Universiteit Leiden

International Studies Master's Program Thesis

Information Operations of the Putin Regime

Name: Daniel Rawle
Student number: S1740776
Email: d.a.j.rawle@umail.leidenuniv.nl
Word count: 16,639
Thesis supervisor: Max Bader

Contents

Introduction

On August 12th 2000, a faulty weld in the casing of a torpedo aboard the Russian Navy's *Kursk* submarine caused an explosion that claimed the lives of all 118 crew onboard (Knight 2002). As the incident occurred just three months after Vladimir Putin's inauguration as President of the Russian Federation, the disaster and the subsequent inadequate response from Kremlin organs would severely damage Putin's image in the public eye. Responses from the Russian media seemed to undermine the leadership capabilities of the new regime, "exposing navy humbug and Kremlin cover-ups, providing the names of the dead when the authorities refused to do so, and frustrating Kremlin attempts to control the coverage," (Traynor 2000) to which the new President responded with contempt:

> "They [the media] are liars. The television has people who have been destroying the state for 10 years. They have been thieving money and buying up absolutely everything (...) Now they're trying to discredit the country so that the army gets even worse." (ibid)

This response reflects the Putin regime's hypersensitivity concerning information dissemination, and the he politicization of information that followed under his regime would eventually coalesce into a conscious effort to absorb information into the remit of its control. State control over information dissemination was no novelty to Russia, as indeed practices of censorship and propaganda propped up the centralized authority of the Soviet Union until Mikhail Gorbachev's principle of *glasnost*, (and rapid developments in the field of commercialized information technology) ultimately sparked popular discontent with the regime and led to its dissolution (Shane 1994). With his KGB background and his famous reference to the collapse of the Soviet Union as a "major political disaster," (Putin 2005) it is clear that Putin has backward-looking tendencies in terms of the freedom of information. However, with the dawn of the information age and the mass availability of global information to the general public since the commercialization of the internet, efforts on the part of the regime to control information have consequently had to adapt.

The surge in the availability of information technology has revolutionized the foundations of society, making information one of the primary sources of productivity in modern day life (Castells 2000a). At the same time, the internet is an instrument of mass media whose empowerment of the individual to engage with popular discourses is causing a proliferation of sources of information that ultimately, under its own weight, undermines its veracity:

> "it is not only the state-controlled media organization that produces propaganda but citizens themselves who actively participate in the creation of disinformation by using new platforms to push their individual opinions to a point of excess, contributing to a new order where disinformation acquires a certain authority." (Mejias & Vokuev 2017: 3)

The combination of these two factors guides the political interest in controlling information. As opposed to industrial societies - where crucial pieces of infrastructure could be easily subject to the control of state power - informational societies are based upon the internet's ubiquity and decentralized infrastructure, forming a foundation of society more difficult to control via state organs in the traditional sense. This implies that informational societies are therefore more susceptible to instability.

The internet enables the individual to share ideas with scores of other people instantly from any location, inviting research into the socio-political impact of modern communication technology on international relations informed by constructivism. Developments in information technology, such as social media, help to produce and reproduce social realities, which - according to constructivism - establish social norms that contribute to the formation of social policy (Eriksson & Giacomello 2006: 233). As will be shown, the information strategy of the Putin regime demonstrates characteristics which can be interpreted through the lenses both of constructivism and neoclassical realism, which via their respective focuses on political identity and grand strategy, have been shown to be complementary (Becker et al. 2016: 117)

This paper will argue that the link between information and national security has sparked a paradigmatic effort on the part of the Putin regime to control the flow of information in the Russian Federation. This conclusion will be predicated upon a discourse analysis of two information security doctrines, one originally published in September 2000 and a revised version published in December 2016. The Putin regime's objectives of publishing these documents are as follows:

1) to outline current issues and vulnerabilities in the domestic information sphere;
2) give measures to be undertaken at the state level in order to remedy them;
3) outline the structural implications of the information age for global order;
4) provide information on preventing psychological attacks on the mass consciousness of society; and
5) assert restrictions on the freedom of information particularly in the media domain,

> "*for the sake of social development, the consolidation of Russian society, and the spiritual rebirth of the multinational people of the Russian Federation."*[1]

The discourse that emerges from these texts reveals what role strategic information control has to play in the grand strategy of the Putin regime to help Russia to re-emerge on the international stage as a great world power. In order to explore the implications of this discourse, this paper proposes the following research question as the basis for analysis:

> *What do the 2000 and 2016 editions of the Information Security Doctrine of the Russian Federation reveal about the dynamic between information, the individual and the State in Russia under the Putin regime?*

In order answer this question, the two editions will be subject to the qualitative research method of discourse analysis, looking in detail at how the language of these documents reflects established legislative and societal norms in Russia, and by tracking how ideas regarding information have altered discourse over time in response to crucial events. The analysis will eventually reveal how the practices of information control on the part of the Putin regime have coalesced in a strengthening of the authoritarian aspects of the regime, a relationship between the public and news sources based on trust, rather than truth, and a growing inclination towards isolationism in the regime's approach to international relations.

1. Literature Review

To support the subject of this paper's analysis, background research in the relevant academic areas has been selected for its relevance to two interrelated questions: firstly, how has the rapid development of information technology in the 20th and 21st century affected the social, political and economic framework of European societies, and consequently, to what extent has the Putin regime embraced such fundamental changes to the international system? *Informationalization* will be shown to be an era-defining phenomenon predicated upon a trivector paradigm of market capitalism, globalization and communications technology, revolutionising paradigms of social interaction and peer-to-peer relationships through "*Networkisation*" (Rončević & Tomšič 2017: 12).

On the social level, informationalization has also had its effect on conceptions of identity: on the basis of Anderson's (2006) contention that the dissemination of *printed* media was instrumental to the rise of national identities (77), the internet's ability to disseminate *mass* media has bolstered the

[1]'Information Security Doctrine of the Russian Federation, Approved by President of the Russian Federation Vladimir Putin on September 9, 2000', Available from: https://goo.gl/Fb5s8q, [Accessed 27.06.17]

value of individual identities. The internet tacitly enables the departure from the nationalist notion of an *imagined* community, for a model of identification with *digital* communities, whose "artificially arranged collective subjectivity" emulates communitarian social principles but with greater freedom of ideological plurality (Syuntyurenko 2015: 208). On the other hand, for the Putin regime, *informationalization* poses two threats: on a domestic level, Putin's thinly veiled authoritarianism and control of the mass media are waning due to the internet's facilitation of a "glasnost 2.0" (Gorham 2014: 171); and on the international stage, Russia's counter-hegemonic agenda and neoclassical realist conception of the international system is being translated into battle for ideological influence via soft power (Becker et. al 2016: 115-116).

1.1. Informational Societies

Nye (1999) describes the international political climate of "the information age" as one characterized by the erosion of sovereignty, the growing irrelevance of classical realism as a prescriptive theory of International Relations, and the rising importance of soft power in determining the structure of the international system (25-30). No longer could states be conceptualized from the within the framework of classical realism as "billiard balls bouncing off one another," (Nye 1999: 25) as the rise of global capitalism and globalization defined the international power structure in economic terms, "deepening the capitalist logic of profit-seeking in capital-labor relationships" and "marshalling the State's support for productivity gains and competitiveness of national economies" (Castells 2000a: 19). The revolutionary developments in technology at the turn of the millennium were integral to the rise of global capitalism by enabling flexible management, professional communication networks and reducing the cost and duration of transactions (Castells 2000a: 19). It is this connection between technology and capitalism that, for Castells (2000a), underpins the definition of an 'informational' society:

> "the term 'informational' indicates the attribute of a specific form of social organization in which information generation, processing and transmission become the fundamental sources of productivity and power because of new technological conditions emerging in this historic period." (21)

Informational societies channel the capitalist logic of profit maximization by instrumentalizing information communication and locating areas in which efficacy and efficiency can be improved. In the time since these initial analyses of informational societies, there has been a deepening and widening in the application of this logic. Fukuyama (2016) argues that the manner in which information communication has enhanced capitalist practices in the private sector is analogous to

the shift in methods of governance towards outsourcing to external organizations in order to contend with the complexities of modern living (95-6). Relationships are now defined by their relative position in a network of both social and political organizations, enabling simultaneously, for Rončević & Tomšič (2017), the existence of a "heterogeneity of institutional forms and practices" (9) and the "decentralization and fragmentation of the State" (13).

With regard to the capacity for the individual to participate in society, networked societies as such have both positive and negative connotations. While decentralization and enhanced communication structures have the advantage of "allow[ing] the horizontal communication between people and organisations with the purpose of sharing information, organizing, mobilizing or providing support" (Cepoi 2017: 141), heterogeneity, pluralistic identities and negative media coverage have established a culture of the self-assertion of legitimacy and of low political, interpersonal and generalized trust (Castells 2000a: 3; Cepoi 2017: 135-6). This dissolution and decentralization of power may point to a structural development of informational society that transcends Foucault's (1980) contention that power exists "in a whole series of power networks" to which the State is exogenous, standing in a "superstructural" position (122). While power is still networked, decentralization has diminished the State's capacity to stand outside the structure and be an agent of so-called "meta power," (ibid) holding instead a position of power relative to that of other actors within the same network.

1.2. The Internet and Identity

The collapse of the Soviet Union famously entailed Russia's political and economic transition respectively to democracy and to market capitalism. A less evident transition, contends Castells (2000a), was the ideological transition from *statism* - "oriented (...) toward increasing the military and ideological capacity of the political apparatus for imposing its goals on a greater number of subjects and at deeper levels of their consciousness" (16) - back to *nationalism* "as the only source of meaning after the crumbling of the historically fragile *sovetskii narod* (Soviet people)." (24)

However, argues Gerrits (2014), despite military intervention in Chechnya at the time of Putin's first election in 2000 having "many of the characteristics of a nationalist conflict and war," nationalism in Russia is largely a concerted effort on the part of the Putin regime to bolster its popularity and assert its legitimacy (97). Due in part to the traditional Russian conception of national identity based upon citizens (*Rossiiskie)* rather than ethnic Russians (*Russkie*), and in part to the ideological vulnerability of incipient democracies to the 'marketplace' of ideas, *national* identity as a phenomenon in Russia is revisionist, fluid and susceptible to manipulation (ibid: 98-9; Snyder & Ballentine 1996: 6). In returning focus to the *Russkie*, the Putin regime has instrumentalized its own brand of national

identity as a boon to asserting its own political legitimacy, by emphasizing its commitment to self-proclaimed 'Russian' values.

As a window onto multitudinous definitions of identity, argues Golob (2017), the Internet is providing Russians with a worldview that goes beyond that of the parochial nationalism being touted by the Putin regime:

> "The massive flow of information erodes traditional role-sets in identity constructions to a certain extent, as exposure to cultural influences from disparate parts of the world unavoidably cause the transformation of rooted images of the social reality." (198)

Taking the constructivist position that the ideas that underpin political mobilization are socially constructed and therefore subject to interrogation (Barnett 2014: 158), the Internet has provided a platform for conflicting identities by providing individuals with the power to voice their personal views and easily form communities based on these views (Marshall et al. 2015: 23). Consequently, this process emulates what Golob (2017) defines as "social embeddedness": the extent to which a person considers themselves integrated into a certain community and that which "determines social imperatives defined by social structure, which provides the reproduction of social systems." (200) However, the sheer volume of information available on the internet indicates that online communities are themselves ideologically parochial, "marked by allegiance to particular sources of information, to particular modes of problem perception and solution, and to particular ways of disregarding information, simplifying information and making sense of the world." (Marshall et al. 2015: 23) In Russia, these "loosely imagined communities not tied to a nation" (ibid) have been crucial to fostering opposition in the authoritarian political climate of the Putin regime, taking advantage of Web 2.0 platforms such as blogs, social media and crowdsourcing websites to provoke political mobilization and provide an alternative communal identity to the nationalistic one being touted by Putin (Gorham 2014: 172).

1.3. The Kremlin and the technology industry

Multiple scholars have noted that Russia's approach to adapting to the requirements of the information age has been looking simultaneously forward (toward technological and socio-economic development) and backward toward Soviet-era surveillance and an isolationist attitude towards interstate technological rivalry (Castells 2000b: 2; Trenin 2009: 64-5; Sakwa 2008a: 138). Retaining Soviet State-centric programs of research and development, financial investment and government secrecy, Russia's capacity for technological development was stunted in the 1990s:

> "The lack of interaction between basic science, applied research, and industrial production led to extreme rigidity in the production system, to the absence of experimentation in scientific discoveries, and to a narrow application of specific technologies for limited uses, precisely at the moment when advancement in information technologies was predicated on constant interaction between different technological fields on the basis of their communication via computer networks." (Castells 2000b: 32)

Soviet practices of surveillance, censorship and government interests in the private sector were also applied to the commercial internet in the 1990s. Internet Service Providers (ISPs) were required to allow the FSB to install devices on their servers that would monitor internet traffic, (Gvosdev 2012: 178; Mejias & Vokuev 2017: 6) and by 2000, the largest ISP commercially available, *Relcom,* was entirely government-owned, "enjoy[ing] a near-monopoly in the market." (Alexander 2004: 611)

While the UN special rapporteur has emphasised that "there should be as little restriction as possible to the flow of information on the Internet," (*UN General Assembly* 2011: 6) the media and its relationship with the government has historically been a contentious issue in Russia. Alexander (2004) characterizes Russia's media environment to be "post-totalitarian": one in which the government "is forced to allow some freedoms in the public and private space, while leaders maintain power and political control through undemocratic means that exclude blunt propaganda, censorship and terror." (624) Albeit inherently controversial, several scholars have posited similar explanations of the subversive practices of the Putin regime in cyberspace, promoting internet access while simultaneously obfuscating and undermining its information-delivery capabilities by "polluting" the information environment with direct and indirect propaganda (Alexander 2004: 624; White 2016: 1; Gvosdev, 2012: 182; Valeriano & Maness, 2012: 146; Thomas 2014: 107). In the words of Gorham (2014), the tacit "glasnost 2.0" evoked by the innovation of the internet is continually under threat from the prohibitive practices of the regime's "cyber curtain." (189)

1.4. Foreign policy

There appears to be a lively scholarly debate regarding the character of the Putin regime's approach to foreign policy. While Oldberg (2007) frames Russian foreign policy in zero-sum conceptions of classical realism - "not content with its present position and wants to improve it at the expense of other states and to recover lost ground" (27) - Tsygankov (2012) argues that this approach oversimplifies Russian attitudes and is indicative of a trend to essentialize Russian behaviour as "authoritarian at heart and expansionist by habit." (698) Furthermore, taking a constructivist perspective, Tsygankov argues that such a designation may be seen as an act of provocation by

foreign actors and may contribute towards the rise of populist political movements in further exacerbating its already strained relations with the West (704). Controversial[2] author Richard Sakwa (2008b) frames the approach of the Putin regime in terms of a neorealist balance between sovereign autonomy and integration in the international system. However, this approach relies heavily on structural constraints and does not account for the concept of a grand strategy in order to transcend them (Lamy 2014: 128). A more convincing theory postulated by Becker et al. (2016) enshrines the foreign policy of the Putin regime in neoclassical realism, "encompassing not only military choices, but the means and ends of politics, economics, and ideology, and all aspects of power and influence at a statesman's disposal to enhance a nation's long-term interests." (117) The grand strategy of the Putin regime is to re-emerge on the world stage as a global superpower (Kanet 2007: 3) through the "strategic use of norms and selective appeals to international standards [as] merely tools to pursue state interests in today's international arena" (Becker et al. 2016: 118). One such example of this strategy can be found in the framing of Russia's annexation of Crimea and circumvention of the 1994 Budapest Memorandum. This treaty should have compelled Russia "to respect the Independence and Sovereignty and the *existing* borders of Ukraine,"[3] (*UN General Assembly* 1994) however, by framing the annexation as analogous to the protective agenda of the UN's own *Responsibility to Protect* doctrine, Putin asserted that "the Russian population in Crimea was under direct threat from the "fascists" who had engineered the 'coup' in Kyiv and therefore needed protecting" (Motyl 2015: 82).

This strategy also includes the strategic dissemination of information via news media in order to achieve particular objectives through information warfare. Yablokov (2015) argues that State-owned international news media outlets such as *Russia Today* (*RT*) were established to counter negative Western conceptions of Russian foreign policy, providing "a satisfactory 'Russian' interpretation" of its actions. (305) Yablokov argues that *RT* uses populist rhetoric in order to convert conspiracy theories into genuine articles of news, disseminate State propaganda, and pursue a political agenda based on 'public diplomacy': "a way of engaging foreign individuals, communities and governments in support of national objectives and foreign policies of an international actor stimulated by the development of global communication." (302-4) Public diplomacy is a strategy of aligning domestic public discourse with political strategy by means of influence, however, the embellishment of the facts and inclination toward sensationalism implicit in the practices of *RT* undermine the true political power of the news media. (ibid: 309)

[2] *see* Kuzio (2016)
[3] emphasis added

1.5. Hybrid Warfare

The language of Russia's 2014 military doctrine reflects the global shift in military strategy away from Clausewitzian norms of armed conflict and toward multivector or "hybrid" methods of warfare, integrating "political, economic, informational or other non-military measures implemented with a wide use of the protest potential of the population and of special operations forces" (*The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland* 2014). Using asymmetric tactics of warfare, success can still be garnered by a weaker adversary through the use of "sabotage, diversionary tactics, disinformation, state terror, manipulation [and] aggressive propaganda," (Darczewska 2015: 7) putting pressure on local populations to challenge the integrity of their own political systems and essentially destabilizing societies from the inside-out. Following Berzins' (2014) contention that "the Russian view of modern warfare is based on the idea that the main battlespace is the mind," (5) scholars have expounded the psychological methods that underpin Russian hybrid warfare strategy. For example, Armistead (2004) analogises the process of strategic information dissemination in target populations as akin to a computer virus, clandestinely affecting processes of mental logic and vicariously channelling the political will of adversarial States (196). Furthermore, academic research has not just looked at *what* is being disseminated, but *how* information can be "weaponized" (Yablokov 2015: 305) and *why* recurrent exposure to certain pieces of information helps to shape social reality. Studies of broadcast media and cognitive behaviourism since the 1960s have coalesced into paradigmatic approaches to identifying the effects of media upon shaping perceptions of social reality: 'cultivation theory' stipulates that

> "living in a symbolic environment in which certain types of institutions with certain types of objectives create certain types of messages, tends to cultivate (support, sustain, and nourish) certain types of collective consciousness." (Morgan & Shanahan 2010: 338-9)

In Russia, where as stated above government propaganda is disseminated via state-owned media institutions, the government has considerable power in shaping social reality and public opinion through the dissemination of ideas cultivated by information technology.

The goal of the informational aspect of hybrid warfare strategies is the psychological implementation of *reflexive control* over an adversary, "a means of conveying to a partner or an opponent special prepared information to incline that person to voluntarily make the predetermined decision desired by the initiator of the action." (Armistead 2004: 197). Thornton (2015) elaborates upon Armistead's definition of *reflexive control*, outlining how it can be used to incite defeatism in an adversary, either by passively persuading the adversary's government that invasion will in fact be beneficial to the

nation-state by bringing greater socio-economic prosperity for the indigenous population, or by asserting that opposition is futile and will lead to unimaginable destruction. (42)

1.6. Conclusion

Thomas (2014) posits that the overall strategy of Russian information warfare can be characterized as "playing catch up while limiting others," (128) reflecting both the inadequacy of the Russian information technology industry as proclaimed in both the 2000 and 2016 *Information Security Doctrine*s, and the regime's recent employment of "media endarkenment" techniques such as disinformation, simplification and embellishment (Lazitski 2013: 901). Furthermore, Information regarding some of the Putin regime's more controversial military actions, such as the Russian-Georgian conflict, the annexation of Crimea, and military occupation of Eastern Ukraine have shown increasing reliance on information-based hybrid tactics (Giles 2016: 2). In chapter 3, the content of the 2000 *Information Security Doctrine* will be compared to the practices of the Putin regime at this time, in order to visualize the initial stages of information warfare, with the overall objective of plotting the trajectory of the development of this practice.

2. Methodology

Discourse analysis offers a normative critique of social processes in order to track the origin and development of social and political norms, and then relate these norms to the structures or mechanisms that created and maintain them (Fairclough 2012: 9). Discourse exists on many levels: it can refer to the particular ways in which certain topics and themes are interwoven into political rhetoric, the collective perspective of reality constructed under the auspices of 'common sense', or it can be seen as the semiotic representation of cultural practices through language, events and material objects. The purpose of discourse is to find normative explanations for human behaviour, in the words of Milliken (1999),

> "discourses make intelligible some ways of being in, and acting towards, the world, and of operationalizing a particular 'regime of truth' while excluding other possible modes of identity and action." (229)

Related to government policy, discourse analysis offers an explanation for how structural mechanisms of power are constructed and maintained by forging a link between language and power, "because it is usually in language that discriminatory practices are enacted, in language that unequal relations of power are constituted and reproduced, and in language that social asymmetries may be challenged and transformed." (Blackledge 2012: 617) Language offers a 'point-of-entry' for

the analysis of relationships between various power structures, and gives insight into the belief structures of political actors that subsequently inform their actions (Larsen 2005).

Concrete events, such as the issuing of Russia's information security doctrines, become part of an intertextual process of analysis, taking into account physical data (such as demographic or economic data), public opinion analysis and discursive events, and identifying how these aspects reflect changing societal structures. The values implicit within the language of the doctrines will be compared to the rhetoric of relevant political actors, while contextualizing information will provide insight into how these values have been absorbed into popular discourse, both on the domestic Russian and international levels. One limitation of this approach is the "tendency to focus on the individual decision-maker" (Larsen 2005: 3) culminating in a failure to address discourse as an intersubjective phenomenon. However, given the central role of Putin in Kremlin affairs, and the central role of the Kremlin in forming popular discourse, the political rhetoric analysed offers prescriptive insight into the social reality within Russia. This will coalesce in a broad overview of the current discourse regarding information security in the Russian Federation and how it has emerged as the result of significant developments since Putin's first inauguration in May 2000.

3. Analysis: Information Security Doctrine of the Russian Federation 2000

The analysis of the 2000 *Information Security Doctrine* will be separated into six sections, the first of which will look at the structure, context and overall tone of the language used in the document, followed by five sections which will each focus upon one particular element that runs thematically throughout. Making reference to "the spiritual rebirth of the multinational people of the Russian Federation," (2)[4] the first theme to be analyzed will be ideology, concerning particularly the interests of the Putin regime in asserting patriotism as the underlying ideology of Russian national identity on both the domestic stage. Next, the doctrine's focus upon internal threats to "harmonious Russian information infrastructure" (2) will be analyzed in the context of the objectives of the Putin regime for domestic reform at the time of its publication. As stated above, international and domestic media are central to the information operations of the Putin regime, and thus the following section will analyse the *original* approach of the Putin regime to this domain. The following section will expand upon the conceptualization of the foreign policy of the Putin regime enshrined in neoclassical realism as put forward in Becker et al. (2016), by applying it to the aspects of the doctrine that refer to interstate interaction. Lastly, the stipulations regarding the governmental structure of the Putin regime will be analyzed, with particular focus on the centralized, vertical structure of government characteristic of the Putin regime.

3.1. Context/Structure

The hasty publishing of the doctrine - only 125 days after his first inauguration as President of the Russian Federation - reflects Putin's tacit prioritisation of information as a fundamental aspect, not only of national security, but of success itself. As described in Frye (2007), information has historically played a pivotal role in Russian (and, arguably, global) politics in the form of *kompromat* (compromising material): information that can be strategically divulged during elections at crucial moments in order to undermine and destabilise the support of political rivals (59). Unlike all other presidential candidates, Putin was selective about the media coverage he received, opting-out of debates with rivals and not giving rallies or speeches to which a base of opposition could have been constructed (Meyers 2015: 178). Instead, Putin gave a series of interviews with just three journalists in which he asserted the need for a strong State for economic prosperity and for protection from the

[4] 'Information Security Doctrine of the Russian Federation, Approved by President of the Russian Federation Vladimir Putin on September 9, 2000', Available from: https://goo.gl/Fb5s8q, [Accessed 27.06.17] (all further page references given in parentheses).

threat of fundamentalist Islam from Chechnya, (White 2001: 486) thus indirectly emphasising his own candidacy through respectively his experience as prime minister and his involvement in the second Chechen war. Furthermore, as the content analysis of media coverage of the elections presented in White et al. (2005) reveals, Putin received a considerable boost in popularity due to positive coverage on State media channels and also benefitted from the lack of mechanisms to suppress negative bias in the media against his opponents. (206-7)

The doctrine is structured around eleven chapters, stipulating the regulation, development and control of the information infrastructure of the Russian federation, including provisions for both domestic and transboundary information dissemination. Although covering several areas of information security, certain subjects are particularly prevalent throughout the document through their repetition: stemming the perceived flow of propaganda aimed at undermining the national image and global prestige of the Russian federation (15; 16; 23; 17); operating under the norms of fundamental human rights and asserting the constitutional rights of the individual (1; 2; 4; 9; 18); inadequate levels of staff and knowledge in the areas of government and information control (5; 11; 13; 22; 28; 29); streamlining the federal system and enhancing the centralized control of the government (10; 11; 15; 31); and asserting a commitment to 'openness' in the execution of all functions of state organs (3; 15; 16; 20; 26). The pertinence of the latter is particularly emphasised by the publishing of the doctrine on the Kremlin website both in Russian and English-language formats, implying an openness not just to the domestic public but to other States as well.

Overall, the general tone of the doctrine conceptualized Russia's entry into the new millennium in overtly bleak terms: threats are referred to explicitly 46 times throughout the document and many more times euphemistically, giving an impression of insecurity and generalized distrust. By framing Russian interests, infrastructure and national security in such bleak terms, the doctrine reaffirms Putin's assertion that the Russian Federation could only achieve prosperity and that the human security of the Russian population could only be ensured through a strengthening of State power, symbolically represented by Putin himself. Furthermore, the assertion of threats and the assurance of "comprehensive security" - encompassing not only human security but dignity and human & civil rights (Rukavishnikov 2007: 65) - undergirded Putin's growing popularity despite polls indicating "widespread dissatisfaction with the government he headed." (Cassiday & Johnson 2010: 685) Such tactics are indicative of the initial stages of Putin's cult of personality, offering "psychological and emotional reassurance, a focus of stability and unity, in a world of uncertainties." (Rees 2004: 4)

3.2. Ideology

The first element of the information sphere in need of protection as stipulated by the doctrine are the "national interests" of the Russian federation, comprising

> "observance of the constitutional rights and freedoms of man and the citizen to receive and use information, the assurance of a spiritual renewal of Russia, and the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country." (2)

In other words, the doctrine frames Russian *national* interests – those which are intrinsic to Russian national identity - as rights, information accessibility, spiritual renewal, morality, patriotism, humanism, culture and science. Despite being a Western movement, defining the national interest in such terms reflects American neoconservatism by its focus upon repairing moral degradation, reaffirming patriotism and protecting cultural matters (Dagger & Ball 2008). Furthermore, neoconservatism departs from conservative ideals of cultural homogeneity toward "the modern liberal ideal of cultural diversity, or multiculturalism—the principle of not only tolerating but also respecting different religions and cultures and encouraging them to coexist harmoniously," (Ibid) reflected in the doctrine's affirmation to commit to a "consolidation of Russian society, and the spiritual rebirth of the *multinational* people of the Russian federation"[5] (2). Neoconservatism's approach to religious fundamentalism is also reflected in the doctrine: 7 of the 8 explicit references to religion refer to the preclusion for religious groups to incite "hatred" or "strife", while the remainder asserts a commitment to "freedom of conscience, including the right freely to choose, possess and disseminate religious or other beliefs." (18) This implies an encouragement of the moral values implicit within religious practice for the betterment of social cohesion without such beliefs coalescing into societal conflict. The discursive shift towards neoconservatism - particularly in the area of religious fundamentalism - also carried the benefit of aligning the interests of the Putin regime with that of the Bush administration, enabling a rapprochement between Russia and the US on the basis of defence from international terrorism, reflected in a joint statement made by Bush and Putin in the wake of the September 11th attacks:

> "'We affirm our determination to meet the threats to peace in the 21st century. Among these threats are terrorism, the new horror of which was vividly demonstrated by the evil crimes of September 11, proliferation of weapons of mass destruction, militant nationalism,

[5] Emphasis added

> ethnic and religious intolerance, and regional instability. These threats endanger the security of both countries and the world at large. Dealing with these challenges calls for the creation of a new strategic framework to ensure the mutual security of the United States and Russia, and the world community." (*USDS Archive* 2001)

Rapprochement on the basis of ideological enmity and mutual strategic military interests would turn out to be short lived, however, as the winding down of the second Chechen war, talks regarding the installation of missile defence systems in Central and Eastern Europe and disagreements regarding US intervention in Afghanistan in 2003 returned US-Russian relations to a position of strain.

On the domestic level, the doctrine expounds a particular struggle for ideological influence upon the youth population of Russia, noting:

> "the inability of contemporary Russian civil society to ensure the formation in *the growing generation*, and maintenance of *socially required moral values, patriotism and civic responsibility* for the *destiny* of the country."[6] (19)

Aware of the multitudinous channels of communication open in the information age, and the potential for such "socially required" values to be eroded by unabated access to information, the doctrine stipulates the need for control of ideological influence upon the youth generation, for whom the term "destiny" indicates their symbolic existence as the future of the Russian Federation. The doctrine advocates for "civilized forms and methods for public control over the formation in society of spiritual values meeting the national interests of the country," (19) which has tacitly coalesced in the creation of patriotic youth groups such as the now defunct *Walking Together* and *Nashi* (*Newsru* 2005; Balmforth 2014) and currently in the politer form of *Project Network*. In 2015, the group channelled the Kremlin-friendly narrative concerning the Euromaidan movement in Ukraine in a video featuring young members from Kaliningrad describing the movement as a "coup", decrying the ousting of former president Viktor Yanukovich and defending the annexation of Crimea (Balmforth 2015). The subject of information control was also prevalent in the video, as one student evocatively states "you ask us to lift the information curtain. Let's do it together so that no one has any doubt" (ibid). *Network*'s self-proclaimed principles are anti-homosexual, pro-Putin and opposed to Anglo-saxon hegemony (*Project Network,* 'Principles'), while its 'spiritual' manifesto emphasises the link between the individual homelands of the Russian people spiritually communicated via the Russian language (*Project Network,* 'Spiritual Ties'). It can therefore be concluded that these groups help the Putin regime to channel the thought processes of impressionable youths away from what it sees to

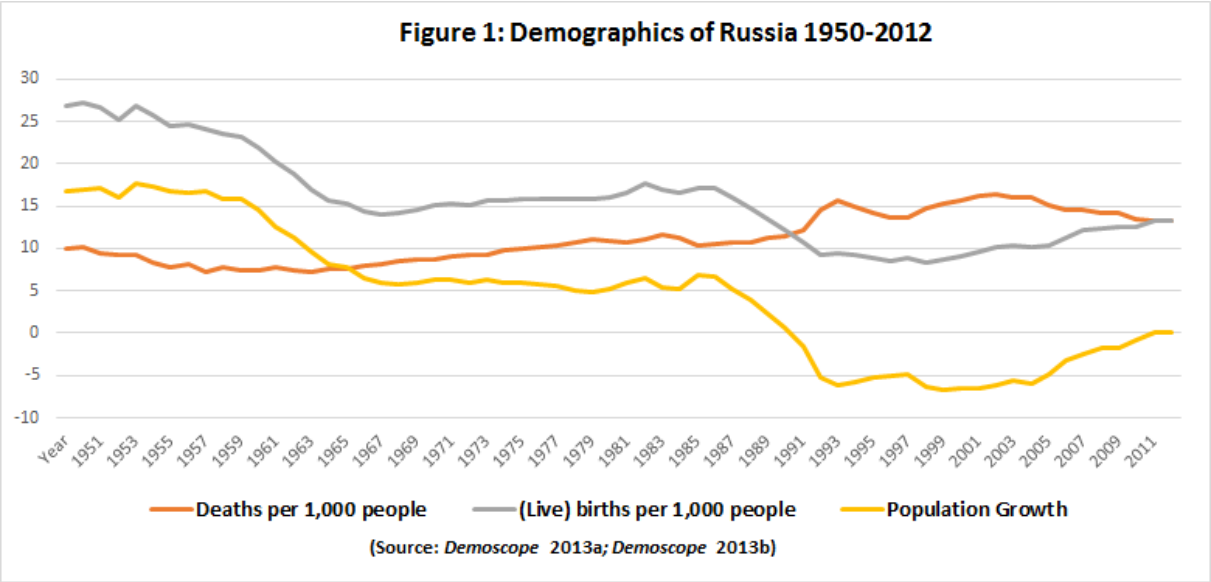
[6] Emphasis added

be socially deviant by imparting conservative social and political ideology aligned with that of the current regime. As the doctrine stipulates, the Putin regime believes in "constitutional restrictions on human and civil rights and freedoms in the interests of keeping up and strengthening the moral values of society, the freedoms of patriotism and humanism," (18) demonstrating an apparent preference for politically/socially acceptable ideology, a restriction on the right for the individual to cultivate their own beliefs, and a narrow allowance for ideological pluralism.

3.3. Internal Threats

On multiple occasions, the doctrine outlines weaknesses in the Russian information infrastructure as a result of insufficient human resources, either in the form of a lack of appropriate staff training regarding information security, (29; 28; 13; 11) personnel shortages, (5) and staff errors. (22) The doctrine blames these factors both on "the ousting from the domestic market of Russian producers of means of informatization, telecommunication and communication" and "an increase in the outflow of specialists and intellectual property rights holders going abroad" (6). However, there is a more prosaic explanation that undergirds this issue, namely the "demographic crisis that threatens to cut [Russia's] population by more than 15 percent by the middle of this century" (Trenin 2009: 72). In the early 2000s, Russia had not recovered from the drastic decline in population growth seen in the 1990s (see figure 1), and the percentage of working-age (16-59) individuals had stalled at 61.3% (Rosstat 2016: 80), while comparatively, the US - Russia's putative technological rival - had a working age population growing between 1990-2005 at average rate of 1.25% per year. (*FRED* 2017) This rivalry is further illustrated in the doctrine, which identifies as a threat:

> "the policy of western countries aimed at further destroying the unified techno-scientific space inherited from the USSR, of the member states of the Commonwealth of Independent States through refocusing onto western countries their scientific and technical ties as well as individual, most promising scientific collectives" (17).



Internal issues such as demographic decline, emigrating technical specialists and disparity concerning technological development compared with the West can be used to explain both the tone of insecurity implicit within the doctrine, and its repetitive assertion of Russia's technological underdevelopment compared to other developed nations (3; 8; 9; 21). The result of such inadequate internal development is the "intensive introduction of foreign information technologies in the areas of activity of the individual, society and the state," leaving the information infrastructure susceptible to the threat of "the information weapon," (9) the precise meaning of which is unclear. Armistead (2004) broadly defines this term as "a specially selected piece of information capable of causing changes in the processes of systems (physical, biological, social, informational) according to the intent of the entity using the weapon," capturing the highly abstract but also deeply disturbing connotations of the term. For example, compared with traditional offensive technology, an "information weapon" will attack its target with great precision and efficiency, whilst minimizing the potential for collateral damage and will thus send a "potent psychological message" about an adversary's far superior capability for warfare (Armistead 2004: 202). In another sense, an "information weapon" has the *influential* power to disrupt, as stated in the doctrine, "the principle of a balance of interests among citizens, society and the state in the information sphere", (28) ultimately undermining the societal cohesion of the State.

3.4. Media

The emergence in the 1990s of the first 24-hour news channels signalled a change in the dynamic between international media broadcasting and global politics. The rise in the accessibility of information inevitably demonstrated to policymakers how their actions were ever more under the watchful eye of global media (Ponce de Leon 2015). Furthermore, as the news channels with the

greatest amount of exposure concurrently had the greatest chance of reaching out and influencing global audiences, governments were obliged to incorporate news media coverage into foreign policy. (Yablokov 2015: 304; Ponce de Leon 2015: 199-200) Under the threat of foreign news agencies supplanting Russian news sources, the doctrine voices concerns regarding a potential "increase in dependence of the spiritual, economic and political areas of public life in Russia on foreign information entities" and a "monopolization of individual sectors or all of the Russian information market" (5). International 24-hour news broadcasts - the first of which being the US channel CNN - could not be subjected to the same Kremlin-friendly standards of self-censorship - what the doctrine terms "state guidance of state media activities" (29) - and therefore risked having the influence of foreign information undermining the Putin regime's 'regime of truth'. Unable to preclude the massive flow of information enabled by developments in telecommunications technology, the Putin regime had to identify which agencies it could trust and those which broadcasted narratives deemed unfriendly to Russian interests. As a general measure for ensuring information security, the doctrine stipulates "making more precise the *status* of foreign news agencies, media and journalists as well as of investors when attracting foreign investment for the development of Russia's information infrastructure,"[7] of which the use of the term "status" raises questions. The "status" of these news agencies and foreign investors could refer to political affiliation with adversarial or rival groups, or it could be referring to the extent to which these groups could be subject to the political pressure of the Putin regime to broadcast news articles aligned with their interests. By categorizing news sources as such, the Putin regime has framed certain news sources as reliable and others as adversarial, attempting to implement aforementioned "information weapons" in order to undermine the spiritual prestige of the Russian Federation, and can thus publicly relegate these sources to the domain of 'fake' news.

State control of the mass media, according to the doctrine, is in the interests of maintaining "a balance of interests among the individual, society and the state in the information sphere" (9) which ostensibly suggests that State restrictions on media freedom exist for the purposes of maintaining domestic societal cohesion. However, these Kremlin-friendly news reports are not limited to Russia's borders, but also spread to "communities for whom the Russian language is not the first language of daily communications but is the dominant language for acquiring information from TV, the internet and other media" (*NATO StratCom COE* 2014b: 10). The linguistic hegemony of the Russian language in the Russian near-abroad facilitates the dissemination of the Putin regime's particular angle on world events in these states. However, the encroachment of foreign news agencies upon the Russian information sphere warranted the creation of Russia's own international and English-language news

[7] Emphasis added

resource. The doctrine's stipulation for support to convey to the "international public *trustworthy* information about the state policy of the Russian Federation and about its official position on socially significant events in Russian and international life"[8] (3) manifested in the creation of *Russia Today* in 2005, funded by the Kremlin and headed by former-Kremlin pool reporter Margarita Simonyan (Evans 2005). The explicit goal of *Russia Today* is not to disseminate propaganda, but to establish a pluralistic global news media by offering "alternative perspectives on current affairs" and to "aquain[t] international audiences with a Russian viewpoint on major global events." (*RT,* 'About *RT')* In the context of the language of the doctrine, *Russia Today* illustrates the attempt by the Putin regime to establish a "trustworthy" source of information for both Russians and foreigners, hinting at implicit biases in the prevailing western-dominated mass media sphere.

3.5. Foreign Policy

The doctrine identifies two key threats evoked by the developments of information age to the domestic security of the Russian federation, namely "toughened international *competition* for technological and informational resources"; and the "increasing [of] the technological edge of leading world powers at *building up their capabilities to create the information weapon.*"[9] (25) With the largest information technology companies based in the US and with their former-Cold War allies in Japan and South Korea, it is not surprising that the doctrine frames the information technology development of the era in terms of 'competition'. This zero-sum conception of global technological development echoes the contention of Castells (2000a) about the dynamic relationship between technology and society:

> "the ability or inability of societies to master technology, and particularly technologies that are strategically decisive in each historical period, largely shapes their destiny." (7)

Taking development in the informational-technological domain as symbolic of state power therefore, the insecurities voiced in the doctrine represent the perception of structural weakness in the Russian Federation, opening vulnerabilities that could be exploited by other, more technologically advanced, states. This view is illustrated by the contention of former Marshal of the armoured troops General S. Bogdanov, regarding the role of information and technology during the first Gulf War:

> "Iraq lost the war before it even began. This was a war of intelligence, EW [Electronic Warfare], command and control, and counterintelligence. Iraqi troops were blinded and

[8] Emphasis added
[9] Emphasis added

> deafened (…) Modern war can be won by informatika and that is now vital for the U.S. and U.S.S.R." (*JP 3-13,* 1998: II:15)

Another foreign policy concern voiced in the doctrine is the crowding out of Russia from issues of global security, illustrated by its condemnation of "international relations based on unilateral solutions to key problems in world politics" and declaration of other states' propensity to "resis[t] the consolidation of Russia's role as one of the influential centers in an emerging multipolar world." (25) One source of this concern, arguably, was the conflict of interests between Russia and NATO regarding bombing campaigns during the 1999 Kosovo crisis, illustrated by the condemnation of Russia's permanent representative on the UNSC, Sergei Lavrov, of the "unilateral use of force against the sovereign Federal Republic of Yugoslavia - carried out in violation of the Charter of the United Nations and without the authorization of the Security Council." (*UNSC* 1999: 2) However, as some scholars have argued, there is a gap between Russian political rhetoric and political action regarding the crisis. Surovell (2012) openly accuses the Russian government of "duplicitous" (289) public relations strategies during the crisis, arguing that in order to appease "an enraged Russian public tired of [the then-President Boris Yeltsin's] pro-Western policies" (291) the leadership in Moscow "undertook a delicate balancing act, trying to appear firm on Kosovo while giving their wholehearted backing to their Western allies." (294). To support this hypothesis, Surovell describes events orchestrated in order to construct an *image* of Russian assertiveness during the crisis, such as Minister of Foreign Affairs Yevgeny Primakov's order to turn around a plane *en route* to Washington upon first hearing the news of NATO's bombing campaign despite having foreknowledge before take-off (296), or the "triumphant" dash by the Russian military for Pristina airport in Kosovo without NATO's authorization, when in fact "the West had deliberately allowed the Russian troops to enter Pristina in order to help burnish Yeltsin's 'anti-Western' image— especially given that the action had little political or military value." (299)

What emerges from this analysis is Russia's reticent position regarding the actions of the West and of western institutions in general during this time: unable to "take any action which might jeopardise the financial and economic support that [Russia] received from western countries and institutions such as the International Monetary Fund," (Latawski & Smith 2003: 98), the Kremlin instead focussed on how information regarding the crisis could be framed to the Russian public that minimized the appearance of marginalization or impotence. (*Idem*, p.92)

3.6. Government Structure

The doctrine frames the information sphere as a new space for potential danger and for the threat of invasion - either physical, psychological or informational - from malicious exogenous forces. Putin's presidential campaign assertion, that both Russian security and prosperity lies with a strengthening of state powers, is reflected in the structure of the doctrine, whose final pages describe the president's top-down control of the federal bodies responsible for ensuring information security (31). Putin's first presidential term was characterised by structural reform and centralization: the establishment of seven federal districts; reducing the political resources of regional heads; reforming regional constitutions to be aligned with the constitution of the Russian Federation; allowing the central government to intervene when a regional governor failed in his/her duties; and abolishing free public elections of regional administrative heads. (Zakharov 2007: 76) This is reflected in the doctrine's repeated stipulation for a "streamlining" of government institutions (10; 11; 15; 31) for the purposes of facilitating the flow of information between these bodies, while accelerating the state's response time to threats to information security. The overall objective of such structural reforms is the reassertion of state control over the information sphere, which the doctrine defines as a "system-forming factor of societal life [that] actively influences the state of the political, economic, defence, and other components of Russian Federation security," (1) hinting at its potential to undermine state authority and state power.

In order to maintain "the moral values of society," the doctrine prescribes "constitutional restrictions on human and civil rights and freedoms" (18) illustrating the aggressive, invasive and authoritarian method by which the state aims to achieve this control. However, such measures are framed in defensive terms, as attacks from so-called 'information weapons' have an impact upon the functioning of cohesive society as a whole, "setting in motion large masses of people experiencing psychic stress; and to a quick rise and spread of panic and commotion." (24-5) Framed in such bleak terms, the Putin regime has enacted control over freedom of speech as a protectionist measure that can only be provided by a strong, centralized and authoritarian government. However undemocratic its policies may be, the Putin regime stresses its commitment to Gorbachev-era norms of *glasnost*, repeatedly advocating for "openness" in realizing the functions of the federal bodies of state authority (3; 15; 16; 20; 26) giving the appearance of functioning democratic institutions, when in reality "the autonomy of these institutions and, therefore, their real capacity to influence the actions of the state will be severely limited" (Lipman & McFaul 2001: 116). Election reform, media control and restrictions on human rights devolve the politics of Russia to the level of pseudo-democracy,

while information control and Putin's "soft cult of personality" (Rukavishnikov 2007: 70) gives the *impression* to the public of real societal control over its politics.

4. Analysis: Information Security Doctrine of the Russian Federation 2016

In order to execute a comprehensive discourse analysis of the two doctrines, it is important to consider not only which themes have been developed in the 2016 doctrine from the original, but also which have essentially retained their content. The 2016 doctrine makes almost identical stipulations in terms of Russia's internal threats and its political and social ideology, while amendments have been made to its themes of foreign policy, government structure, and the media. As a result, this analysis will focus less explicitly on the themes of ideology and internal threats, and will instead feature a new section looking at the theme of cybersecurity. Although this theme was vaguely present in the original, it has received considerably more attention in the 2016 doctrine, warranting further attention. This is due largely to the developments in information technology that have subsequently expanded the scope for national security to be compromised via cyber means, and the growing attention this topic has received in terms of global and national security.

4.1. Context/Structure

The publication of the 2016 Information Security Doctrine followed period of great discrepancy in the narrative framing of world events by Russian and Western sources of information, the most prominent of which being the competing versions of events regarding Russia's annexation of the Crimean Peninsula in 2014, and the continuing military conflict in eastern Ukraine. After the Euromaidan demonstrations and the ousting of pro-Russian Ukrainian president Viktor Yanukovych in February 2014, Western news media sources framed the action as an embarrassing and infuriating loss for Russia's sphere of influence, as Ukraine seemed to gravitate towards the EU as a more viable economic and political partner (White 2014). On the other hand, the version of events provided by the Putin regime asserted that the movement was an illegal coup instigated by "[n]ationalists, neo-Nazis, Russophobes and anti-Semites" with the direct intention to infringe upon the rights of the Russian ethnic minority population living in Ukraine (Putin 2014a). The period of 2014-2016 was also characterized by the Putin regime's reticent position on the involvement of Russian soldiers violating Ukraine's territorial integrity, both on the Crimean Peninsula before its referendum voting in favour of joining the Russian Federation, and in eastern Ukraine. After originally asserting that "local self-defence forces" were responsible for taking over government buildings and military bases in Crimea (Chappel & Memmott 2014), Putin later appeared in a 2015 documentary appearing to praise the Russian military for their instrumentality during the crisis (*Russia24* 2015). A similar about-turn was

taken regarding the presence of Russian soldiers in eastern Ukraine: after initially asserting in April 2015 "outright and unequivocally that there are no Russian troops in Ukraine," (Putin 2015) Putin later contradicted this statement in a press conference in December of the same year by asserting that "[w]e never said there were not people there who carried out certain tasks including in the military sphere" (Walker 2015a). These practices are indicative of the Kremlin's strategic regime of information control, designed to provide alternate interpretations of world events which cast Russian actions in a positive light while simultaneously undermining the veracity of global news media through the deliberate dissemination of untruths.

Another significant contextualizing event during this period was Putin's declaration that 2014 would be Russia's 'year of culture': "a year of enlightenment, emphasis on our cultural roots, patriotism, values and ethics" (Putin 2013a). This move reflects a deepening of the efforts of the Putin regime to reinforce Russian national identity and emphasise Russia's status as a great civilization, encouraging the view that the regime leads Russia's spiritual renewal and helping to align public opinion with the actions of the regime (*The Moscow Times* 2017).

At less than half the length of the 2000 *Information Security Doctrine*, yet retaining most of its stipulations, the 2016 doctrine is essentially a boiled-down revision of the original. Once again, the 2016 doctrine envisions international relations in bleak terms by explicitly referring to "threats" 46 times, making it the 11th most frequently used word in the document.

4.2. Foreign Policy

While the 2000 doctrine emphasises the threat that information operations pose to its own territory, the 2016 doctrine extends this threat to Russia's allies, international peace, and global and regional security. "[C]ertain States and organizations" are accused of performing "actions inconsistent with international law," implying the existence of aggressive and malevolent adversaries "seek[ing] to undermine the sovereignty, political and social stability and territorial integrity" of other States (15)[10]. The lambasting of these 'certain' states is putatively directed at Western states, to whom Putin has employed similar rhetoric to describe:

> "Our western partners, led by the United States of America, prefer not to be guided by international law in their practical policies, but by the rule of the gun." (Putin 2014a)

[10] The 2016 lacks page numbers, thus citations are given referencing paragraph number and subsection (if applicable).

By establishing a discourse that frames the US-led West as arbitrarily following international law in the pursuit and maintenance of its own hegemonic power, the Putin regime has set about establishing its own norms of international relations based upon the strategic dissemination of ideas, (Roberts 2017: 50 55) such as the discourse regarding ethnic and national identities used to justify actions in Crimea, as discussed above. Putin has emphasised that "the desire for independence and sovereignty in spiritual, ideological and foreign policy spheres is an integral part of [Russian] national character," (Putin 2013b) encapsulating the perception of the threat of invasion not only in a physical sense, but from psychological pressures and from the loss of strategic influence. The expansion of NATO into the Baltic states, and the US support of 'colour' revolutions in Georgia and Ukraine, contends Oldberg (2007), were seen as Western interference in Russia's sphere of influence, (20-21) and engages with the 2016 doctrine's addition of "information sovereignty" (8; e) as an aspect of Russian national interests. This battle for influence came to a head during the 2008 Russo Georgian war, where over the previous decade, the US had provided $1.2 billion in aid to Georgia and deployed its own military advisors, "which the Kremlin saw as evidence of America's bias and lack of recognition of Russia's role in the region" (Tsygankov 2012: 708). It has been inferred by scholars that conflict in Georgia encouraged Russia to become more offensive in its foreign policy, both in terms of using "international broadcasting as a way of influencing public attitudes on the global scale" (Yablokov 2015: 303) and by creating "a military that would be a much more effective lever of Russian power on the international stage" (Thornton 2015: 40-1). Both of these tactics shared the common aim of boosting Russia's image as both a significant world player and as an essential provider of security, achieved through the implementation of a modern strategy of warfare outlined in Russian Chief of Staff Valery Gerasimov's 2013 article in *Military Industrial Courier*. The so called 'Gerasimov Doctrine' outlines a multivector model of "non military means" enacted simultaneously to evince the capitulation of an adversary:

> "The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures — *applied in coordination with the protest potential of the population*"[11] (Gerasimov 2013).

This hybrid strategy is designed to have a profound effect on the psychology of the mass consciousness of society, using subversive tactics to obfuscate the state of war while simultaneously using "protest potential" to turn populations against their own governments. The mixture of informational, psychological and military tactics coalesces in a formidable demonstration of power

[11] Emphasis added

on the part of the belligerent, while limiting the potential for images of violence and conflict to come under the scrutiny of international media. The execution of the Gerasimov doctrine led to success for Russia in its annexation of Crimea, where "in just three weeks, and without a shot being fired, the morale of the Ukrainian military was broken and all of their 190 bases had surrendered," (Berzins 2014: 4) sending a potent message about Russia's renewed military capabilities and its influential significance in the region to its Western opposition.

4.3. Media

The rise of social media has enabled the individual direct access to discourse reflecting the thoughts and opinions of the collective consciousness of society as a whole (Mejias & Vokuev 2017). While state-owned media outlets have been instrumental in shaping perceptions of social reality in Russia, social media's ability to transform the individual into a vector of information dissemination undermines the Putin regime's monopolistic influential control in the information sphere. This is reflected in the 2016 doctrine's description of the regime's commitment to "*countervailing* information and psychological actions, including those aimed at undermining the historical foundations and patriotic traditions related to defending the homeland" (21; e) and "*neutralizing* the information impact intended to erode Russia's traditional moral and spiritual values" (23; j).[12] This use of language frames the activity of the Putin regime in the information sphere in defensive terms: 'countervailing' and 'neutralizing' imply actions undertaken with the objective of achieving strategic deterrence, which in itself is paradoxical as it requires a clear conception of an adversary and their respective capabilities. However, given the decentralized structure of the internet and under the doctrine's self-proclaimed commitment to freedoms of speech, how exactly does the Putin regime aim to counter anti-Russian sentiment from being published?

Recent evidence has surfaced which indicates the existence of clandestine government activity on the internet designed to counter and outbalance Russia-negative opinions and information resources with representations of opinion aligned with the interests of the regime. Various Western news sources have reported upon the existence of so-called 'troll-factories', where government-funded individuals emulate ordinary citizens in online communities, disseminating information that reflects a pro-Russian and pro-government stance, with the ultimate objective of fabricating popular discourse and swaying public opinion in favour of government activity (Seddon 2014; Walker 2015b; Gregory 2014). According to an interview conducted by *The Guardian* newspaper with a former employee of one of the Putin regime's troll factories, each employee would maintain several fake accounts on

[12] Emphases added

social media, and would be instructed to post specific pieces of propaganda interspersed with seemingly ordinary social media behaviour in order to seem genuine:

> "We had to write 'ordinary posts', about making cakes or music tracks we liked, but then every now and then throw in a political post about how the Kiev government is fascist, or that sort of thing." (Walker 2015b)

The 2016 doctrine stipulates the development of "a national system of the Russian Internet segment management" (29; e) as a future provision for information security, however, until this level of control has been achieved, we are likely to see the Putin regime continue "to promote Internet access and ISP proliferation, and then use the Internet for direct and indirect propaganda" (Alexander 2004: 624). Similar to its position on foreign media sources, speculation regarding the existence of fabricated information being purposefully disseminated on the internet also helps the Putin regime to achieve the goal of undermining the veracity of the internet as a source of accurate information, thus inciting individuals to look to other, more Kremlin-friendly sources for reliable information.

4.4. Cybersecurity

A prevalent theme of both the 2000 and 2016 doctrines is the growing threat of critical infrastructure coming under attack via cyber-enabled means. While this topic's presence in the 2000 doctrine may have been in response to cybernetic attacks designed to temporarily shut down computer systems using viruses or Distributed Denial of Service (DDoS) attacks - which "may not have the shock value that a conventional physical attack may demonstrate" (Valeriano & Maness 2012: 154) - the 2016 doctrine was published under the context of more sophisticated level of cyber-enabled attack, capable of inflicting physical damage upon critical infrastructure. Between late 2009 and early 2010, speculation arose regarding the possibility that an Iranian uranium enrichment facility had sustained critical damage as the result of a computer worm of purported Israeli origin, whose "unusual sophistication…. prompted speculation that it is the work of a well-financed team working for a nation state, rather than a group of rogue hackers" (*The Economist* 2010). While cyber-attacks have been employed by the Putin regime as hybrid warfare strategies to disrupt societal cohesion, limit the ability for governments to communicate during crises and put populations under psychological pressure, (Russell 2014) the threat of *physical* attacks on critical infrastructure is reflected in the language of the 2016 doctrine:

> "Information security in the sphere of State and social security is characterised by a continued increase in the complexity, scope, and coordination of computer attacks on objects of critical information infrastructure (…) as well as a growing risk that information technologies will be used to infringe on the sovereignty, territorial integrity, or political and social stability of the Russian Federation." (16)

Following the hypothesis posited in Thomas (2014) that the grand strategy of the Putin regime is characterized by "playing catch-up while limiting others," (128) it is reasonable to argue that the regime has been working on its own methods of executing physical attacks using cyber means. For example, in December 2015, after months of conflict between Russian and Ukrainian forces (Walker 2015), a large-scale cyber-attack was carried out on Ukraine's power grid network, causing power outages for more than 225,000 Ukrainian homes (Sanger 2016). Similar to the attack on Iran's nuclear enrichment facilities, the level of sophistication of the attack indicated a coordinated and strategically planned approach not typically associated with hacker groups or individuals, as one report emphasises:

> "the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronised, multi stage, multi site attack." (E-ISAC 2016: 5)

Although attribution for the attack could not definitively be given to the Putin regime, the outage demonstrated the capacity for computer-based technologies to affect pieces of critical infrastructure and the instrumentalization of cyber warfare to affect physical damage during an ongoing military conflict. Furthermore, the attack was ostensibly designed to send a political message, as cyber security expert Robert M. Lee contends, "[i]t was large enough to get everyone's attention and small enough not to prompt a major response," (Sanger 2016) emulating another crucial aspect of the information warfare strategy of the Putin regime, namely the obfuscation of the identity of seemingly politically-motivated attacks. By compromising a piece of critical infrastructure remotely, an actor can intimidate the political leaders of an adversary while remaining anonymous, using a hybrid strategy to evince capitulation via psychological pressure and enhancing the latter's sense of vulnerability. This shift in discourse concerning warfare is reflected in the language of former Russian military officers S.G. Chekinov and S.A Bogdanov's article *The Nature and Content of New-Generation War,* asserting that the "[r]emote engagement of the enemy 'at arm's length' is turning into the principal tactic to achieve the goals of a combat action or an operation." (S.G. Chekinov & S.A Bogdanov 2013: 12-3) These remote attacks also carry the benefit of obfuscating the provenance of

the attackers (a tactic similarly used by the Russian military during its occupation of Crimea) and thus enables the Putin regime to acquit themselves of culpability for attacks under the auspices of plausible deniability.

4.5. Government Structure

The language of the 2000 doctrine framed the role of the President in democratic terms, "direct[ing] within his constitutional remit national security agencies and forces," (31) tacitly avoiding authoritarian overtones by emphasising the institutional role of federal agencies. The 2016 doctrine, however, frames the President as the main determinant of the information security system, while the language reflects the veritably authoritarian nature of the Putin regime in describing one of its key objectives:

> "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." (6; a)[13]

The two emphasised phrases in the above passage, absent from the 2000 doctrine, are indicative of the Putin regime's shift away from an ostensibly democratic system of governance towards a hybrid regime with both democratic and authoritarian characteristics (Krastev & Holmes 2012: 33). The fact that the 2016 doctrine can refer to such a hybrid system of governance in explicit terms is surprising, given that the authoritarianism implicit in the Putin regime's system of "managed democracy" formed the basis of mass protests in opposition of Putin's re-election (Barry 2011). The self-proclaimed 'Power Vertical' system of governance implies that Putin has the final word on State activity, and "defines the regime of Russia as a system of faithfulness, loyalty and complete subordination to one person," (Laurinavičius 2016: 121) establishing Putin as the central symbol of the State. The regime's political survival, therefore, is intrinsically linked to the Putin's personal popularity, which dramatically rose from its level at the time of the so-called 'Snow Revolution,' to 86% at the time of the Crimean annexation in 2014 (see figure 1.1). What is responsible for this rise in popularity despite popular opposition against the Putin regime's inherent authoritarianism? One explanation arises from the analysis of Putin's populist rhetoric used in reference to the annexation, which channelled two discursive themes: firstly, Putin emphasised that the basis for Russian

[13] Emphasis added

intervention in Crimea was not out of an expansionist desire on the part of the regime, but evinced by the collective will of the Crimean population:

> "There was not a single armed confrontation in Crimea and no casualties. Why do you think this was so? The answer is simple: because it is very difficult, practically impossible to fight against the will of the people" (Putin 2014a).

Secondly, Putin employed a rhetoric of otherness in regards to Western states, envisioning Russia as a paragon of international law in opposition to a hypocritical West:

> "what do we hear from our colleagues in Western Europe and North America? They say we are violating norms of international law. Firstly, it's a good thing that they at least remember that there exists such a thing as international law – better late than never" (ibid).

Viewed from within the framework of neoclassical realism, these tactics form part of the Putin regime's grand strategy to use populism and the reframing of international legal norms to achieve geostrategic goals while simultaneously concealing the authoritarian nature of the regime (Becker et al. 2016). The success of this strategy can be measured by comparing data from public opinion surveys, which demonstrate that Putin's recent rise in personal popularity coincided with a growing negative sentiment among the public towards western states (see figures 2.1, 2.2, 2.3). The authoritarian nature of the Putin regime is enabled by coasting on Putin's personal popularity, which has been the subject of a rigorous public relations campaign designed to disseminate information to the public painting the president in a positive light (Walker 2014). This has seemingly enabled the Putin regime to maintain popularity in spite of its authoritarianism, demonstrated by the above quote from the 2016 doctrine, and other suspicious events such as the murder of opposition leader Boris Nemtsov in 2015 (*BBC News* 2015).

Figure 2.1

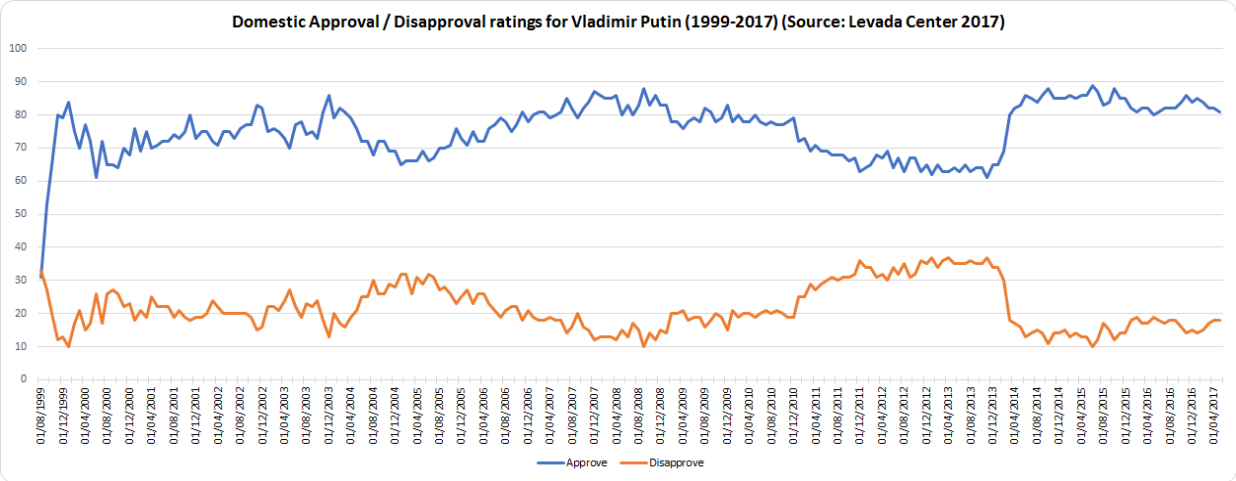


Figure 2.2

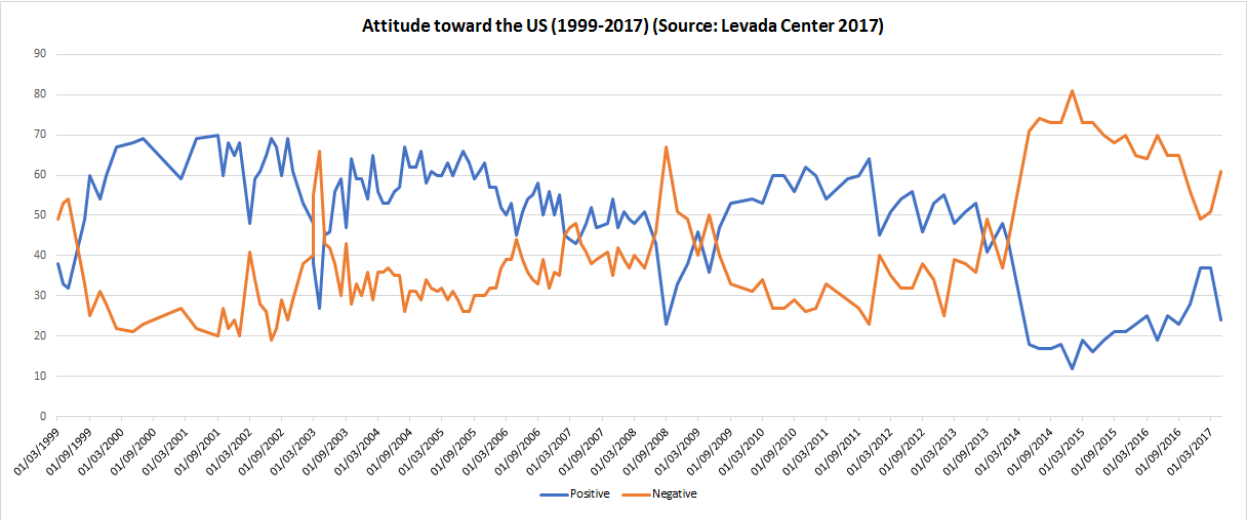
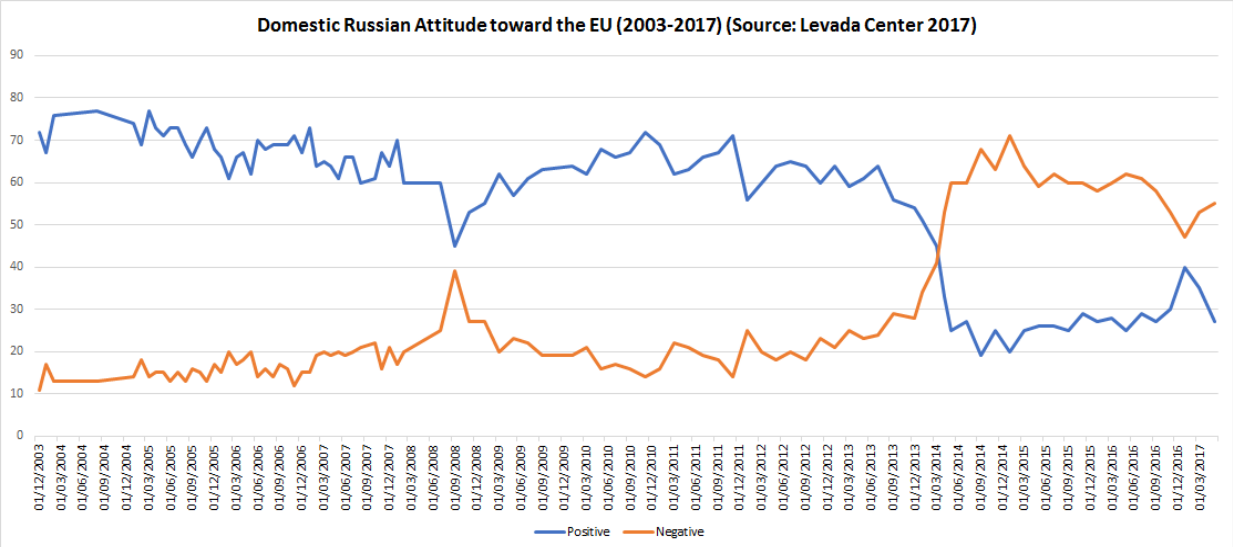


Figure 2.3



5. Analysis

This analysis has predominantly pursued a descriptive analysis of the themes included in the 2000 and 2016 drafts of *Russia's Information Security Doctrine*. Due to the structural limitations of this thesis, the analysis has not been exhaustive and instead has focused on extracts concerning particular instances where the language has been particularly indicative of discursive shifts relevant to the themes identified. A summary of findings can be found in the tables below:

5.1. Foreign Policy

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● Structure of international relations based upon "toughened international *competition* for technological and informational resources." ● The propensity of other States to "resis[t] the consolidation of Russia's role as one of the influential centers in an emerging multipolar world ● Foreign States developing the capacity to implement "information" weapons ● "international relations based on unilateral solutions to key problems in world politics."	● Information operations being perpetrated by "certain" States ● An increase in the utilisation of psychological tools for warfare ● An emphasis on protecting the sovereignty and territorial integrity of other states

The language used in the 2000 doctrine envisions Russia as a weak state with a negative image on the international stage, and characterizes international relations on the basis of inter-State rivalry. In the information age, information from a multitude of sources had the potential to disseminate ideas and instigate political mobilization, undermining the political authority of the ruling power. As a result, the Putin regime set out a discourse of the information space as a area of contestation, cultural invasion and vulnerability in its *Information Security Doctrine*, establishing the threat of malicious 'others' existing in the information space seeking to further undermine Russia's economic and spiritual re-emergence from its turbulent post-Soviet era. These 'others' are imagined as acting arbitrarily and self-interestedly on the global stage, acting "unilaterally" and therefore undermining the neoliberal ideals of international consensus and global peace. As

information began to become more and more available due to developments in information technology, the awareness of strategically disseminated information in order to psychologically affect individuals or groups has grown, increasing the use of *reflexive control (*Armistead 2004: 197; Thornton 2015: 42) in military operations. In the 2016 doctrine, information is framed as a foreign threat, reflective of the regime's insecurity of Russia being "politically encircled abroad and culturally colonized by Western values at home," (Galeotti & Bowen 2014: 18). The notion of foreign information being used to undermine sovereign state power is reflected in Putin's framing of the Arab Spring pro-democracy movement between 2010-2012, asserting that "[s]tandards were imposed on these nations that did not in any way correspond to their way of life, traditions, or these peoples' cultures. As a result, instead of democracy and freedom, there was chaos, outbreaks in violence and a series of upheavals." (Putin 2014a). For the regime, any foreign information has the potential to become politicized and therefore dangerous, justifying invasive government policy to ensure the security of sovereign boundaries in the information space.

5.2. Media

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● "An increase in dependence of the spiritual, economic and political areas of public life in Russia on foreign information entities" ● Implementing the "state guidance of state media activities" ● Establishing the "status" of foreign media agencies	● Preventing the "monopolization of individual sectors or all of the Russian information market." ● "*countervailing* information and psychological actions, including those aimed at undermining the historical foundations and patriotic traditions related to defending the homeland" ● "*neutralizing* the information impact intended to erode Russia's traditional moral and spiritual values."

The differences in the way media is referred to in the two doctrines reflects the growth of international news media and the spilling over of Western media giants into the information spheres of other States. While the 2000 doctrine warns of Russian news sources being crowded out of the national information space by international sources, the 2016 doctrine accuses foreign media

sources of publishing "an increasing number of materials containing biased assessments of State policy of the Russian Federation," (12) and asserts that the "Russian mass media often face blatant discrimination abroad" (ibid). This elevation in tone demonstrates the insecurity of the Putin regime regarding Russia's image abroad, and the perception of an information war being propagated against the Russian Federation by foreign states in order to undermine Russia's capacity for soft power. This siege mentality is reflected in a statement made by Margarita Simonyan, editor-in-chief of *RT*, in regards to defending Russia in the information space:

> "I can see very clearly why I continue to work for a channel that stands alone (!) face to face with thousands and tens of thousands of Western news outlets, showing everybody the other side of the story, under daily attacks from the media that it is hardly managing to fight back." (Simonyan 2014)

The 2000 doctrine framed the dependence on foreign news agencies as having the potential to undermine Russian societal cohesion, and thus stipulates the creation of a state-led Russian media to deliver information to the Russian population. However, the 2016 doctrine demonstrates that the objectives of Russia's information campaign have developed beyond the media of its own country, as actions in the media space of other countries are framed as threats that also need to be neutralized. While the 2000 doctrine introduced measures for domestic media control, the 2016 doctrine can be seen as an attempt to preclude unfavourable information from exogenous and non-government-friendly sources from affecting the public opinion of the Russian people. This is achieved by undermining its credibility through publicly lambasting foreign news agencies as instruments of international state governments, polluting the information space with deliberate untruths and establishing a pro-Kremlin movement on social media.

5.3. Internal Threats

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● "the ousting from the domestic market of Russian producers of means of informatization, telecommunication and communication." ● "the policy of western countries aimed at further destroying the unified techno-	● Sparsely mentioned. ● Russia's information technology industry as of 2013 generates 8.5% of Russia's GDP and 2.5% of its trade (Soldatov & Borogan 2015: 299).

scientific space inherited from the USSR, of the member states of the Commonwealth of Independent States through refocusing onto western countries their scientific and technical ties as well as individual, most promising scientific collectives." ● "insufficient legislative and normative regulation of the exchange of information in the law enforcement and judicial spheres."	

The 2000 doctrine introduced a plan to modernize Russia's information technology industry in order to make it more competitive on the global stage. On the internal level, Russia's underdeveloped technology industry posed a threat to its incipient market economy, given the significant global economic interest in this domain and its potential to attract foreign investment. This would also demonstrate an attempt to diversify Russia's economy, whose entry into the system of global capitalism was tarnished by the 1998 Russian financial crisis, itself partially a result of reliance on US oil prices and dependence of EU gas consumption trends (Rukavishnikov 2007: 62). It is significant to note that 'western' countries are only explicitly mentioned in the 2000 doctrine to describe their intentions as aimed toward "destroying the unified techno-scientific space inherited from the USSR", reflecting historical rivalry between the USSR and the West, reinvigorated in the post-Cold War era via competition in the information technology industry.

In the information age, information technology has become an instrument of foreign policy: dominance in the international market for information technology is framed as enhancing state capacity to disseminate socio-political ideology (among other pieces of information) and achieve influence via soft power, therefore foreign policy must adapt not only to cover physical human security in Russia, but psychological security from malicious foreign influences. Conceptualizing the objective of western states as the undermining of the stability of the Russian federation further reflects the Putin regime's populist tactic of using 'otherness' in order to assert its legitimacy, justify its authoritarian actions and align social reality with the norms set by the regime. Since 2000, the regime has had relative success in making its economy more diverse and in developing its IT industry, which, as of 2013, generates 8.5% of Russia's GDP and 2.5% of its trade (Soldatov & Borogan 2015: 299).

5.4. Cybersecurity

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● Receives little attention in the doctrine. ● Brief reference to the threat of "computer crime", specifying "networks of banks and other credit organizations" as principal targets	● "Information security in the sphere of State and social security is characterised by a continued increase in the complexity, scope, and coordination of computer attacks on objects of critical information infrastructure." ● "a growing risk that information technologies will be used to infringe on the sovereignty, territorial integrity, or political and social stability of the Russian Federation."

The treatment of cybersecurity in the two doctrines reflects global discourse regarding the potential for danger in integrating more and more technology into the infrastructure of society. The 2000 doctrine was written in an era where economic institutions and banks had benefitted the most from technological integration, demonstrating the emergence of a discourse regarding the potential for cyber-attacks to inflict damage to societal infrastructure and undermine social stability. Since the early 2000s, information technology has been integrated into more and more pieces of societal infrastructure - comprising the so-called 'Internet of Things' (IoT) - enhancing organizations and governmental institutions' ability to collect and access data, monitor significant developments and respond to major events, while also opening up the potential for such objects of infrastructure to become compromised at arm's length via cyber-attack. It is for this reason that events such as the cyber-attacks in Iran and Ukraine mentioned earlier have been particularly instrumental in contributing to a discourse that frames the deepening of information technology as a threat to global security. To paraphrase a quote from Castells (2000a) used earlier, a society's mastery of contemporary technology largely shapes its destiny, therefore, when viewed from within the framework of cybersecurity, exploiting vulnerabilities in a State's' information technology infrastructure is indicative of that State's weak capacity for self-determination and overall security. Furthermore, plausible deniability is implicit in the nature of cyber-attacks due to the difficulty in asserting the identity of online attackers, rendering the establishment of legal norms concerning online behaviour nebulous. Despite international law stipulating that states must not "allow

knowingly its territory to be used for acts contrary to the rights of other States," (International Court of Justice 1949: 22), the ubiquity of the internet and its empowerment of the individual to execute clandestine political activity renders the capacity for States to prevent non-State actors from causing diplomatic problems particularly difficult.

5.5. Government structure

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● "constitutional restrictions on human and civil rights and freedoms." ● "streamlining" of government institutions.	● "strengthening the vertical management system." ● "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."

As a platform for free communication without a central authority to govern it, the 'information sphere,' abstracted in a political sense, essentially exists under the condition of anarchy. State governments may implement certain restrictions on the commercial web, however, the ubiquity of 'personal' information technology devices capable of transferring information, along with the relative ease of concealing one's identity on the internet or bypassing government restrictions, mean that the government must employ aggressive tactics that invade the personal freedoms if they desire to fully control the information sphere. While the 2000 doctrine introduced some regulation establishing the relative powers of the State, the individual and organizations in the information sphere, the use of language of an explicitly authoritarian nature in the 2016 doctrine indicates that the Putin regime now desires to implement a system of top-down control on a putatively anarchical information sphere, "directly drawing on a classic Russian dichotomy between autocracy and anarchy" (Galeotti & Bowen 2014: 18). Furthermore, both doctrines frame the multitudinous sources of information made available by technological development as a threat to the 'spiritual renewal' of the Russian civilization, via its ability to spread socially deviant ideas and norms incompatible with the socially-accepted values implicit in Russian national identity. When viewed from within the neoclassical realist conception of the Putin regime postulated in Becker et al. (2016), information anarchy undermines the ideas-based public relations campaign that underpins the regime's grand strategy to

establish a global image as a strong and legitimate world power. By taking an active role in the production and propagation of popular political discourse, the Putin regime has been able to disseminate ideas with the objective of establishing societal norms aligned with the interests of the regime. Through authoritarianism, the Putin regime can strategically manipulate what is considered to be 'common-sense' knowledge in Russia, engaging with what Foucault (1980) describes as a "regime of truth" (133) through the dissemination of certain ideas and the marginalization of others.

5.6. Ideology

Information Security Doctrine 2000	***Information Security Doctrine 2016***
● The "consolidation of Russian society, and the spiritual rebirth of the *multinational* people of the Russian federation" framed as an objective. ● Stressing the individual's "freedom of conscience, including the right freely to choose, possess and disseminate religious or other beliefs." ● Developing in the youth of Russia "socially required moral values, patriotism and civic responsibility."	● "neutralizing the information impact intended to erode Russia's traditional moral and spiritual values." ● "Realization of national interests in the information sphere aims at shaping a safe environment for the circulation of reliable information, and an information infrastructure capable of resisting different kinds of impacts in order to guarantee constitutional human and civil rights and freedoms."

Although lacking any explicit reference to a particular political ideology, the 2000 doctrine still acts as a vehicle for disseminating ideas of Russia's self-perception, both domestically as a nation and globally as a State. Russia's "national interests" - poorly articulated and vaguely formulated under the Yeltsin regime (Rukavishnikov 2007: 54) - were redefined in terms of human and constitutional rights, moral values and a spiritual connection designed to bind the patchwork nationhood of Russia under one distinctive banner. The re-establishment of norms of national identity was incremental to the populist strategy of the Putin regime, averting the dangerous and confrontational nature of nationalistic ideology by applying it under the civic veneer of patriotism, a "banal, benign and fundamentally positive phenomenon, far removed from nationalism's more dangerous, atavistic or 'hot' manifestations" (Sutherland 2012: 74). The inclusion of language referring to national identity in an information security doctrine is significant, as this reflects how the rapidly expanding availability

of information was helping to spread ideas that undermined the very notion of a nation-state's potential for a homogenous collective identity with implicit values. To counter this, the Putin regime has pursued a conservative agenda in asserting Russian values, a political ideology which Putin asserts "prevents movement backward and downward, into chaotic darkness and a return to a primitive state" (Matthews 2014). The regime has attempted to construct a Russian identity in opposition to a morally decadent West, in order to foster popular support for the Putin regime's anti-Westernism, the so-called "vehicle by which Putin advances his personal power interests" (Roberts 2017:36).

Conclusion

Since Peter the Great, national image has historically played a significant role in determining Russian actions on the global stage, as Wohlforth (1998) contends, "Russia's rulers have taken risks, spilled their subjects' blood, and emptied Kremlin coffers for the honor, prestige, or reputation of the state" (22). Leading up to his election, the restoration Russian prestige on the global scale featured predominantly in Putin's rhetoric, albeit in bleak terms:

> "For the first time in the past 200-300 years, [Russia] is facing the real threat of slipping down to the second and possibly even third rank of world states." (Putin 1999)

Assuming the role of president in Russia's new democratic political climate, where the spilling of blood and the emptying of coffers would have served only to further denigrate Russia's image, Putin's strategy for restoration was instead predicated on the strategic control of information, the defining element of the global system at that time.

The 2000 draft of the Putin regime's *Information Security Doctrine* demonstrates the regime's shrewd and contemporary understanding of how interstate dynamics and social reality had been affected by the dawn of the information age, and its subsequent efforts to use the norms of the age to its advantage in the shape of policy formation. The doctrine identifies and proposes remedies to both internal and external threats to Russia's information infrastructure, asserting a model for control in the information space. The language of the 2016 *Information Security Doctrine* reflects themes of political discourse pertinent to the Putin regime during Putin's third term as President, most prominently: a bleak perspective on international relations; a coordinated campaign of strategic disinformation; a reassertion of the civilizational greatness of the Russian identity; and a political ideology enshrined in conservatism. The doctrine frames these themes in defensive terms, which implies that the protection of the ethnic Russian civilization from immoral and malevolent

outside forces is a prerogative of the Putin regime. The doctrine frames information as a political tool that governs interstate relations, forms part of military strategy and has the potential to incite societal chaos due to mass psychological pressure. As a result, information as a concept is envisioned as inherently political, and grants actors the ability to achieve geostrategic goals - such as the undermining of social stability or political legitimacy - at an arm's length.

While information as a concept may comprise the strategy of the Putin regime, the *grand* strategy of the regime is to interact with the structure of the international system in such a way that asserts power while limiting such interactions from attracting global attention. Under the guise of modern-day conservatism, the Putin regime and its authoritarian agenda have slowly eroded away the public's right to freedom of expression, while Putin's "soft cult of personality" (Rukavishnikov 2007: 70) has secured political legitimacy at the domestic level. Today, modern information technology enables ideas to be shared across borders and between groups or individuals at an unprecedented rate. The way in which ideas affect a person's decision-making (or rather how these ideas are framed in order to pursue a particular psychological objective) invites a constructivist analysis of how States – no longer the principal sources of world knowledge - exert power through public relations (PR) campaigns. The analysis presented here has focused upon how Russia specifically has used PR to mitigate the effects of Russia's entry into the information age, mostly because the publishing of the two information security doctrines and because of the relapse of authoritarianism that characterizes the Putin regime. That is not to say, however, that affecting the public consciousness by strategic information dissemination and PR campaigns is not a practice of liberal States, and similar analyses of information control in these States would inform constructivist approaches to International Relations.

As a final note, the Putin regime has been eager to restore the State to the centre of society, while simultaneously improving how Russia is perceived abroad. These dual objectives – respectively domestic and international – have been achieved by effectively adapting to the social changes that occurred towards the end of the 20th century and that have deepened since, namely, globalization and the beginning of the information age. Similarly to how industry and its control propped up the various regimes of the Soviet period, information has now features predominantly in Russian political strategy, helping to achieve the grand strategy of the Putin regime's objective to restore Russian prestige after a tumultuous post-Soviet period. For the study of IR, this implies that the classical realist treatment of the security dilemma can no longer be said to apply to the non-physical domain of the information space, while more modern theories such as constructivism and neoclassical realism are more instrumental for analysis.

Bibliography

1. Alexander, Marcus (2004). 'The Internet and democratization: the development of Russian Internet Policy', *Demokratizatsiya, 12, 4*, pp.607 627

2. Anderson, Benedict., (1991), *Imagined Communities*, (London: Verso)

3. Armistead, Leigh (2004). *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington DC: University of Nebraska Press)

4. Ball, Terrance & Dagger, Richard (2008). 'Neoconservatism', *Encyclopaedia Britannica*, URL:https://goo.gl/2ksj6F, [Accessed 28.06.17]

5. Balmforth, Tom (2014). 'Network, Son of Nashi: New Youth Group Seeks to Woo Russia's Middle Class", *Radio Free Europe* (3 July 2014) URL: https://goo.gl/LNtG9Q, [Accessed 02.06.17]

6. Balmforth, Tom (2015). '"We fight for democracy" Russia's pro Kremlin youth respond to propaganda warning', *The Guardian* (3 February 2015) URL: https://goo.gl/n8bWTc, [Accessed 02.06.17]

7. Barnett, Michael (2014). 'Social Constructivism' in John Bayliss, Steve Smith and Patricia Owens (eds.,) *The Globalization of World Politics* (Oxford: Oxford University Press) pp.155 168

8. Barry, Ellen (2011). 'Rally Defying Putin's Party Draws Tens of Thousands', *The New York Times*, (10 December 2011) URL: https://goo.gl/xkbBNa, [Accessed 23.06.17]

9. *BBC News* (2015). 'Russian opposition politician Boris Nemtsov shot dead', (28 February 2015) URL: https://goo.gl/yguJvB, [Accessed 23.06.17]

10. Becker, Michael E., Cohen, Matthew S., Kushi, Sidita & McManus, Ian P. (2016). 'Reviving the Russian empire: the Crimean intervention through a neoclassical realist lens', *European Security, 25, 1,* pp.112 133

11. Berzins, Janis (2014), 'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy' *National Defense Academy of Latvia, Center for Security and Strategic Research, Policy Paper No. 2*

12. Blackledge ,Adrian (2012). 'Discourse and power', in James Paul Gee & Michael Handford (eds.,) *The Routledge Handbook of Discourse Analysis*, (London & New York: Routledge), pp.616 627

13. Cassiday, Julie A. & Johnson, Emily D. (2010). 'Putin, Putiniana and the Question of a Post Soviet Cult of Personality', *The Slavonic and East European Review, 88, 4,* pp. 681 707

14. Castells, Manuel (2000a). *The Rise of Network Society*, *2nd Edition*. (Malden, MA, USA & Oxford, UK: Blackwell)

15. Castells, Manuel (2000b). *End of Millennium*, *2nd Edition* (Malden, MA, USA & Oxford, UK: Blackwell)

16. Cepoi, Victor , (2017). 'Trust and Participation in the Information Society: New and Traditional Information Sources', in *Information Society and its Manifestations: Economy, Politics, Culture* (Frankfurt am Main: Peter Lang) pp.135 152

17. Chappel, Bill & Memmott, Mark (2014). 'Putin Says Those Aren't Russian Forces In Crimea', *NPR* (4 March 2014) URL: https://goo.gl/ENCpQ9, [Accessed 14.06.17]

18. Chekinov, S.G. & Bogdanov, S.A (2013). 'The Nature and Content of New Generation War', *Military Thought, 4,* pp.12 23

19. Darczewska, Jolenta (2015). "The Devil is in the Details: Information Warfare in The Light of Russia's Military Doctrine', *OSW Point of View, 50*

20. *Demoscope* (2013a) 'Mortality Rate', *Institute of Demography of the National Research University "Higher School of Economics"*, URL: https://goo.gl/qUeqDu, [Accessed 02.06.17]

21. *Demoscope* (2013b) 'Fertility Rate', *Institute of Demography of the National Research University "Higher School of Economics"*, URL: https://goo.gl/qUeqDu, [Accessed 02.06.17]

22. E ISAC (2016) 'Analysis of the Cyber Attack on the Ukrainian Power Grid' [Accessed 22.02.17] URL: https://ics.sans.org/media/E ISAC_SANS_Ukraine_DUC_5.pdf

23. Eriksson, Johan and Giacomello, Giampiero (2006). 'The Information Revolution, Security, and International Relations: (IR)Relevant Theory?', *International Political Science Review, 27, 3,* pp.221 244

24. Fairclough, Norman. (2012). 'Critical Discourse Analysis', in James Paul Gee & Michael Handford (eds.,) *The Routledge Handbook of Discourse Analysis*, (London & New York: Routledge), pp.9 20

25. Foucault, Michel (1980). 'Truth and Power' in Colin Gordon (ed.), *Power/Knowledge* (trans. Colin Gordon, Leo Marshall, John Mepham, Kate Soper) (Harlow, UK: Pearson Education Limited) pp.109 133

26. *FRED* (2017) 'Working Age Population: Aged 15 64: All Persons for the United States', URL: https://goo.gl/hkq4PH, [Accessed 02.06.2017]

27. Frye, Timothy. (2007). 'Vladimir Putin and the Succession Dilemma', *Problems of Post Communism, 54, 6,* pp.59 60

28. Fukuyama, Francis (2016). 'Governance: What Do We Know and How Do We Know It?', *Annual Review of Political Science, 19,* pp.89 105

29. Galeotti, Mark and Bowen, Andrew S. (2014). 'Putin's Empire of the Mind', *Foreign Policy, May/June 2014*, pp.16 19

30. Gerasimov, Valery (2013). 'Tsennost Yennost Nauki v Predvidenii' *Voenno Promishlenniy Kuryer* (Military Industrial Courrier) (5 March 2013) [Accessed 09.04.17] URL: https://goo.gl/abwhnk ; english translation taken from: Robert Coalson (2013), 'Top Russian General Lays Bare Putin's Plan for Ukraine', *The World Post,* [accessed 09.04.17], URL: https://goo.gl/Ma2saJ

31. Gerrits, André (2016). *Nationalism in Europe Since 1945* (London & New York: Palgrave Macmillan)

32. Giles, Keir (2016), 'The Next Phase of Russian Information Warfare', *Nato StratCom COE*, URL: https://goo.gl/Q96RpH, [Accessed 09.04.17]

33. Golob, Tea (2017). 'Instrumental Identities and Information Society Deploying the Issue of Social Fields', in *Information Society and its Manifestations: Economy, Politics, Culture* (Frankfurt am Main: Peter Lang) pp.197 216

34. Gorham, Michael S. (2014), *After Newspeak: Language, Culture and Politics in Russia from Gorbachev to Putin* (Ithica, USA: Cornell University Press)

35. Gregory, Paul Roderick (2014). 'Putin's New Weapon in The Ukraine Propaganda War: Internet Trolls', *Forbes*, (9 December 2014) [Accessed 09.04.17] URL:http://goo.gl/Jpsxwe

36. Gvosdev, Nikolas K. (2012). 'The Bear Goes Digital: Russia and its Cyber Capabilities' in Derek S. Reveron (ed.,) *Cyberspace and National Security Threats* (Washington: Georgetown University Press) pp.173 189

37. *JP 3 13* (1998). 'Joint Doctrine for Information Operations', (9 October 1998) URL:https://goo.gl/8h7ECU

38. Kanet, Roger E. (2007) 'Introduction: The Consolidation of Russia's Role in World Affairs', in *Russia: Re Emerging Great Power* (Basingstoke & New York: Palgrave Macmillan) pp.1 12

39. Knight, Will. (2002). 'Torpedo fuel leak sank Kursk', *New Scientist*, (26 July 2002) URL: https://goo.gl/FcQSKe, [Accessed 27.06.17]

40. Krastev, Ivan & Holmes, Stephen (2012). 'An Autopsy of Managed Democracy', *Journal of Democracy, 23, 3,* pp.33 45

41. Kuzio, Taras (2016). 'When an academic ignores inconvenient facts', *New Eastern Europe* (21 June 2016) URL:https://goo.gl/VuocXv, [Accessed 26.05.17]

42. Lamy, Steven L. (2014). 'Contemporary mainstream approaches: neo realism and neo liberalism' in John Bayliss, Steve Smith and Patricia Owens (eds.,) *The Globalization of World Politics* (Oxford: Oxford University Press) pp.126 140

43. Larsen, Henrik (2005). *Foreign Policy and Discourse Analysis: France, Britain and Europe,* (London & New York: Routledge)

44. Latawski, Paul & Smith, Martin (2003). *The Kosovo Crisis and the evolution of post Cold War European security* (Manchester, UK: Manchester University Press)

45. Laurinavičius, Marius (2016). 'Putin's Russia: The Nature and Contradictions of the Regime', *Lithuanian Annual Strategic Review, 14,* pp.119 138

46. Lazitski, Olga (2013), 'Media Endarkenment: A Comparative Analysis of 2012 Election Coverage in the United States and Russia', *American Behavioural Scientist*, *58, 7,* pp.898 927

47. *Levada Center* (2017). 'Putin's Approval Rating', URL: https://goo.gl/CEXuGY, [Accessed 22.06.17]

48. Lipman, Masha and McFaul, Michael (2001). '"Managed Democracy" in Russia: Putin and the Press', *Press/Politics, 6, 3,* pp.116 127

49. Marshall, Jonathan Paul, Goodman, James, Zowghi, Didar and da Rimini, Francesca (2015). *Disorder and the Disinformation Society* (London & New York: Routledge).

50. Mejias, Ulises A. & Vokuev, Nikolai E. (2017). 'Disinformation and the media: the case of Russia and Ukraine', *Media, Culture and Society, January 2017*, pp.1-16

51. Jennifer Milliken, (1999). 'The Study of Discourse in International Relations: A Critique of Research and Methods', *European Journal of International Relations*, *5, 2,* pp.225-254

52. Matthews, Owen (2014). 'Vladimir Putin's new plan for world domination', The Spectator (22 February 2014) URL: https://goo.gl/lfqtG2, [Accessed 06.06.17]

53. Morgan, Michael & Shanahan, James (2010). 'The State of Cultivation', *Journal of Broadcasting and Electronic Media, 52, 2*, pp.337-355

54. Motyl, Alexander J. (2015). 'The Surrealism of realism: misreading the war in Ukraine', *World Affairs, 177, 5,* pp.75-84

55. Meyers, Steven Lee (2015). *The new Tsar: The rise and reign of Vladimir Putin* (New York: Alfred A. Knopf)

56. *Newsru* (2005). 'The Kremlin is preparing a new youth project for the replacement of "Moving Together"' (21 February 2005) URL: https://goo.gl/IOpytZ, [Accessed 02.06.17]

57. *Nato StratCom COE* (2014b) 'Analysis of Russia's Information Campaign Against Ukraine', [Accessed 09.04.17] URL: https://goo.gl/4Er4uX,

58. Nye, Jospeh S. Jr (1999). 'Redefining the National Interest', *Foreign Affairs, 78, 4,* pp.22-35

59. Oldberg, Ingmar (2007) 'Russia's Great Power Ambitions and Policy Under Putin', in *Russia: Re-Emerging Great Power* (Basingstoke & New York: Palgrave Macmillan) pp.13-30

60. Ponce de Leon, Charles L. (2015). *That's the Way It Is: A History of Television News in America* (Chicago: University of Chicago Press)

61. *Project Network,* 'Principles', URL:https://goo.gl/FKVHmC, [Accessed 02.06.17] (In Russian)

62. *Project Network,* 'Spiritual Ties', URL: https://goo.gl/hba1fZ, [Accessed 02.06.17] (In Russian)

63. Putin, Vladimir (1999). 'Russia at the Turn of the Millennium', *Nezavisimaya,* (30 December 1999). URL: https://goo.gl/8XyX4i, [Accessed 22.06.17] (translation provided by Google)

64. Putin, Vladimir (2005). 'Annual Address to the Federal Assembly of the Russian Federation', *Kremlin English-language Website*, (25 April 2005), URL: https://goo.gl/txAJxK, [Accessed 24.04.17]

65. Putin, Vladimir (2013a). 'Presidential Address to the Federal Assembly', *Kremlin.ru*, (12 December 2013) URL: https://goo.gl/pvVbWQ, [Accessed 28.06.17]

66. Putin, Vladimir (2013b). 'Meeting of the Valdai International Discussion Club', *Kremlin.ru* (19 September 2013) URL: https://goo.gl/xZpdSj, [Accessed 28.06.17]

67. Putin, Vladimir (2014a). 'Address by President of the Russian Federation', *Kremlin.ru,* (18 March 2014) URL: https://goo.gl/FbdPCg, [Accessed 28.06.17]

68. Putin, Vladimir (2014b). 'Conference of Russian ambassadors and permanent representatives', *Kremlin.ru*, (1 July 2014) URL: https://goo.gl/bXzkVS, [Accessed 28.06.17]

69. Putin, Vladimir (2015). quoted in 'Direct Line with Vladimir Putin', *Kremlin.ru,* (16 April 2015), URL: https://goo.gl/DPJ6m3, [Accessed 11.04.17]

70. Rees, E.A. (2004). 'Leader Cults: Varieties, Preconditions and Functions', in Balázs Apor, Jan C. Behrends, Polly Tones and E. A. Rees (eds.,) *The Leader Cult in Communist Dictatorships: Stalin and the Eastern Bloc* (New York: Palgrave Macmillan) pp.3-26

71. Roberts, Kari (2017). 'Understanding Putin: The politics of identity and geopolitics in Russian foreign policy discourse', *International Journal, 72, 1,* pp.28-55

72. Rončević, Borut & Tomšič, Matevž (2017). 'Perspectives of Information Society: Bricolage of Manifestations' in *Information Society and its Manifestations: Economy, Politics, Culture,* (Frankfurt am Main: Peter Lang) pp.9-21

73. Rosstat (2016) 'Russia in Figures 2016', URL: https://goo.gl/VMVOcb [Accessed 02.06.17]

74. RT, 'About *RT',* URL: https://goo.gl/zDALrf, [Accessed 28.06.17]

75. *Russia24* (2015). 'Crimea. The Way home. Documentary by Andrey Kondrashev', *Youtube.com*, (15 March 2015), URL: https://goo.gl/xoWOs0 [Accessed 11.04.17]

76. Rukavishnikov, Vladimir., (2007) 'Choices for Russia: Preserving Inherited Geopolitics Through Emergent Global and European Realities', in *Russia: Re-Emerging Great Power* (Basingstoke & New York: Palgrave Macmillan) pp. 54-78

77. Russell, Alison Lawlor (2014). *Cyber Blockades*, (Washington: Georgetown University Press)

78. Sakwa, Richard (2008a) *Putin: Russia's Choice* (London: Routledge)

79. Sakwa, Richard (2008b). '"New Cold War" or Twenty Years' Crisis? Russia and International Politics', *International Affairs, 84, 2,* pp.241-267

80. Sanger, David E. 'Utilities Cautioned About Potential for a Cyberattack After Ukraine's' from *The New York Times* (29 February 2016) [Accessed 06.10.16] URL: http://nyti.ms/1TMOUL4

81. Seddon, Max (2014), 'Documents Show How Russia's Troll Army Hit America', *Buzzfeed*, (2 June 2014) [Accessed 09.04.17] URL: https://goo.gl/Yg7eLO

82. Shane, Scott (1994). *Dismantling Utopia: How Information Ended the Soviet Union*. (Chicago: Ivan R. Dee)

83. Simonyan, Margarita (2014). 'About Abby Martin, Liz Wahl and media wars', *RT* (6 March 2014), URL: https://goo.gl/VoJD3i, [Accessed 24.05.17]

84. Snyder, Jack & Ballentine, Karen. (1996), 'Nationalism and the marketplace of ideas', *International Security, 21, 2*, pp.5-40

85. Surovell, Jeffrey (2012). 'The Great Deception: Post-Soviet Russia and the Wars in the Former Yugoslavia', *The Journal of Slavic Military Studies*, *25, 3,* pp.284-301

86. Sutherland, Claire (2012). *Nationalism in the Twenty-First Century. Challenges and Responses*. (Houndmills, Basingstoke: Palgrave).

87. Syuntyurenko, O.V. (2015) 'Network Technologies for Information Warfare and Manipulation of Public Opinion', *Scientific and Technical Information Processing, 42, 4,* pp.205-210

88. Traynor, Ian. (2000). 'Putin aims Kursk fury at media', *The Guardian* (25 August 2000) URL: https://goo.gl/H9iYJ1, [Accessed 27.06.17]

89. *The Economist* (2010). 'A Cyber-missile aimed at Iran?', (24 September 2010) URL: https://goo.gl/52xtp6, [Accessed 21.06.17]

90. *The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland* (2014). 'The Military Doctrine of the Russian Federation' (25 December 2014) URL: https://goo.gl/pVVGVK, [Accessed 27.05.17]

91. *The Ministry of Foreign Affairs of the Russian Federation* (2016), 'Doctrine of Information Security of the Russian Federation', (5 December 2016), URL: https://goo.gl/AxW7ZT, [Accessed 11.04.17]

92. *The Moscow Times* (2017). 'Russians Take Pride in Crimea Annexation - Poll', (1 March 2017) URL: https://goo.gl/seYBbN, [Accessed 15.06.17]

93. Thomas, Timothy (2014), 'Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?' *The Journal of Slavic Military Studies, 27, 1,* pp.101-130

94. Thornton, Rod (2015). 'The Changing Nature of Modern Warfare: Responding to Russian Information Warfare', *The RUSI Journal, 160, 4*, pp.40-48

95. Trenin, Dmitri (2009). 'Russia Reborn: Reimagining Moscow's Foreign Policy', *Foreign Affairs, 88, 6,* pp.64-78

96. Tsygankov, Andrei P. (2012). 'Assessing Culture and Regime-Based Explanations of Russia's Foreign Policy: "Authoritarian at Heart and Expansionist by Habit"', *Europe-Asia Studies, 64, 4,* pp.695-713

97. *UN General Assembly* (1994). 'Memorandum on Security Assurances in connection with Ukraine's accession to the Treaty on the Nonproliferation of Nuclear Weapons', *General Assembly Document A/49/765, UN Security Council document S/1994/1399* (19 December 1994) Available from: https://goo.gl/CgBtlo, [Accessed 24.05.17]

98. *UN General Assembly* (2011). 'Promotion and protection of the right to freedom of opinion and expression', *A/66/290,* (10 August 2011), Available from: https://goo.gl/2FS1K3

99. *UNSC* (1999) 'Report of the 3988th Meeting of the United Nations Security Council', *S/PV.3988* (24 March 1999) , Available from: https://goo.gl/cNyybV, [Accessed 04.06.17]

100. *USDS Archive* (2001). 'A New Relationship Between the United States and Russia', (13 November 2001) URL:https://goo.gl/cagG5d, [Accessed 28.06.17]

101. Valeriano, Brandon & Maness, Ryan (2012), 'Persistent enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare' in Derek S. Reveron (ed.,) *Cyberspace and National Security Threats* (Washington: Georgetown University Press) pp.139-156

102. Walker, Maxton (2014). 'Putin the action man - in pictures', (3 January 2014), *The Guardian* URL: https://goo.gl/X1jUZ9, [Accessed 23.06.17]

103. Walker, Shaun (2015a). 'Putin admits Russian military presence in Ukraine for first time', *The Guardian* (17 December 2015) URL: https://goo.gl/RLc3Ts, [Accessed 14.06.17]

104. Walker, Shaun (2015b). 'Salutin' Putin: inside a Russian troll house', *The Guardian* (2 April 2015) [Accessed 09.04.17] URL: https://goo.gl/23M6qF

105. White, Stephen (2001). 'The Russian presidential election, March 2000', *Electoral Studies, 20,* pp.463-501

106. White, Stephen., Oates, Sarah. and McAllister, Ian. (2005). 'Media Effects and Russian Elections, 1999-2000', *British Journal of Political Science, 35, 2,* pp.191-208

107. White, Gregory L. (2014). 'Russia Stung By Ally Yanukovych's Defeat in Ukraine', *The Wall Street Journal* (22 February 2014) URL: https://goo.gl/EuzqPx, [Accessed 14.06.17]

108. White, Jon (2016). 'Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation', *Institute for European Studies, Policy Brief, Issue 2016/13*, Available from: http://www.ies.be/node/3689, [Accessed 24.05.17]

109. Wohlforth, William C. (1998), 'Honor as Interest in Russia' in Elliot Abrams (ed.,) *Honor Among Nations: Intangible Interests and Foreign Policy,* (Washington D.C.: Ethics and Public Policy Center) pp.21-44

110. Yablokov, Ilya (2015). 'Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of *Russia Today* (RT)', *Politics. 35, 3-4*, pp.301-315

111. Zakharov, Andrei (2007). 'The Russian Parliament and Vladimir Putin's Presidency' in Katlijn Malfliet & Ria Laenen (eds.,) *Elusive Russia: Current Developments in Russian State Identity and Institutional Reform Under President Putin* (Leuven: Leuven University Press)