosystem.

Russia's Federal Security Service (FSB)

The FSB has been created after the newly independent Russian Federation dismantled the KGB in the early 1990s and took over most of the KGB's role and responsibilities. (Hill and Gaddy, 2015, p. 41) Even though cyber security and cyber capabilities were transferred to the Federal Agency of Government Communications and Information (FAPSI) that acted as Russia's equivalent of the National Security

Agency (NSA). (Greenberg, 2019, p. 235) Just like its predecessor the KGB, FSB's main role and responsibilities were domestic, ensuring security within the Russian Federation and was highly involved in both Chechen wars. (Gessen, 2014, p. 39 and 189.) For instance, the FSB was operating the Russian state internal cyber surveillance system and the Federal Service for Supervision in the Sphere of Telecommunications, IT and Mass Communications (*Roskomnadzor*), which is responsible for monitoring the Russian media. (Connell and Vogler, 2017, p. 7) In 2003, the FSB cannibalized the FAPSI becoming the lead security agency dominating Russia's domestic and foreign information capabilities. (Lilly and Cheravitch, 2020, p. 139) It is widely accepted in the literature that the FSB was the lead organization carrying out information and influence operations throughout the 1990s, 2000s and early 2010s. (Greenberg, 2019, p. 236) For instance, the weight and dominating position of the FSB in this domain in the early 2010s is highlighted by the FSB public dismissal and refusal to allow the GRU to develop information troops in 2011. (Lilly and Cheravitch, 2020, p. 140)

The FSB leadership in the information domain was characterized by a lack of in-house skilled operators forcing the FSB to engage external actors, including nationalist hacktivists and cyber-criminal groups. For instance, it is believed that the infamous Siberian Network Brigade that launched several DDoS attacks against Chechen websites in the early 2000s enjoyed legal cover from the FSB. (Lilly and Cheravitch, 2020, p. 140) Furthermore, anonymous sources from the FSB told Western reporters that their organization was employing illegal hackers to make up for its staffing deficiencies and that when recruiting external support, the FSB officials were creating an atmosphere depicting Russia as needing help. (Lilly and Cheravitch, 2020, p. 139) This need to employ external groups to carry out information and influence operations are aligned with the KGB/FSB institutional culture of co-opting willing and unwilling operators to carry out their mission. (Greenberg, 2019, p. 241) FSB's lead on the cyber front can be considered a specific period in Russia's information warfare capabilities, characterized by low sophistication attacks mainly using bots and slave computers to carry out DDoS attacks on government and other strategic servers to disrupt services for a short period of time. For instance, the attacks that hit Estonia in 2007 and Georgia in 2008 fall under this first period, as in both cases, FSB operators used Russian language blogs to carryout orders and provide lists of targets and defaced official public websites. (Greenberg, 2019, p. 82 and p. 93) In addition, the Advanced Persistent Threat (APT) 28 is believed to be an hacktivist group associated with the FSB or to be an FSB unit. (Beazner, 2018, p. 13) Although Russia's information warfare capabilities used in coordination with a traditional military campaign were for the first time used in Georgia in 2008, the methods used remained similar to the one employed against Estonia. This may be explained by the fact that in Georgia, the GRU was relegated to traditional military intelligence gathering in direct support of the military. (Greenberg, 2019, p. 236) Things seemed to have changed by the time of Russia's invasion of Crimea in 2014.

Russia's Main Military Intelligence Directorate (GRU)

Initially called the Registration Directorate, the GRU was created by Lenin in 1918 to serve as the eyes and ears of the Red Army. (Greenberg, 2019, p. 227) Its prime objective was to conduct foreign operations and contrary to the KGB did not participate in domestic surveillance and elimination of enemies of the state. (Greenberg, 2019, p. 227) This historical distinction may have been the reason the GRU survived the collapse of the USSR as it did not share the same terrifying reputation in Russia as the KGB did. (Greenberg, 2019, p. 227) Despite surviving the collapse of the USSR, the GRU languished under post-Soviet malaise, shortage of skilled workers and meager budgets for decades. (Lilly and Cheravitch, 2020, p. 140) Following the Georgian war of 2008, Russian Ministry of Defence announced its intention of creating a branch responsible for conducting information operations and employing specially trained and equipped troops. (Connell and Vogler, 2017, p. 8) These specially trained troops would include hackers, journalists, specialist in strategic communications and psychological operations and linguists. (Connell and Vogler, 2017, p. 8) In 2011, the FSB, probably anxious of seeing the GRU encroaching on their area of responsibility publicly disapproved and criticized this idea and the program was abandoned for now. (Connell and Vogler, 2017, p. 8) The FSB seems to have only delayed the inevitable, as two years later, the Russian government announced its intention of establishing a cyber unit in the military whose responsibilities would include offensive and defensive cyber operations and cyber research and development. (Connell and Vogler, 2017, p. 8) A year later, Ukraine's main intelligence agency the Security Service of Ukraine (SBU) believed the GRU to be behind the hacker group called CyberBerkut, which carried out multiple cyber-attacks on Ukraine's election, and Ukrainian power grids. (Greenberg, 2019, p. 225) (Connell and Vogler, 2017, p. 24) Although the attribution to Russia of cyber-attack is usually made easier by the clues Russian Cyber threat actors leave behind, the accurate attribution to any specific threat actor in Russia is a complex and difficult process. (Valeriano et al., 2018, p. 139) In addition, the following APT groups are believed to be either closely tied to the GRU or be GRU units: APT 28, Sandworm, Pawn Storm and FancyBear. (Beazner, 2018, p. 13; Jasper, 2020, p. 122) However, the Ukrainian conflict that started in 2014 certainly marked the beginning of a new period in Russia's information warfare in the cyberspace, characterized by the leadership of the GRU. (Gilles and Akimenko, 2020, p. 70) Since the Russian government announcements of the creation of a military information operation unit (*voyska Informatsionnykh*) in 2013 and later in 2017, Western governments and private sector forensic teams started identifying the GRU as the lead military and security agency behind information and influence operations targeting the West. (Lilly and Cheravitch, 2020, p. 141) This change of leadership in Russia's information and influence operations in the cyberspace from a civil to a military agency highlights the militarization process of Russia's information warfare capabilities. This structural shift may be the result of a perceived need for more structured, professionalized, sophisticated and lethal information warfare capabilities to respond to a perceived asymmetry with Western capabilities. Indeed, the U.S. created the U.S. Cyber Command in 2009 (Lilly and Cheravitch, 2020, p. 140) and Russian elites and prominent scholars, such as Panarin, have often claimed that the Arab Spring and the December movement of protestations in Russia in 2011-2012 were the results of Western information warfare campaigns. Putin might have been under the impression that the FSB approach to information warfare was falling short of emerging security threats. In addition, the rise of the GRU as the lead security agency in information warfare in the cyberspace also align with the Russian military strategists' understanding of modern warfare as expressed by Gerasimov and Russia's Military Doctrine since 2010. (Valeriano et al., 2018, p. 114)

Compared with the previous period when the FSB was the lead security agency for information warfare in the cyberspace, the GRU appears to have developed in-house capabilities and showed more appetite for higher risk and complex operations targeting critical infrastructure of adversaries (Greenberg, 2019, p. 241) and targeting great powers, such as the U.S. Indeed, the FSB as the main heir of the KGB might have preferred discretion and covert operations, which would be better suited to the secretive nature of civilian intelligence agency. The GRU seems to have a warrior like culture akin to the special forces *spetsnaz* it is hosting. (Greenberg, 2019, p. 242) This warrior-like culture can be observed in the GRU recruiting advertisements, which feature a Kalashnikov assault rifle propped next to a computer, symbolizing the action-oriented nature of the organization. (Lilly and Cheravitch, 2020, p. 142) For instance, a former FSB cyber officer arrested in 2016 for trying to expose the GRU and seemingly annoyed with the GRU approach to information warfare claimed that the GRU "impertinently, roughly, and brutishly breaks into servers always led to their attribution. (Lilly and Cheravitch, 2020, p. 141)

The Internet Research Agency (The Troll Farm)

The Internet Research Agency (The Troll Farm) is only one of the Russian troll farms, but certainly the most well-known and documented. The Troll Farm is believed to have been created in 2013 and funded by Evgueni Prigojine a Russian businessman in St-Petersburg. (Marangé and Quessard, 2021, p. 130) It has become known in the West due to its participation in the Russian influence operation against the U.S. in 2016 during the presidential campaign. (OTAN, 2018, p. 8) However, The Troll Farm started its operation back in 2011 amid the popular unrest in Russia, following the announcement of Putin coming back to the Russian presidency. (Connell and Vogler, 2017, p. 25) The trolls were paid to comment negatively on anti-Putin news articles and anti-regime videos on YouTube and maintain pro-Putin blogs. (Connell and Vogler, 2017, p. 25) They were used to compete against the opposition's messages and sentiment in the Russian information space, not only to increase pro-Putin sentiment, but mainly to crowd-out messages of opposition members in Russia's information space. (Connell and Vogler, 2017, p. 25) More recently, as observed in the 2016 U.S. election campaign, Russian trolls are used to influence the international information space and destabilize the adversary's society by encouraging existing inflammatory topics and social views. The idea is not so much about convincing people in the West that Russia is right, but rather "to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the internet as a democratic space." (Connell and Vogler, 2017, p. 25)

Russian Hacktivists

Hacktivists are a non-state cyber threat actors that are motivated by political or ideological drivers and their attacks are usually considered unsophisticated due to the lack of resources and time. (CCCS, 2021, p. 2) Although, hacktivists are non-state cyber threat actors, they can be state-sponsored, either by paying for their services, or by offering them tacit legal protections. Russian Hacktivist groups were often used in the period prior and in the early period of the Ukrainian conflict in 2014, when the FSB was the lead security agency on information warfare. For instance, cybercriminals helped spread pro-Russia messaging during the Euromaiden protest and Russia annexation of Crimea by taking control of computer and video game consoles and forcing them to visit specific sites to generate ads revenue and to watch pro-Russian videos. (Jensen et al., 2019, p. 17) In addition, experts on Russia's cyber capabilities described, "a symbiotic relationship between the cyber-criminal underworld and the Russian intelligence services." (Valeriano et al., 2018, p. 115) Russian hackers, if arrested, are often released on technical grounds, and based on connections to governmental officials. (Valeriano et al., 2018, p. 115) The use of Russian Hacktivists was clear in Chechnya in the early 2000s, Estonia in 2007, and Georgia in 2008 and served mainly to avoid attribution by obfuscating the ties between nationalist hackers and the Russian state. Today, it seems that Russia's main information warfare capabilities are professionalized and militarized under the leadership of the GRU.

Russian Cyber Threat Actors *Modus Operandi*

Based on the assessment of Russia's doctrinal documents and Russia's main actors involved in information warfare, we can conclude that Russia's information warfare is based on three main operational underpinnings:

1) **The realm of cyber is embedded into a holistic understanding of information security** as a theatre of conflict enabled by the new international technological context and formed with countries' information space. The concept of national information space understood as part of nation states' attributes led Russia to consider the Russian information space as a strategic resource. As any other national strategic resources, the Russian information space must serve the interest of the state, while also constituting a target of value that must be protected by Russia's national security and defence apparatus. This means that any information advocating for an alternative narrative, or a counter-narrative criticizing Putin's regime is perceived by Russian authorities as a threat to Russia's national interest and even an attack on Russia itself. Finally, this doctrinal approach based on national information space erases the distinction between war and peace as a strategic analytical frame. The information space is not clearly delimited like territories are, meaning there will always be a certain level of perceived encroachment and infringement between countries' national information space. Therefore, in considering the Russian information space as a strategic resource that must be defended by the state, Russian strategists have created an analytical frame through which Russia is perceived as in an ongoing and never-ending state of information war against Western information space. This creates a discursive context favourable to support Putin's discourse portraying Russia as a besieged fortress. (Herd, 2022, p. 155) This particular understanding of information space is not new, as it was present in Russian information security doctrines since 2000. (Carman, 2002, p. 359) However, the creation of internet-based media and social media in the second half of the 2000s increased the perceived Western pressure or informational encroachment on Russian information space. (Doctrine on Information Security of the Russian Federation, 2016) In that context, controlling traditional Russian media was not enough

anymore, Putin's regime perceived that it needed to move over to the offensive and actively counter alternative or critical narratives about Russia and the Russian state. (Giles and Akimenko, 2020, p. 71)

2) **Information and influence operations are state governance tools** to achieve information supremacy in the information space. Based on the doctrines of active measures and reflexive control developed decades earlier during the Soviet era, Russian strategists have a very good understanding of the social and informational mechanism and interactions underpinning social reality. (Rid, 2020, p. 429) The Russian state is using information and influence operations as a governance tool to achieve information supremacy within the Russian information space to establish a specific social reality in Russia anchored in the Russian information space advocating, reinforcing and giving legitimacy to Putin's regime. Russia's doctrine on information warfare in the cyberspace is considering the three following operation levels (see figure 2):

- First, the **information space**, is where the overarching discursive objectives are set underpinning national identity**.** The information space can roughly translate to the Strategic level of operation and is therefore the long-term level of consideration. The information space is where the aggregation of societies' discursive actions and messages forming national identities based on foundational narratives, which are often historically and collectively rooted, happens. For instance, at the national identity level, Canada is seen and understood by many in Canada and around the world as a peaceful internationalist power as it is recognized as being the creator of the United Nations (U.N.) Peacekeeper programs (Blue Helmets). (Massie, 2013, p. 39) This national identity trait persists throughout time in Canada's information space, even though Canada's contributions to U.N. Peacekeeping missions declined dramatically since the second half of the 1990s. (Young, 2020, p. 153) Structurally, the domestic information space is where the information created in and received from other information space is located; hence it is where individual, group and organizations navigate to gather information and interact with other individuals or entities. (Bagge, 2019, p. 46) According to Russia's definition of information space, it includes traditional media (paper-based, radio or television-based, and online), untraditional media (Brangetto and

Veenendaal, 2016, p. 119) such as social media and streaming platforms (Reddit, Facebook, Twitter, Instagram, Vkontakt, YouTube, TikTok, etc.) and instant messaging applications (Telegram, WhatsApp, etc.).

- Second, the **information and messages**, which can translate to the operational level, include short to mid-term considerations tied to specific operations' objectives. The aim is to influence people and organizations' understanding of specific events and support specific discursive elements of the national identity. (Brangetto and Veenendaal, 2016, p. 116) The information is the content carried by messages and both together are shaping the perception individuals, groups and organizations have about their immediate environment, situation, and circumstances. (Bagge, 2019, p. 47) The information can be understood as raw informational data forming a message. In itself, information does not necessarily have meaning other than the facts it claims to present. However, once the information is packaged in a message the information acquires discursive powers, providing meaning and context to the informational data carried in the message. (Bagge, 2029, p. 47) As such, information and message considerations are not only about actual message embedded in the attack, such as the defacement of a website with pro-Russian content. It is also about considering the overall discursive impacts of the cyber-attack. How it will be perceived by the targeted organization, government, and the country's information space, including Russian information space. In that context, from Russia's perspective, information and message are the basis of perceived social reality, which takes form in the information space, and it can be influenced using information and influence operations. (Marangé and Quessard, 2021, p. 324) Perceived social reality is constructed, maintained, and changed by discursive actions structuring collective understanding of social reality reflected in the information space via messages. (Rid, 2020, p. 430) For example, leaking sensitive information that has been tempered, using Wikileaks platform. As Wikileaks's reputation is well known to be an anti-establishment group, the leak is messaged as a social justice operation with an undertone of populism with not only a higher potential to be retaken by traditional news media, but also has a polarization effect, because it plays on the well-established "elites vs. common folks" narrative. (Valeriano et al., 2018, p. 139) Another example of influence operation is Russia's use of internet trolls to create fake blogs and online profiles generating pro-Kremlin content to increase Russia's narratives and visibility in the information space, while also crowding out alternative narratives online. (Connell and Vogler, 2017, p. 23) Therefore, leveraging information by distorting, disrupting, and altering the information present in mainstream messages have the potential to overtime influencing the information space of targeted countries (e.g., Ukraine, Russia, the U.S., etc.) and then influencing individuals, groups and organizations understanding of certain historical and current events.

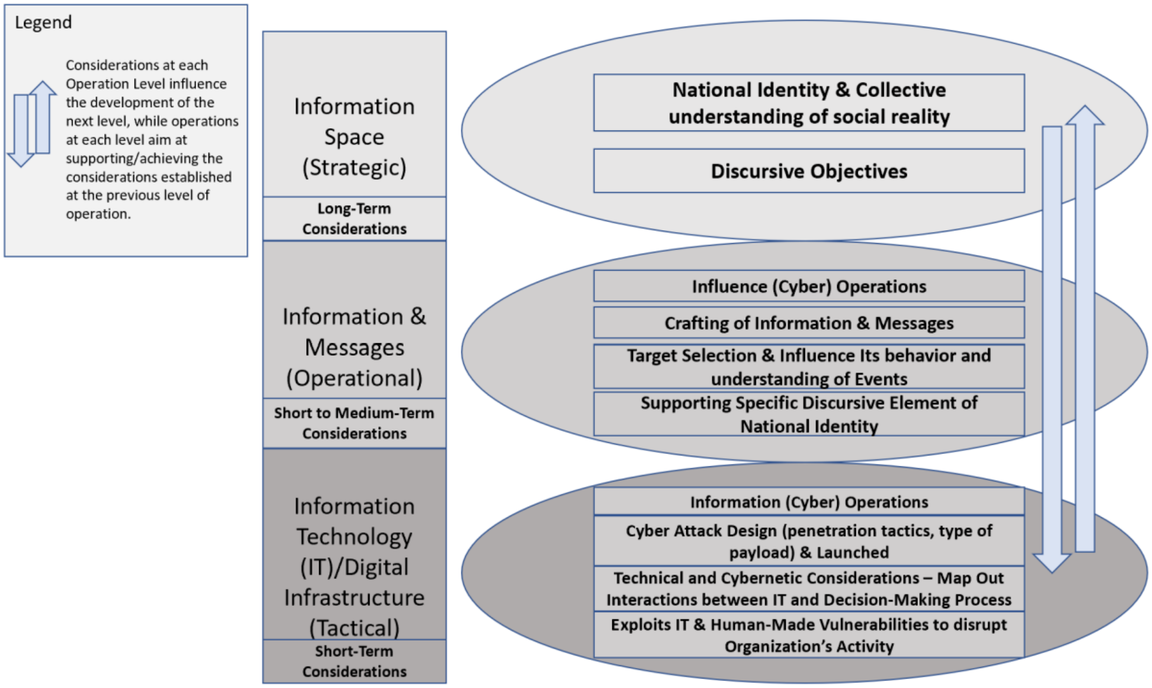
- Third the **IT infrastructure**, which can be translated as the tactical level of operation, includes short-term technical considerations. The IT infrastructure is the technical component of the information space, providing digital manifestations to the first two levels. (Bagge, 2019, p. 47) However, this level of operation is more than solely hacking their way into systems to damage or steal data. It is also designed to understand the interaction between systems and the individual, group, or organization operating them. Tied to the Russian concept of "cybernetic"[11] the intent is to understand and map the way digital and IT infrastructure are designed, used, and maintain by an entity, and how it affects its decision-making process. Indeed, IT infrastructure is not ideologically agnostic, as architecture designs are often influenced by legacy digital infrastructure patterns and policies based on an older technological context and considerations. In addition, architecture patterns or habits are influenced by specific organizational culture, policies, and other considerations than cyber security (e.g., administrative simplicity and economic efficiency) which

[11] In "Slavic languages *Kybernetika* (cybernetic), consist of technological/digital and cognitive perceptional components." (Bagge, 2019, p. 45) Contrary to "cyber" focusing on IT/Digital infrastructure and systems, cybernetics is a discipline that explores the interface between human and IT/digital systems and how it shapes individuals, groups, and organizations decision-making process in a complex environment made of systems-of-systems. (Bagge, 2019, p. 45) A somewhat equivalent Western Cybersecurity concept would be "social engineering," although it has a narrower meaning, as it mainly means identifying and taking advantage of human errors for specific hacking purposes. Russia's cybernetic concept goes as far as studying how people's consumption of digital content affect their decision-making process and how it can be leveraged to manipulate governments and entire populations.

could create vulnerabilities that can be exploited by Russia. Russia’s “information warriors” are conducting a wide range of information operations, from DDoS attacks and cyber espionage to data infiltration/exfiltration and digital sabotage. (Connell and Vogler, 2017, p. 23) As it will be demonstrated in the next section, Russian cyber threat actors are often exploiting human made vulnerabilities, such as phishing methods and un-patched legacy systems, then move laterally across the targeted network undetected, due to lack of active network monitoring and compromise unsecured and unnecessary privileged user accounts. In addition, Russian information operations are designed to be partially deniable, using front organization and false flag operations, including disguising an attack as a ransomware and co-opting well-known hacktivist groups and platforms (Anonymous, Wikileaks, etc.). (Connell and Vogler, 2017, p. 23) Russia’s operations are partially deniable, as they do not really seek to conceal their origin or the nationalities of the cyber threat actors, but rather seek to obfuscate who specifically carried the attack to manage the conflict escalation. For instance, Russia’s cyber threat actors are renowned to leave clues that they are Russian behind, however, pinpointing whether the attack was carried out by any specific hacktivist group or state organization is much harder. (Valeriano et al., 2018, p. 139) Russian cyber threat actors are also often using false flag operations, by mimicking the behaviour of known cyber threat actors, including cybercriminal groups. For instance, Russia’s cyber threat actors have used certain types of malware that are usually associated with cybercriminal activities, such as ransomware to make it seems like the attack was carried out by cybercriminals. Using Ransomware types of malware allows Russia to add another layer of anonymity to avoid formal attribution, to conceal the real motivations behind an attack, delay the investigation, and deceive the targeted organization or government into launching a criminal investigation instead of triggering national security or national defence responses. Using either wittingly or unwittingly actors also provide an additional layer of anonymity and concealment (Connell and Vogler, 2017, p. 23), as the leaks appear to be from groups well known for their hacktivism, such as Wikileaks or Anonymous. Internet trolls are

> used to create fake blogs and online profiles to create pro-Kremlin content, increasing their visibility and crowd out opposing material and comments online. (Connell and Vogler, 2017, p. 23)

Figure 2: Russia's Information Warfare Levels of Operation


Legend
Considerations at each Operation Level influence the development of the next level, while operations at each level aim at supporting/achieving the considerations established at the previous level of operation.
Information Space (Strategic)
Long-Term Considerations
Information & Messages (Operational)
Short to Medium-Term Considerations
Information Technology (IT)/Digital Infrastructure (Tactical)
Short-Term Considerations
National Identity & Collective understanding of social reality
Discursive Objectives
Influence (Cyber) Operations
Crafting of Information & Messages
Target Selection & Influence Its behavior and understanding of Events
Supporting Specific Discursive Element of National Identity
Information (Cyber) Operations
Cyber Attack Design (penetration tactics, type of payload) & Launched
Technical and Cybernetic Considerations – Map Out Interactions between IT and Decision-Making Process
Exploits IT & Human-Made Vulnerabilities to disrupt Organization's Activity

3) Contrary to traditional warfare, **information warfare is not affected by peacetime/war time strategic framing**, nor the state of diplomatic relations between Russia and the West. (Jasper, 2020, p. 83) Due to the complexity and changing nature of the information space, sporadic and context-dependent operations are not sufficient to influence it. The information space is a highly dynamic discursive structure formed by an almost infinite number of informational inputs and entry points aggregating societies' discursive actions. As a result, to have a chance to produce an informational impact and influence a targeted information space in the long-term, the Russian government must carry out a high amount of information operations of all scale and size notwithstanding the state of the relationship between Russia and its targeted adversaries. (Jasper, 2020, p. 83) To sustain this high rate of operation, Russia has established a highly decentralized command and control structure, allowing Russia to carry out a significant amount of information and

influence operations on short notice, while also allowing for constant innovation and testing of new cyber methods, including the development of more effective and sophisticated malware and network penetration tools, which is contributing to Russia's ongoing information warfare against the West. It is important to note that this high amount and high-rate level of Russian information operations means that not all of them are large-scale operations nor successful operations. It is almost impossible to track every Russian information operations, but it is reasonable to assume that only the most ambitious and impactful ones are being detected and observed by Western agencies.

4 - CASE STUDY OF UKRAINE: 2014-2018

Ukraine represents a key symbol in Putin's national narrative about Russia, due to its close historical and cultural proximity. Ukraine, in Putin's narrative, is the historic heart of the Russian civilization as expressed in the Medieval *Kievan Rus* Kingdom that existed between the IX to the XIII century, in which the territory covered a large part of modern Ukraine, stretching out to Novgorod close to modern St. Petersburg. Ukraine is considered to be the birthplace of the Russia civilization and the Orthodox Christianity in Eastern Europe. (Putin, 2021) This simplistic interpretation of history is crucial for Putin's information strategy, as it gives the situation in Ukraine a great discursive power that is being leveraged in Russia's information warfare against Western democracies. Ukraine as the symbol of the Russian civilization (*Ruskii Mir*) myth of origin establishes Russia as a millennium civilization rooted in Orthodox traditions, giving it historical legitimacy as a predestined great power. (Herd, 2022, p. 32) To the contrary, in this narrative, Ukraine is stripped of its state agency and legitimacy as an independent and sovereign state, and any attempt to showcase Ukraine's independence is understood as being similar to an act of secession. (Herd, 2022, p. 32) Indeed, as Ukraine is the heart of Russian civilization, any sign of Western influence in Ukraine is represented in Russia's information space as Western imperialistic encroachment and attempt to carve out Ukraine from its historically and rightful place as a territory belonging to the Russian civilization. (Putin, 2021) In Putin's national narrative, a Westernized Ukraine would be equal to losing Ukraine by military conquest, impacting both the myth of origin of Russian civilization as distinct from Western societies and weakening Russia's status as a great civilizational power in the world. (Putin, 2021) In the fight for informational supremacy in Russia's informational sphere, losing Ukraine would be a major blow to Putin's national narrative and may encourage alternative narratives suggesting that Russia, like Ukraine is a Western or at least a European society, which should emulate Western values and liberal democratic political systems. Ukraine's close cultural and historical ties to Russia facilitate the ideological juxtaposition in Russian's collective imaginary, comparing the potential success story of a democratic

Ukraine integrated in the European Union and Russia's situation. Russians may think - if Ukraine did it, why not us!

Coherent with Putin's narrative, the 2014 Euromaidan and the resignation of the Ukrainian president Viktor Yanukovych is considered to be a Western-supported military coup disguised in pro-democratic movements overthrowing Ukraine's legitimate government. (Marangé and Quessard, 2021, p. 129) In that context, the Euromaidan is not a real pro-democratic revolution, but only the latest of staged revolutions orchestrated by the West. (Bertelsen, 2021, p. 363) In multiple instances, Russian's state TV channels and even Russian officials have stated that the current pro-western government in Kyiv is in fact a puppet government control by a Nazi military junta, supported by the U.S. (Bertelsen, 2021, p. 363) Paradoxically, Russia is also benefiting from instability and chaos in Ukraine, as a chaotic situation in Ukraine supports another core element of Putin's national narrative, which is Russia being surrounded by aggressive Western/NATO forces. This discourse refers to Russia as a historically besieged fortress, as a result of its great power and civilizational status. Putin had mentioned multiple times in public speeches that "historical Russia"[12] has always been surrounded and under attack from other empires and civilization wanting to grab Russian lands. (Herd, 2022, p. 33) Therefore, instability and conflicts in Russia's zone of privileged interest, such as in Ukraine is providing a geopolitical context that facilitates and supports Putin's discourse about Russia as a besieged fortress which is portraying him as a president on the frontline fighting tirelessly for Russia and its survival. (Herd, 2022, p. 88)

Context in Ukraine since its independence

Since its independence in 1991, Ukraine has always been somewhat divided following ethnic and linguistic lines, between a Western mainly Ukrainophone and an Eastern Ukraine mainly Russophone. (Loshkariov and Sushentsov, 2016, p. 3) However these divisions reached their breaking points level in 2014, amid the

[12] The term "historical Russia," refers to an historical construction of the Russian state as a continuity of all other forms it took throughout history (e.g., Feudal Russia – Kievan Russ; Imperial Russia – Tsarist Russia; Soviet Russia – Soviet Union; and modern Russia – Post-Soviet Russia under Putin). (Herd, 2022, p. 30)

Euromaidan protests, the resignation of the Ukrainian President Viktor Yanukovych and the start of the civil war in Eastern Ukraine. It is important to note that, like Russia's information warfare in the U.S., they leveraged existent grievances and societal divisions. Societal division between a Western European Ukraine and a Russian Eastern Ukraine has been fuelled by the Ukrainian state's bold national-building efforts, leveraging a nationalist discourse and sentiments rooted mainly in Western Ukraine. (Loshkariov and Sushentsov, 2016, p. 4) The Ukrainian state launched a program to change the nation historiography in an attempt to consolidate an interpretation of Ukraine's history, supporting the idea of an independent Ukraine being part of Western historiography instead of Russians. (Gobert, 2018, p. 22) These efforts highlighted a nationalist interpretation of crucial historical events, including the Ukrainian independence declaration of 1917, the Holodomor famine of 1932-1933, the Ukrainian nationalist resistance against the USSR and Nazi Germany during the Second World War, etc. (Gobert, 2018, pp. 24-25) The aim was to reinforce the idea of an independent Ukraine apart from the historic Russia construct, which was crucial to build a strong national identity in Ukraine. However, the lack of nuances in the Ukrainian historiography also fuelled ultranationalist and far-right groups, including the Azov battalion, which are trying to legitimize their role throughout Ukraine's history to claim a seat at the political table of modern Ukraine. (Gobert, 2018, p. 28) For instance, many Western Ukrainians believe that the Russophones living in the Donbass are not "Ukrainians, but Russians who replaced real residents of the region after the massive starvation deaths in the 1930." (Loshkariov and Sushentsov, 2016, p. 4) Meanwhile, since 2014, Russia's information war in Ukraine has leveraged and exploited Ukrainian nationalistic discourse and Russophones grievances in the East to discredit the Ukrainian government and contest the existence of a Ukraine outside of historic Russia. (Blank, 2017, p. 91) The compounded effect of the Ukrainian state efforts to rewrite Ukraine's historiography and Russia's information warfare in Ukraine has overtime rendered the term Russian and by extension Russophones similar to foreign oppressors in Ukraine. (Gobert, 2018, p. 30)

As a result, Ukraine is mainly divided in two distinct informational spheres. Ukrainophones population outside of the separatist region of the Donbass – the provinces of Luhansk and Donetsk – are part of the

European/Western information space, where exposure to Russian state media is very limited. For instance, following the start of the war against pro-Russian separatists in the East and the annexing of Crimea by Russia, Russophones news agencies, including *RT* and *Sputnik* have been banned from Ukrainian soil. (Peisakhin and Rozenas, 2018, p. 537) In the separatist regions, the opposite applies. Ukrainian leaving in pro-separatist regions in the East and in Crimea is part of Russia's information space and thus mostly cut-off from Western information feeds. (Marangé and Quessard, 2021, p. 129) Maintaining this clean-cut division between Eastern Ukraine, Crimea and the West is important for Putin, as it enables the Kremlin to achieve information supremacy in these regions. (Beazner, 2018, p. 14) Achieving information supremacy in Russia's information space on the topic of Ukraine is definitely a priority for Putin, as of 2019 almost half of Russia's state media disinformation narratives were about the situation in Ukraine or related to Ukraine as a general topic. (EUvsDisInfo, 2019) Although it is hard to evaluate the overall effectiveness of Russia's information warfare in Ukraine, several surveys conducted in Russia since 2014, consistently shows that most Russians believe the Kremlin official narratives about the situation in Ukraine and the threats emanating from Western powers. (Blank, 2017, p. 91)

Russia's Information Warfare in Ukraine: A Cyber Perspective

In 2004, during the Ukrainian Presidential election pinning pro-Western candidate Viktor Yushchenko against Russian-backed candidate Viktor Yanukovych, Yushchenko was poisoned and left permanently disfigured; districts known to be for the pro-Russian candidate suddenly acquired millions of new voters; and masked men harassed pro-western voters at polling stations. (Polyakova and Boyer, 2018, p. 2) Ten years later, during the 2014 presidential election, Russia would launch an information war against Ukraine, carrying out information and influence operations in the cyberspace to destabilize and influence the situation in Ukraine. During this period of ten years, Russia's active measures and reflexive control strategy extended from physical to the digital realm. (Polyakova and Boyer, 2018, p. 2) In that context, information and influence operations in the cyberspace is a sub-component of Russia's approach to information warfare. (Marangé and Quessard, 2021, p. 49)

Just like conventional warfare, information warfare's strategy is an "act of creating power" characterized by a "dialectic of opposing wills that revolves around a set of ideas about how to employ instruments of power to advance a defined objective." (Jensen et al., 2019, p. 2) Russia's information warfare in the cyberspace against Ukraine since 2014 supports Putin's main political objective, which is regime survival. At the strategic level, Russia's information warfare in the cyberspace aims at achieving the three discursive pillars of Putin's national narrative: 1) Portraying Russia as a besieged fortress, by creating a narrative bubble claiming that Russians and Russian society are constantly under threat from Western militaries and its malicious influence; (Herd, 2022, p. 155) 2) Amplifying positive narratives on Russia and his regime, while at the same time suppressing and delegitimizing negative ones; and (Marangé and Quessard, 2021, pp.121-122) 3) Weakening Western soft power by exposing, distorting and amplifying Western societal tensions and issues. (Marangé and Quessard, 2021, p. 135) To achieve that, Russia's information and influence operations in the cyberspace against Ukraine aim at achieving the three following discursive objectives: a) Undermining the Ukrainian democratic government's legitimacy to rule and demonstrating the danger of democratic revolutions; b) Portraying pro-western Ukrainians and the government as a direct threat to Russia, reinforcing the notion of Russia being besieged by Western powers, thus legitimating Putin's authoritarian governance model; and c) Demonstrating Western states' perceived hypocrisy and double standard in international affairs, including Western support to illegitimate, totalitarian and oppressive governments, military interventions (e.g., Kosovo in 1999 and Irak in 2003), hence diminishing Western influence worldwide and alleviating Western Soft power pressure on Russia.

Russia's information and influence operations in the cyberspace targeting Ukraine since 2014 have consistently used a false flag approach impersonating Ukrainian hacktivist groups, such as Anonymous Ukraine, and CyberBerkut. CyberBerkut is also known as APT 28, Sandworm, Pawn Storm or FancyBear and it is believed to be either closely linked to the GRU or to be GRU units. (Beazner, 2018, p. 13; Jasper, 2020, p. 122) Russia's information operations fall into three main categories of attack, such as DDoS, website defacement and malware infection. (Beazner, 2018, p. 10)

DDoS

DDoS are considered to be technically unsophisticated cyber-attacks, which require taking control of a large number of computers infected by botnets (also called zombies) and sending requests to the targeted network. (Brangetto and Veenendaal, 2016, p. 123) The large influx of traffic trying to connect at the same time to the targeted network causes the server to shut down, preventing individuals to access the website temporally. (Peterson, 2021, p. 18) Although, DDoS attacks can undermine the targets' credibility they do not cause material damages to the digital infrastructure nor infringed on the confidentiality or integrity of networks and data and are pretty simple to mitigate. (Brangetto and Veenendaal, 2016, p. 123) Therefore, state-backed DDoS attacks are rarely conducted in isolation. They often "serve as distraction to monopolize the attention of the Computer Emergency Response Team (CERT) of the targeted institution." (Beazner, 2018, p. 10) Indeed, while the emergency response team is busy fighting off DDoS attacks, cyber threat actors are often carrying out other more sophisticated attacks on the network, including setting backdoors to ensure persistent access to the network and installing more lethal malware. (Beazner, 2018, p. 10) For instance in early 2014, during the Euromaidan protests Ukrainian civilian and pro-democratic organization servers were often taken offline as a result of an intense barrage of DDoS attacks. (Valeriano et al., 2018, p. 138)

Website Defacement

Website defacement is considered to be a type of cyber vandalism (Brangetto and Veenendaal, 2016, p. 123) as it consists in breaching a web server either by using stolen credentials or by elevating the account privilege to system administrators and edit the content displayed on the targeted website. Once the website server has been breached, the attacker "changes the visual appearance of the website or replaces pages with their own materials." (Beazner, 2018, p. 10) The aim of such attack is to sow confusion and undermine trust in institutions, while supporting disinformation and specific narrative elements about the targeted organization. (Brangetto and Veenendaal, 2016, p. 123) For instance, since the Euromaidan revolution, several Ukrainian government websites were defaced by replacing their original content with pictures, symbols, and messages reinforcing Russia's narrative that the Ukrainian government is a fascist military junta, backed by the U.S. (Valeriano et al., 2018, p. 138) Another example is the hacking of Kyiv's publicity billboards across the city, in 2014, replacing the original advertisement content with pictures and videos of war casualties in Eastern Ukraine, while also portraying Ukrainian officials as war criminals. (Valeriano et al., 2018, p. 139)

Malware Infection

Malware infection is usually considered to be a more sophisticated form of cyber-attack and often requires higher skills and more sophisticated tactics. Malware is a malicious code that is being secretly installed on the targeted machine to perform unauthorized tasks and compromise the data, applications and/or the operating system of the victim. (Jasper, 2020, p. 14) Malwares fall into two main categories – virus and worm. A virus is a malware that is knowingly or unknowingly installed on the victim's computer and is designed to copy or replicate itself in documents or programs in a computer, altering the computer's operations or damaging it. (Peterson, 2021, p. 22) A worm operates in a similar fashion; however, it replicates and infects computers by itself, spreading through networks autonomously. (Peterson, 2021, p. 22) In Ukraine, malware infections were mainly carried out using "spear-phishing"[13] campaigns. Some of the most famous malware used by Russia are BlackEnergy3 and CrashOverride. (Beazner, 2018, p. 10)

BlackEnergy3 is the latest iteration of the original BlackEnergy malware developed in 2007 by a Russian hacker name Dmytro Oleksiuk, which sold it on a Russian-language hacker forum in 2007. (Greenberg, 2019, p. 10) Originally designed to take over machines and use them as bots in DDoS attacks (Greenberg, 2019, p. 10), it was updated to now include tools to target "Supervisory Control and Data Acquisition (SCADA)"[14] systems and added new features, including, establishing backdoors, KillDisk, which rendered

[13] Contrary to phishing, which involves less sophisticated and indiscriminate phishing attempts targeting large number of people, Spear phishing is a tactic that uses social engineering to tailor e-mails to individuals or groups based on their line of work, interest, or personal characteristics. (CCCS, Cyber Hygiene)

[14] SCADA is a system managing the communication between industrial machines and equipment and user-friendly software and devices through a human-machine interface (HMI), allowing operators to send commands to the equipment. (Brook and Lucchesi, 2017, p. 2)

the infected computers unusable. (Beazner, 2018, p. 10) BlackEnergy3 was used in both the December 2015 and December 2016 attacks against Ukrainian power grid systems. (Jasper, 2020, p. 17) CrashOverride, was discovered in 2017 by forensic analysts studying the second attack on Ukrainian power grid in 2016. (Slowik, 2019, p. 1) CrashOverride is a malware specifically design to attack SCADA industrial systems autonomously. Once installed on a compromised computer, the malware will search through the network to find the SCADA system, scan it to identify what type of industrial control system protocol it is using, then use one of the four payloads it carries to disrupt the system. (Slowik, 2019, p. 3) CrashOverride is also equipped with KillDisk and Denial-of-Service (DoS)[15] capabilities. (Slowik, 2019, p. 3) These two malware will be discussed in more details, while examining the attacks on Ukrainian power grid.

As Ukraine is an active target of Russia's information warfare, since 2014, this chapter will examine only three major cyber events that hit Ukraine in 2014, 2016 and 2017, and demonstrate how their purpose was mainly discursive and embedded within Russia's information war against Western democracies.

Ukraine Presidential election of 2014

Following the departure of the former Ukrainian President Yanukovych and the public referendum in Crimea in favour of secession on March 16, the pro-Russian hacker group CyberBerkut compromised the Ukrainian Central Election Commission (CEC) on May 21, during the presidential election. (Jasper, 2020, p. 57) The attackers breached CEC's networks and disabled core network nodes and components of the Ukrainian election system, including the real-time display of the election result on the official CEC's website. (Brangetto and Veenendaal, 2016, p. 121) While CEC's CERT was trying to put the system back online, CyberBerkut published photos of the Election Commissioner's and his wife's passports and leaked emails from Western officials to the Ukrainian election commission to demonstrate Western's control over

[15] DoS attack is similar to a DDoS attack as both aim at flooding a server, or system with high volume of traffic to disable it temporarily. The main difference, is that DoS attack comes from one system, which is carrying out the attack, as opposed to DDoS, which leveraged a multitude of machines to carry out the attack.

Ukrainian election process. (Rid, 2020, p. 360) On May 25, an hour after the polls closure, Russian Channel One declared Dmitry Yarosh, a far-right political leader, victorious with 37 percent of the vote, which was fabricated information from the CyberBerkut group. (Jasper, 2020, p. 58) Channel One presenter's Irada Zeynalova claimed the results had been just published on the CEC's official website, officializing Yarosh victory. (Rid, 2020, p. 361) However, the chart broadcast on Channel One was never broadcast on CEC's official website. (Rid, 2020, p. 362) The next day, in an attempt to humiliate CEC's further, CyberBerkut falsely declared online that they had permanently damaged their computer network and systems and published stolen internal emails from employees as proof. (Valeriano et al., 2019, p. 139) Later forensic analysis revealed two attacks on the CEC's network and system, one targeting the live display of the election results, and another one using sophisticated obfuscation methods aimed at placing fake election results on the CEC's official website set to be broadcast not long after the polls closure. (Rid, 2020, p. 362)

In addition, forensic evidence revealed that CyberBerkut launched the reconnaissance phase for this second attack more than two months earlier in March, and CERT assessment discovered signs of a breach in late April. (Koval, 2015, p. 57) Without being detected, CyberBerkut successfully uploaded the fake chart into CEC's system eight minutes before the closure of the polls, but they made a mistake. (Koval, 2015, p. 56) It seems that CyberBerkut had not fully understood CEC's network architecture and design, and uploaded the fake chart to the wrong server, which prevented it from being broadcast on the CEC's official website after the closure of the polls. Indeed, in preparation to the expected high volume of traffic on CEC's website and to mitigate the risk of DDoS attack on the night of the election, CEC had mirrored its website on several servers. (Rid, 2020, p. 362) The mirroring of CEC's website on several servers meant that CyberBerkut needed to identify which servers were the masters projecting the website on to the other servers. Probably unaware of this specific architecture, CyberBerkut uploaded their fake chart to one of the mirroring servers, which prevented the broadcasting of the chart online on CEC's official website. (Rid, 2020, p. 362) Forensic analysis suggested that after having uploaded the fake chart on one of CEC's servers, CyberBerkut had forwarded the Universal Resource Locator (URL) to Russia's Channel One journalists, because the servers' logs show several access requests from multiple employees working at the TV station approximately 30 minutes after the closure of the polls. (Rid, 2020, p. 362) It is difficult to know whether Russia's Channel One employees were effectively working with the CyberBerkut group, or had they just jumped on what appeared to be a scandalous piece of news aligned with their editorial line. However, in either case, it shows that Russia's cyber groups are leveraging Russia's state media to spread their messages into Russian information space.

Although mostly unsuccessful, the operation aimed at reinforcing one of the key pillars of Russian narrative on Ukraine, which advocate that the pro-democratic revolution in Ukraine in 2014 was in fact a fascist revolution orchestrated by the U.S. (Jensen et al., 2019, p. 15) The aim was not to actually influence or change the outcome of the Ukrainian election, as displaying forged results on the CEC's website did not supersede the manual counts of the paper ballots taking place at polling stations across Ukraine. (Koval, 2015, p. 56) The goal was to discredit the Ukrainian state capacity to organize and held democratic elections (Brangetto and Veenendaal, 2016, p. 121) and also to underline that democracy is fostering extremism in a society. Russia's influence operation did not end, the night of the election, as for days after the CEC's CERT publication of their incident report, CyberBerkut was active online, contradicting the findings of the report. For instance, CyberBerkut doubled down on their claim that they had extensively damaged CEC's network and systems, preventing the CERT to restore their system, and also continue to affirm that the chart broadcast on Channel One was the legit one, confirming that the far-right candidate had actually won the popular vote. (Rid, 2020, p. 363)

This cyber event exemplifies Russia's holistic approach to information warfare, as it highlights sophisticated penetration methods to breach into the network during the information operation phase, then the use of carefully crafted messages anchored in a mixed of socio-cultural and historical references during the influence operation phase to influence the targeted information space.

Attacks on Ukrainian Power Grid in 2015-2016

On December 23, 2015, control systems of three distribution stations from three different Ukrainian energy companies were compromised, which resulted in a power outage that touched more than 225,000 Ukrainians for more than three hours. (Polyakova and Boyer, 2018, p. 13) Using BlackEnergy3, the attackers had remotely accessed the company's SCADA systems and manually opened breakers at 30 substations, plunging hundreds of thousands of Ukrainians in the dark. (Blank, 2017, p. 92) In addition, as the attack was taking place, thousands of fake calls flooded the companies' call centres making it impossible for affected Ukrainians to report the incident to the companies. (Lee et al., 2016, p. 2) The attack ended with the use of KillDisk malware, which wiped many systems disrupting the recovery and forensic efforts of the companies' CERT. (Jasper, 2020, p. 16)

The attacks were coordinated and showed signs of extensive reconnaissance efforts of the Ukrainian energy companies' networks and systems. Forensic analysis showed evidence that the reconnaissance stage of the attack, including mapping of the companies' networks and employee credential stuffing started in the spring of 2015 with spear phishing campaigns targeting IT staff and system administrator accounts. (Lee et al., 2016, p. 3) The phishing emails appeared to be from the Ukrainian parliament and included a compromised Microsoft Word document, which contained the BlackEnergy3 payload as an attachment. (Jasper, 2020, p. 16) If opened, a pop-up alert was asking them to enable a macro and upon acceptance the BlackEnergy3 malware was loaded on the computer enabling the attackers to take control of the machine and established backdoor connections to the attacker's server for further infections. (Lee et al., 2016, p. 6) Once inside the network the attackers were able to move laterally and map the companies' networks undetected and eventually, they gained access to Windows domain controllers and harvested workers' credentials. (Jasper, 2020, p. 17) The Ukrainian companies were following basic cyber security practices, including having a segmented network, which separated their corporate network from the operational network hosting the SCADA system and servers, but the company had not instituted a multi-factor authentication (MFA) policy. (Lee et al., 2016, p. 2) Therefore, the attackers were able to access the company virtual private network

(VPN) to access the network hosting the SCADA systems and servers remotely, leveraging legit employee credentials. (Blank, 2017, p. 92) At two of the three stations, once inside the SCADA system, the attackers were able to reconfigure the power supply systems of both the main electric connectors, which are connecting the station to the power grid and of the backup batteries, so they could be turned off during the attack. (Lee et al., 2016, p. 7) In addition, the attackers also cloned the companies' control software, which allowed them to control the breakers remotely (Jasper, 2020, p. 17), and reconfigured the stations' serial-to-ethernet converters[16] preventing the workers from remotely controlling the breakers. (Lee et al., 2016, pp. 8-9) At the third distribution stations, the attackers did not use a cloned firmware to turn off the breakers, instead they used a privileged IT account to exploit the company's IT helpdesk tool and took direct control of the mouse movements on the operators' machines, while also locking them off the system and then manually turned the breakers on in front of the helpless operators. (Greenberg, 2019, p. 64)

In December 2016, a year after the precedent cyber-attack, a second attack targeted the regional transmission station of the distribution company Ukrenergo in Northern Kyiv. The Northern Kiev transmission station carried significantly more electricity than all of the distribution stations and substations that have been hit a year before, which revealed a serious escalation in Russia's information operations in Ukraine. (Greenberg, 2019, p. 130) However, the actual impact on the ground was significantly smaller than the 2015 attack, as the outage lasted for roughly an hour, instead of three. (Slowik, 2019, p. 3) Similar to the precedent attack, the attackers had undertaken extensive reconnaissance of the station's network and systems, with some evidence pointing at a breach, using BlackEnergy3 malware as early as January 2016, which is almost a year before the attack took place. (Greenberg, 2019, p. 131) Although this second attack resembled the previous one, it was more sophisticated as it used CrashOverride to automate the attack. (Slowik, 2019, p. 3)

[16] A serial-to-ethernet converter is used to translate modern internet communications into a form that can be interpreted by older IT devices and equipment. (Greenberg, 2019, p. 63)

Similar to the precedent attack, the attackers used spear-phishing tactics, carrying BlackEnergy3 to get access to operators' machines, but it also deployed a tool called Mimikatz[17] to move laterally within the station's computers and networks undetected. (Greenberg, 2019, p. 132) The attackers were also able to dig into the temporary memory cache created when an application crashes down to retrieve sensitive credentials being saved there for rebooting purposes. (Greenberg, 2019, p. 132) Similar to the previous attack, the lack of MFAs made it easy for the attackers to leverage the credentials that have been harvested with Mimikatz exploit and gain access to the main database server of the company. The data based was used to keep records of the utility's operations, collecting data from physical equipment to make them available on the corporate network. (Greenberg, 2019, p. 132) The main issue with this main database was its ability to not only receive information, but also to send commands to the systems managing the station's physical equipment functionalities. (Greenberg, 2019, p. 132) Therefore, through the database, attackers were able to inject malicious code to the SCADA systems controlling the breakers and other physical components of the station.

The major novelty was that BlackEnergy3 contained the CrashOverride malware and loaded it on the operators' machine, along with hidden files containing four payloads using different SCADA system protocols.[18] (Slowik, 2019, p. 3) The malware was able to scan through the station's network, access the station's SCADA system and locate the industrial systems operating the physical equipment such as the breakers and finally identify the type of protocol being used to communicate to the systems. (Brook and Lucchesi, 2017, p. 7) Once the type of protocol was identified, CrashOverride selected the corresponding payload from the hidden file and establish a direct connection to the system embedded in the physical equipment, bypassing SCADA. (Brook and Lucchesi, 2017, p. 7) Once the attack was launched, CrashOverride was sending "open" commands to the breakers in an automated and rapid-fire fashion,

[17] Mimikats is a hacking tool able to exploit a vulnerability in "older version of Windows that leaves passwords accessible in a computer's memory. (Greenberg, 2019, p. 132)

[18] A protocol is a simple set of predetermined rules or procedure for transmitting data between devices and systems. Knowing the protocol of a device or system allows communication to it. https://www.britannica.com/technology/protocol-computer-science

preventing operators to close them, as they were instantly reopened. (Brook and Lucchesi, 2017, p. 7) Similar to the precedent attack on Ukrainian power grid in 2015, the attack ended with a KillDisk wiping out the station's computers to delay recover efforts and disrupt later forensic analysis of the event. (Slowik, 2019, p. 3) Notwithstanding its sophistication the blackout only lasted about an hour, after what the company's CERT was able to reboot all systems and resume normal operations. Many assumed that the rapid recovery from the attack, may indicate that it was not the attacker's intention to cause extensive damages to Ukrainian power grid, but only to signal their capabilities. (Greenberg, 2019, p. 147) However, recent forensic analysis of the event suggests that the attack was designed to cause more damage, but as a result of coding flaws in the CrashOverride malware the attack was not carried out to its full potential. (Slowik, 2019, p. 5) It seems that CrashOverride tried to neutralize the station's protective relays through a DoS attack, but it failed to execute the command. (Slowik, 2019, p. 6) If such attack had succeeded, once the station crew had manually restored the power, it would have caused a massive overload of current in the station's transformers, resulting in burned power lines. (Slowik, 2019, p. 9)

Although, the 2016 attack on Ukraine's power grid did not create significant damages to Ukraine's critical infrastructure, the multi-payload capacity of the CrashOverride malware demonstrated that such an attack on critical infrastructure of a country can be automated and scalable for larger-scale attack targeting different companies, types of equipment and countries simultaneously. (Brook and Lucchesi, 2017, p. 11)

NotPetya Ransomware Attack in 2017

In June 2017, media across the world reported an unprecedented Ransomware attack in Ukraine called NotPetya. The NotPetya worm spread quickly outside of Ukraine infecting hundreds of thousands of computers in 64 countries. (Polyakova and Boyer, 2018, p. 14) Hundreds of multinationals around the world were impacted, resulting in billions of dollars in damages. For instance, Maersk based in Norway, which is the second world largest shipping company was forced to shut down its global network, locking down ports around the world, causing an estimated lost of USD 300 million to the company; Mersk's a Jersey-based pharmaceutical lost fifteen thousand Windows computers in ninety seconds before the company had the time to shut down its network to limit the spread of the worm, causing USD 870 million in damages; Saint-Gobain a French construction company was forced to shut down its operation worldwide, losing USD 400 million. (Greenberg, 2019, pp. 197-199) According to a U.S. report on the NotPetya cyber event, the malware causes an estimated of USD 10 billion in damages worldwide. (Bendiek and Matthias, 2021, p. 24) In comparison, the WannaCry cyber event, which happened a few months prior to NotPetya is estimated to have caused USD 4 billion in damages worldwide. (Greenberg, 2019, p. 199)

The attackers reused the same codes from a well-known ransomware strain called Petya and used the U.S. National Security Agency (NSA) EternalBlue and EternalRomance exploits leaked by the ShadowBroker in 2016, which was also used in the WannaCry ransomware a few months earlier. (Polyakova and Boyer, 2018, p. 14) The recycling of publicly available exploits was meant to make NotPetya looked like a legitimate criminally motivated ransomware attack. (Polyakova and Boyer, 2018, p. 14) However, the criminally motivated veneer of NotPetya fell quickly, mainly as a result of the badly managed ransom payment element. Indeed, the attackers "carelessly provided an email address (wowsmith123456@posteo.net) to the victims to send proof of payment, and that address was promptly and simply blocked by the provider, which made it impossible for victims to recover a decryption key for their files." (Bendiek and Matthias, 2021, p. 24) In addition, forensic analysis of the NotPetya worm revealed that the attackers had installed a simple kill switch in the malware, indicating the intention to be able to control the spread of the worm, which is unusual in criminally motivated malware infections. (Jasper, 2020, p. 100) As the ransom payment element of NotPetya was subject to a single point of failure and thus extremely vulnerable, suspicion about NotPetya being in fact a state commissioned false-flag attack instead of a criminally motivated ransomware attack gained traction worldwide. (Bendiek and Matthias, 2021, p. 24)

Contrary to a typical ransomware attack, NotPetya was designed to wipe out data on infected computers "by encrypting the master file table (a database used by the operating system to retrieve a file)." (Polyakova and Boyer, 2018, p. 14) In addition, the level of sophistication of NotPetya and of the infection tactics, was high compared to criminally motivated cybercrime.

The initial infections showed a sophisticated and planned approach, which consisted of compromising the Ukrainian M.E.Doc tax and accounting software (Bendiek and Matthias, 2021, p. 23) which is the equivalent of TurboTax in Canada. (Jasper, 2020, p. 100) The attackers compromised the software's customer updates functionality to install NotPetya on machines using the accountant software developed by the Ukrainian company Linkos Group. (Bendiek and Matthias, 2021, p. 23) Compromising the software's customer update function required a high level of sophistication, as the attackers must have breached into several layers of protection in Linkos Group's network, while also being able to hide their intrusion and presence for a long period of time. (Greenberg, 2019, p. 206) Later, forensic analysis of Linkos Group's network revealed that the attackers exploited a vulnerability in the company's web content-management software used to edit its website's content and appearance, and installed a "web shell[19] on the server, acting as a foothold inside the computer, letting them install their own software on it at will." (Greenberg, 2019, p. 210) From there they gained access to the M.E.Doc update server and corrupted the software customer update functionality. (Bendiek and Matthias, 2021, p. 24) The first wave of infection went undetected as the malware was installed on customers' machines using M.E.Doc software's architecture and functionalities, blending the malware activities with the software's normal and legitimate operations and communication to Linkos Group's servers. (Greenberg, 2019, p. 210) To spread across companies' networks, NotPetya used two promulgation methods. First, it used an updated version of the Mimikatz password-cracking tool to steal account credentials "and hand off the credentials to the legitimate Windows administration tool PsExec or the legitimate Windows Management Instrumentation Command-line (WMI) tool to access other local systems." (Jasper, 2020, p. 101) The second method was the use of EternalBlue and EternalRomance exploits, "which used a flawed implementation of Microsoft's SMB

[19] A Web Shell is a type of backdoor designed to leverage the Web browser of the targeted computer. https://malware.expert/general/what-is-a-web-shell/?msclkid=19398d96b90511ec95cea6f023a934c1

protocol to access files and printers on other machines on the same network." (Bendiek and Matthias, 2021, p. 23) However, as NotPetya was designed to spread via internal networks and not via internet like the WannaCry worm, forensic experts believe the attack was targeting Ukraine specifically, but the attackers may have underestimated the contagiousness of the worm. (Jasper, 2020, p. 101) In addition, deeply buried into NotPetya's code was an instruction to stop certain components of NotPetya from running if a file called "perfc" was found in the main Windows directory of the targeted computer. (Greenberg, 2019, p. 208) This piece of code, may have been a legacy artifact from the ransomware design on which NotPetya was based on preventing that data to be encrypted twice (Greenberg, 2019, p. 208) or it may have been a way to shield friendly computers from being infected with the malware avoiding "friendly-fire" type situations.

Ukrainian and U.S. intelligence services attributed NotPetya to Russia's GRU or to the APT 28 groups, which are likely the same group. (Bendiek and Matthias, 2021, p. 25) Other private cyber security companies attributed NotPetya to the Sandworm group/CyberBerkut, finding forensic evidence of ties with previous attacks performed by the group, especially the attack against Ukrainian CEC during the 2014 presidential election (Greenberg, 2019, p. 224); against the Ukrainian power grid in 2015 and 2016, and also several attacks against Ukrainian ministries since 2014, wiping data using the same kind of KillDisk malware that was found in NotPetya. (Bendiek and Matthias, 2021, p. 25) Although almost impossible to empirically confirm, it is most likely that all of these groups either work closely with Russian intelligence agencies or are in fact Russian intelligence units. (Baezner, 2018, pp. 12-13)

How are these Attacks Supporting Russia's Information Warfare Objectives?

Russia's information and influence operations in the cyberspace against Ukraine must be understood as compounded discursive actions aimed at influencing the Western/Ukrainian and Russian information space by supporting, reinforcing and legitimizing core discursive elements of Putin's national narrative. First, to delegitimize and mitigate democratic aspirations at home and in Ukraine, Russia's information and influence operations aim at demonstrating that post-Euromaiden Ukraine is a failed state unable to rule Ukraine. (Herd, 2022, p. 88) The idea that Ukraine is not a real functioning state is popular in Russia and is part of Russia's historiography going back centuries, as exemplified in the *Russkii Mir* civilizational myth of the *Kievan Rus* and Russia foreign policy concept of Near Abroad. (Stent, 2020, pp. 176-185) Putin himself told George W. Bush, then president of the U.S., at the NATO Bucharest summit in 2008, regarding Ukraine potential future NATO membership: "George, you have to understand that Ukraine is not even a country. Part of its territory is in Eastern Europe and **the greater part was given to us**." (Stent, 2020, p. 131) This objective is achieved by targeting its sovereignty and democratic institutions; demonstrating Kyiv's inability to deliver basic public services to Ukrainians; and the government's inability to provide a domestic environment conducive to economic stability and growth. Second, Russia's information and influence operations aim at portraying post-Euromaiden Ukraine as an existential threat to Russia, by claiming that history is repeating itself in Ukraine in the form of a resurgence of a fascist power meant to destroy Russia, like Nazi Germany, during the Second World War. Finally, Russia's information and influence operations in Ukraine aim at highlighting Western hypocrisy and double standards in the international arena, by demonstrating that the post-Euromaiden Ukrainian government is an artificial creation controlled and sustained by Western powers to diminish Russia's great power status. (Herd, 2022, p. 108)

The attack on Ukraine CEC in 2014 started with CyberBerkut's information operation allowing the group to breach into CEC's network, shutting down the real-time display of election results as a decoy attack, obfuscating the injection of BlackEnergy malware and the establishment of backdoors to CEC's servers. These two staged and somewhat sophisticated information operations against CEC, paved the way for Russia's cyber threat actor to carry out an influence operation following the closure of Ukrainian polls, designed to simultaneously delegitimize the Ukrainian government's institutions in the Ukrainian information space, and demonized the Euromaidan democratic aspiration of Ukrainian in the Russian information space. Russian influence operation aimed at delegitimizing the Ukrainian government's institutions in the Ukrainian information space lasted for several days after the election. CyberBerkut openly challenged online the CEC CERT's incident report seemed to have aimed at maximizing the discursive impact of its information operation, by trying to humiliate CEC's technical expertise and ability to protect their network, while also insinuating that the Ukrainian government was hiding the real results of the election, as it would have exposed the fascist underpinning of Ukraine's pro-democratic political movements. In addition, the CyberBerkut group's name makes explicit reference to the Ukrainian special policy unit called Berkut, which is believed to be responsible for opening fire on pro-Euromaiden protesters in 2014. Hence, by claiming credit for the attack on the CEC, CyberBerkut had established a false flag operation narrative advocating that Ukrainians were behind the attack on their democratic process, hiding Russia's involvement in the operation (Rid, 2020, p. 363), while also projecting an image of division in Ukraine. Overall, by attacking post-Euromaiden Ukraine democratic processes, Russia is trying to create, reaffirm and maintain a narrative into the Russian information space, which highlights the potential danger of Western-inspired democratic revolutions and advocate for a political status quo in Russia. (Herd, 2022, p. 108) In addition, propagating the narrative that Ukraine Post-maiden democratic processes is a scheme concealing Western states effective control over Ukraine and linking the Ukrainian government to far right and fascist movements contribute to diminishing Western influence globally and to portray Russia as a besieged fortress. (Bertelsen, 2021, p. 156)

First, describing the Ukrainian government as a puppet government controlled by Western powers seek to underline perceived Western hypocrisy and double standards in the international arena, as both wanting to impose liberal and democratic values around the world, while also, when convenient, supporting authoritarian regimes that are beneficial to their imperialistic interests. (Jasper, 2020, p. 83) Second, by portraying Ukrainian government as fascist, Russia is linking post-Euromaiden Ukraine to Nazi Germany and leverage its symbolism in Russian historiography as the main enemy threatening Russia. (Herd, 2022, p. 149) The narrative of a Nazi Ukraine, also highlight the moral imperative of Russia to defeat it, just like the USSR did during the Second World War. Therefore, by portraying Ukraine as a fascist and puppet government, Putin is juxtaposing two historical threats to Russia, namely Nazism during the Second World War and Western's imperialism, during the Cold War period.

Although Russian narrative sounds unconceivable to Western audiences, we should not underestimate the effectiveness and medium to long-term impacts of Russia's information warfare on the international stage. Certain elements of Russia's narrative such as the idea that Ukraine is a puppet state controlled by the West and filled with fascist elements seem to gain traction outside the Western information space. For instance, the narrative portraying Russia as a besieged fortress trying to defend itself in Ukraine, against Western aggressive imperialism, and Putin's moral duty to "denazify" Ukraine has been noted to be a popular point of view in countries around the world. (Eligon, 2022) South Africa's President Cyril Ramaphosa stated in front of the parliament in March, "the war could have been avoided if NATO had heeded the warnings from amongst its own leaders and officials over the years that its eastward expansion would lead to greater, not less instability in the region." (CNN, March 23, 2022)

The attack on Ukrainian power grid in 2015 and 2016 revealed the willingness of Russia to escalate its information warfare to the limit of what is permissible under the threshold of conflict. The targeting of critical infrastructure is usually off limit for under the threshold of conflict operations, due to the higher risks of crossing the red line and triggering open interstate war. However, as these attacks were limited in scope and not carried out alongside conventional military operations, we can assume that, although risky, their main purpose was discursive. (Brangetto and Veenendaal, 2016, pp. 115-116) These two attacks on Ukraine's power grid in one year of interval demonstrated the ability of Russia's information operations to strike critical infrastructure whenever they like, while also challenging the Ukrainian government ability to protect its critical infrastructure and provide basic, but crucial services to Ukrainians. Indeed, attacking critical infrastructure in Ukraine has a direct impact on the government credibility, as it touches one of the core functions of any modern government, which is to deliver reliable public services to its citizens. Therefore, by demonstrating that cyber groups, like CyberBerkut or Sandworm can disrupt the provision of electricity to hundreds of thousands of Ukrainians at will, faith in the ability of their government to provide public services is challenged and diminished. From a Russian perspective, these events carried out as false flag operations are fuelling Russia's media with news portraying Ukraine as a land in perpetual chaos ruled by an incompetent government unable to ensure the provision of basic and crucial public services to its citizens. (Bertelsen, 2021, p. 161) Again, this is being instrumentalized in Russia's information space to underline the danger of political and societal changes, hence effectively reinforcing the importance of maintaining the status quo in Russia at all costs. (Herd, 2022, p. 147)

Although NotPetya infected computers across the world, the way the cyber threat actors leveraged a Ukrainian accountant software suggested that Ukraine's businesses and economy were the primary target. (Bendiek and Matthias, 2021, p. 25) This assumption aligns with Russia's information warfare strategy to destabilize neighbouring countries wanting to get closer to the Western influence sphere (Marangé and Quessard, 2021, p. 135) while also aligning with its informational tactic in Ukraine to portray Ukraine as a land of chaos since the Euromaiden revolution in 2014. (Herd, 2022, p. 88) Indeed, NotPetya was an historical event that caused billions in damages to businesses worldwide and enjoyed a lot of press (Bendiek and Matthias, 2021, p. 23) including in Ukraine, which accounted for more than 70% of the infected computers. (Rid, 2020, p. 420) In addition, the efforts to disguise NotPetya as a criminally and financially motivated ransomware attack, targeting Ukrainian businesses and Western Multinationals operating in Ukraine (Rid, 2020, p. 420) also support the Russian narrative that Ukraine is an international conflict hotspot and a lawless land where cyber criminals proliferate because of the Euromaidan coup. (Marangé and Quessard, 2021, p. 129) In that context, the cybercriminal veneer of NotPetya might have been an attempt to influence the Western information space by highlighting the financial and technological risks for businesses operating in Ukraine, hence reducing Ukraine's economic attractiveness for Western companies. In addition, this historical attack also supported the narrative that the Ukrainian government is unable to ensure an environment that is conducive to business and economic growth, which constitutes another important function of any modern government.

Russia's invasion of Ukraine on 24 February 2022 and Putin's public announcements showed a persistent continuity in Russia's information warfare against Ukraine and Western democracies since 2014, as the same topics or discursive themes are expressed, including Western hypocrisy hiding its true imperialistic nature to export liberal and decadent values that are dangerous for Russia; Portraying post-Euromaiden Ukraine governments as an aggressive and fascist state controlled by the west that need to be ‘denazified’; and Russia as an under-siege fortress fighting for the survival of the Russian civilization. (Bloomberg, 2022)

5 – CONCLUSION

There are three main interlinked factors that led to the Putin regime's interest in using information and influence operations as regime survival tools. 1) New international technological context characterized by fast-paced IT development and government reliance on them; enhanced interconnectedness of IT infrastructure worldwide crossing national borders; and the almost instantaneous sharing and production of information created a well-suited environment to adapt old Soviet active measures and reflexive control methods to the cyberspace environment. (Rid, 2020, pp. 7-8) 2) Putin's background as a former KGB case officer deployed in Dresden, East Germany, and then later in St. Petersburg gave him first-hand experience of both the risks of the free flow of information and political freedom for authoritarian regimes, and also how information can be leveraged to ensure regime longevity. As information operations and reflexive control methods are important concepts used by Security and Defense Departments (*silovyye struktury*) since Russia's imperial era (Stepanov, 1999, p. 6) it is reasonable to assume that someone like Putin with a *siloviki* background is more receptive and inclined to use these methods as governance tools. 3) Russian information security and defence doctrines do not distinguish information security and cyber security, nor do they distinguish information warfare from cyber warfare.

Through the lens of a *siloviki* cynical of liberal democracy and values, Putin and his close allies and supporters with similar backgrounds took power in Russia in 2000 and pledged right away to bring political and economic stability back in Russia, after a decade of political and economic turmoil and public unrest. (Belton, 2020, p. 167) His vision for Russia, as expressed in the Millennium Message, was to establish a "managed democracy" characterized by a strong state held above everything else (Hill and Gaddy, 2015, p. 40) reject foreign democratic and liberal values as national threats (Putin, 1999, p. 7) restrict political, social and information freedom; and place himself at the centre of it all. (Herd, 2022, p. 111) We cannot understand Russia's information and influence operations at home and abroad without understanding Putinism. Indeed, after 22 years in power, Putinism has aimed at blurring the lines between Putin and the Russian state. The takeover, by Putin's regime of Russia's political, economic and informational sectors is so significant that separating them from Putin’s regime is almost impossible. (Belton, 2020, p. 276) Resembling Russia’ tsarist era, official state narratives are portraying Putin as being Russia. By claiming that everything is centred on Putin’s regime, it is reasonable to assume that such a governance model over emphasizes considerations like regime self-conservation in the decision-making process. In that context, Putinism is key to understand why contrary to Western governments, Russia is leveraging all sectors of Russian society to carry out total information war against the countries like Georgia, Ukraine, and Western countries. From a structuralist approach, governance model influence not only state’s decision-making processes, but also policymakers. As such, in a governance model where everything is centralized and subordinated to one political leader, institutional divisions and considerations have no or very limited impact. (Ledeneva, 2013, p. 80) Therefore, there is no legal, organizational, and administrative constraints preventing Putin from leveraging all sectors of the Russian state’s activity to achieve his political objectives. In that context, everything can be designed as being part of Russia’s national interests, just like everything can be designed as state strategic resources including, oil, minerals, Russia’s information space, Russian language and culture, Russia’s history, etc. Putin’s authoritarianism and specific approach to information security are not new as they are part of Putin’s governance model since he was elected in 2000. However, a shift in his stance against the West happened when he came back to the presidency in 2012, after Medvedev’s mandate. Putin’s regime has always been critical of the West, especially on the NATO expansion front, and during the colour revolutions in what Russia claims as it’s “Near Abroad,” but these were mainly criticism targeting a domestic audience. (Tsygankov, 2019, p. 202) During his third mandate as President of the Russian Federation, Putin and his regime became more and more aggressive in their rhetoric and actions against the West. (Shiraev and Khudoley, 2019, p. 92) As official Kremlin’s narratives claim, it may have been caused by NATO's eastward expansion and Russia’s perceived military threat it poses. (Tsygankov, 2019, p. 187) However, based on Russia’s governance model, and the fact that NATO had almost no contingents in Eastern Europe before 2014, it is more likely that Putin was reacting to perceive informational threats to his regime, which were enabled or at least enhanced by new technological innovations in the information domain. Putin’s 2010s more aggressive rhetoric against the West coincides with three major events that have been interlinked conceptually in Russia and in the West, but under different angles: the significant use and popularity of social media; the Arab Spring in the Maghreb and the Middle East; and the November movements in Russia. In the West as in Russia, social media have been identified as a tool enhancing the sharing of political ideas and facilitating the organization of democratic protests and political events. In the West, this was seen as a positive means to strengthened democracy and foster the democratic idea and aspirations around the world, as was demonstrated by the Arab Spring and the November movements. (Marangé and Quessard, 2021, p. 12) In Russia, social media was seen as a tool used by Western intelligence services to conduct information and influence operations abroad to topple down dictators in Arab countries and even in Russia. (Stent, 2020, p. 267) Whether Putin personally believes this is impossible to know. However, it is reasonable to assume that from a *siloviki* and an authoritarian governance perspective, these tools fostering the sharing of ideas and facilitating political mobilizations was seen as much as a threat as an opportunity. Internet-based media increases the perceived political risks from Putin's regime, as it provides Russians with a free flow of information bypassing state's information regulations and state-controlled media. (Marangé and Quessard, 2021, pp. 122-123) On the other hand, if these new information technologies make Russia's information space permeable to Western values and ideas, then the Western information space too is permeable to Russia's values and ideas. Of course, the major difference is that Western values and ideas are propagated by its soft power based on real attributes of Western societies, such as democracy, political and social freedom, high standard of living, culture, etc., while Russia lacks most of these appealing attributes. (Mérand, 2020, pp. 138-139) Therefore, Putin must fabricate them through information and influence operations influencing perceived reality in Russia and about international events, which is not too dissimilar from Soviet era active measures, and reflexive control operations against the West. (Mérand, 2020, p. 151)

It is important to note that Russia's information and influence operations leverage the full information tools spectrum, including disinformation, misinformation, propaganda, and forgeries to exacerbate social grievances and existing social tensions within the targeted information space. (Bertelsen, 2021, p. 168 and

p. 178) In that context, like Russia’s overall foreign policy, Putin’s information warfare in the cyberspace responds principally to domestic considerations, as Putin seeks the effect of foreign information and influence operations to reflect back on Russian information space. (Stent, 2020, p. 41) By destabilizing Western-leaning societies such as Ukraine and Western societies in general, Putin is trying to diminish Western influence and soft power worldwide and demonstrating to Russians that the Western democratic model of society is worse or at least not better than Russia’s model of society. (Jasper, 2020, p. 83) The idea of Russia as a besieged fortress supports this overarching discursive objective also, as it portrays the West as the main enemy to Russians (Bertelsen, 2021, p. 156) while also framing the West as anti-Russian rejecting Russian society, values and culture, hence reinforcing this idea that even if Russia wanted to get closer to the Western model, it could never be accepted as a Western European country.

Aligned with this holistic understanding of information warfare, Russian strategists have developed a holistic approach to information and influence operations in the cyberspace. (Lilly and Cheravitch, 2020, p. 135) Russian cyber threat actors are considering three operational levels when carrying out information and influence operations. At the strategic level, Russian cyber threat actors consider the targeted information space, which is where the aggregation of societies’ discursive actions and messages forming national identities is located. (Bagge, 2019, p. 46) Therefore, influencing the targeted information space, including Russia, is the main long-term objective, as it influences perceived reality. At the operational level, Russia’s cyber threat actors consider the information and messages embedded in their cyber-attacks. (Bagge, 2019, p. 47) Information and messages considerations are not only about the actual message included in the payload of the attack as for instance the defacement of a website with pro-Russian content. It is also about considering the discursive impacts of the cyber-attack, how it will be perceived by the targeted organization, government, and the country information space, including how it will be perceived in the Russian information space. (Brangetto and Veenendaal, 2016, p. 116) At the tactical level, Russian cyber threat actors consider the targeted IT infrastructure. (Bagge, 2019, p. 47) At this level, technical considerations and decision are made based on previous considerations made at the other two levels, including the reconnaissance period, the type of cyber-attack, DDoS, website defacement, malware injections, etc. (Connell and Vogler, 2017, p. 23) Since the early 2000s, Russia's cyber threat actors have evolved significantly, gaining in professionalization and technical effectiveness. One of the major shifts has been the growth of the GRU influence and leadership in Russia's information and influence operations. (Lilly and Cheravitch, 2020, p. 140) Before 2014, most Russian information and influence operations in the cyberspace were led by the FSB, which relied heavily on cybercriminals and hacktivists. (Greenberg, 2019, p. 236) However, during the Ukraine conflict experts have seen the GRU or groups related to the GRU taking the lead. (Giles and Akimenko, 2020, p. 70) This might have been caused by a need for more sophisticated and professional cyber capabilities to address Western countries enhancing their cyber security posture overtime.

While not a Western European country, Ukraine is very important in Russia's historiography, as it represents the birthplace of the Russian/Slavic civilization. For Putin's regime, this historical simplification is important as it can be exploited to portray Ukraine's Western and democratic aspirations as a direct attack on Russia's historical, spiritual, and cultural core. (Putin, 2021) This has significant discursive power in Russia's information space, due to cultural affinities with Ukraine, and in the international space, due to the perceived legitimacy of Russia to defend its fundamental identity core. In that context, destabilizing and creating chaos in Ukraine is an opportunity for Russia to project on post-Euromaiden Ukraine the full length of Putin's national narrative to reinforce his regime's grip of power. Putin's overarching goals in the information space are the following: 1) Creating a narrative bubble in Russia, where it appears as if Russians and their society are constantly under threat from the West; 2) Amplifying positive narratives on Russia and its regime, while at the same time suppressing negative ones; 3) Weakening Western soft power by exposing, distorting and amplifying Western societal tensions and issues. To achieve that, Russia's information and influence operations in the cyberspace against Ukraine aim at achieving the three following discursive objectives: a) Undermining the Ukrainian democratic government's legitimacy to rule and demonstrating the danger of democratic revolutions; b) Portraying pro-western Ukrainians and the government as a direct threat to Russia, reinforcing the notion of Russia being besieged by Western powers, thus legitimating Putin's authoritarian governance model; and c) Demonstrating Western states' perceived hypocrisy and double standard in international affairs, including Western support to illegitimate, totalitarian and oppressive governments to diminish Western influence worldwide and alleviating Western Soft power pressure on Russia's information space.

Therefore, Putin's overall informational strategy is to seal as much as possible Russia's information space, as a defensive measure, while carrying out a total information war against the West, leveraging every sector of activities of the Russian state, including information and influence operations in the cyberspace. Evaluating the effectiveness of Russia's information warfare is hard, as indicators are either hard to identify or hard to define. For instance, some surveys demonstrated that a significant part of Russian society believes the state official narrative about Ukraine. (Blank, 2017, p. 91) However, in an authoritarian country, it may be normal to see a high rate of support for the state, due to the general fear of repression and being identified as a dissident by the regime. In that context, it is hard to prove direct correlation between Russia's information and influence operations and Putin's regime approval rate. Although, it is clear that Putin's regime has been quite successful in staying in power, as Putin's 22 years in power demonstrates, it is hard to evaluate and quantify the role of Russia's information and influence operations in Putin's regime longevity. In any case, the level of effort and resources deployed in carrying out such operations indicates clearly that Putin's regime believes they are either effective or at least they have enough effects to support his regime political goals.

What does this mean for Western Democracies?

This paper does not advocate for Western democracies to emulate Russia's specific understanding of national information space, nor to adopt Russia's approach to information warfare and information security. Indeed, to carry out Russian type of information and influence operations require a governance structure that would go against Western democratic values and governance pillars, including, political and social freedom, freedom of press, pluralistic ideas, fact-based decision-making process, etc. (Rid, 2020, p. 11)

However, the understanding of cyber security, as a concept and a field of practice must evolve to be able to encapsulate the new international technological context along with new cyber threats it enables. Currently the main body of literature on cyber security limits the cyber domain to technical and IT security considerations, without considering the crosscutting impacts of cyber threats on information in general. (Dubova, 2019, p. 16) One approach would be to reconceptualize cyber security as a mid-level field encompassing IT security technical considerations and Information Security informational considerations. Refocusing cyber security conceptually to include both IT and information security considerations will allow Western governments and policymakers to better understand the role and importance of cyber security for democratic societies. (Dubova, 2019, pp. 17-18) In addition, this new approach may facilitate the implementation of a more holistic approach to cyber security, which would enable a better understanding of Russian cyber threat actors' objectives and target selection process. (Dubova, 2019, pp. 17-18) While it is important that Western governments continue to invest in IT security elements to continuously enhance their institutions' cyber security posture, framing cyber security in a more information-oriented way would provide policymakers and the public with a better understanding and ability to grasp these emergent cyber threats. In addition, this new holistic approach to cyber security will facilitate the reorganization of existing institutional resources and enhanced interdepartmental cooperation to address these emergent, sophisticated, and cross-cutting informational threats in the cyberspace. Although further in-depth research on this subject is needed, some countries such as the United Kingdom and France have started investing resources and efforts into a more holistic approach to information security, placing countering information and influence operations into a bigger theoretical framework supporting information and cyber security resilience. (Marangé and Quessard, 2021, p. 314) Other countries, including the U.S. have chosen to enhance their cyber offensive capabilities to deter and counter cyber threat actors, characterized by the creation of the Cyber Command in 2008. Cyber Command is carrying out "Defence Forward" type of operations, which consist in identifying upcoming attacks, including in the information security domain and pre-emptively striking them to disrupt their operation before they can launch their attacks. (Marangé and Quessard, 2021, p. 279) This approach is based on the military approach to deterrence and may prove effective to disrupt and deter cybercriminal groups that have limited resources. However, this offensive-oriented approach may prove ineffective in deterring state-sponsored cyber threat actors, benefiting from significant resources and time to design and carry out sophisticated attacks.

From an information security perspective, to increase Western information space resilience to Russia's information and influence operations, Western governments must foster general understanding of cyber security and how it intersects with information security considerations, through education and awareness campaigns on state cyber threat actors' information and influence operations, such as Russia. For instance, several non-governmental and governmental organizations have been created in Europe, such as the Digital Forensic Lab, Bellingcat, Institute for Statecraft, EUvsDisInfo, to identify Russia's propaganda and disinformation campaigns and to inform governments and citizens about the different narratives that they may be exposed to. (Marangé and Quessard, 2021, p. 248) However, Western governments should refrain from engaging in information and influence operations, as it would significantly impact citizens' trust towards their government and democratic institutions. Instead, Western governments should continue to strengthen the pillars of a democratic and open society, such as democratic values and practices, pluralism of information, transparency, freedom of speech, and freedom of press. Contrary to authoritarian regimes such as in Russia, Western governments main strength is in their structural flexibility and ability to allow social change to take root and channel them into democratic institutions that would influence and reshape governmental structures accordingly.

Finally, further study and research on information and influence operations as general governance tools used by authoritarian regimes, extending beyond Russia is needed to understand better how authoritarian regimes are leveraging the new international technological context to ensure their longevity. Indeed, the war in Ukraine seems to highlight the significant human, materials, and economic costs of modern interstate war, due to several factors, including the proliferations of easy to use and to field defensive weapons, including portable anti-armoured, anti-air, and drone weapon systems. (Donato, 2022) Therefore, in an international context, where the costs of interstate conventional war seem to have increased significantly, active measures and reflexive control operations, including in the cyberspace may increase and be elevated to main levers of power projection domestically and abroad.

Bibliography

Assemblée Parlementaire de l'OTAN, (2018), *Parades au menaces hybrides émanant de la Russie : Une mise à jour*, Commission sur la dimension civile de la Sécurité, 22 p.

Bagge, Daniel P., (2019), *Unmasking Maskirovka: Russia's Cyber Influence Operations*, Defense Press, New York, 251 p.

Baumann, Mario, (2020), *Propaganda Fights and Disinformation Campaigns: The Discourse on Information Warfare in Russia-West Relations*, University of Kent, Kent Academic Repository, online: 'Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations: Contemporary Politics: Vol 26, No 3 (tandfonline.com)

Beazner, Marie, (2018), *Cyber and Information Warfare in the Ukrainian Conflict (version 2)*, CSS Cyber defence Hotspot Analysis, Center for Cyber Studies ETH Zürich, 54 p.

Belton, Catherine, (2020), *Putin's People: How the KGB Tool Back Russia and Then Took on the West*, Farrar, Straus and Giroux, New York, 624 p.

Bendiek, Annegret and Matthias Schulze, (2021), *Attribution: a major challenge for EU cyber sanctions; an analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW,* German Institute for International and Security Affairs, SWP Research Paper 11, Berlin, 42 p.

Bertelsen, Olga, (2021) *Russian Active Measures: Yesterday, Today, Tomorrow, Soviet and Post-Soviet Politics and Society,* Ibidem, Vol. 224, 380 p.

Blank, Stephen, (2017), *Cyber War and Information War à la Russe*, Edits. George Perkovich and Ariel E. Levite, Georgetown University Press, Chap. 5 in Understanding Cyber Conflict, Washington, pp. 81-98.

Bloomberg News, (2022), *Transcript: Vladimir Putin's Televised Address on Ukraine,* online: https://www.bloomberg.com/news/articles/2022-02-24/full-transcript-vladimir-putin-s-televised-address-to-russia-on-ukraine-feb-24.

Brangetto, Pascal and Matthijs A. Veenendaal, (2016), *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*, NATO CCD COE Publications, 8th International Conference on Cyber Conflict, Tallinn, pp. 113-126.

Brook, Aviv and Dominic Lucchesi, (2017), *Analysis of the First Malware to Attack a Power Grid*, Computer Science and Engineering, UC Santa Cruz, 12 p., online: https://dca.ue.ucsc.edu/system/files/dca/1426/1426.pdf.

Busari, Stephanie, (2022), *Analysis: Why some African Countries are thinking twice about calling out Putin*, CNN, March 23, 2022, online: https://www.cnn.com/2022/03/21/africa/africa-leaders-ukraine-response-cmd-intl/index.html?msclkid=3f25e59bb8d311ecb5ebfc6d2aa3e69a.

a) Canadian Center for Cyber Security, (2021), *An Introduction to Cyber Threat Environment,* Report, 11 p., online: https://www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf.

Carman, Douglas, (2002), *Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity,* Washington International Law Journal, Vol. 11, No. 2, pp. 339-369.

Committee to Protect Journalist, *Database of attacks on the press*, online: https://cpj.org/data/imprisoned/2021/?status=Imprisoned&cc_fips%5B%5D=RS&start_year=2021&end_year=2021&group_by=location.

Communications Security Establishment, *Cyber Hygiene*, Guidance, online: https://cyber.gc.ca/sites/default/files/publications/cse-its-cyber-hygiene-e.pdf.

Communications Security Establishment, (2021), *Cyber Threats to Canada's Democratic Process: July 2021 Update*, Report, 44 p., online: threat-to-democratic-process-2021-3-web-e.pdf (cyber.gc.ca)

Connell, Michael and Sarah Vogler, (2017), *Russia's Approach to Cyber Warfare*, CNA, Report, 29 p.

DGAP, (2020), *Deciphering Russia's "Sovereign Internet Law: Tightening Control and Accelerating the Splinternet"*, Rapport, No. 2, online: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

Donato, Joseph, (2022), *Putin's Bad Math: The Root of Russian Miscalculation in Ukraine*, Modern War Institute, United States, online: https://mwi.usma.edu/putins-bad-math-the-root-of-russian-miscalculation-in-ukraine/.

Dubova, Mariia, (2019), *Cybersecurity and Defense of Critical Energy Infrastructure in Ukraine: Frame Analysis of the Discourse,* Masarykova Univerzita, Faculty of Social Studies, Master's Thesis, Brno, 65 p.

Duncan, Andrew J., (2017), *New Hybrid War or Old Dirty Tricks? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment*, Canadian Military Journal, Vol. 17, No. 3, pp. 6-16.

Eligon, John, (2022), *In some Parts of the World, the War in Ukraine Seems Justified*, New York Times, March 17, 2022, online: https://www.nytimes.com/2022/03/17/world/war-russia-china-putin-support.html?msclkid=f7632499b8d511ec8e98395aeec43844.

EUvsDisInfo, (2019), *Ukraine will Turn Into a Banana Republic: Ukraine Elections on Russian TV*, News and Analysis, online: https://euvsdisinfo.eu/ukraine-will-turn-into-a-banana-republic-ukrainian-elections-on-russian-tv/.

Fish, Steven M., Vladimir Kara-Murza, Leon Aron, Lilia Shevtsova, Vladislav Inozemtsev, Graem Robertson, and Samuel Greene, (2017), "*What Is Putinism?*", *Journal of Democracy*, Vol. 28, No. 4, pp. 61-75.

Gessen, Masha, (2014), *The man without a face: the unlikely rise of Vladimir Putin*, Riverhead Books, 342 p.

Gallant, Tim, (2021), *War is War: The Relevance and Practicality of the Principles of War for Future Combat*, Canadian Military Journal, Vol. 21, No. 4, pp. 51-60.

Giles, Keir, Valeriy Akimenko, (2020), *Russia's Cyber and Information Warfare*, Asia Policy, The Future of Cybersecurity across the Asia-Pacific, pp. 67-75.

Gobert, Sebastien, (2018), *En Ukraine, le passé toujours vivant* , *Études*, No. 5, pp. 19-30, online: En Ukraine, le passé toujours vivant | Cairn.info

Greenberg, Andy, (2019), *Sandworm : A new era of cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers,* Anchor Books, New York, 348 p.

Herd, Graeme P., (2022), *Understanding Russian Strategic Behavior: Imperial Strategic Culture and Putin's Operational Code*, Contemporary Security Studies, Routledge, 248 p.

Heuer Jr., Richards J., (1999), *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Central Intelligence Agency, 184 p.

Hill, Fiona and Clifford G. Gaddy, (2015), *Mr. Putin: Operative in the Kremlin,* Brookings Institution Press, Washington, 533 p.

Jasper, Scott, (2020), *Russian Cyber Operations: Coding the boundaries of conflict*, Georgetown University Press, Washington, 215 p.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness, (2019), "*Fancy bears and digital trolls: Cyber strategy with a Russian twist", Journal of Strategic Studies*, 22 p.

Kari, Martti J. and Katri Pynnöniemi, (2019), "*Theory of strategic culture: An analytical framework for Russian cyber threat perception*", *Journal of Strategic Studies*, pp. 1-29.

Kenneth N. Waltz, (2001), *Man the State and War: a theoretical analysis,* Columbia University Press, New York, 263 p.

Kostyuk, Nadiya and Yuri M. Zhukov, (2019), "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?", *Journal of Conflict Resolution*, Vol. 63, No. 2, pp. 317-347.

Kotkin, Stephen, (2008), *Armageddon Averted: The Soviet Collapse 1970-2000*, Oxford University Press, 280 p.

Koval, Nikolay, (2015), *Révolution Hacking*, *Cyber War in Perspective: Russian Aggression Against Ukraine*, Chapter 6, NATO CCDOCOE, Tallinn, pp. 55-58.

Ledeneva, Alena V., (2013), *Can Russia Modernise?: Sistema, Power Networks and Informal Governance*, Cambridge University Press, Cambridge, 313 p.

Lee, Robert M., Michael J. Assante and Tim Conway, (2016), *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, SANS, Electricity Information Sharing and Analysis Center, Washington, 23 p.

Lilly, Bilyana and Joe Cheravitch, (2020) *The Past, Present, and Future of Russia's Cyber Strategy and Forces,* 2020 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, Tallinn, pp. 129-155.

Limonier, Kevin, (2018), *Ru.net: Géopolitique du cyberespace russophone*, L'Inventaire, L'Observatoire Centre D'analyse de la CCI France Russie, Paris, 127 p.

Loshkariov, Ivan A. and Andrey A. Sushentsov, (2016), *Radicalization of Russians in Ukraine: From accidental diaspora to rebel movement,* Southeast European and Black Sea Studies, 20 p.

Macleod, Alex and Dan O'Meara, (2010), *Théories des relations internationales: Contestations et résistances*, Centre d'études des politiques étrangères et de sécurité, Athéna, Québec, 659 p.

Marangé, Céline et Maud Quessard, (2021), *Les guerres de l'information à l'ère numérique*, Presse Universitaire de France, Paris, 448 p.

Massie, Justin, (2013), *Francosphère : L'importance de la France dans la culture stratégique du Canada*, Presses de l'Université du Québec, Québec, 295 p.

McFaul, Michael, (2021), *Russia's Road to Autocracy*, Journal of Democracy, Vol. 32, No. 4, pp. 11-26 Project MUSE - Russia's Road to Autocracy (jhu.edu)

McWhorter, Dan, (2014), *APT28: A Window into Russia's Cyber Espionage Operations?*, FireEye Special Report, 44 p.

Medvedev, Sergei A., (2015), *Offense-Defense: Theory Analysis of Russian Cyber Capability,* Graduate thesis, US Naval Post Graduate School, Monterey, 93 p.

Mérand, Frédéric, (2020), *Coping with Geopolitical Decline,* McGill-Queen's University Press, Montreal, 270 p.

National Institute of Standards and Technology (NIST), *Glossary*, U.S. Department of Commerce: online https://csrc.nist.gov/glossary/term/cyberspace#:~:text=A%20global%20domain%20within%20the,and%20embedded%20processors%20and%20controllers.

Peisakhin, Leonid and Arturas Rozenas, (2018), *Electoral Effects of Biased Media: Russian Television in Ukraine*, American Journal of Political Science, Vol. 62, No. 3, pp. 535-550.

Peterson, Kent, (2021), *Cybersecurity, Cyberwar and Cyberweapons: A beginner's guide to understanding cyber security and how it affects you,* Kent Peterson, United States, 142 p.

Polyakova, Alina and Spencer P. Boyer, (2018), *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, The New Geopolitics Europe, Brookings, 19 p.

Putin, Vladimir Vladimirovich, (2021), *On the Historical Unity of Russians and Ukrainians*, Essay published on the Russian Federation President Website, online: https://can01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fen.kremlin.ru%2Fevents%2Fpresident%2Fnews%2F66181&data=04%7C01%7Cbenoit.morin%40tbs-sct.gc.ca%7C83d9cbfe166245ca5ab108da1b036d3b%7C6397df10459540479c4f03311282152b%7C0%7C0%7C637851999177844233%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=n4yRe%2BExxEFb1wZG80ZTYRi57sazC192lRaLUN%2FjZ9k%3D&reserved=0.

Putin, Vladimir Vladimirovich, (1999), *Russia at the turn of the millennium*, Nezavisimaia gazeta, No. 4, Translated in ENG in *First Person: An Astonishingly Frank Self-Portrait by Russia's President Vladimir Putin*, pp. 209-229.

Putin, Vladimir Vladimirovich, Nataliya Gevorkyan, Natalya Timakova, and Andrei Kolesnikov, (2000) *First Person: An Astonishingly Frank Self-Portrait by Russia's President Vladimir Putin*, Public Affairs, 208 p.

Pynnöniemi, Katri, (2019), *Information-psychological warfare in Russian security strategy*, in Roger E. Kanet (Ed.), Routledge Handbook of Russian Security, City, pp. 214-226.

Rashid, Asma, Anum Yar Khan and Syed Wasif Azim, (2021), *Cyber Hegemony and Information Warfare: A Case of Russia*, Liberal Arts & Social Sciences International journal, Vol. 5, No. 1, pp. 648-666.

Rid, Thomas, (2021), *Active Measures: The Secret History of Disinformation and Political Warfare*, Picador, New York, 513 p.

Robertson, Graeme, (2013), *Protesting Putinism: The Election Protests of 2011-12 in Broader Perspective*, University of North Carolina at Chapel Hill, Problems of Post-Communism, Vol. 60, No. 2, pp. 11-23.

Russian Federation, (2000), *Doctrine of Information Security of the Russian Federation*, EN, online: https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpublicintelligence.net%2Fru-information-security-2000%2F&data=05%7C01%7Cbenoit.morin%40tbs-sct.gc.ca%7C0d70334775e24e70759208da3746d351%7C6397df10459540479c4f03311282152b%7C0%7C0%7C637883074570445519%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Xh%2BSXcMNk%2BSY4jAPnR05dHiHsMCWmcvL6MOwOOUq8WM%3D&reserved=0.

Russian Federation, (2016), *Doctrine of Information Security of the Russian Federation*, EN, online: https://can01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.scrf.gov.ru%2Fsecurity%2Finformation%2FDIB_engl%2F&data=04%7C01%7Cbenoit.morin%40tbs-sct.gc.ca%7C6eda19ebc3914362845108da1a3b9975%7C6397df10459540479c4f03311282152b%7C0%7C0%7C637851140524627094%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=nCrt1KphaNbPF3C%2BPZDXGJE2wBkL%2Fv41aPEwmWPhITU%3D&reserved=0.

Seaboyer, Anthony, (2018), *Influence Techniques Using Social Media*, Defence Research and Development Canada, Royal Military College of Canada, Kingston, 37 p.

Seaboyer, Anthony and Keir Giles, (2018), *Russian Reflexive Control,* Defence Research and Development Canada, Royal Military College of Canada, Kingston, 66 p.

Shiraev, Eric and Konstantin Khudoley, (2019), *Russian Foreign Policy,* Red Glob Press, London, 297 p.

Slowik, Joe, (2019), *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*, Gragos Inc, 16 p., online: CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack (pylos.co)

Spechler, Dina R. and Martin C. Spechler, (2019), *Putin and His Neighbors: Russia's Policies toward Eurasia*, Lexington Books, London, 152 p.

Statista, (2021), *Do you approve of the activities of Vladimir Putin as the president (prime minister of Russia)* online: https://cc.bingj.com/cache.aspx?q=Polls+of+Putin+popularity+by+age&d=4806403732998085&mkt=en-CA&setlang=en-CA&w=vSiOC9U_a1aJs1wQc0t5be4Vg2wsEdWA.

Stepanov, Sergei A., Charles A. Ruud, (1999), *Fontaka 16: The Tsars' Secret Police*, McGill-Queen's University Press, Montreal, 394 p.

The Guardian, (2012), *Putin's World Outlook*, Gleb Pavlovsky, Interview by Tom Parfitt, online: https://newleftreview.org/issues/ii88/articles/gleb-pavlovsky-putin-s-world-outlook.

Tsygankov, Andrei P., (2019), *Russia's Foreign Policy: Change and Continuity in National Identity,* Fifth Edition, Rowman & Littlefield, San Francisco State University San Francisco, 306 p.

Valeriano, Brandon, Benjamin Jensen and Ryan C. Maness, (2018) *Cyber Strategy: The evolving character of power and coercion*, Oxford University Press, New York, 386 p.

Young, Graeme, (2020), *Political Decision-making and the decline of Canadian peacekeeping*, Canadian Foreign Policy Journal, Vol 25, No. 2, pp. 152-171