UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Research Paper

Volume 12:26 September 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

THE WESTERN ALLIANCE IN THE FACE OF THE RUSSIAN (DIS)INFORMATION MACHINE: WHERE DOES CANADA STAND?*

Sergey Sukhankin

SUMMARY

In the years since the dissolution of the USSR in 1990, Russia has used advances in technology to create new and more diverse channels for the spread of propaganda and disinformation. However, the West often holds misconceptions and falls prey to blanket generalities about the strength of the Russian propaganda machine.

This paper examines Russia's propaganda capabilities through Russian-language sources themselves, to give a more balanced and nuanced picture of the situation, particularly with regard to Canada. While propaganda was always a staple of both Russia and its predecessor, the Soviet Union, the 2014 conflicts in Ukraine and Crimea touched off a more intensive information war against the West. However, Russia's resources are finite and its capabilities against Canada are limited. The peril exists – and thanks to the latest technology, it is being perpetrated by bots, trolls, hacktivists and other entities – but it should be neither under- nor over-estimated.

* This research was financially supported by the Government of Canada via a partnership with Western Economic Diversification.

Countering Russia's information warfare requires a deeper study of Russian culture, history and traditions than analysts in the West tend to engage in. Understanding the Russian mindset – especially Russia's historic and lingering dread of global marginalization – is essential. This knowledge would enable the West to play off those fears by using proven cases of cyber-attacks and fake news to increase international pressure to isolate and marginalize the Kremlin.

The West also needs to understand that it must stick to confronting the Kremlin on an international stage and avoid the temptation to meddle in Russia's domestic affairs. Engaging in the latter risks backfiring – it could motivate ordinary Russians to close ranks around the Putin regime rather than renounce it.

Another tactical error on the West's part – and one which unwittingly gives Russia a psychological edge – is to label as disinformation or propaganda every news item emanating from Russia. This creates the perception of a Russian disinformation machine that is much more powerful than it really is.

Unlike in the Soviet and Cold War eras, contemporary Russian propaganda is no longer ideological. It is carefully designed to appeal to the full political spectrum and it focuses on undermining Western institutions rather than promoting Soviet ones. While this disinformation campaign sticks to simplistic narratives, its structure is anything but simple. Not limiting itself to cyber- and information components, the campaign is also composed of psychological operations, public affairs, military threats, strategic communications, bribery and corruption.

The Kremlin has a growing interest in dominating the Arctic, where it sees Russia as in competition with Canada. This means Canada can anticipate escalations in information warfare, particularly from hacktivists fomenting cyber-attacks. Perceived as one of Russia's chief adversaries in the Arctic region, Canada is a prime target in the information wars, with Russia potentially even meddling in the October 2019 federal election. Ottawa should be ready for a new surge in cyber-attacks, disinformation and propaganda levelled against Canada in the near future.

UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Research Paper

Volume 12:26 September 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

L'ALLIANCE OCCIDENTALE FACE À LA MACHINE À (DÉS) INFORMATION RUSSE : OÙ EN EST LE CANADA?*

Sergey Sukhankin

RÉSUMÉ

Depuis la dissolution de l'URSS en 1990, la Russie met à profit les progrès technologiques pour créer de nouveaux canaux de diffusion de propagande et de désinformation. Cependant, l'Occident tombe souvent dans les grandes généralisations et garde une fausse idée de la force de la machine de propagande russe.

Ce document examine les capacités de propagande de la Russie par l'intermédiaire des sources en langue russe afin de donner une image plus équilibrée et nuancée de la situation, en particulier en ce qui concerne le Canada. Alors que la propagande a toujours été un élément de base de la Russie et de sa prédécesseure, l'Union soviétique, les conflits de 2014 en Ukraine et en Crimée ont déclenché une guerre de l'information plus intensive contre l'Occident. Cependant, les ressources de la Russie sont limitées comme le sont ses capacités contre le Canada. Il y a tout de même un certain danger – matérialisé par des robots, des trolls, des hacktivistes

* Cette recherche a été soutenue financièrement en partie par le gouvernement du Canada via Diversification de l'économie de l'Ouest Canada.

et d'autres entités grâce aux nouvelles technologies –, danger qui ne doit être ni sous-estimé, ni surestimé.

Pour contrer la guerre de l'information russe, il faut étudier la culture, l'histoire et les traditions russes plus profondément que ne le font actuellement les analystes occidentaux. Il est essentiel de comprendre la mentalité russe, en particulier la peur historique et persistante d'une marginalisation mondiale. Cette connaissance permettrait à l'Occident de mettre à profit ces craintes en invoquant les cas avérés de cyberattaques et de désinformation afin d'accroître la pression internationale pour isoler et marginaliser le Kremlin.

L'Occident doit également comprendre qu'il doit s'en tenir à affronter le Kremlin sur la scène internationale et qu'il doit éviter la tentation de se mêler des affaires intérieures de la Russie, car cela risque de pousser les Russes ordinaires à se rallier au régime de Poutine plutôt que d'y renoncer.

Une autre erreur tactique de la part de l'Occident – et qui donne involontairement à la Russie un avantage psychologique – consiste à qualifier de désinformation ou de propagande chaque information émanant de la Russie. Cela donne l'impression d'une machine de désinformation russe beaucoup plus puissante qu'elle ne l'est en réalité.

Contrairement à l'époque soviétique et à l'époque de la Guerre froide, la propagande russe contemporaine n'est plus idéologique. Elle est soigneusement conçue pour faire appel à tout l'éventail politique et se concentre sur la sape des institutions occidentales plutôt que sur la promotion des institutions soviétiques. Bien que cette campagne de désinformation s'en tienne à un discours simpliste, sa structure est tout sauf simple. Sans se limiter aux éléments cybernétiques ou d'information, la campagne se caractérise aussi par des opérations psychologiques, des interventions dans les affaires publiques, des menaces militaires, des communications stratégiques, des pots-de-vin et la corruption.

Le Kremlin montre un intérêt croissant envers l'Arctique, où il considère que la Russie est en concurrence avec le Canada. Le Canada peut donc anticiper une escalade de la guerre de l'information, en particulier de la part d'hacktivistes fomentant des cyberattaques. Perçu comme l'un des principaux adversaires de la Russie dans la région arctique, le Canada est une cible de choix dans la guerre de l'information et la Russie pourrait même s'immiscer dans les élections fédérales d'octobre 2019. Ottawa devrait se tenir prêt pour une nouvelle vague de cyberattaques, de désinformation et de propagande dirigées contre le Canada dans un proche avenir.

INTRODUCTION

Russia's annexation of Crimea and the ensuing conflict in southeast Ukraine led to a debacle in political relations between Russia and the West. In the Kremlin's discourse, Russia's actions were a response to a series of containment policies aggressively implemented by the vanguard of anti-Russian forces – the U.S., the European Union (EU) and Canada. In Russian parlance, these "anti-Russian policies" came to be known as "hybrid warfare" – a collection of non-military measures levelled against Russia and its political leadership that aimed to stir up domestic disturbance and downgrade Russia's position in the global arena. In spite of Russia's economic, military and demographic inferiority to the West, its counter-actions succeeded due to the West's asymmetric beliefs about Russia's power (Thornton 2017, 18-28). Following the thought of Sun Tzu, the Russian side has asserted that a stronger party's strength can be turned into weakness through manipulation and deception (Chekinov and Bogdanov 2015a). This can be achieved through imposing their own will on the enemy via the deliberate distortion of facts, such as disinformation, and psychological pressure.

This paper analyzes Russia's propaganda efforts against Western countries, with an emphasis on Canada, after the outbreak of the Ukrainian crisis. From a methodological perspective, the author pays particular attention to literature in the Russian language, since the prime objective of this research is to trace and convey the logic of the Russian side; thus, there is limited mention of Western scholarship.

FROM LENIN TO PUTIN: DIFFERENCES AND SIMILARITIES BETWEEN RUSSIAN AND SOVIET PRACTICES

The roots of Russia's current propaganda and disinformation techniques can be traced to the Soviet period. Lenin's maxim that "propaganda should be a matter of action rather than words," points to the practice-oriented nature of Soviet propaganda. A trend emerged in 1919 with the creation of the *Komintern* and continued in 1920 with the *Agitprop's* formation. Subsequently, with the emergence of the International Department of the Central Committee of the Communist Party of the Soviet Union (ID) and the introduction of propaganda as a subject (*spetspropaganda*) in the Soviet Military Institute of Foreign Languages (1942), the Soviets managed to greatly boost their capabilities in the realm of information operations (IOs).

According to Edward Lucas and Peter Pomerantsev (2017, 7), Soviet disinformation rests on two major precepts. The first one is reflexive control, a form of psychological warfare in which an attack does not destroy the enemy from outside but rather leads it to self-destruct via "self-disorganization" and "self-disorientation." As Michael Kofman (2016) notes, this results in capturing the enemy's resource base and using it to benefit the attacker. In other words, the success of this technique allows a party to gain control over "the specific process of imitating the enemy's reasoning or imitating the enemy's possible behavior

and causes him to make a decision unfavorable to himself," by influencing "the opponent's communication system to deceive either his decision-making elite or public opinion" (Bittman 1985, 96). The second precept is active measures**,** a clandestine intervention in the politics of another country to influence its policies, undermine popular confidence and trust in its leadership via discreditation, and damage its international reputation (United States Department of State Bureau of Public Affairs 1981). Tactics include written or spoken disinformation and efforts to control foreign media (this varies on a country-by-country basis). It also includes the use of communist parties and front organizations (such as the World Peace Council, the World Federation of Trade Unions, the World Federation of Democratic Youth and the Women's International Democratic Federation), clandestine radio broadcasting (Bruk 2013) and blackmail (via *kompromat* and forgeries). According to Ladislav Bittman, this is premised on two categories: "The first category includes misleading information (disinformation) that contributes to poor policy decisions among government leaders … The second type, propagandistic forgery, seeks to mold public opinion in a target country" (Golovchenko, Hartmann and Adler-Nissen 2018). Political influence operations and the use of academics and journalists finalize the list of active measures**.**

Despite their initial success, particularly between 1943 and 1972, Soviet propaganda efforts were greatly reduced by a combination of such factors as the over-ideologization of foreign policy, a highly inefficient economic model and aging ruling elites committing one strategic blunder after another. Incidentally, notable contemporary Russian theorists of information warfare agree that the Soviet defeat in the Cold War was pre-ordained after the forfeiture of strategic initiatives on the information battlefield in the second half of the 1980s.

After the Soviet Union's dissolution in 1991, Russia's stance on information security underwent several rounds of evolution. The early 1990s were marked by political havoc and economic turmoil that witnessed the near-collapse of Russian policies in the realm of information security. Yet, the first Chechen War (1994-1996) and the war in Serbia (1999) were wake-up calls for the Russian elites. In his book, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Russian army Gen. Makhmut Gareev (1998, 51-52) highlighted the role of "psychologically- and ideologically-biased materials of (a) provocative nature, mixing partially truthful with false pieces of information," as one of the key challenges to Russian statehood.

In 2000, the changing attitude of the Russian ruling elites was reflected in the foreign policy concept of the Russian Federation (June 28) that prioritized the importance of "developing Russia's own means to influence public opinion abroad," and the Doctrine of Information Security (September 2000) that identified the range of issues, challenges and tasks to be dealt with in the short to medium term (Sukhankin 2019a). The doctrine envisaged the application of both defensive and counter-offensive information operations.

Between 2003 and 2008, Russian perception of the concept "information" underwent a dramatic evolution, thanks to two developments. First, the war in

Iraq explicitly demonstrated that information superiority played a crucial role in terms of this new type of armed conflict (Makarenko 2017). Second, the colour revolutions in Georgia, Ukraine and Kyrgyzstan exposed Russia's backwardness and inferiority in terms of pre-emptive and counter-offensive IOs. The turning point for Russia's transformation into one of the main global actors in the cyber-arena occurred in August 2008. Anatoliy Tsyganok, then deputy chief of the General Staff of the Russian Armed Forces, noted: "Georgia won the information war at the preliminary stage of the conflict but lost at the end of it" (Thomas 2010). This marked Russia's gradual departure from Soviet patterns of propaganda and disinformation techniques. Russian authorities recognized the internet as a powerful tool for confrontation that erases borders and allows the free transnational flow of information. Also, the post-2008 period was marked by a dramatic increase of "black propaganda" – an outward vilification of the opponent with very little (if any) consideration for facts. According to Russia's top political technologist, Gleb Pavlovsky, "the main difference between propaganda in the USSR and the new Russia is that in Soviet times the concept of truth was important. Even if they were lying, they took care to prove what they were doing was 'the truth.' Now no one even tries proving the 'truth.' You can just say anything. Create realities" (Pomerantsev and Weiss 2014). This is an extremely important argument, for it means that spreading lies is one of several tools that serves Russia's main goal by creating an "alternative reality," a different view of the world, where "nothing is real, but everything is possible."

Leaving the discussion of specific actors and their activities to a forthcoming segment of this paper, it would be worthwhile to underscore key features of Russian post-2008 information operations:

(1) ***Flexibility and de-ideologization:*** Unlike Soviet propaganda, current IOs are free of a surfeit of ideology. They are equally appealing to both the far left (anti-capitalism, anti-fascism, anti-Americanism) and the far right (anti-immigration, anti-liberal, ultra-conservative) groups (Sukhankin 2017c);

(2) ***Straightforwardness and (ostentatious) simplicity***: Russian propaganda deliberately abstains from using sophisticated narratives. The key to success is explaining complex issues in the simplest and thus easily digestible terms, which renders Russia's main narratives extremely appealing to the broader public. Most general examples based on the analysis of Russian sources of narratives include such macro narratives as: "The West is decadent, deceitful and hypocritical"; "The United States is a selfish, ruthless, profit-oriented power, seeking global domination"; "Euro-Atlantic security is a sham, an instrument of geopolitical expansion to the East and a living embodiment of a cynical betrayal of promises made to the Soviet Union"; "The European Union is home to greed, false beliefs, moral degradation and russophobia" and "Russia is the sole custodian of European conservative values, morality and an example of spiritual rejuvenation." Such narratives are usually supplemented by open or tacit provocations, the release of *kompromat*, intimidation and strategic military exercises. The most dangerous aspect of these seemingly absurd concepts is the fact that every narrative

generated by the Russian propaganda machine contains a minuscule kernel of truth encased in an impenetrable, thick layer of deception, making it very hard (especially for ordinary individuals) to distinguish between facts and deliberately crafted fiction.

(3) *Suasion through dissuasion*: Russian propaganda does not aspire to persuade the opponent, but rather to dissuade the opposing party. If convincing the opponent that the Russian model is superior to the Western one is impossible to achieve, then the main focus is placed on undermining popular trust in Western institutions (information outlets), fostering apathy, disbelief and mistrust (the idea that "everyone is telling lies, and the West does it more than Russia"), demotivating the broader public, and nurturing passivity and indifference.

(4) *Industrial scale* (Joyal 2016)[1]: Perhaps the main obstacle the West encounters is debunking fake news generated and disseminated by Russian media and disinformation outlets. The enormous bulk of fake stories and disinformation from Russia overwhelms Western attempts to confront it effectively. Ultimately, this becomes a highly time- and resource-consuming endeavour, which is precisely what Russia seeks to achieve.

(5) *Close alliance with the military and the intelligence community*: The re-birth of Russian capabilities in the realm of IOs can be attributed to the pivotal role played by the military-intelligence community. In 1996, the chief of the General Staff, Gen. Viktor Samsonov, noted that the "high effectiveness of information warfare systems, in combination with highly accurate weapons and non-military means of influence, make it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population" (Joyal 2016). In 2004, prominent Russian military academic Vladimir Slipchenko claimed that "information has become a destructive weapon just like a bayonet, bullet or projectile" (Gareev and Slipchenko 2005).

Subsequent reflection not only maintained, but greatly enhanced this vision. Former deputy chief of the General Staff Lt.-Gen. Aleksandr Burutin (2008) claimed that: "information weapons can be used in an efficient manner in peacetime as well as during war" (Giles 2016), by drawing on the nascent idea of the perpetuity of the information war (Pirumov 2003). At the same time, attempts to analyze the post-1991 regional conflicts and colour revolutions led former chief of the General Staff Yuriy Baluyevsky to conclude that the vector of threats has changed from military to non-military-related ones, including information influence (Mukhin 2014). In 2011, the Russian Ministry of Defence defined information warfare (*informatsionnaja wojna*), "as the ability to … undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents" (Allen and Moore 2018). In his analysis, Chief of

[1] This element will be discussed later in the paper with some practical examples given.

the General Staff Gen. Valery Gerasimov outlined his vision of an existing ratio between non-military and military measures, which according to him should be estimated at four to one. Gerasimov also classified so-called non-military threats as a compendium of economic sanctions, disruption of diplomatic ties, political and diplomatic pressure, and information operations (IO). Other notable writers from the military-strategic community generated similar ideas. As Bogdanov and Chekinov (2015b, 44-45) argued:

> Wars will be resolved by a skillful combination of military, non-military, and special nonviolent measures … a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority. Information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources).

The period between late 2010 (the Arab Spring) and 2013/14 (developments in Ukraine) witnessed a dramatic expansion of the role of the *siloviki*, primarily the Ministry of Defence, the FSB (federal security service) and the SVR (foreign intelligence service) in Russian information security-related policies. For instance, the emergence of the cyber-troops and research units (controlled by the MoD) (Sukhankin 2017b) vested the process of headhunting and selection of the most talented young specialists in the hands of the armed forces. On the other hand, the FSB and the *Rosgvardia* (Russia's National Guard) were allocated additional responsibilities in terms of monitoring the domestic segment of the internet's content (*Runet*) (Sukhankin 2018b). The Cossacks have emerged as yet more players within Russia's information security structure. In 2017, the first Cossack cyber-squads (*kiber druzhina*), consisting of "highly qualified volunteers from the Cossack Institute of Technology and Design" (Newkaliningrad 2017) dealt with "dangerous information content" on the *Runet* in 15 Russian cities including Kaliningrad, Penza, Volokolamsk, Smolensk, Temruk, Briansk, Samara and Omsk.

In the final analysis, one of the main difficulties Western analyses face pertaining to the Russian information warfare strategy is a lack of understanding of its structure. It is not confined to cyber- and information components, yet it presents a sophisticated combination of various elements, including cyber-operations, electronic warfare (EW), strategic deception and psychological operations, public affairs, strategic communications, bribery and corruption, and (in)direct military threats.

OPERATIVE PRINCIPLES: HOW RUSSIA'S PROPAGANDA MACHINE FUNCTIONS

Igor Panarin (2003), one of the founding fathers of Russia's post-1991 theory of information confrontation, defines five key instruments that states exercise in

the information struggle. These are 1) propaganda (black, grey and white); 2) intelligence (information collection); 3) analysis (media monitoring and situation analysis); 4) organization (co-ordinating and steering channels and influencing media to shape the opinions of politicians and the mass media) and 5) other combined channels. In terms of vehicles, Panarin mentions social control, social maneuvering, information manipulation, disinformation, the purposeful fabrication of information and lobbying, blackmail and extortion.

These elements are tightly connected with the Soviet-era practices, yet new technologies have expanded the ways in which they are used. As one study notes: "The Kremlin's Cold War-era propaganda was often stiff and dull. Today, the content is emotionally engaging, combining glossy entertainment formats and production values with a strong sense of patriotism and nostalgia" (Lucas and Pomerantsev 2017, 7). As Giles and Hagestad (2012) note, one of the Russian side's main achievements has been "securing its national information space" and "preventing breaches" in it. A second pivotal aspect greatly contributing to the sophistication of Russia's capabilities in the domain of information warfare stems from its duality, as Giles (2016a, 9) notes:

- *Information-psychological warfare* to affect the personnel of the armed forces and the population, conducted on a permanent basis, both in peace- and war-time;
- *Information-technology warfare* seeking to affect technical systems that receive, collect, process and transmit information, a process primarily applied during wars and armed conflicts. Usually, as a preliminary part of military confrontation, and later as an integral supplement. This type of information warfare also includes EW and radio-electronic warfare (*radio-elektronnaja borba*), which greatly differs from Western reading of the notion.

Russia's propaganda campaigns greatly depend on the operational theatres and targets chosen for the assault. The two main theatres are internal (domestic) and external. It would be fair to say that in terms of outward operations,[2] Russian disinformation is primarily concerned with two sub-theatres (Helmus et al. 2018). The first major theatre is the "near abroad" (Estonia, Latvia, Lithuania, Ukraine, Georgia and Moldova), where the Kremlin's main objective is fostering friction between ethnic Russians and the particular nation. As Giles (2016b) has argued, in this area "Russian-backed media companies and their broadcasting services work in lockstep with the Russian political authorities." Causing confrontation and furthering internal divisions within these countries is key, as is demonstrating the unsuccessfulness of the post-Soviet transformation, the consequences of which are still suffered by these (on the surface independent), yet economically, politically and demographically feeble entities. [3]

[2] Internal IOs constitute a different topic and should be looked at separately.

The second theatre is the "further abroad" where Russia seeks to sow confusion, generate apathy and erode trust in Western (Euro-Atlantic) and democratic institutions. Andrew Wilson (2015) has separated Russia's outward propaganda into three categories:

- The first is intended to induce paralysis through propaganda.
- The second seeks to target entities that already have entrenched world views with anti-systemic leanings and nudge them in useful directions.
- The third attempts to fashion alternative realities in which a particular media narrative is reinforced by a supporting cast of pro-Kremlin political parties, NGOs, churches and other organizations.

Pomerantsev and Weiss (2014) present perhaps one of the most succinct ways to map Russia's outward disinformation:

- In Ukraine, it can help create complete havoc.
- In the Baltic States, it can destabilize.
- In Eastern Europe, it can co-opt power.
- In Western Europe, it can divide and rule.
- In the U.S., it can distract.
- In the Middle East and South America, it can fan flames.

The impact of Russian propaganda is also based on the frequent under-estimation of its potential. Ruslan Deynychenko, co-founder of StopFake, rightly argues: "Our project proved that … Russian media disseminate not facts, not news, but propaganda. Unfortunately, this ignorance of this threat cost our country too much" (Paulo 2018).

However, Russia has managed to successfully diversify both its internal and external (dis)information, while avoiding Soviet mistakes and effectively integrating new means of information delivery. As Giles (2016c) has argued, "the Russian approach is much broader than simply sowing lies and denial, for instance maintaining that Russian troops and equipment are not where they plainly are. Instead, the Russian state and nonstate actors have exploited history, culture, language, nationalism and more to carry out cyber-enhanced disinformation campaigns with much wider objectives."

NUTS AND BOLTS OF RUSSIAN PROPAGANDA: WHO DOES WHAT

Western scholars and policy-makers tend to look at two main sources of Russian propaganda and disinformation (Weisburd, Watts and Berger 2016): The "white" outlets are agencies directly linked to the Russian government and enjoy a high level of credibility through the façade of objectivity, while the "grey" outlets are not officially tied to the Russian state. This classification requires a more detailed

description, so I shall divide the main actors into nine groups:

(1) GONGOs (government-organized non-governmental organizations): Numbering nearly 150, these entities are closely related to Russia's government (and the people close to the government), the Ministry of Foreign Affairs (MFA) and the Ministry of Defence (MoD). However, this segment does not present a homogeneous group; rather, it should be viewed as a compendium of loosely connected, diverse entities that are assigned different roles and tasked with targeting different segments. For instance, (ultra)conservative think tanks clearly aim to convey the Kremlin's messages by participating in various international platforms. (Pseudo)human rights groups, such as the Moscow Bureau of Human Rights (Kasparov.ru 2005), and election observers (such as the Commonwealth of Independent States-Election Monitoring Organization (CIS-EMO) and the Organization for Democracy and the Rights of People) are designed to create an aura of pluralism and adherence to democratic principles as part of Russia's greater strategy to increase its role in various (primarily non-Western) international organizations. As well, special attention should be paid to youth groups. The most influential ones include the Youth *Sodruzhestvo*, the Russian Youth Association and the All-Russian "Young Army" National Military Patriotic Social Movement Association (*Yunarmia*). Alla Hurska (2019, parts 1 and 2) argues that Kremlin-promoted youth groups not only extensively contribute to the "militarization of public conscious(ness) in Russia," but can also be seen as an example of Russia's covert policy aimed at increasing its popularity abroad. Finally, the Eurasianist integration groups, such as Internationalist Russia, the Foundation for Support of Eurasian Integration, Eurasians-New Wave and Young Eurasia, present an interesting selection of actors whose main task is promoting Russian agendas in the post-Soviet arena with a special emphasis on Eurasianist sentiment.

(2) State-sponsored foundations and authorities: These include a number of players such as the *Russkiy Mir* Foundation, the Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Co-operation (*Rossotrudnichestvo*) and the Alexander Gorchakov Public Diplomacy Fund. These entities are considered a bridge between Russia and its compatriots abroad, which according to Putin constitute 25 million ethnic Russians living outside of Russia.

(3) Pro-Kremlin media resources such as RT, Sputnik, L!FE, Russia Insider and *Rossiya Segodnya*.

(4) Cross-border religious groups represent a convergence of interests between the Russian Orthodox Church (ROC) and the private sector, including orthodox oligarchs such as Konstantin Malofeev (chair of the St. Basil's Foundation, which sponsored the Strelkov raids in Crimea and the Donbass region) and Vladimir Yakunin (chair of the St. Andrew's Foundation).

(5) Digital propaganda: This realm could be conditionally separated into two sub-categories. The first is represented by trolls. In the majority of cases, these are persons acting for pecuniary reasons and employed for the purpose of undermining an opponent by using lies and faulty logic. Political trolling became an integral part of Russia's information war techniques in late 2013, and matured over the next two years.[3] Its main goal is "to undermine, or suspend, the normative foundations of key areas and principles of liberal governance, by invoking those principles rhetorically, but also ridiculing and deriding their content in actual practice" (Popescu and Secrieru 2018). Yevgeny Prigozhin, also known as "Putin's cook," has a key organizational and financial role in the troll farms. Prigozhin sponsored the infamous troll factory known as the Internet Research Agency, based in St. Petersburg. He is closely connected to Russia's well-known private military company, a de facto private army called the Wagner Group (Sukhankin 2018f).

Bots present a different side of the same phenomenon. They are easier to detect and quantify by applying network analysis, since a bot is a software application, not a human. According to the NATO Strategic Communications Centre of Excellence (2018), between February and April 2018 only seven per cent of active users posting in Russian were recognizable as humans or institutions and the remaining 93 per cent were news accounts, bots, hybrid or anonymous. Similarly, Twitter published a study that traced 3,841 bot accounts co-ordinated through the troll factory, as well as some 770 Iran-based accounts, that since 2009 have published 10 million tweets and more than two million images (Lindell and Balenko 2018). Russia's reported attempts to interfere in the 2016 U.S. presidential election were, according to various Western analyses, done via trolls, botnets and fake accounts (Kriel and Pavliuc 2019).

(6) High-profile discussion platforms: The Valdai Discussion Club has a central role, hosting more than 1,000 high-level visitors from 63 countries between 2004 and 2018. Founded by the Council on Foreign and Defence Policy, the Russian International Affairs Council (RIAC), the Moscow State Institute of International Relations of the Ministry of Foreign Affairs of the Russian Federation (MGIMO University), and the National Research University Higher School of Economics, this entity is the intellectual muscle assisting Moscow in conveying its messages abroad. Leading foreign and Russian journalists, scholars, policy-makers and analysts, as well as top politicians including Putin and Dmitry Medvedev attend the Valdai Club's annual meetings. It is widely believed that the Valdai Club conference held in 2008, in the aftermath of the Russo-Georgian conflict, was of critical importance in allowing the Kremlin to ease Russia's looming international isolation (Institute of Modern Russia 2012).

[3] In 2005, Vladislav Surkov expressed the idea of using groups of bloggers to confront the Orange threat.

(7) Russian-funded political parties and organizations (such as the National Front and Jobbik).

This topic has attracted significant attention among Russian, European and North American scholars and practitioners. In reaching out to its actual and potential supporters in the West (primarily the EU), the Kremlin is pursuing two main objectives. First, it seeks to undermine political cohesion within the EU, disrupting its ties with the immediate surrounding countries and inflaming anti-EU sentiment. It also exploits the anti-immigration and anti-NATO themes, appealing to anti-American sentiments among EU member-states (Noack 2017). Second, Moscow seeks to win the support of marginal groups, both far right and left, as well as of russophones living in the EU, primarily in the three Baltic States. It is curious that the above-mentioned forces, even though seemingly occupying different sides of the political spectrum, do form highly controversial ad hoc alliances (Hurska 2018). In co-operation with European far-right forces, ultra-conservative philosopher Aleksandr Dugin occupies a central position. Dugin has played a crucial role in bridging ties between the Kremlin and, among others, the French (the National Front) and Hungarian (Jobbik) rightist forces. With the growth of both rightist and leftist sentiments in European countries, Russia's efforts to increase contact with these groups are likely to trend upward.

(8) Hacktivists:[4] Putin calls these people "patriotic hackers" who "are reading the news and quite naturally attacking those who are trying to present Russia in a bad light" (Radio Svoboda 2017). Their activities in many ways replicate some of the Soviet practices in terms of collecting and releasing of *kompromat*, yet with some notable differences. Namely, (pro)Russian hacktivists have actively interfered in foreign countries' domestic affairs – including the infamous episodes with the 2016 U.S. election.[5] Hacker attacks also became part and parcel of Russian actions in the initial stage of the Ukrainian crisis and the annexation of Crimea, when critical infrastructure in Ukraine was temporarily partially paralyzed, disrupting command and control and effective communication. Four-star retired Gen. Philip Breedlove, former head of the U.S. European Command, has pointed out that Russian actions in Ukraine presented "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare" (Vandiver 2014).

(9) "Heavy-metal diplomacy"[6]: According to Mark Galeotti (2016), the leading European expert on Russian disinformation and propaganda, "coercive 'heavy-metal diplomacy' is intended to divide, distract, and deter Europe from challenging Russia's activities in its immediate neighbourhood." The first attempts to use strategic military exercises to influence the European public go back to 1999, when

---

4 This group differs from the trolls/bots primarily due to its functions. Trolls' and bots' main purpose is to create antagonism, whereas the hacktivists are used for technical functions, such as stealing personal information and data corruption.

5 This topic is beyond the scope of this research, since it requires more proof and corroborating data.

6 Heavy-metal diplomacy is usually seen as a way to intimidate Russia's opponents by (para)military means (including direct and indirect threats and coercion).

for the first time since the dissolution of the USSR, Russia held strategic military exercises called *Zapad-99*. Subsequently, these exercises under the same code name (2009, 2013 and 2017) have become an effective coercive tool for Russia, causing alarm and a great deal of fear among East European countries, especially the three Baltic States, Poland and Ukraine (Sukhankin 2017).

The above list is by no means exhaustive. For example, major energy-related projects, even though they are not a part of IOs per se, may be considered yet another aspect of information warfare aimed at furthering divisions within the EU. Also, although frequently overlooked, the Ministry of the Russian Federation for Affairs for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters (MChS) is playing an increasingly powerful role. Much criticized at home, the MChS has become an important tool to promote a positive Russian image abroad both in specific countries or regions and among international institutions (Sukhankin 2018e).

IS CANADA A TARGET OF RUSSIAN DISINFORMATION?

As an integral part of the Western ("capitalist" in Soviet parlance) world, Canada has been targeted for Soviet and Russian disinformation (as a part of "active measures") since the early 1920s. This trend continued after the outbreak of the Cold War and intensified the ideological confrontation between the USSR (and its allies) and the Western bloc (Clément 2000). Soviet attempts to interfere in Canadian domestic affairs reached a zenith with the infamous Heine affair (Cartledge 1966). The affair vividly demonstrated the Soviet toolkit for dealing with Canada, which primarily involved attempts to undermine its democratic institutions via proxy organizations, *kompromat* release, slander and (where possible) the manipulation of elections. After the USSR's dissolution, Russia was concerned with its own problems and had neither the interest nor the capability to continue anti-Canadian/Western campaigns. Yet, between 2006 and 2013, Canada – as well as other, "unfriendly" from the Kremlin's point of view, countries – started to receive increasingly more negative coverage in the Russian media. In Canada's case, the bone of contention became the Arctic region (frequently seen as Russia's *Lebensraum*), where Russia assumed an increasingly tougher stance (Laruelle 2014).

These policies, however, took on a more definitive shape after the Ukrainian crisis erupted in late 2013. Canada was one of the first countries to react to Russia-provoked destabilization in southeast Ukraine by introducing sanctions in March 2014. Canada displayed an unyielding support for Kyiv, a staunch position on sanctions-related issues and the ultimate deployment of forces in the Baltic Sea region. In Moscow's eyes, this made Canada one of the main russophobes of the Western world. It is not surprising that Prime Minister Justin Trudeau is listed among the top 10 russophobes (branded as a bandwagon russophobe), a ranking that RT created in 2018.

Arguably, Canada has even surpassed the U.S. in the rank of perceived russophobes. One Russian publication claimed that "Canada is even more russophobic than the U.S.," owing to "a huge diaspora of the 'unfinished Banderites' who have formed a powerful lobby within Canada … as well as the fact that the U.S. needs Russia to deal with a number of international issues, whereas Canada is not involved in such issues and therefore does not need Russia at all" (Blog Turbolunakhoda 2015). Their assessment by and large reflects key narratives entertained by Russian propagandists regarding Canada. The most dangerous aspect of Russia's IOs is that their propagandists use information that may not necessarily be incorrect (such as the large Ukrainian diaspora and liberal traditions); yet, by adding a deliberate slant and twisting historical facts in a desired way, the final product is drastically different from the original idea. To show Russia's main narratives pertaining to Canada, it would make sense to uncover key themes entertained by the Russian propaganda.

Theme 1. *Canada as a safe haven of russophobia and (neo)fascism*. According to Russian propaganda, Canadian "affection for fascism" has a long pedigree, dating back to the mid-1930s. This is due to a synergy between a "staunch, innate hatred of the Soviet Union," "admiration of Adolf Hitler" and the "powerful Roman Catholic Church" – a combination that first "won the hearts and minds of the francophones in Quebec" and later gripped the entire country. Thus, the decision by Mackenzie King's government to "welcome the remnants of Nazi collaborators in Europe, particularly from western Ukraine" was nothing but a strong desire to extinguish the nascent popularity of communism among the Canadian working class – the line of behaviour that "has been successfully continued by the governments of Harper and Trudeau" (Abramov 2018). As a result of massive Ukrainian immigration to Canada, the country has allegedly developed a powerful Ukrainian lobby, which resulted in a long-standing tradition of "Canada (in addition to Australia) playing the role of initiator in the most russophobic initiatives in the Euro-Atlantic bloc" (Muromskiy 2018). For instance, many Russian observers and commentators blame Russia's eviction from the G7/8 on Canadian instigators (Natsionalnaya sluzhba novostey 2015). As a result, Russia thinks the Group of Seven is progressively becoming an "anti-Russian platform sowing russophobia" (Ishchenko 2018).

Russia's promulgation of the "Canadian fascism" theory is inseparable from the personality of Foreign Affairs Minister Chrystia Freeland, whom Russian propaganda has singled out as an example of the continuity in Canadian far-right traditions. In his article[7] entitled "Canada and Fascism," ultra-conservative writer and pseudo-historian Nikolay Starikov (2017), who is one of the main proponents of neo-Stalinism in Putin's Russia, accused Freeland of "concealing the fact that she is a granddaughter of Mykhailo Khomiak, who was the editor-in-chief of pro-Nazi, anti-Semitic *The Krakivs'ki Visti* newspaper … and close collaborator of Nazi Germany's chief jurist in occupied Poland, Hans Frank." Russia also launched a

[7] In effect, one out of several dozens of articles on the matter produced by Russian information outlets since 2014.

disinformation campaign against Liberal MP Borys Wrzesnewskyj, whom Russia's notorious broadcaster, Dmitry Kiselyov, names as a pro-Nazi actor, dictating Canada's anti-Russian policy (Levytsky 2019). Kiselyov is anchor of the prime-time *Vesti Nedeli* TV program and is infamous for his statement about Russia being able to turn the U.S. into "a pile of radioactive ashes."

These and similar messages are primarily designed for the Russian public and to a lesser extent russophones in countries of the former Soviet Union, aiming to demonstrate that anti-Russian forces abroad are still headed by neo-Nazi elements and their posterity. According to Russia's logic, the main supporters of the post-2014 Ukraine – the "instigators" of the Euromaidan – are the stalwarts of fascism and outspoken russophobes, implicated in the "ethnic cleansing" in the Donbass region. Therefore, Russia's support, now openly admitted by Putin, for the local separatists as well as the annexation of Crimea are absolutely legitimate and even necessary steps to protect Russian speakers in Ukraine against their physical extermination.

Theme 2. *Canada as part of the colonial forces in the Baltic Sea region*. Canada's decision to deploy its military contingent on the shores of the Baltic Sea has angered the Russians, and this has translated into increasing propaganda efforts, in the guise of cynical comments ridiculing the Canadian Armed Forces (CAF) and disseminated by pro-Kremlin information outlets. It should, however, be pointed out that Canadian policies are rarely separated from NATO's collective actions in the region. Russia's main narratives pertaining to NATO's presence in the Baltic Sea region are premised on two pillars and a number of sub-elements. The abhorrent behaviour of NATO soldiers, reflected in "numerous instances" of drunken debauchery, desecration of national symbols, inappropriate behaviour toward local women and open defiance of local police has reportedly tainted major war exercises in the region (Open Spirit in 2014 and Saber Strike in 2016), and is now common in areas hosting NATO forces – especially in Latvia (Riga and Ventspils) and Lithuania (Klaipeda, Kaunas and Druskininkai). They are known as "the most economically depressed and russophobic states, losing their sovereignty to the Euro-Atlantic bloc" (Veretennikov 2014; Veretennikov 2016 and Sevastyanov 2018). Russian IOs within this realm seek to create a repugnant image of NATO forces, acting not as protectors, but "colonizers," "masters" or "occupation forces." This portrayal of foreign contingents has a clear goal – to draw parallels with the conduct of Nazi Germany and its allies on Soviet territory and juxtapose those actions with the Soviet one. Russian political scientist Alexander Zamowsky has noted that "unlike the Soviet 'occupiers,' who were always polite and friendly with the locals, treating them as citizen of the Soviet Union … NATO soldiers perceive them as being inherently inferior … people" (Sokirko 2016). Russian propaganda tends to draw on the opinions of the local, frequently openly pro-Russian, politicians and members of the business community unhappy with the growing NATO presence in their countries. For instance, Russian information outlets ardently hyped an interview with Aivars Lembergs, a Latvian politician and oligarch, who stated that "foreign military have acted as an occupation force, who

do not recognize Latvian sovereignty," an episode that produced a great deal of controversy in Latvia and beyond.

Currently, the focus of Russian propaganda efforts has spread beyond the Baltic States, shifting to northern Europe. Russian mass media issued a torrent of publications during and after the Trident Juncture 18 (TRJE18) military exercises that NATO held in October-November 2018. The main theme was behaviour that was "inappropriate (including urinating and defecating close to public spaces) and (the) highly reckless demeanour of NATO soldiers in Norway, which caused 442 complaints from locals, and some public protests" (Eurasia Daily 2018; Gazeta.ru 2018). Specific examples of the anti-Canadian slant included fake stories about Canadian troops "living in luxury apartments at local taxpayers' expense" as well as "stories suggesting Russell Williams, the former air force colonel and convicted serial killer, still commanded Canada's biggest air base." On top of that, a Russian-language blog post suggested NATO troops in Latvia were "weak, p-ssy, gay, losers, (who) couldn't find (a) job in any other field" (Blackwell 2017).

A second narrative boils down to an argument about the futility of NATO's mission. Among other aspects, Russian information outlets heavily draw upon an alleged lack of qualifications and an unpreparedness for combat on the part of some NATO players, including Canada. Authoritative Russian mass media ridiculed Slovenian and Dutch soldiers and their high command for "being inappropriately dressed for the Norwegian weather" (Lenta.ru 2018; Ria.ru 2018). The media also gloated about a fire in the starboard gas turbine on the Canadian frigate Halifax, as well as a June 21 incident with the German frigate Sachsen (Dynamic Mongoose military exercises near Norway) when a Standard SM-2 Block IIIA rocket detonated. Indeed, Canadian media also made critical comments about the matter, yet the Russians' tone and the purpose of such publications had nothing to do with constructive criticism. Instead, the Russians were strongly determined to ridicule the CAF, depicting them as lacking qualifications and essential skills. These incidents have led Russian experts and analysis to conclude that NATO forces do not present a homogeneous and skilled presence in terms of combat readiness (Soyustov 2018). Similarly, pro-Kremlin media are promoting the idea of NATO's indifference to the fate of the Baltic States. According to the Russian sources, the "level of contradictions within NATO troops is so high, that soldiers from different countries would rather shoot each other than get into a fight over the Baltic States." Developing this assumption, the Russian side refers extensively to the "phoney war" and (in) actions of the British-French forces in 1939, attempting to draw parallels with the present (Denburg 2018). In addition to NATO's general inefficiency and lack of cohesiveness, Russian sources point out the allegedly overwhelming military supremacy of their own armed forces. Speaking about the Canadian mission in the Baltic Sea region, the Russian side holds that Ottawa's decision to deploy troops there has nothing to do with protecting the Baltic States per se, meaning that the Canadians will not risk their lives in case of a military escalation (Saideman 2016).

Theme 3. *Canada as Washington's useful satellite*. After the electoral defeats of Stephen Harper and Australia's Tony Abbott – the main russophobes in the Western political milieu, according to many Russian observers – a significant number of Russian commentators pinned their hopes on Trudeau, "who might want to stop looking for (the) American nod of approval in each and every decision," and said the "relations between Ottawa and Moscow could become more cordial" (Stepushova 2015). Russia's dreams were vanquished in 2017, when Canada introduced its version of the *Magnitsky Act*, which Moscow construed as "yet another adverse gesture by Canada, which is trying to satisfy the U.S. in its anti-Russian frenzy … this is a typical behaviour of a satellite that is now experiencing its heyday … Canada is trying to make it up for the U.S., which is failing in each and every direction, whether it be Syria, Afghanistan, Korea or Iran, and is now trying to put the blame on the Russian side" (Muromskiy 2017).

Theme 4. *Canada as a testing ground for the practical implementation of immoral Western values.* In Russian discourse, Canada is frequently presented as a pioneer and a testing ground, where abnormal or deviant behaviour such as same-sex marriages and legalization of light drugs is construed as a new normality. It is curious that after 2014, Russian propaganda re-launched a previous narrative about pedophilia in Canada. Various Russian information outlets and institutions, including the Russian Orthodox Church (Molodets 2012), defend their belief in the "powerful pedophile lobby" that reportedly exists in Canada. The Russian narrative goes on to claim that this lobby is putting a great deal of its weight behind legalizing pedophilia, using the legalization of same-sex marriage as a template. Russian sources have claimed that some Canadian elites are purposefully trying to normalize "homosexual behaviour" and "pedophilia" as a type of sexual orientation – not a criminal act against minors (Dinkevich 2011). Therefore, the argument goes that "it is inevitable that pedophilia will take the same route as homosexual behaviour and will be recognized as a distinct form of sexual orientation" (Knyazev 2017). To make differences between the West (and Canada) and Russia even more striking, Russian media have cited Putin stating that unlike the West, Russia will never accept pedophilia as normal behaviour and that "the Russian people would rather take up arms than follow the lead of the West in this issue" (Politus.ru 2018). Another theme exploited by Russian media is the "Islamization of Canada" (as the outcome of the liberal course the country is pursuing). Russian propagandists have chosen Defence Minister Harjit Sajjan as the target of this narrative (Fisher 2017).

CONCLUDING REMARKS

The essential feature of Russian disinformation is that it is inseparable from the Kremlin's non-linear strife against its opponents, which has taken an asymmetric form on the basis of valuable experience gained by the Russian side since 2010 to 2014. Three important aspects need to be underlined. First, Russia's information warfare strategy does not comply with Western understanding of this phenomenon. Its ambit and the number of tools employed in an integrated manner make it extremely sophisticated. Second, Russia's IOs and disinformation

campaigns are not stand-alone phenomena. They are used together with other means, since disinformation on its own is unlikely to yield a long-lasting effect. This paradigm change has yielded certain results. Specifically, since 2014 internal discord on the issue of anti-Russian sanctions within the EU (Moscow's main trading partner) has grown exponentially, with some major players openly demanding non-compliance with anti-Russian sanctions. At the same time, despite vigorous protests against Russia's actions, the West seems to have recognized that Ukraine is Russia's sphere of influence. The best proof of this is the notorious Kerch incident in November 2018 and the unfolding creeping annexation of parts of the Donbass region in April 2019 through the policy of issuing Russian passports (similar to the pre-2008 conflict in the South Caucasus). Third, Russian IOs target the following audiences, prioritized from greatest to smallest:

- The Russian domestic audience
- The post-Soviet area (including the russophones in the three Baltic States)
- The Balkans and east-central Europe
- Western and southern Europe
- The U.S.
- The rest of the world

Two main aspects characterize the Russians' discourse about Canada. First, the Russians don't see Canada as a fully independent political actor. Canada's "anti-Russian" posture is seen as a byproduct of the U.S.'s imposed will and internal pressure from the "Ukrainian lobby." The second aspect is premised on the fact that Russia's anti-Canadian propaganda, which still plays a marginal part compared to other theatres, is primarily tailored for domestic Russian consumption – it is not designed for a Canadian audience. The "ugly" side of democracy and liberalism has been deemed repugnant to the majority of Russians. Moscow aims to show its public that the path Western society has chosen is a road to self-destruction. This, however, does not rule out a chance that Russia might want to apply pressure on the most potentially sensitive issues, such as Islamophobia, U.S.-phobia (based on President Donald Trump's image in Canada), or the issue of the francophone population and its rights. Also, Russian media and (dis)information outlets might use such themes as the CAF's deployment in Europe and Canada's political leadership, especially those of Ukrainian ancestry, for domestic purposes. Russian IOs against Canada have visible limits and should not be compared with Russia's actions in Ukraine, Georgia or the Baltic Sea region. In any case, Alexander Lanoszka (2019) notes, the actual impact of Russian propaganda should be neither diminished nor overrated since either extreme could be dangerous.

This means Canada should anticipate potential escalations in the realm of information security. The most palpable danger stems from the information technology side of Russia's growing capabilities – the hacktivists. This threat is proportionately increasing with Russia's growing interest in the Arctic (Sukhankin 2018d), where Moscow is concerned about potential competition with Canada.

So far, a number of Western states have experienced cyber-attacks allegedly conducted by the Russians. It is extremely difficult to ward off the danger completely, and it's an even more arduous task to find a responsible party. As Sergey Shoygu states: "It is very difficult to look for a black cat in a dark room, especially if it is not there. All the more stupid to look for it there if this cat is clever, brave and polite" (Lenta.ru 2014).

Russia could exploit two potential IO zones against Canada. First, as a democratic country, Canada does not exercise control over its domestic media (or private Twitter/Facebook accounts) as Russia does. Therefore, as Alexandra Chyczij (2019) says: "The Kremlin's propaganda machine will increasingly target our country with anti-Canadian fabrications in an attempt to sow discord, conflict, and to undermine our democratic institutions" – which Moscow might attempt during the 2019 Canadian federal election. Second, and from this author's point of view, Moscow's next theme could be the Arctic. In his book *Battle for the Arctic* (2010), Artur Indzhiev speaks of the ways Russia needs to confront the Western alliance in the Arctic. He writes: "When the population of Greenland starts pursuing a more independent policy, it will rid itself of American military bases … What we need to do is to help them in their struggle for independence … which could trigger similar sentiments in Alaska and Canada. Russia should understand one thing – the fight against NATO's expansion should not be fought on our borders, but on the territory of the Alliance" (Sukhankin 2019b). With Russia's growing drive toward increasing its domination in the Arctic (Sukhankin 2019c, d) and with Moscow seeing Canada as one of its chief adversaries in this pursuit, Ottawa should be ready for a new surge of active measures levelled against Canada in the near future.

REFERENCE LIST

Abramov, Igor. 2018. "Kanadskiy professor-istorik: Pochemu Kanada zashchishchaet ukrainskiy fashyzm." March 13. Available at http://www.warandpeace.ru/ru/analysis/view/128854/.

Alandete, David. 2018. "RT, Sputnik and the New Russian War." *El Pais*. Jan. 2. Available at https://elpais.com/elpais/2018/01/02/inenglish/1514887171_124173.html.

Allen, T.S., and A.J. Moore. 2018. "Victory without Casualties: Russia's Information Operations." *Parameters*. U.S. Army War College Publications, vol. 48, no. 1. Spring: 59-71. Available at https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/9_Allen_VictoryWithoutCasualties.pdf.

Azar, Ilya. 2015. "'Soviet Propaganda Abroad was always Highly Successful': Meduza Speaks to Renowned Human Rights Activist and Chair of the Memorial Society, Sergei Kovalev." *Meduza.* Aug. 27. Available at https://meduza.io/en/feature/2015/08/27/soviet-propaganda-abroad-was-always-highly-successful.

Bittman, Ladislav. 1985. *The KGB and Soviet Disinformation: An Insider's View*. Oxford: Pergamon Press.

Blackwell, Tom. 2017. "Russian Fake-News Campaign against Canadian Troops in Latvia Includes Propaganda about Litter, Luxury Apartments." *National Post*. Nov. 17. Available at https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments.

Blog Turbolunakhoda. 2015. "Pochemu Kanada bolee rusofobskaya strana, chem SSHA." June 5. Available at https://turbolunokhod.livejournal.com/433277.html.

Bruk, Boris V. 2013. "International Propaganda: The Russian Version." Institute of Modern Russia. Prepared for delivery at the 45th Annual Convention of the Association for Slavic, East European and Eurasian Studies (ASEEES), Nov. 21-24. Part of this paper was presented at the 2013 annual meeting of the American Political Science Association (APSA) in Chicago, Illinois.

Cartledge, Jerry. 1966. "Heine: Spy, Liar or Hero?" *The Baltimore News-American.* May 15. Available at https://www.cia.gov/library/readingroom/docs/CIA-RDP75-00001R000400190006-8.pdf.

Chekinov S.G., and S.A. Bogdanov. 2015a. "Voennoe Iskustvo na Nachal'nom Etape XXI Stoletya: Problemy i Suzhdeniya." *Voennaya Mysl*, no. 1.

———. 2015b. "Prognozirovanie kharaktera i soderzhaniya voyn budushchego: problemy i suzhdeniya." *Voennaya Mysl*, no. 10, 2015: 44-45.

Chyczij, Alexandra. 2019. "Canada is a Target of Russia's Disinformation. Let's Be Ready." *The Hill Times*. Jan. 30. Available at https://www.ucc.ca/wp-content/uploads/2019/01/Alexandra-Chyczij-in-Hill-Times.-Canada-is-a-target-of-Russian-disinformaiton.-Lets-be-ready.pdf.

Clément, Dominique. 2000. "The Royal Commission on Espionage and the Spy Trials of 1946-9: A Case Study in Parliamentary Supremacy." *Journal of the Canadian Historical Association / Revue de la Société historique du Canada*, 11 (1): 151-172. https://doi.org/10.7202/031135ar.

Denburg, Valeriy. 2018. "Soldaty NATO v Evrope skoree perestrelyayut drug druga, chem zashchityat Pribaltiku." *Baltnews*. July 19. Available at https://baltnews.ee/authors/20180719/1016810238.html.

Dinkevich, Maksim. 2011. "Psihologi SSHA I Kanady vystupayut za legalizatsyyu pedofilii." *Vesti.ru*, Nov. 22. Available at https://www.vesti.ru/doc.html?id=638189.

DW. 2018. "V Dume predlozhyli nakazyvat za publikatsii, neuvazhytelnye k vlastyam." Dec. 12. Available at https://www.dw.com/ru/в-думе-предложили-наказывать-запубликации-неуважительные-к-властям/a-46704222?maca=rusrss_rus_Facenews_Maintopics_Fulltxt-19555-xml-mrss

Echo Moskvy. 2012. "Uchastniki vstrechi mezhdunarodnogo kluba "Valday" s Vladimirom Putinym ostalis eyu razocharovanny." Oct. 26. Available at https://echo.msk.ru/news/944594-echo.html.

EU vs Disinfo. 2018. "Seven Commandments of Fake News – New York Times Exposes Kremlin's Methods." Nov. 21. Available at https://euvsdisinfo.eu/seven commandments-of-fake-news-new-york-times-exposes-kremlins-methods/.

Eurasia Daily. 2018. "Amerikanskie soldaty oskvernili v Kaunase flag Litvy." May 14. Available at https://eadaily.com/ru/news/2016/05/14/amerikanskie-soldaty-oskvernili-v-kaunase-flag-litvy.

Fandos, Nicholas, and Kevin Roose. 2018. "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts." *New York Times*. July 31. Available at https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html.

Fedotova, Aleksandra. 2016. "Tolko ya eto … russkaya." Lenta.ru. May 10. Available at https://lenta.ru/articles/2016/05/10/russophobia/.

Fisher, Matthew. 2017. "At War with the Philippine Strongman: Duterte Calls for Martial Law to Remain on Mindanao." *National Post*. Dec. 25, 2017. Available at https://nationalpost.com/news/world/matthew-fisher-sajjan-a-target-of-russian-cyber-campaign-aimed-at-undermining-natos-presence-in-baltic-republics.

Galeotti, Mark. 2016. "Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe since 2014." *The ECFR* (London). Dec. 19. Available at https://www.ecfr.eu/publications/summary/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since.

Gareev, Makhmut. 1998. *If War Comes Tomorrow? The Contours of Future Armed Conflict.* Jacob W. Kipp, editor. Routledge.

Gareev, Makhmut and Vladimir Slipchenko. 2005. *Budushchaya Voyna*. Moscow: Polit.ru OGI.

Gazeta.ru. 2018. "442 zhaloby: soldaty NATO pomochilis na Norvegiyu." Nov. 12. Available at https://www.gazeta.ru/army/2018/11/12/12055543.shtml.

Giles, Keir. 2011. "'Information Troops' – a Russian Cyber Command?" Oxford, U.K.: Conflict Studies Research Centre.

———. 2016a. "Handbook of Russian Information Warfare." Rome: NATO Defense College. November.

———. 2016b. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." Chatham House. March 6. Available at https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

———. 2016c. "The Next Phase of Russian Information Warfare." NATO Strategic Communications Centre of Excellence. March 20. Available at https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Giles, Keir, and William Hagestad. 2012. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." NATO Cooperative Cyber Defence Centre of Excellence. June 2012.

Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. 2018. "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation." *International Affairs,* vol. 94, issue 5. September: 975-994.Available at https://academic.oup.com/ia/article/94/5/975/5092080.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. 2018. "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe." RAND Corporation. doi: 10.7249/RR2237. Available at https://www.rand.org/pubs/research_reports/RR2237.html.

Hern, Alex, Pamela Duncan, and Helena Bengtsson. 2017. "Russian 'Troll Army' Tweets Cited More Than 80 Times in UK Media." *The Guardian*. Nov. 20. Available at https://www.theguardian.com/media/2017/nov/20/russian-troll-army-tweets-cited-more-than-80-times-in-uk-media.

Hurska, Alla. 2018. "Pro-Russian Demonstrations in Riga: The 'Spanish Trace' and Potential Repercussions." *Eurasia Daily Monitor,* vol. 15, issue 144. Washington DC: The Jamestown Foundation. Oct. 12. Available at https://jamestown.org/program/pro-russian-demonstrations-in-riga-the-spanish-trace-and-potential-repercussions/.

———. 2019. “Putin Seeks to Garner Support of Russian Youth through Military-Patriotic Upbringing (Part One).” *Eurasia Daily Monitor,* vol. 16, issue 51. Washington DC: The Jamestown Foundation. April 10. Available at https://jamestown.org/program/putin-seeks-to-garner-support-of-russian-youth-through-military-patriotic-upbringing-part-one/ and “Putin Seeks to Garner Support of Russian Youth through Military-Patriotic Upbringing (Part Two).” *Eurasia Daily Monitor,* vol. 16, issue 53. Washington DC: The Jamestown Foundation. April 15. Available at https://jamestown.org/program/putin-seeks-to-garner-support-of-russian-youth-through-military-patriotic-upbringing-part-two/.

Institute of Modern Russia. 2012. “The Propaganda of the Putin Era. Part Two: The Kremlin’s Tentacles.” Dec. 5. Available at https://imrussia.org/en/politics/344-the-propaganda-of-the-putin-era.

Ishchenko, Rostislav. 2018. “‘Bolshaya semerka’: rusofoby, byurokraty I nablyudateli.” *Sputnik*. April 24. Available at https://ru.sputnik.md/columnists/20180424/18768490/g7-bolishaja-semiorka-rusofoby-biurokraty-nabliudateli.html.

Joyal, Paul M. 2016. “Cyber Threats and Russian Information Warfare.” Washington DC: Jewish Policy Center. Winter. Available at https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/.

Kasparov.ru. 2005. “Kollektivnoe pismo rossiyskih pravozashchitnikov v otnoshenii Aleksandra Broda.” July 15. Available at http://www.kasparov.ru/note.php?id=482B0A1C46614.

Knyazev, Svyatoslav. 2017. “I Kanada vooruzhaetsya …” *Stoletie*. June 14. Available at http://www.stoletie.ru/rossiya_i_mir/i_kanada_vooruzhajetsa_447.htm.

Knyazev, Yuriy. 2018. “Prigozhynskie trolli sozdavali napryazhenie v britanskom obshchestve, razzhygaya islamofobiyu v Twitter - issledovanie Demos.” *The Insider*. Nov. 1, 2018. Available at https://theins.ru/news/125439?fbclid=IwAR1ECSEzMuN4zoxih8QalF2IQrv6MDCF062kBFo3qfhTvuqVTlG7L-hpAtw.

Kofman, Michael. “Russian Hybrid Warfare and Other Dark Arts.” War on the Rocks. March 11. Available at https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Korotkov, Denis. 2014. “Sotni trolley za million.” *Fontanka*. May 29. Available at https://www.fontanka.ru/2014/05/29/170/

Korzova, Sofiya. 2014. “IA FAN – novyy proekt Evgeniya Prigozhyna?” Lenizdat.ru. October. Available at https://lenizdat.ru/articles/1124585/.

Kriel, Charles, and Alexa Pavliuc. 2019. “Reverse Engineering Russian Internet Research Agency Tactics through Network Analysis.” *Defence Strategic Communication*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, vol. 6. Spring 2019: 199-227. doi: 10.30966/2018.RIGA.6. Available at https://www.stratcomcoe.org/ckriel-apavliuc-reverse-engineering-russian-internet-research-agency-tactics-through-network

Lanoszka, Alexander. 2019. "Disinformation in International Politics." *European Journal of International Security,* 1-22. doi:10.1017/eis.2019.6.

Laruelle, Marlene. 2014. *Russia's Arctic Strategies and the Future of the Far North*. New York, London: M.E. Sharpe Armonk.

Lenta.ru. 2014. "Shoygu nazval paranoyey obvineniya kievskih vlastey." April 17. Available at https://lenta.ru/news/2014/04/17/shoygu/.

———. 2017. "Gollandskie voennye poehali na ucheniya v Norvegiyu I zamerzli." Sept. 27, 2018. Available at https://lenta.ru/news/2018/09/27/holodno_v_lesu/.

Levytsky, Marco. 2019. "Russian Cyber Warfare Threat is Very Real." *New Pathway*. Jan. 22. Available at https://www.newpathway.ca/russian-cyber-warfare-threat-is-very-real/.

Lindell, Dada, and Evgeniya Balenko. 2018. "Twitter opublikoval dannye ob aktivnosti rossiyskoy 'fabriki trolley'." *RBK*, Oct. 17. Available at https://www.rbc.ru/technology_and_media/17/10/2018/5bc75c169a79475ae7d76139?from=newsfeed.

Lucas, Edward, and Peter Pomerantsev. 2017. "Winning the Information War: Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe." CEPA. Washington DC: Information Warfare Project in Partnership with the Legatum Institute.

Makarenko S. 2017. Informatsionnoe protivoborstvo I radioelektronnaya borba v setetsentricheskih voynah nachala XXI veka. Spb: Naukoemkie tekhnologii.

Mironenko, Petr. 2017. "'Fabrika' iznutri: kak rossiyskie trolli rabotali v Facebook." *The Bell*. Oct. 17. Available at https://thebell.io/fabrika-iznutri-kak-rossijskie-trollirabotali-v-facebook/.

Molodets, Petru. 2012. "Pedofiliya – skrytaya ustanovka gomoseksualizma." Pravoslavie.ru, July 3. Available at http://pravoslavie.ru/54602.html.

Mukhin, Vladimir. 2014. "Moskva korrektirujet vojennuju doktrinu." *Nezavisimaya*. Aug. 1. 2014. Available at http://www.ng.ru/armies/2014-08-01/1_doctrine.html.

Murakhovskiy, Viktor. 2019. "Krymskaya operatsiya – ochevidnyj marker kachestvenno novogo urovnya razvitiya Rossiyskoy armii." *Natsionalnaya oborona*. (№4) April. Available at http://oborona.ru/includes/periodics/maintheme/2014/0623/113513418/detail.shtml.

Muromskiy, Ilya. 2017. "Na volne rusofobii: zachem Kanade analog 'zakon Magnitskogo'." *Bditelnost*. May 22. Available at http://bditelnost.info/2017/05/22/na-volne-rusofobii-zachem-kanade-analog-zakona-magnitskogo/.

———. 2018. “Kanadskie ukraintsy proklyali by besslavnoe detishche Maydana: ekspert ocenil slova Poroshenko o ‘luchshem druge’ Kieva.” *Federalnoe agentstvo novostey*. July 2. Available at https://riafan.ru/1073105-kanadskie-ukraincy-proklyali-by-besslavnoe-detishe-maidana-ekspert-ocenil-slova-poroshenko-o-luchshem-druge-kieva.

NATO Strategic Communications Centre of Excellence. 2018. “Robotrolling.” Issue 2. Available at https://www.stratcomcoe.org/robotrolling-20182-0.

Natsionalnaya sluzhba novostey. 2015. “Potomki galichan prevratili Kanadu v zhupel rusofobii v ‘Semerke’?” June 5. Available at http://nsn.fm/in-the-world/potomki-galichan-prevratili-kanadu-v-glavnogo-rusofoba-bolshoy-semyerki-.php.

Newkaliningrad. 2017. “V Kaliningrade sobirayutsya sozdat pervuyu kazachjyu kiberdruzhynu.” March 17. Available at https://www.newkaliningrad.ru/news/briefs/community/12881722-v-kaliningrade-sobirayutsya-sozdat-pervuyu-kazachyu-kiberdruzhinu.html.

Nimmo, Ben. 2015. “Anatomy of an Info-War: How Russia’s Propaganda Machine Works, and How to Counter It.” *Stopfake*. May 19. Available at https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

Noack, Rick. 2017. “The European Parties Accused of Being Influenced by Russia.” *Washington Post*. Nov. 17. Available at https://www.washingtonpost.com/news/worldviews/wp/2017/11/17/the-european-parties-accused-of-being-influenced-by-russia/?noredirect=on&utm_term=.358dc8fa1e01.

Panarin, I.N. 2003. *Tekhnologiya informatsyonnoy voyny*. Moscow: KPS+.

Paulo, Derrick A. 2018. “How Fake News Fanned the Flames of War in Ukraine.” *CNA Insider*. Dec. 22. Available at https://www.channelnewsasia.com/news/cnainsider/how-fake-news-sparked-war-ukraine-russia-crimea-select-committee-11055154.

Pirumov V.S. 2003. *Informatsyonnoe protivoborstvo. Chetvertoe izmerenie protivostoyaniya.* Moscow: Oruzhyei tekhnologii.

Politus.ru. 2018. “Legalizatsyya pedofilii: popytka psihopatov sozdat obshchestvo po ih sobstvennomu podobiyu.” Feb. 21. Available at https://politus.ru/v-mire/3348-legalizaciya-pedofilii-popytka-psihopatov-sozdat-obschestvo-po-ih-sobstvennomu-podobiyu.html.

Pomerantsev, Peter, and Michael Weiss. 2014. “The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money.” Institute of Modern Russia. Nov. 22. Available at http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/.

Popescu, Nicu, and Stanislav Secrieru, eds. 2018. "Hacks, Leaks and Disruptions: Russian Cyber Strategies." European Union Institute for Security Studies. Chaillot Papers. October. Available at https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-––russian-cyber-strategies.

Radio Svoboda. 2017. "Putin: deystviya hakerov zavisyat ot ih 'patrioticheskogo nastroya'." June 1. Available at https://www.svoboda.org/a/28522589.html.

Ria.ru. 2018. "Slovenskie voyennye zamerzli na ucheniyah NATO v Norvegii." Nov. 12. Available at: https://ria.ru/20181112/1532643381.html.

RT. 2018. "Top 10 Russophobes of 2018: See Who Made RT's Prestigious List This Year." Oct. 16. Available at https://www.rt.com/news/441417-top-10-russophobes-2018/.

Rubaltik. 2018. "Matvienko obvinila Latviyu I Estoniyu v sozdanii zon aparteida v tsentre Evropy." Oct. 29. Available at https://www.rubaltic.ru/news/29102018-matvienko-obvinila-latviyu-i-estoniyu-v-sozdanii-zon-aparteida-v-tsentre-evropy/.

Saideman, Stephen. 2016. "Globe and Mail: Dlya Kanady sderzhyvat Rossiyu v Evrope i deshvle, i bezopasnee." *RT*. June 24. Available at https://russian.rt.com/inotv/2016-06-24/Globe-and-Mail-Dlya-Kanadi.

Sevastyanov, Konstantin. 2018. "'Pyanye mochilis na vitriny': kak soldaty NATO huliganyat v Pribaltike." Ria.ru. June 14. Available at: https://ria.ru/20180614/1522643942.html.

Smagliy, Kateryna. 2018. "Pro 'viysko' Kremlya v gibrydniy viyni proty Zakhodu." *Den'*. Nov. 16. Available at https://day.kyiv.ua/uk/article/ekonomika/pro-viysko-kremlya-v-gibrydniy-viyni-proty-zahodu?fbclid=IwAR11dTJ60kx865I_BKGmQ0Y03Nn0SO3vlyoiwmgjJ99SWQocD-2eVdSq_dg.

Sokirko, Viktor. 2016. "Samyy uzhasnyy gost: pochemu natovtsy v Pribaltike vedut sebya, kak agressivnye svin'i." TV Zvezda. Nov. 5, 2016. Available at https://tvzvezda.ru/news/vstrane_i_mire/content/201611050815-btf5.htm.

Soyustov, Andrey. 2018. "Stolknoveniya, ranenye, pozhar: ucheniya NATO Trident Juncture 18 vyhodit iz-pod kontrolya." *Federalnoe agentstvo novostey*. Oct. 29, 2018. Available at https://riafan.ru/1115315-stolknoveniya-ranenye-pozhar-ucheniya-nato-trident-juncture-18-vykhodyat-iz-pod-kontrolya.

Spruds, Andris, Anda Rožukalne, Klavs Sedlenieks, Martins Daugulis, Diana Potjomkina, Beatrix Tölgyesi, and Ilvija Bruge. 2015. "Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia. *NATO Stratcom*. July 29. Available at https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

Sputnik. 2018. "Lavrov: rusofobiya v ryade evropeyskih stran stanovitsya chut li ne ideologoey." Nov. 21, 2018. Available at https://sputnik.by/politics/20181121/1038777143/Lavrov-rusofobiya-v-ryade-evropeyskikh-stran-stanovitsya-chut-li-ne-ideologiey.html.

Starikov, Nikolay. 2017. “Kanada i fashyzm.” Starikov Blog. March 3. Available at https://nstarikov.ru/blog/75840.

Stepushova, Liubov. 2015. “Kakoy primer podala Kanada miru?” Pravda.ru. Oct. 21, 2015. Available at https://www.pravda.ru/world/northamerica/usacanada/21-10-2015/1279038-canada-0/.

Sukhankin, Sergey. 2016a. “The “Russkij Mir” as Mission: Kaliningrad between the ‘Altar’ and the ‘Throne’ 2009-2015.” *Ortodoxia* (56). University of Eastern Finland.

———. 2016b. “Russia Flexes ‘Iskander’ Muscles on Its Northwestern Flank.” *Eurasia Daily Monitor,* vol. 13, issue 163. Washington DC: The Jamestown Foundation. Oct. 12. Available at https://jamestown.org/program/russia-flexes-iskander-muscles-northwestern-flank/.

———. 2017a. “Lithuania: The Old-New Target of Russian ‘Hybrid Warfare?’” Blog. Washington DC: The Jamestown Foundation. Jan. 27. Available at https://jamestown.org/lithuania-old-new-target-russian-hybrid-warfare/.

———. 2017b. “Russian ‘Cyber Troops’: A Weapon of Aggression.” *Eurasia Daily Monitor*, vol. 14, issue 63. Washington DC: The Jamestown Foundation. May 11, 2017. Available at https://jamestown.org/program/russian-cyber-troops-weapon-aggression/.

———. 2017c. “The ‘Trump Cards’ of the Russian Propaganda and Disinformation Operations.” Notes Internacionals (176) CIDOB, Barcelona (June). Available at https://www.cidob.org/en/publications/publication_series/notes_internacionals/n1_176/the_trump_cards_of_the_russian_propaganda_and_disinformation_operations.

———. 2017d. “Zapad-2017: What Did These Military Exercises Reveal?” *Diplomaatia* (Tallinn). Oct. 24. Available at https://icds.ee/zapad-2017-what-did-these-military-exercises-reveal/.

———. 2018a. “The End of ‘Hide and Seek’: Russian Iskanders Permanently in Kaliningrad.” *Eurasia Daily Monitor,* vol. 15, issue 28. Washington DC: The Jamestown Foundation. Feb. 23. Available at: https://jamestown.org/program/end-hide-seek-russian-iskanders-permanently-kaliningrad/.

———. 2018b. “The FSB: A Formidable Player in Russia’s Information Security Domain.” *Eurasia Daily Monitor,* vol. 15, issue 46. Washington DC: The Jamestown Foundation. March 27. Available at https://jamestown.org/program/fsb-formidable-player-russias-information-security-domain/.

———. 2018c. “Russian PMCs, War Veterans Running ‘Patriotic’ Youth Camps in the Balkans.” (parts 1, 2). *Eurasia Daily Monitor,* vol. 15, issue 151. Washington DC: The Jamestown Foundation. Oct. 24. Available at https://jamestown.org/program/russian-pmcs-war-veterans-running-patriotic-youth-camps-in-the-balkans-part-one/.

———. 2018d. “China’s ‘Polar Silk Road’ versus Russia’s Arctic Dilemmas.” *Eurasia Daily Monitor,* vol. 15, issue 159. Washington DC: The Jamestown Foundation. Nov. 7, 2018. Available at https://jamestown.org/program/chinas-polar-silk-road-versus-russias-arctic-dilemmas/.

———. 2018e. “The Russian Emergency Situations Ministry: ‘Ministry of Corruption’ or Driver of the Kremlin’s ‘Soft Power?’” *Eurasia Daily Monitor,* vol. 15, issue 161. Washington DC: The Jamestown Foundation. Nov. 12. Available at https://jamestown.org/program/the-russian-emergency-situations-ministry-ministry-of-corruption-or-driver-of-the-kremlins-soft-power/.

———. 2018f. “‘Continuing War by Other Means’: The Case of Wagner, Russia’s Premier Private Military Company in the Middle East.” In *Russia in the Middle East*, Theodore Karasik and Stephen Blank, eds. Washington DC: The Jamestown Foundation. December: 290-319. Available at https://jamestown.org/product/russia-in-the-middle-east/.

———. 2019a. “The Offensive and Defensive Use of Information Security by the Russian Federation.” In *Russia’s Military Strategy and Doctrine*, Glen E. Howard and Matthew Czekaj, eds. Washington, DC: The Jamestown Foundation.

——— . 2019b. “Culture, Money, Propaganda: Russia’s Approach Toward Greenland and the Faroe Islands.” *Eurasia Daily Monitor,* vol. 16, issue 90. Washington DC: The Jamestown Foundation. June 20. Available at https://jamestown.org/program/culture-money-propaganda-russias-approach-toward-greenland-and-the-faroe-islands/.

———. 2019c. “‘Icebreaker Diplomacy’: Russia’s New-Old Strategy to Dominate the Arctic.” *Eurasia Daily Monitor,* vol. 16, issue 87. Washington DC: The Jamestown Foundation. June 12. Available at https://jamestown.org/program/icebreaker-diplomacy-russias-new-old-strategy-to-dominate-the-arctic/.

———. 2019d. “Russia’s Two-Pronged Approach to Militarizing the Arctic.” *Eurasia Daily Monitor,* vol. 16, issue 70. Washington DC: The Jamestown Foundation. May 14. Available at https://jamestown.org/program/russias-two-pronged-approach-to-militarizing-the-arctic/.

Thomas, Timothy L. 2010. “Russian Information Warfare Theory: The Consequences of August 2008.” In *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. Stephen J. Blank and Richard Weitz, eds. Carlisle PA: Strategic Studies Institute.

Thornton, Rod. 2017. “The Russian Military’s New ‘Main Emphasis’.” *RUSI Journal*, 162:4, 18 28. doi: 10.1080/03071847.2017.1381401.

Toler, Aric. 2018. “Anatomiya novostnogo sayta rossiyskoy ‘fabriki trolley’.” *Bellingcat*. June 14. Available at https://ru.bellingcat.com/novosti/russia/2018/06/14/anatomy-troll-site/

United States Department of State Bureau of Public Affairs. 1981. "Soviet Active Measures: Forgery, Disinformation, Political Operations." *Special Report No. 88.* October. Available at http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf.

Vandiver, John. 2014. "SACEUR: Allies Must Prepare for Russia 'Hybrid War.'" *Stars and Stripes*. Sept. 4. Available at https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

Veretennikov, Vladimir. 2014. "Kazus oskvernennoy klumby, ili priklyucheniya natovtsev v Pribaltike." *Ritm Evrazii*. June 1. Available at https://www.ritmeurasia.org/news--2014-06-01--kazus-oskvernennoj-klumby-ili-prikljuchenija-natovcev-v-pribaltike-13008.

———. 2016. "Otbornye NATO. Kakie vykhodki pozvolyayut sebe soldaty alyansa v Pribaltike." Lenta.ru. June 16. Available at https://lenta.ru/articles/2016/06/16/nato_pribaltika/.

Weisburd, Andrew, Clint Watts, and J.M. Berger. 2016. "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy." War on the Rocks. Nov. 6. Available at https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

Wilson, Andrew. 2017. "Four Types of Russian Propaganda." *Aspen Review*, issue 4. Available at https://www.aspenreview.com/article/2017/four-types-of-russian-propaganda/.

Zakharov, Andrey, and Polina Rusyaeva. 2017. "Rassledovanie RBK: kak iz 'fabriki trolley' vyrosla 'fabrika madia'." *RBK*. March 24. Available at https://www.rbc.ru/magazine/2017/04/58d106b09a794710fa8934ac?from=subject.

About the Author

Dr. Sergey Sukhankin is a Fellow at the Jamestown Foundation, where he is currently heading a project on Russia's use of Private Military Companies (PMCs). His areas of scientific interest primarily concern Kaliningrad and the Baltic Sea region, Russian information and cyber security, A2/AD and its interpretation in Russia, as well as the development of Russia Private Military Companies (PMC) after the outbreak of the Syrian civil war. He is currently teaching at the University of Alberta and MacEwan University (Edmonton).

ABOUT THE SCHOOL OF PUBLIC POLICY

The School of Public Policy has become the flagship school of its kind in Canada by providing a practical, global and focused perspective on public policy analysis and practice in areas of energy and environmental policy, international policy and economic and social policy that is unique in Canada.

The mission of The School of Public Policy is to strengthen Canada's public service, institutions and economic performance for the betterment of our families, communities and country. We do this by:

- *Building capacity in Government* through the formal training of public servants in degree and non-degree programs, giving the people charged with making public policy work for Canada the hands-on expertise to represent our vital interests both here and abroad;
- *Improving Public Policy Discourse outside Government* through executive and strategic assessment programs, building a stronger understanding of what makes public policy work for those outside of the public sector and helps everyday Canadians make informed decisions on the politics that will shape their futures;
- *Providing a Global Perspective on Public Policy Research* through international collaborations, education, and community outreach programs, bringing global best practices to bear on Canadian public policy, resulting in decisions that benefit all people for the long term, not a few people for the short term.

The School of Public Policy relies on industry experts and practitioners, as well as academics, to conduct research in their areas of expertise. Using experts and practitioners is what makes our research especially relevant and applicable. Authors may produce research in an area which they have a personal or professional stake. That is why The School subjects all Research Papers to a double anonymous peer review. Then, once reviewers comments have been reflected, the work is reviewed again by one of our Scientific Directors to ensure the accuracy and validity of analysis and data.

The School of Public Policy
University of Calgary, Downtown Campus
906 8th Avenue S.W., 5th Floor
Calgary, Alberta T2P 1H9
Phone: 403 210 3802

DISTRIBUTION
Our publications are available online at www.policyschool.ca.

DISCLAIMER
The opinions expressed in these publications are the authors' alone and therefore do not necessarily reflect the opinions of the supporters, staff, or boards of The School of Public Policy.

ISSN
ISSN 2560-8312 The School of Public Policy Publications (Print)
ISSN 2560-8320 The School of Public Policy Publications (Online)

DATE OF ISSUE
September 2019

MEDIA INQUIRIES AND INFORMATION
For media inquiries, please contact Morten Paulsen at 403-220-2540. Our web site, www.policyschool.ca, contains more information about The School's events, publications, and staff.

DEVELOPMENT
For information about contributing to The School of Public Policy, please contact Catherine Scheers by telephone at 403-210-6213 or by e-mail at catherine.scheers@ucalgary.ca.

RECENT PUBLICATIONS BY THE SCHOOL OF PUBLIC POLICY

ALTERING THE TAX MIX IN ALBERTA
https://www.policyschool.ca/wp-content/uploads/2019/09/Tax-Mix-Alberta-McKenzie-final-version.pdf
Kenneth McKenzie | September 2019

SOCIAL POLICY TRENDS: CANADA AND U.S. FERTILITY RATES, 1920-2018
https://www.policyschool.ca/wp-content/uploads/2019/08/Social-Policy-Trends-Birth-Rates-August-2019.pdf
Ronald Kneebone | August 2019

SLOW, SUBJECTIVE AND STRESSFUL: A GUIDE TO CANADA'S ASYLUM SYSTEM
https://www.policyschool.ca/wp-content/uploads/2019/08/Asylum-System-Falconer-Final.pdf
Robert Falconer | August 2019

REGULATING FINTECH IN CANADA AND THE UNITED STATES: COMPARISON, CHALLENGES AND OPPORTUNITIES
https://www.policyschool.ca/wp-content/uploads/2019/08/Fintech-Clements-final.pdf
Ryan Clements | August 2019

UNDERSTANDING CONSULTATION AND ENGAGEMENT WITH INDIGENOUS PEOPLES IN RESOURCE DEVELOPMENT
https://www.policyschool.ca/wp-content/uploads/2019/07/Indigenous-Consultation-Boyd-Lorefice-final2.pdf
Brendan Boyd and Sophie Lorefice | August 2019

WHERE IN THE WORLD ARE CANADIAN OIL AND GAS COMPANIES? 2017
https://www.policyschool.ca/wp-content/uploads/2019/07/Where-in-the-World-2017-Larson.pdf
Braeden Larson | July 2019

TRADE POLICY TRENDS: BREXIT: IMPLICATIONS FOR CANADA-UK TRADE
https://www.policyschool.ca/wp-content/uploads/2019/07/Trade-Policy-Trends-Brexit-final.pdf
Dylan Klemen and Eugene Beaulieu | July 2019

SOCIAL POLICY TRENDS: FINANCIAL SUPPORT FOR REFUGEES AND ASYLUM SEEKERS
https://www.policyschool.ca/wp-content/uploads/2019/07/Financial-Supports-for-Refugees-and-Asylum-Seekers-FINAL-version.pdf
Robert Falconer | July 2019

ENERGY AND ENVIRONMENTAL POLICY TRENDS: OUR PLANET IN 2040: COMPARING WORLD ENERGY OUTLOOKS
https://www.policyschool.ca/wp-content/uploads/2019/07/Energy-Trends-World-Energy-Outlooks-final-2.pdf
G. Kent Fellows, Victoria Goodday, Rabia Ladha, and Jennifer Winter | July 2019

HISTORY OF DEVELOPMENTAL DISABILITY POLICY IN ALBERTA
https://www.policyschool.ca/wp-content/uploads/2019/07/History-of-Disability-Sonpal-Valias.pdf
Nilima Sonpal-Valias | July 2019

THE URBAN POLICY CONTEXT IN MEDIUM-SIZED EUROPEAN METROPOLITAN AREAS
https://www.policyschool.ca/wp-content/uploads/2019/07/Mid-Sized-Cities-Barati-Stec.pdf
Izabella Barati-Stec | July 2019

TAX POLICY TRENDS: CORPORATE TAX POLICY: ALBERTA GOES ITS OWN WAY
https://www.policyschool.ca/wp-content/uploads/2019/06/TPT-June-AB-Corporate-Tax-METR.pdf
Philip Bazel and Jack Mintz | June 2019

REFORMING THE FEDERAL FISCAL STABILIZATION PROGRAM
https://www.policyschool.ca/wp-content/uploads/2019/06/Fiscal-Stabilization-Dahlby-final2.pdf
Bev Dahlby | June 2019