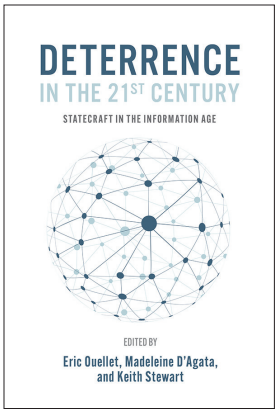
UNIVERSITY OF CALGARY
Press



DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

4

Understanding Russia's Approaches to Information Warfare

Rachel Lea Heide

Introduction: The Russian Strategic Threat

Information operations conducted by the Russian Federation under the Vladimir Putin regime, against foreign nations considered strategic threats, have been ongoing for more than a decade. Nevertheless, information operations have been brought to the attention of the West by Russia's recent interference in the United Kingdom's 2016 Brexit vote, the United States' 2016 presidential election, and numerous 2017 European election campaigns. This chapter has researched the question "What does Russian information warfare mean for the defence and security of Canada, its allies, and the West?" and proposes a proactive way ahead for Canada and its like-minded allies and partners to counter Russia's war on information.

The current Russian government has identified the West, the North Atlantic Treaty Organization (NATO), and the United States as Russia's most significant security threats. Putin's regime blames the West for encircling Russia with democracies; militarizing and causing an arms race in the eastern European region; promulgating an image of Russia as the enemy in the eastern European region; strengthening far-right nationalist ideologies in this region; and working to destroy Russian traditional culture and values by inserting competitive foreign values into the Russian population's consciousness (Oliker, 2016; Rumer, 2017).

Russia has two strategic aims: to challenge and undermine the West, Europe, and NATO, and to promote its own national interests and great power ambitions. As a means of promoting itself as a viable alternative global

leader, Russia is working to tear apart Western alliances and to tear down the West as a beacon of moral superiority. As part of the effort to challenge the idea of the West, the Russian government aims to undermine Western liberal values and democratic systems, especially in Europe, but recently also in the United States (Chivvis, 2017b; Lucas & Nimmo, 2015; Polyakova et al., 2016; ODNI, 2017). Russia is supporting the rise of right-wing extremist ideologies as a foil for Western liberal democracy (Stewart, 2017). Putin also desires to destroy Western societies from within by sowing discord and divisions within Western nations (Higgins, 2017; Watts, 2017). Additionally, Russia is exploiting Western openness and pluralism, turning these values into vulnerabilities (Polyakova et al., 2016). Russian political leaders are challenging American hegemony, influence, and morality. The intention is to reverse US global dominance, counteract its foreign policy efforts, and undermine faith in America's democratic processes and public institutions (Bugajski, n.d.; Bugajski, 2016; Lucas & Pomerantsev, 2017; ODNI, 2017). Russia is promoting multilateralism and a poly-centric world order as the preferred alternative to the Western-led international world order (Gorenburg, 2019; Russian Federation, 2015).

The Russian government's information operations activities are not random and innocuous irritants directed at strategic competitors as mere distractions. The Putin regime purposely targets chosen audiences and propagates deliberate messages to achieve specific strategic, diplomatic, and defence policy outcomes and reactions. To achieve this plethora of strategic aims, Russia disseminates strategic narratives to domestic and foreign audiences as one means of gaining support for—or at least diminishing opposition to—its goals and initiatives. These narratives paint Russia's adversaries (the West, the United States, NATO, Europe, and eastern European nations) as perpetrators of injustices while projecting an image of Russia as a desirable global leader (Iasiello, 2017; Lucas & Pomerantsev, 2016; Nimmo, 2015; Rasmussen, 2015; Rumer, 2017). As a means for justifying its foreign policy positions, Russia's leadership speaks out against what they characterize as the nefarious intentions and actions of the West.

This chapter will describe Russia's information warfare concept and methods, as well as offer a detailed case study of Russia's interference in the 2016 US presidential election. The chapter will then offer recommendations for improving the understanding, response, and coordination of Canada, its allies, and the West regarding Russia's information warfare attacks. Russia's

use of information operations to challenge Western alliances, institutions, and the rules-based liberal world order will continue and expand if left unchallenged by Western nations. Russia's governing leaders have declared that their nation is in a perpetual state of information warfare against the West. Consequently, Western nations—including Canada—need to be in a perpetual state of self-defence and deterrence by methodically defending, through strategic communications, the concepts, institutions, and military missions that Russia is attacking. Canada and its Western allies also need to proactively and pre-emptively disseminate strategic narratives that decrease support for Russian aggressive policies and military actions and consequently deter the Russian government from continued attacks. The aim of this chapter's look at Russian information warfare is to convey the gravity and pervasiveness of the Russian threat and to reiterate that a reactive approach is inadequate for the security of Canada as a nation and the liberal-democratic way of life.

Russia's Information Operations: Battling for Control of the Adversary's Mind

Disinformation has become an important aspect of Russia's military doctrine, and Russian political and military leaders put a greater emphasis on information and psychological warfare than their Western counterparts (Fedyk, 2017; Lucas, 2015; MacFarquhar, 2016). For Russia, information warfare is the starting point for any operations since information superiority is imperative for future victories and should be gained as early as possible (Gilles, 2016b; Iasiello, 2017; Koshkin, 2015; Thomas, 2016). Russia considers the main battlespace to be the mind; hence, Russian officials focus on conducting war inside human consciousness through information and psychological warfare. This type of warfare is intended to lay the groundwork for victory—perhaps even without the need to start combat operations and physically invade a specific territory—by demoralizing both the adversary's population and uniformed personnel and destroying any desire to carry out resistance (Chekinov & Bogdanov, 2013; Duncan, 2017; Fedyk, 2017; Galeotti, 2014; Thomas, 2016).

The Russian government has specific objectives it wishes to achieve when attempting to influence domestic and international audiences: the Putin regime uses information operations to philosophically attack the West, specific adversaries, Western military operations, the concept of truth, and to promote Russia's agenda. The wide variety of methods to communicate carefully

constructed narratives through information operations, and the advent of the Internet and social media, have increased Russia's potential reach and influence. These tools and these objectives enable and motivate the Putin regime to directly contact adversaries' populations in an attempt to influence them in favour of Russian strategic aims and security threat interpretations.

Russia's Information Operations Concept

For the objectives of attacking the West, adversaries, military operations, and the concept of truth, as well as promoting Russia's agenda, the Russian government uses carefully constructed narratives that it communicates through information operations messages to audiences around the world—foreign and domestic, decision makers and the public. Disseminating these messages is part of the Russian government's concept of information warfare. This section will describe the key elements of Russia's information operations concept, including the different types of information warfare in addition to Soviet-era practices.

Western military doctrine recognizes separate disciplines for intelligence, counter-intelligence, information warfare, psychological warfare, influence operations, strategic communications, computer network operations, electronic warfare, and military deception. In the Russian context, all these aspects are part of a unified conception of information warfare and confrontation (Gilles, 2016a; Porotsky, 2017b; Tomášek, 2015; Vowell, 2016). Russia's information space includes both the cyber and cognitive domains. In Russian military doctrine, information warfare is divided into two types: information-technical (which aims to affect any technical system that receives, collects, processes, or transmits information) and information-psychological (which aims to affect civilian populations and armed forces personnel). This means that any information source—be it the adversary's computers, smart phones, print media, television, or human minds—are targets for Russian information warfare. Russia's weaponization of information encompasses electronic warfare, cyber warfare, and psychological influence (Foxall, 2016; Gilles, 2016a; Gunzinger, 2017).

Within the information warfare concept, information operations are the starting point for engaging an adversary. The aim is to achieve strategic goals without having to resort to armed conflict by using information warfare to establish favourable political, economic, and military situations and hopefully weaken the adversary and incapacitate the enemy state before armed conflict

breaks out. Targeting mass consciousness and influencing an adversary's military forces and civilian population to capitulate without armed intervention violates that state's sovereignty without the physical seizure of territory. The goal is to influence the adversary to carry out the Russian government's wishes and defeat the enemy without having to engage in costly or risky combat operations (Duncan, 2017; Fedyk, 2017; Gilles, 2016a; Gunzinger, 2017; Iasiello, 2017; Polyakova et al., 2016; Vowell, 2016).

For Russia, there is a persistent and permanent state of conflict; peacetime and the absence of information operations simply do not exist. Whether Russia and another nation are in a state of co-operation or of hostility, Russian leaders believe that enemies are using information warfare against their country. Consequently, Russia must take the offensive and perpetually and permanently conduct information operations against its rivals (Gilles, 2016a; Porotsky, 2017b; Russian Federation, 2014; Shane, 2017). Current Russian information operations use two practices from Soviet-era doctrine: reflexive control and active measures. Reflexive control is defined as the "means of conveying to a partner or opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (Thomas, 2010, p. 237). Reflexive control is the deliberate attempt by the Russian government to create a permissive environment by influencing an adversary's decision makers and population in such a way that they make a decision or carry out actions that are not only to Russia's advantage but were also predetermined by Russia's information operations efforts (Duncan, 2017; Gilles, 2016a, 2016b; Iasiello, 2017; Kepe, 2017; Lucas & Pomerantsev, 2016; Ramussen, 2015; Thomas, 2010).

The second Soviet tactic being applied by the current Russian government is active measures, which is the use of overt and covert techniques (violence, proxies, counterfeits, and information operations) to influence the actions and behaviours of a foreign government and its population. There are three avenues for shaping other nations' foreign policies: state-to-state, state-to-people, and people-to-people. Russia's active measures purposely sidestep state-to-state traditional diplomacy; instead, the Russian government directly contacts adversarial nations' populations or uses proxies such as trolls and think tanks to do so. The World Wide Web and social media have made this contact with foreign audiences extremely easy, immediate, and direct (Duncan, 2017; Gilles, 2016a; Lucas & Pomerantsev, 2016; Porotsky, 2017b; Watts, 2017; Weisburd et al., 2016).

Russia's Information Operations Methods

For the purpose of this chapter, the plethora of techniques and narratives Russia uses for information operations will be categorized as technologically focused, false information, degraded information, overwhelming quantities of information, state involvement, third-party participation, specifically targeted audiences, or the use of all available platforms. Cyber-attacks fall into the category of an information-technical approach to Russian information operations. Cyber-attacks aiding information operations are about denying information to an adversary: "all efforts to disrupt, deny, degrade, destroy the information that . . . [computers] rely upon, store, process, and generate" (Porotsky, 2017b). Russia has conducted distributed denial of service (DDOS) campaigns against its adversaries as part of conflict (e.g., Georgia, Ukraine) and non-kinetic attacks to disrupt states in peacetime, including government, media, financial institutions, and other private targets. In addition to purposely overloading websites so that they crash and cannot be accessed by any user, Russia also purposely defaces websites and replaces content with inaccurate information; corrupts data files; steals funds, intellectual property, and government secrets; shuts down commerce; or attacks critical infrastructure (Gilles, 2016a, 2016b; Iasiello, 2017; Joyal, 2016; Kepe, 2017; Lucas & Pomerantsev, 2016; Porotsky, 2017b; Waltzman, 2017).

Hacking into computer systems is a common Russian information operations activity. The most high-profile hackings recently have been of the Hillary Clinton campaign in the 2016 US presidential election and the Emmanuel Macron campaign during France's 2017 presidential election. Spear-phishing emails are sent to broad communities (campaign workers, politicians' staffers, public servants, government contractors, and related non-profit organizations) with malicious links that will download malware and allow the hackers to see and steal information stored in the compromised email account or the owner's computer. The emails encouraging people to click certain links are crafted to look legitimate. Often the scenario used by hackers is a realistic message warning recipients to log into their commercial email or social media account to reset a password after a suspicious login attempt has supposedly been identified. Another common lure is targeted news articles reflecting the user's extracurricular interests (e.g., sports or Hollywood stories). All it takes is one unsuspecting recipient to click a link to give Russian hackers access. This happened in the United States, not only to

Clinton's campaign chairman, John Podesta, the Democratic Congressional Campaign Committee, and the Democratic National Convention in 2016, but also previously to the White House, State Department, Department of Defense, and Joint Chiefs of Staff. Instead of just gathering information for future use, hackers during the 2016 US elections uploaded the Clinton-related documents they stole onto publicly available websites for the public to consume, and hackers distributed the links over social and conventional media (Calabresi, 2017; Foxall, 2016; Gilles, 2016a; Hern, 2017; Lipton et al., 2016; Shane, 2017; Weisburd et al., 2016). Russia has also hacked the social media accounts and smart phones of NATO soldiers deployed in the Baltic region; the goal is to glean intelligence regarding military operations as well as compromising information that could be used for blackmail, intimidation, or harassment against individuals or to destroy the credibility of that nation's deployed forces (Kepe, 2017).

Security and intelligence analysts have characterized Russia's manipulation of the truth as directing a "firehose of falsehoods" against the West's "squirt gun of truth" (Paul & Courtney, 2016). While ordinary citizens around the world may accidentally participate in propagating misinformation (the unintentional and inadvertent spreading of inaccurate information without malicious intent), the Russian government and its information operations apparatus create and disseminate disinformation (intentionally inaccurate or manipulated information) (Lucas & Pomerantsev, 2017; Paul & Courtney, 2016). Disinformation can take the shape of lies, hoaxes, conspiracy theories masquerading as facts, false facts, the denial of facts, fake videos and altered pictures, propaganda, and deliberate state narratives (Chen, 2015; Duncan, 2017; Gilles 2016a, 2016b; Iasiello, 2017; Joyal, 2016; Kepe, 2017; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Nimmo, 2016; Polyakova, 2016; Pomerantsev, 2014; Skaskiw, 2017; Waltzman, 2017; Watts & Weisburd, 2016). Russian information operations have invested much effort into disseminating disinformation through fabricated news, staged videos of reporters supposedly on the site of events, and fake sock-puppet websites meant to look like legitimate news sources. These are then amplified by social media posts, the sharing of these posts, and conventional Western media reporting (Chivvis, 2017b; Gilles 2016a, 2016b; Guide, 2017; Iasiello, 2017; Lucas & Pomerantsev, 2016; Vowell, 2016; Watts, 2017). Russian information operations use other means of degrading the accuracy of information that Russia distributes. Instead of completely fabricating stories, these efforts can conceal

information, exaggerate, provide half-truths, destroy facts, present selective facts, misquote or falsify attribution, simplify complex topics, or change meanings or original statements by altering the context or translation (Gilles, 2016a, 2016b; Kepe, 2017; Lucas & Pomerantsev, 2017; Paul & Matthews, 2016).

Russian officials use information operations messages that attack the concept of truth. These narratives aim to pollute and degrade the information space for decision makers and populations alike. With so many versions of explanations, the goal is to make it impossible to discern fact from fiction, and to get readers to question what is purported as truth. The Putin regime wants to erode people's confidence in media, experts, and academia's objectivity, professionalism, and accuracy (Bugajski, n.d.; Calabresi, 2017; Dewey, 2016; Gilles, 2016b; Iasiello, 2017; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Porotsky, 2017c; Watts, 2017; Weisburd et al., 2016). The end goal is to create distrust and doubt in what is being communicated in the West and to cause confusion, panic, and internal conflict within Western societies (Boot, 2017; Bugajski, n.d., 2016; Gilles, 2016a, 2016b; Iasiello, 2017; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Porotsky, 2017c; Vowell, 2016; Waltzman, 2017; Watts, 2017; Weisburd et al., 2016). The Russian government does not just promulgate one consistent message with its information operations activities. Different, and sometimes conflicting, messages are disseminated: these are tailored for different audiences, and sometimes the fabricators are testing to see which themes resonate with audiences the best. Since the ultimate goal is to undermine truth, the communications are not intended to necessarily be credible or universally persuasive (Duncan, 2017; Gilles, 2016a, 2016b; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Paul & Courtney, 2016; Paul & Matthews, 2016; Waltzman, 2017). The Russian government uses a multi-channel approach so that audiences are more likely to be exposed to Russia's messages, so that an atmosphere of consensus is created, and so that recipients have the impression that the information must be true since it can be found within so many different sources (Gilles, 2016b; Paul & Matthews, 2016). The Russian government uses its multitude of narratives to change the conversation away from themes disadvantageous to its policies and prestige. Overly sophisticated arguments, presented with ample evidence (even though false), confuse people into accepting the conclusions as true, even if the recipient did not fully understand the argument. Russian information operations can elicit emotional responses of helplessness, dismay, or anger by dismissing critics, deliberately distorting facts, or appealing to fears, divisions, and

discontent (Dawsey, 2017; Gilles, 2016a; Lucas & Pomerantsev, 2016; Nimmo, 2015; Raju et al., 2017; Skaskiw, 2017; Waltzman, 2017).

Identifying truth and falsehoods is made even more difficult with the existence of white, grey, and black outlets, all of which Russia uses to propagate its narratives and disinformation. White channels are overt Russian sources such as state-sponsored and pro-Russian news networks (such as RT and Sputnik News) and legitimate professional Western news networks. Russian information operations use grey outlets, such as English-language dump sites (DC Leaks and WikiLeaks) and conspiratorial websites that sensationalize fake news, hoaxes, and conspiracies. Legitimate Western news networks often report news found on grey channels, thus amplifying, disseminating, and legitimizing the disinformation among Western audiences. Grey channels can be controlled by Russia (but this is harder to trace) or promoted by "useful idiots" who chose to regurgitate Russian themes voluntarily and without any ties to Russia. Black outlets are covert operations where hecklers, hackers, and bots use fake or hacked social media accounts that appear to be those of ordinary citizens residing in Western countries. This information is even more difficult to link to official Russian direction, but these information operations efforts are deliberately sinister and purposely intend to distribute and amplify disinformation, propaganda, and Russian narratives (Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Porotsky, 2017c; Watts, 2017; Weisburd et al., 2016).

The use of third parties allows the Russian government to be disconnected enough from information operations to claim plausible deniability. Russian officials use proxies—groups that are sympathetic to Russian objectives or policies—around the world to carry out information operations messaging. This can be Russian gangs and biker clubs that engage in intimidation tactics domestically; or European protest movements or far-right political parties; or Russian diasporic populations in the Baltics that perpetuate complaints of discrimination and mistreatment; or American citizens who use social media to amplify links to websites, articles, or ads created by Russian sources on divisive social issues. Local actors are easier to believe and more difficult to tie to the Russian government (Chivvis, 2017b; Duncan, 2017; Guide, 2017; Iasiello, 2017; Lauder, 2017).

Russian information operations have achieved a high impact through social media by using humans and automation to disseminate and amplify disinformation and propaganda. Russian disinformation agencies hire people

to hold multiple fake social media accounts (usually under false identifies, often pretending to be from the United States or other Western countries) so that they can engage other social media users for the purpose of propagating Russia's strategic narratives, polluting the information environment with disinformation, polarizing online communities by focusing on controversial social and political issues, and diverting and suppressing actual political debate. Called "trolls," these individuals use their hacked, hijacked, or black-market social media accounts to flood news site comment sections and social media with sensational views and links to fake news stories or websites featuring stolen/hacked documents. Agencies with ties to the Russian government have hired so many of these online hecklers that they are called troll farms or factories. The Internet Research Agency (IRA), based in St. Petersburg, has been identified as such a troll factory; it operates around the clock with over a thousand employees each working twelve-hour shifts to meet individual daily quotas, such as 135 posted comments, each of 200 characters minimum, as well as 80 comments and 20 shares of internally created blogs, for propagating assigned themes and messages over Live Journal, VKontakte, Facebook, Twitter, Instagram, and various chat rooms, discussion fora, and news comment sections (Bertrand, 2017; Boot, 2017; Calabresi, 2017; Chen, 2015; Chivvis, 2017b; Fedyk, 2017; Gilles, 2016b; Iasiello, 2017; Lapowsky, 2017; MacFarquhar, 2018a; Porotsky, 2017c; Shane, 2017; Shane & Goel, 2017).

Trolls not only hold multiple identifies over numerous social media platforms to increase the quantity of disinformation each individual can push into global communications systems; they also further amplify their impact by using bot networks—groups of computers and/or social media accounts that have been automated to send out messages based on built-in instructions. Thousands of Russian-linked Twitter accounts have been automated, and they repeatedly send out the identical message, seconds apart and in alphabetical order based on the bots' account names on the automation list. Cyborg accounts are heavily automated but require some human involvement in their operation. During the 2016 US presidential election, six hundred troll and bot accounts were synchronized with news being broadcast from the RT and Sputnik News websites, further amplifying official Russian narratives. The use of humans and bots increases the proficiency with which malicious actors can flood and pollute the information space with manipulated material; in many cases, they eventually succeed in getting legitimate media sources to report on the inaccurate and false stories as if they constituted genuine breaking news

(Bertrand, 2017; Gilles, 2016b; Porotsky, 2017c; "Russian Twitter accounts," 2017; Rutenberg, 2017).

Some trolls take on a more intimate interactive role with targeted social media users—also known as the role of a honeypot. Based on the historical use of attractive female spies to lure adversaries' agents into compromising situations, the online honeypot sets up a social media profile that might feature an attractive profile picture, but more often than not, online honeypots present themselves as having common interests (e.g., hobbies, political views) so that they can befriend other online users, who have purposely been selected through social engineering to be susceptible to Russian information operations efforts. After building trust and lowering defences via these commonalities, the honeypot will start to work on the target's political views by introducing political discussions that propagate Russian influence narratives; sending links to supposed articles of interest that in reality will download malware onto the target's computer; attempting to entrap the target in a compromising situation or find embarrassing information on their electronic devices in order to blackmail them and secure their compliance; or bringing an agent of influence into the conversation, under the guise of introducing a friend, to expertly argue Russian positions regarding political and geopolitical issues. The goal is to convert this local individual into a believer of Russian positions so that they will share Russian narratives and propaganda links, shut down healthy debate among his/her own friends, or vote against politicians who oppose Russian policy positions (Porotsky, 2017c; Watts, 2017; Weisburd et al., 2016).

Although the Russian government uses proxies for hacking computers and disseminating information operations messages over social media, the state is directly involved in shaping the information sphere. Russia is able to control the messages heard by domestic audiences through censorship of anything that does not support state narratives and policies and through state ownership or state control of the television, newspapers, and radio stations that Russian citizens access. The propaganda with which domestic audiences are inundated encourages citizens to feel paranoid and to believe that their nation, culture, and way of life is under siege by the West (Pomerantsev, 2014; Skaskiw, 2017).

State-owned and state-controlled media also carry the Russian government's propaganda and narratives to international audiences as well. RT (formerly known as Russia Today) and Sputnik News are both operated by

a company that is funded by the Russian government. Margarita Simonova Simonyan has been editor-in-chief of RT since 2005; on 31 December 2013, she was also made editor-in-chief of the government-owned news agency Rossiya Segodnya (which runs the Sputnik News agency, websites, and radio broadcasting services). RT, which now reaches international audiences (in English, Arabic, German, and Spanish), originally aimed at changing the world's view of Russia, but the network has rebranded itself for greater impact (and responsiveness to the Russian government's information operations efforts), such that it now questions more and purposely features stories that have not been reported by the mainstream media. Sputnik News provides an alternative to the Western media's unipolar world view and aims to tell what it claims is the untold story. This agency is anti-Western, anti-establishment, and is purposely hostile toward mainstream media; it targets disenfranchised audiences, and its gives disproportionate coverage to dissident members of European countries' governments. RT and Sputnik News propagate news stories that have been approved by the Russian government; these stories contain a mixture of truthful fact and skewed and manipulated information. These television and Internet articles are amplified over RT's and Sputnik News's social media accounts (and associated trolls and bots). The Russian government attracts non-Russian audiences in Ukraine and the Baltics because the Russian programming there tends to be more professional-looking and entertaining than local media productions. These audiences tune in to Russian television for the serials and talent shows, but viewers end up continuing to watch the news and current affairs programs, thus becoming exposed to Russian propaganda, narratives, and interpretations of world affairs (Chivvis, 2017b; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Nimmo, 2016; ODNI, 2017; Paul & Courtney, 2016; Rutenberg, 2017; Weisburd et al., 2016).

Besides controlling media messaging through its control of domestic audiences, the Russian government skews academic research by funding academic institutions and think tanks with the purpose of producing allegedly credible reports to support Russian policies, claims, and narratives. Russia also funds European politicians and protest movements that expound Russian positions and criticize the United States and other Western organizations (Chivvis, 2017b; Lucas & Pomerantsev, 2016; Stewart, 2017; Thomas, 2016; Waltzman, 2017).

By using all forms of information dissemination—state and commercial television, newspapers, radio, the Internet, social media platforms, and in-person influence agents, along with trolls, bots, and false accounts, conventional and social media synchronization;, and white/grey/black sources and outlets—Russian information operations efforts have been structured to reach as wide a range of audiences as possible. In addition to controlling the messages heard by domestic audiences and crafting propaganda to maintain domestic support for the Russian government and its actions, Russian information operations are directed at audiences in eastern Europe, western Europe, the United States, and their allies. Russian information operations target discontented groups around the world, looking for individuals who will believe and disseminate Russian narratives over social media. Information operations target journalists and politicians' staff to see who might be willing to engage in pro-Russian dialogue and to promote pro-Russian policies and narratives.

Influencing the selection of decision makers during elections requires the targeting of an adversarial nation's domestic population. Information operations are used to influence public opinion, affect mass consciousness, manipulate popular perceptions, and perhaps even destabilize a nation from within or suppress voter segments by severely dividing opinion or causing people to lose faith in the potential/resulting mandate (Gilles, 2016a, 2016b; Gunzinger, 2017; Iasiello, 2017; Joyal, 2016; Lucas & Pomerantsev, 2016; Porotsky, 2017b; Raju et al., 2017; Thomas, 2016; Tomášek, 2015; Shane, 2017; Waltzman, 2017; Weisburd et al., 2016).

Elections offer a target-rich environment where voters turn to the Internet to get the latest news on candidates' platforms and to social media to discuss contrasting policy views. The Russian government turned the Western media's tools and practices for supporting democratic debate against European and American establishment candidates in 2015, 2016, and 2017, flooding the Internet and social media with propaganda, disinformation, and stolen private correspondence resulting from computer hackings, as well as through Russian news agencies, social media trolls and bots, and independent users convinced and confused by Russian information operations efforts. The following section will detail Russia's information operations efforts during the 2016 US presidential election and how it sowed confusion and division by offering multiple conflicting narratives and amplifying already contentious topics.

Russian Information Operations during the 2016 US Presidential Election

The Russian government has been evolving its use of hybrid warfare and information operations over the past decade. On the one hand, after the information attack on Estonia in April 2007, the Putin regime has combined information operations with conventional warfare in its near-abroad, as seen in Russia's interventions in Georgia and Ukraine (Crimea) (Chivvis, 2017b; Duncan, 2017; Fedyk, 2017; Foxall, 2016; Iasiello, 2017; Joyal, 2016; Lucas & Pomerantsev, 2016; Polyakova, 2016; Vowell, 2016). On the other hand, Russia has depended more on information operations techniques when it comes to intimidating Baltic nations, potential NATO members, and NATO missions (Brewster, 2017; Campion-Smith, 2017; Gilles, 2016a; Henderson, 2016; Kepe, 2017; Lucas & Pomerantsev, 2016; MacFarquhar, 2016; Read, 2016). More recently, the Russian government has discovered the impact it can have by systematically using the Internet and social media to interfere with democratic elections in the United Kingdom, France, Germany, Spain, and the United States (Alandete, 2017; Daniels, 2017; "France's Macron," 2017; Schwirtzsept, 2017; Stelzenmüller, 2017; Watts, 2017). All of these examples demonstrate that Russia is actively conducting information operations to support its strategic objectives against its adversaries, those from both near and abroad. The logical conclusion is that the Russian government will continue to practise and perfect these methods unless Western nations disrupt Russia's information operations capabilities. Russia has had the greatest information warfare success when countries are not prepared for Russian information operations interference. Whether the nation is a small country or one of the Western powers, Russia's ability to hack computer networks and directly reach the voting public can have serious and detrimental consequences if a government is unsuspecting or complacent in terms of technical and psychological preparations and protections. The case study of Russian interference in the 2016 United States presidential election is of relevance since it directly impacts Canada's closest ally as well as the defence of North American democracies.

EXPECTED AND UNEXPECTED ELECTION INTERFERENCE: ELECTRONIC POLL BOOKS AND EMAIL HACKING

When American officials considered how the Russian government might interfere with the 2016 presidential election, the inclination was to protect voting technology against tampering so that voting counts could not be changed. It appears that these protection efforts were successful; there has

been no evidence of this type of vote tampering. Nevertheless, Russian hackers did interfere with some states' electronic poll books (laptops and tablets loaded with voter check-in software). For example, VR Systems, the electronic poll book supplier for North Carolina, was hacked by the GRU (Glavnoye Razvedyvatelnoye Upravlenie, Russia's military intelligence body) in August 2016. The hackers then sent spearphishing emails from fake VR Systems email accounts to 122 local and state election jurisdictions in the hope that some election officials would be tricked into downloading malware that would allow the hackers to take over computer systems linked to the US election process. On Election Day, the hackers manipulated electronic poll books to keep some Americans from casting their votes. At the polling stations, people were told that, according to the electronic poll books, they had already cast ballots, or were ineligible to vote, or needed to go to another polling station (where they were turned away again since this information was wrong). Some North Carolina counties experiencing electronic poll book problems reverted to paper registration lists, but this slowed the voting process so much that large numbers of voters gave up waiting and left the polling stations without casting a ballot. Electronic poll book problems often occurred in counties where the largest cities were located. Russian hackers targeted the election systems of twenty-one states during the 2016 presidential election. Russian spies had been collecting intelligence since 2014 on US election processes and technological equipment, and they determined that the most profitable course of action would be to avoid altering vote tallies and instead target Internet-based systems such as email accounts, voter databases, election websites, electronic poll book vendors, and back-end election services (Perlroth et al., 2017).

The Russian government's interference with the US political system did not just begin during the 2016 presidential election campaign. Hacking efforts and social media disinformation operations both started in 2014, and these grew more extensive the closer the election came. Hackers linked to the Russian government penetrated unclassified email systems in the State Department in November 2014, and the Joint Chiefs of Staff in July 2015, by successfully installing malware that took data out of the hacked email accounts. In March 2016, the State Department was hacked again, and in June 2016, hackers stole one hundred thousand individual tax returns from the Internal Revenue Service. Hackers have been using spearphishing emails to install malware on computers by including supposed links to stories likely to be of interest to the email account holders. During the summer of 2015, the

group of Russian hackers known as Cozy Bear sent spearphishing emails to government agencies, government contractors, and non-profit organizations in Washington, DC. In 2016, messages were sent to ten thousand Department of Defense Twitter users with links, masquerading as special interest stories, that would download malware. The day after the November 2016 election, Cozy Bear hackers sent another five waves of spearphishing emails, this time to think tanks and non-profits, hoping to get access to more email accounts after the successful hacking of Democratic Party members during the 2016 election (Calabresi, 2017; Foxall, 2016; Lipton, 2016).

Russian hackers had been trying to hack into members of the Hillary Clinton election campaign more than a year before the presidential election. Cozy Bear hackers had successfully hacked into the Democratic Congressional Campaign Committee (DCCC) email system before September 2015, which is the month that an individual from the Federal Bureau of Investigation (FBI) contacted the DCCC to let them know that at least one of their computers had been compromised by Russian hackers. The DCCC contact who took the FBI's call did not believe he had really been speaking with the FBI, and hence did not follow up with the caller's information. DCCC information technology specialists did not immediately see evidence of Russian hackers in their computer systems, and thus did not hire cyber-security experts to help until April 2016. In the meantime, the hackers were gleaning information with impunity, first to simply gather intelligence; this subsequently evolved into an operation to harm Clinton's election campaign. The DCCC's realization concerning the breech came a month after Cozy Bear had hacked into the DCCC and sent spearphishing emails to Clinton campaign members. A campaign worker clicked a link to change a supposedly compromised Google email password, which resulted in campaign chairman John Podesta being hacked and sixty thousand of his emails stolen. In May 2016, a member of the GRU publicly bragged that Hillary Clinton would experience payback for her 2011 influence operation against Putin and her role in orchestrating the mass protests in Russia during Putin's 2012 election campaign. Three days before the DCCC meeting, on 22 July 2016, WikiLeaks began publishing sensitive emails stolen from the DCCC. Podesta's emails were leaked to the public on 7 October 2016, one month before the presidential election vote. Russian hackers timed these leaks to ensure that voters were inundated with the media's reports of, and reactions to, the emails' politically embarrassing contents during critical decision points (Calabresi, 2017; Lipton, 2016).

THE INTERNET RESEARCH AGENCY TROLL FARM

An additional surprise to American election officials, voters, and politicians was Russia's level of cognitive interference in the 2016 election through a deliberate disinformation campaign that used fake news, fake websites and videos, fake advertisements, fake persona, and fake accounts on social media, all of which were fed directly into American voters' Facebook, Twitter, and Instagram accounts. After the 2016 presidential election, it was discovered that false personal social media accounts and Twitter bot accounts were involved in Russian disinformation activities, and these were linked to the well-known Russian troll factory called the Internet Research Agency (IRA) (Lapowsky, 2017; Mueller, 2018; Stretch, 2018). In 2011, Russian opposition groups hostile to Putin used social media to convince Russian citizens to carry out anti-government protests. Putin reacted by taking greater control of the Internet: bloggers had to register with the government, some websites were censored, and some social media platforms experienced government pressure while Kremlin allies took control of other platforms. The government instituted purposeful posting of pro-government messages on social media to drown out opposition voices as well; one such messaging factory, the IRA, was established in 2013 as a Kremlin-backed propaganda arm for Putin. Originally, it focused on communicating with domestic audiences by flooding social media with messages that attacked opposition figure Aleksei Navalny, praised the stability of Putin's regime, criticized the chaos and moral corruption of the United States and the West, condemned the West's economic sanctions, and supported the annexation of Crimea and the separatist insurgency in eastern Ukraine. Putin aimed to spoil the Internet for Russian citizens; he wanted to cultivate an atmosphere of hate and negativity with the trolls' activities so that most people would not want to use the Internet. People were attracted to the IRA by the salaries it offered recruits—which were notably higher than typical Russian wages. By late 2014, approximately four hundred people were working twelve-hour shifts for the IRA, thus enabling the troll factory to send out messages 24/7 (Calamur, 2018; Davlashyan & Titova, 2018b; MacFarquhar, 2018a, 2018c; Mueller, 2018; Taylor, 2018).

In 2014, the Russian government decided that the approach of officially disseminating Russian narratives and denigrating adversaries could work against foreign audiences as well, so efforts began to communicate directly with Western audiences over social media. In April 2014, the IRA formed a

separate department to oversee the Translator Project—disinformation activities targeted specifically against the United States, carried out over Facebook, Twitter, Instagram, and YouTube. The Translator Project was part of a larger interference operation called Project Lakhta, which included all of the IRA's disinformation targeting both domestic and foreign audiences, with the goal of solidifying Putin's support in Russia and spreading confusion and distrust of government institutions in the West. The strategy to interfere with the 2016 US presidential election was devised in May 2014. Employees at the IRA began monitoring American social media accounts focused on politics and other sources of information about the 2016 election. The goal of the IRA's trolls was to spread distrust about US candidates and the political system in general and to create discord and tensions among the electorate before the vote took place. The IRA grew to over one thousand employees by 2015. There were approximately eighty to ninety people working on the Translator Project, the majority being students from St. Petersburg University. Not only were they highly skilled in the English language, but they were also working on degrees in international relations, linguistics, or journalism. Because of this specialized expertise, their pay rates were double those of the trolls working in the domestic operations department (Apuzzo & LaFraniere, 2018; Calamur, 2018; Davlashyan & Titova, 2018a, 2018b; MacFarquhar, 2018a, 2018b, 2018c; Mueller, 2018; Scannell et al., 2018).

By early 2016, the Putin regime and the IRA purposefully began supporting the Republican Party's presidential candidate, Donald Trump, and attacking the Democratic candidate, Hillary Clinton. On 10 February 2016, officials at the IRA circulated guidance that social media posts should contain content about the US elections, including derogatory information about Clinton. Employees were encouraged to denigrate other Republican candidates as well, such as Ted Cruz and Marco Rubio, but instructions were given to be supportive of Democrat Bernie Sanders in addition to Trump. It has also been reported that Putin believed that Clinton sponsored the release of the Panama Papers (stolen documents from the legal firm Mossack Fonseca, which specializes in facilitating offshore banking). Because these documents implicated Putin and his close friends in crime and corruption related to $2 billion worth of offshore deals and loans, Putin reportedly decided in April 2016 to retaliate against Clinton by attacking her election campaign efforts (Apuzzo, 2018; Gregory, 2016; Harding, 2016; Mueller, 2018; Taylor, 2017).

By the summer of 2016, the IRA's monthly budget for Project Lakhta was US$1.25 million, which was being funded by the wealthy Russian oligarch Yevgeny Prigozhin through the entities that make up his Concord Management and Consulting group of companies. Prigozhin became a favoured business contact of Putin. Once known as Putin's chef (since Prigozhin frequently provided Putin with catering services), Prigozhin has financially benefited from being willing to conduct favours and less savoury tasks for Putin, such as recruiting soldiers to fight in Ukraine and Syria, providing soldiers to protect Syrian oil fields, and establishing an online news service that disseminates nationalist views; he is the founder and head of the private military contractor organization known as the Wagner Group. Putin rewarded Prigozhin's loyalty and work through lucrative government contracts (he has received US$3.1 billion worth in the five-year period 2012–17) and a percentage of Syria's oil revenues. Since Prigozhin not only funded the IRA's disinformation operations, but has also met and communicated frequently with the IRA's top official, General Director Mikhail Bystrov, he both controls and approves of the IRA's work against the United States and the West. Because of the Putin regime's relationship with the IRA's patron, US government officials and security analysts have determined that Putin and his government endorse the IRA's mandate and operations while enjoying the plausible deniability of working through an intermediary. According to security analysts, individuals in developed states do not launch private wars against the world's superpower; hence, the type of Russian troll attacks that were occurring throughout the US election would have needed the Russian government's approval (Calamur, 2018; Davlashyan & Titova, 2018b; MacFarquhar, 2018a, 2018b; Mueller, 2018; Scannell et al., 2018).

IRA SOCIAL MEDIA ACTIVITY IN THE US 2016 PRESIDENTIAL ELECTION

The IRA's trolls interfered with the 2016 US presidential election by opening social media accounts using false identities; these fake profiles were intended to convince other users that they belonged to Americans, ranging from ordinary citizens to politically engaged individuals to political activists (Apuzzo, 2018; Edgett, 2017; Mueller, 2018). In addition to opening accounts on Facebook and Twitter under fake identities, these IRA trolls also created Twitter bot accounts that were programmed to relay propaganda automatically without human involvement; hundreds of these automated accounts would often amplify the same message at the same time, in alphabetical order

of the account names on the IRA's distribution lists. In addition to 2,752 IRA-linked Twitter accounts producing organic content (free messages and posts, as opposed to paid advertisements), Twitter was able to identify 36,746 bot accounts more widely linked to Russia (Edgett, 2017, 2018; Lapowsky, 2017; Mueller, 2018; Popken, 2017; Porotsky, 2017c; Smith, 2017; Solon & Siddiqui, 2017; Stretch, 2017).

IRA employees used stolen identities (social security numbers, addresses, and dates of birth) and illegally purchased credit cards and bank account numbers to pass verification checks when opening PayPal accounts. Such accounts were often used to purchase advertisements on multiple social media platforms. The IRA had 470 Facebook accounts involved in spending over US$100,000 to purchase 3,000 ads on Facebook. Nine Russian-linked Twitter accounts conducted ad campaigns. Two RT Twitter accounts carried out 44 ad campaigns (costing $234,600 for ads targeting US audiences), while the other seven accounts spent US$1,184 to run 50 ad campaigns in the United States. Twitter earned US$1.9 million from all of RT's advertising efforts. Google determined that Russians spent US$4,700 on advertising over its platforms, as well as eighteen YouTube channels where 1,108 videos (amounting to forty-three hours of viewing material) had been uploaded in connection with the US election (Apuzzo, 2018; Dawsey, 2017; Edgett, 2017; Guide, 2017; McCabe, 2017; Mueller, 2018; Popken, 2017; Raju et al., 2017; Seetharaman, 2017a; Solon & Siddiqui, 2017; Stretch, 2017, 2018; Walker, n.d.).

IRA trolls' social media accounts were actively posting organic messages during the election campaign. The 470 Facebook accounts identified as linked to the IRA created 80,000 pieces of organic content. Between September and November 2016, the 2,752 IRA Twitter accounts pushed out election-related tweets, half of which were automated messaging. Social media investigators discovered 170 IRA Instagram accounts that posted over 120,000 pieces of content during the election. Social media platform executives estimated that approximately 150 million Americans were exposed to Russian election propaganda (Lapowsky, 2017; Smith, 2017; Solon & Siddiqui, 2017; Stretch, 2017).

IRA employees used Facebook to help organize political events in the United States, such as protests and rallies. By January 2018, Facebook investigations determined that the IRA had set up thirteen Facebook pages through which trolls created 129 events and sent out notifications announcing these events, aims, times, and locations. These Facebook event notices were seen

by 338,300 Facebook accounts, and 62,500 users indicated that they would be attending at least one of the IRA's events. With information available in October 2017, the *Wall Street Journal* found that eight IRA Facebook accounts had publicized, and even financed, 60 events; the Facebook notices for these 60 events alone were liked two million times. It has been confirmed that at least 22 of the 60 events actually took place. IRA trolls pretended they were politically engaged Americans who wanted to organize public gatherings on a variety of topics, some of which conflicted: supporting police shot in the line of duty versus protesting police shootings of civilians; wanting to make Muslim neighbourhoods safer versus opposing an Islamic centre in Houston; pro-Trump rallies versus African Americans protesting the election of Trump; anti-Clinton rallies versus rallies supporting Clinton because she supported Muslims and Islamic law. Although some events were sparsely attended, others garnered media coverage, thus increasing their legitimacy. IRA employees had impact within the United States using their Facebook pages and accounts: people attended events; there were actual confrontations between protesters and counter-protesters; Americans helped organized events on behalf of one of the IRA's fake American personas, who could not attend; and the organizing and advertising of events via Facebook got other American activists to volunteer to help with future IRA political events (Lapowsky, 2017; Mueller, 2018; O'Sullivan, 2017; Scannell et al., 2018; Seetharaman, 2017b; Shinal, 2018; Stretch, 2018).

SPECIFIC IRA MESSAGES AND GOALS IN THE US 2016 PRESIDENTIAL ELECTION

With the potentially global exposure offered by social media, the IRA had three objectives for their accounts, bots, ads, and events: to divide the American electorate with divisive messages on political issues; to support Trump and harm Clinton's campaign; and to suppress voter turnout. Russian trolls helped inflame discord among American voters during the 2016 election with their purposely anti-immigration messaging designed to appeal to supporters of Trump's hardline positions (e.g., the proposed Muslim travel ban). IRA employees promoted anti-Muslim messages in ads, organic posts, and events. Other controversial topics included ethnic and racial issues, the right to gun ownership, religion, and lesbian, gay, bisexual, and transgender rights (Apuzzo, 2018; Dawsey, 2017; Lapowsky, 2017; Mueller, 2018; O'Sullivan, 2017; Raju et al., 2017; Satter & Vasilyeva, 2018; Solon & Siddiqui, 2017; Stretch, 2017; Taylor, 2018).

In keeping with the direction given by Putin and IRA management, the IRA's social media material began in 2016 to explicitly support candidate Trump and denigrate Clinton's credibility as a potential president. Attacks on Clinton included fake stories about her having Parkinson's disease, running a pedophile ring, and being involved in murder. IRA employees used social media ads to try to convince voters that Clinton supported the institution of sharia law in the United States. Furthermore, IRA Facebook and Twitter accounts (human and bot) disseminated links to hacked email dumps on WikiLeaks and DCLeaks.com (Apuzzo, 2018; Calabresi, 2017; Dawsey, 2017; Edgett, 2017; Mueller, 2018; ODNA, 2017; O'Sullivan, 2017; Porotsky, 2017c; Shane, 2017). IRA employees, using their fake American social media personas, contacted members of the Trump campaign in Florida and New York more than once seeking co-operation during IRA rally or protest events. There is evidence that some Trump campaign workers did respond to these fake personas (e.g., a volunteer from Trump's New York campaign agreed to provide signs for a pro-Trump rally march organized by the IRA) (Mueller, 2018; Scannell et al., 2018).

Voter suppression occurred when IRA-linked Twitter accounts sent messages instructing Clinton supporters to vote online, by text, or over the phone—methods that had not been implemented by American election institutions. IRA-linked social media accounts encouraged Muslim Americans to boycott the 2016 elections, claiming that Clinton would continue the war against Muslims in the Middle East if elected. Other messages told African-American readers they were better off not voting (rejecting both Clinton and Trump) or voting for a third-party candidate such as Jill Stein. More generally, IRA-linked accounts aimed to discourage voters from taking part in the election with allegations of voter fraud by the Democratic Party (Edgett, 2017, 2018; Mueller, 2018; Satter, 2018).

With the quantity of information shared on social media about an individual's personal preferences, political views, and opinions on social issues, social media platforms (as well as outside companies such as Cambridge Analytica) have created algorithms that can segment users into subgroups, identify the hot-button issues most likely to garner reactions from certain individuals, and enable other users to target audiences with specific messages and disinformation that speak to their interests, pull emotional strings, and elicit a desired response (Brannelly, 2017; Calabresi, 2017; Porotsky, 2017a).

IRA social media accounts were known to target individuals, specific social groups, and particular geographical regions with their messages, posts, and ads. Russian information operations have targeted the social media accounts of journalists deemed to be more gullible or likely to believe conspiracy theories. These accounts are then flooded with links to false stories, with the expectation that the targeted journalist will report on these links in mainstream media and disseminate them to his or her social media followers. IRA employees used social media to identify which congressional aides might be favourable to Russia's policy objectives; these staffers would then begin to receive stories, ads, and posts about Russian policies, with the IRA operatives hoping the staffers would share their personal opinions and views with their members of Congress in an effort to gain support for the issue by an elected member of the US government. IRA trolls would target specific social groups based on the organizations that these users were following, pages they had liked, or key words that were common in their posts and profiles (e.g., "Christianity," "God," "conservatism," "family," "country," "American," "patriotic," "and military"). Russian disinformation operations over social media platforms, such as Facebook ad campaigns, were seen to have targeted three states that were key to Trump's election victory: Wisconsin, Michigan, and Pennsylvania. The goal was to reinforce pre-existing divisive views in order to get chosen users to convince friends and family to vote the same way (i.e., for Trump), to nudge other voters to solidify their pro-Trump tendencies by committing to voting for him; to persuade those who were undecided to vote for Trump on a specific issue about which the disinformation campaign informed them; and to discourage Democratic voters who were not thrilled with Clinton as a candidate from supporting her on Election Day, either by not voting at all, voting for a third-party candidate, or voting for Trump as a protest vote (Calabresi, 2017; O'Sullivan, 2017; Porotsky, 2017b, 2017c; "Presidential election results," 2017; Raju et al., 2017; Watts, 2016, 2017).

ESTIMATING THE POTENTIAL IMPACT OF IRA SOCIAL MEDIA INFORMATION OPERATIONS

Without further data identifying the number of American social media users who saw Russian ads, events, or posts, and the number of American voters who made their political choice in 2016 based on Russian-linked social media material and interactions, it will remain unknown exactly how much impact Russian information operations had on the 2016 US election in taking votes

away from Clinton and increasing support for Trump: Russian influence could have been manifested by Democratic voters' choosing not to vote at all because they were turned off from supporting Clinton due to IRA social media messaging and disinformation, by potential Democratic voters casting protest votes for Trump or a third-party candidate, by persuading individual voters to choose Trump based on specific policy preferences, or by solidifying anger over divisive issues to such an extent that typically complacent individuals decided to cast ballots in order to make sure their voices were heard. There were three states where Trump won the Electoral College votes by less than 45,000 votes: in Pennsylvania (representing 20 Electoral College votes), Trump won by 44,292 votes; in Wisconsin (10 Electoral College votes), Trump won by 22,748 votes; and in Michigan (16 Electoral College votes), Trump won by 10,704 votes. Consequently, Trump won the US presidency based on a difference of 77,744 votes over three states. If Clinton had been able to garner merely 77,745 votes across these three states, she would have won 46 extra Electoral College votes and, consequently, the presidency. It is possible that Russian information operations could have changed the votes of less than 78,000 voters (which is 0.56 per cent of the electorate) in these states' total 13,940,012 votes cast—out of 4,799,284 total votes in Michigan, 2,976,150 in Wisconsin, and 6,165,478 in Pennsylvania—and hence the outcome of the 2016 election (Borchers, 2017; "Presidential election results," 2017; Raju et al., 2017; Scannell et al., 2018).

Although Facebook and Twitter executives tried to downplay the impact of Russian social media activities (e.g., by emphasizing that the quantity of Russian-linked content present on Facebook's newsfeeds was estimated to be only 0.004 per cent of all newsfeed content), the fact that 150 million Americans were exposed to Russian disinformation over social media shows that a significant portion of the American voting population was subject to the nefarious actions of a foreign power. In 2016, the US population was approximately 323.1 million people; approximately 235.3 million of these people were of voting age. This means that 63.8 per cent of the voting population could have been exposed to Russia's social media content (150 million out of 235.3 million). Among Americans old enough to vote, 65 per cent used the Internet as their leading source of election news; this translates to 152.945 million voters who were using online information to stay informed on election-related issues. This means that 98 per cent of voting Americans using the Internet for election information could have been exposed to Russian

social media disinformation (150 million out of 153 million). These calculations are simply meant to demonstrate that the number of Americans exposed to Russian social media disinformation was by no means insignificant. Of course, not every American voter using the Internet for news uses social media for that purpose. Furthermore, of the 150 million Americans exposed to Russian information operations material, it is unknown how many of these users are duplicate users across multiple social media platforms. Although the current data does not allow analysts to calculate how many people were turned away from voting for Clinton, were influenced to vote for Trump, or remained uninformed by debate due to cloistering themselves in echo chambers and avoiding exposure to other opinions and points of view, former Central Intelligence Agency director John Brennan's assessment that it is "implausible that Russian actions did not influence the views and votes of at least some Americans" is nevertheless both sobering and probably true (Edgett, 2018; Scannell et al., 2018; Stretch, 2017, 2018; Walker, n.d.).

Examples of recent Russian information operations and interference should be a call to action for Western leaders to better protect citizens and governments against Russian influence narratives causing confusion and division. The following section will outline some recommended measures that the West, its allies, and Canada could take in order to counter Russian information operations and diminish adversaries' information warfare capabilities.

Recommendations: Deliberate Strategic Communications Efforts Needed

The Russian government, under the leadership of Putin, has deliberately designed an omnipresent information operations threat. Russia not only acts within a persistent state of information warfare; its use of information operations to challenge Western alliances, institutions, and the rules-based liberal world order will continue and indeed expand if left unchallenged by Western nations. By comparison, some analysts argue that the Western response to Russian information operations has been slow, reactive, piecemeal, amateurish, and inadequate (Nimmo, 2015). Unless Western nations counter Russian information operations with the same level of persistent, deliberate messaging, accompanied by their own thoughtful development of information operations concepts and methods for global audiences, Russia will continue to maintain information operations superiority and do damage to Western ideals, alliances, societies, democracies, government institutions, election

processes, and the belief in truth. The failure to substantively react to election meddling and interference efforts by Russia means these activities will continue into future elections and evolve into something even more insidious (Berthiaume, 2017; Boutilier, 2018; Bronskill, 2021; Canada, 2017; Nanji, 2017; Wherry, 2017). This final section will outline recommendations for improving the West's (and Canada's) information operations capabilities.

Russia is spreading disinformation about Western nations and NATO members, which forces the attacked countries to try to undo the damage and dispel myths by sharing truthful accounts after the fact. Psychological studies have shown that it is harder to dispel people's beliefs in information they have already internalized and accepted. Western nations need to carry out strategic communications campaigns that proactively tell audiences what Western democracies represent before disinformation has been distributed by adversaries. To this end, the Government of Canada needs to develop a narrative that explains to domestic, international, allied, neutral, and adversarial audiences what defines Canada, its beliefs, and its actions. For example, Ian Schugart (deputy minister of foreign affairs at the time) articulated the following vision for Canada to a Department of National Defence/Canadian Armed Forces audience in late February 2018: Canada believes in, will work for, and will defend open trade, free navigation of the seas, multilateralism, multilateral institutions, a rules-based world order, human rights, and democratic and coalition-based solutions to international problems. Such a narrative needs to be officially created and disseminated proactively by whole-of-government strategic communications capabilities.

Government strategic communications expertise is not just needed in military theatres during combat missions; strategic communications capabilities are also needed in peacetime as a means of maintaining public support and pre-emptively deterring some adversarial information operations attempts. For each known object of Russian attack, there needs to be a deliberate and proactive Western response to deliberately defend what the Putin regime is specifically trying to destroy. Nations that support the rules-based liberal world order need to develop and disseminate narratives that promote democracy and democratic institutions, defend liberal values and the concept of truth, and protect the countries' being attacked by Russia by promoting these nations' positive contributions and right to self-determination, and by exposing Russia's aggression, hypocrisy, corruption, and detrimental actions toward neighbours and the international community (Calabresi, 2017; Fedyk,

2017; Gilles, , 2016a, 2016b; Guide, 2017; Lucas & Pomerantsev, 2016; Nimmo, 2015; Šuplata & Nič, 2016; Synovitz, 2017; Watts, 2017).

Western nations need to create and support organizations—either within government or through non-governmental organizations—that are dedicated to identifying, monitoring, tracking, studying, analyzing, and advising on Russia's (or any adversarial actors') information operations efforts. Strategic communications organizations need to be stood up that consist of expert researchers, professional writers, and technology platform operators to disseminate the necessary material across social media, the Internet, and other telecommunications platforms. Civilian and military researchers at such interdisciplinary institutions would study information attack examples to clearly identify what Russia attempts to do and actually accomplishes, what protections have worked and what capability gaps exist, and what lessons can be learned by Western nations to better enhance peacetime and home-front defences, as well as in-theatre protections and wartime information operations. The researchers would also need to focus on the regions where threats exist and counter-narratives are needed by analyzing regional adversaries, audiences, culture, linguistics, politics, allies, adversarial messaging, and Western strategic communications reception (Fried & Polyakova, 2018; Gilles, 2016a; Gould, 2017; Iasiello, 2017; Kepe, 2017; Lucas & Nimmo, 2017; Lucas & Pomerantsev, 2016; Nimmo, 2015; Polyakova, 2016; Šuplata & Nič, 2016; Tomášek, 2015; Waltzman, 2017).

There needs to be more decisive counter-information operations from the West. In addition to committing to deliberate Western narratives and proactive Western strategic communications efforts, members of NATO and the European Union need to better define critical infrastructure and harden its protection; expand cyber security; investigate Russian information operations funding and cut it off; restrict access to Western telecommunications for Russian news outlets (television, radio, and Internet) that carry out state disinformation and propaganda campaigns; educate the public and media organizations as to the nature and danger of, and how to identify, Russian information operations efforts; and rate Internet news sites to improve/ensure media quality and identify fake news and sock-puppet websites (Chivvis, 2017b; Iasiello, 2017; Lucas & Pomerantsev, 2016; McClintock, 2017; Paul & Courtney, 2016; Paul & Matthews, 2016; Polyakova et al., 2016; Šuplata & Nič, 2016; Watts, 2017).

Conclusion

The Putin regime has declared that it is in a perpetual state of conflict against the West and will consequently persist in its information operations activities. Hence, Western nations—including Canada—need to be in a perpetual state of concerted self-defence and deterrence by methodically defending, through strategic communications, the concepts, institutions, and military missions that Russia is attacking, and by proactively and pre-emptively disseminating strategic narratives that decrease support for Russia's aggressive policies and military actions and consequently deter the Russian government from continued attacks. Since Putin is carrying out a war against information, Canada and its Western allies must carry on a war against Russian deceit and disinformation. If left unchallenged, Russia will always have the advantage as long as it does not have to abide by the same rules and faces only a disjointed Western reaction after the fact rather than deliberate, proactive, and coordinated information operations and counter–information operations campaigns that come to the defence of truth, democracy, and the rules-based liberal world order that the West has enjoyed and cultivated since the end of the Second World War.

REFERENCES

Berthiaume, L. (2017, 16 June). Canada's spy agency expects cyberattacks during 2019 federal election. *CBC News*. http://www.cbc.ca/news/politics/cse-report-elections-cyber-threats-1.4163868

Bertrand, N. (2017, 2 August). A new website named after a founding father is tracking Russian propaganda in real time. *Business Insider*. http://www.businessinsider.com/russian-propaganda-website-tracker-2017-8

Boot, M. (2017, 13 October). Russia has invented social media blitzkrieg. *Foreign Policy*. http://foreignpolicy.com/2017/10/13/russia-has-invented-social-media-blitzkrieg/

Borchers, C. (2017, 1 November). Four takeaways from the Senate intelligence hearing with Facebook, Twitter and Google. *Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2017/11/01/four-takeaways-from-the-senate-intelligence-hearing-with-facebook-twitter-and-google/?utm_term=.cbe1ad21bfcd

Boutilier, A. (2017, 16 June). Canada's political parties, media vulnerable to foreign disinformation hacks: Spy agency. *Toronto Star*. https://www.thestar.com/news/canada/2017/06/16/canadas-political-parties-media-vulnerable-to-foreign-hacks-spy-agency-says.html

Boutilier, A. (2018, 8 February). Trudeau to Facebook: Fix your fake news problem—or else. *Toronto Star*. https://www.thestar.com/news/canada/trudeau-to-facebook-fix-your-fake-news-problem-or-face-stricter-regulations/article_691b0e16-1ad4-5197-9452-247acc10b428.html

Brannelly, K. (2017, 4 November). Trump campaign pays millions to overseas big data firm. *NBC News*. https://www.nbcnews.com/storyline/2016-election-day/trump-campaign-pays-millions-overseas-big-data-firm-n677321

Brewster, M. (2017, 17 February). Canadians prepare to face cyberwarriors and fake news in Latvia mission. *CBC News*. http://www.cbc.ca/news/politics/canada-latvia-deployment-1.3988719

Bronskill, J. (2021, 22 July). CSIS warns of increasingly sophisticated state-sponsored activity targeting elections. *CTV News*. https://www.ctvnews.ca/politics/csis-warns-of-increasingly-sophisticated-state-sponsored-activity-targeting-elections-1.5519606

Bugajski, J. (n.d.). The geopolitics of disinformation. *Center for European Policy Analysis*. Retrieved 4 October 2017 from http://www.infowar.cepa.org/The-geopolitics-of-disinformation

Bugajski, J. (2016, 13 September). Moscow's war on Washington. *Center for European Policy Analysis*. Retrieved 25 September 2017 from http://cepa.org/Moscows-war-on-Washington

Calabresi, M. (2017, 1 May). Inside Russia's social media war on America. *Time*. http://time.com/4783932/inside-russia-social-media-war-america/

Calamur, K. (2018, 16 February). What is the Internet Research Agency? *The Atlantic*. https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/

Campion-Smith, B. (2017, 17 February). Canadian troops brace for Russian propaganda campaign. *Toronto Star*. https://www.thestar.com/news/canada/2017/02/17/canadian-troops-brace-for-russian-propaganda-campaign.html

Canada. (2017). Cyber threats to Canada's democratic process. *Communications Security Establishment*. https://publications.gc.ca/collections/collection_2017/cstc-csec/D96-2-2017-eng.pdf

Chekinov, S. G., & Bogdanov, S. A. (2013). The nature and content of a new-generation war. *Military Thought, 4*, 12–23. https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf

Chen, A. (2015, 2 June). The agency. *New York Times*. https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Chivvis, C. S. (2017a, 22 March). Addendum: Understanding Russian "hybrid warfare" and what can be done about it [Testimony]. *U.S. House Committee on Armed Services*. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468z1/RAND_CT468z1.pdf

Chivvis, C. S. (2017b, 22 March). Understanding Russian "hybrid warfare" and what can be done about it [Testimony]. *U.S. House Committee on Armed Services*. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Daniels, L. (2017, 23 April). How Russia hacked the French election. *Politico*. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/

Davlashyan, N., & Titova, I. (2018a, 19 February). Ex-workers at Russian troll factory say Mueller indictments are true. *Time*. Retrieved 21 February 2018 from http://time.com/5165805/russian-troll-factory-mueller-indictments/

Davlashyan, N., & Titova, I. (2018b, 19 February). Former workers at Russian "troll factory" say US charges are well-founded. *Toronto Star*. https://www.thestar.com/news/world/2018/02/19/former-workers-at-russian-troll-factory-say-us-charges-are-well-founded.html

Dawsey, J. (2017, 26 September). Russian-funded Facebook ads backed Stein, Sanders, and Trump. *Politico*. http://www.politico.com/story/2017/09/26/facebook-russia-trump-sanders-stein-243172?lo=ap_a1

Dewey, C. (2016, 19 October). One in four debate tweets comes from a bot. Here's how to spot them. *Washington Post*. https://www.washingtonpost.com/news/the-intersect/wp/2016/10/19/one-in-four-debate-tweets-comes-from-a-bot-heres-how-to-spot-them/?utm_term=.6e370538b560

Duncan, A.J. (2017). New "hybrid war" or old "dirty tricks"? The Gerasimov debate and Russia's response to the contemporary operating environment. *Canadian Military Journal, 17*(3), 6–16. http://www.journal.forces.gc.ca/Vol17/no3/page6-eng.asp

Edgett, S. (2017, 31 October). Testimony of Sean J. Edgett, acting general counsel, Twitter, Inc. *US Senate Committee on the Judiciary Subcommittee on Crime and Terrorism*. https://www.judiciary.senate.gov/download/10-31-17-edgett-testimony

Edgett, S. (2018, 15 January). Questions for the record. *Senate Select Committee on Intelligence Hearing on Social Media Influence in the 2016 U.S. Elections*. https://www.intelligence.senate.gov/sites/default/files/documents/Twitter%20Response%20to%20Committee%20QFRs.pdf

Fedyk, N. (2017, 4 May). Russian "new generation" warfare: Theory, practice, and lessons for US strategists. *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists-0

Foxall, A. (2016). Putin's cyberwar: Russia's statecraft in the fifth domain. *Henry Jackson Society Russia Studies Centre*. Retrieved 18 October 2017 from https://henryjacksonsociety.org/wp-content/uploads/2016/05/Cyber-FINAL-copy.pdf

France's Macron, alongside Putin, denounces two Russian media for election meddling. (2017, 29 May). *Reuters*. https://www.reuters.com/article/uk-france-russia-influence/frances-macron-alongside-putin-denounces-two-russian-media-for-election-meddling-idUKKBN18P1T8

Fried, D., & Polyakova, A. (2018). Democratic defense against disinformation. *Atlantic Council*. Retrieved 28 July 2013 from https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf

Galeotti, M. (2014, 6 July). The "Gerasimov Doctrine" and Russian non-linear war. *In Moscow's Shadows*. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Gilles, K. (2016a). The handbook of Russian information warfare. *NATO Defense College Research Division*, Fellowship Monograph 9. http://www.ndc.nato.int/download/downloads.php?icode=506

Gilles, K. (2016b). *Russia's "new" tools for confronting the West: Continuity and innovation in Moscow's exercise of power*. Chatham House. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

Gorenburg, D. (2019). Russian foreign policy narratives. *George C. Marshall European Center for Security Studies*. https://www.marshallcenter.org/en/publications/security-insights/russian-foreign-policy-narratives-0

Gould, J. (2017, 23 March). EUCOM commander: US needs stronger response to Russian disinformation. *Defense News*. http://www.defensenews.com/global/europe/2017/03/23/eucom-commander-us-needs-stronger-response-to-russian-disinformation/

Gregory, P. R. (2016, 5 April). Putin caught in huge Panama Papers scandal. *Forbes*. https://www.forbes.com/sites/paulroderickgregory/2016/04/05/putin-caught-in-huge-panama-papers-scandal/#3c7310ff7d31

Guide, K. (2017, 15 March). Russia's 5th column. *Center for American Progress*. https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/

Gunzinger, M., Clark, B., Johnson, D., & Sloman, J. (2017). Force planning for the era of great power competition. *Center for Strategic and Budgetary Assessment*. http://csbaonline.org/uploads/documents/CSBA6302_%28Developing_the_Future_Force%29_PRINT.pdf

Harding, L. (2016, 3 April). Revealed: The $2bn offshore trail that leads to Vladimir Putin. *The Guardian*. https://www.theguardian.com/news/2016/apr/03/panama-papers-money-hidden-offshore

Henderson, N. (2016, 23 November). Russian disinformation: How U.S. information operations need to adapt. *Cornell Policy Review*. http://www.cornellpolicyreview.com/russian-disinformation-how-u-s-information-operations-need-to-adapt/

Hern, A. (2017, 8 May). Macron hackers linked to Russian-affiliated group behind US attack. *The Guardian*. https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack

Higgins, A. (2017, 16 February). Fake news, fake Ukrainians: How a group of Russians tilted a Dutch vote. *New York Times*. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html

Iasiello, E. J. (2017). Russia's improved information operations: From Georgia to Crimea. *Parameters, 47*(2), 51–63. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

Joyal, P. (2016). Cyber threats and Russian information warfare. *Jewish Policy Center*. https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/

Kepe, M. (2017, 7 June). NATO: Prepared for countering disinformation operations in the Baltic states? *RAND Blog*. https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.html

Koshkin, P. (2015, 2 April). The paradox of Kremlin propaganda: How it tries to win hearts and minds. *Russia Direct*. Retrieved 23 October 2017 from http://www.russia-direct.org/analysis/paradox-kremlin-propaganda-how-it-tries-win-hearts-and-minds

Lapowsky, I. (2017, 1 November). Eight revealing moments from the second day of Russia hearings. *Wired*. https://www.wired.com/story/six-revealing-moments-from-the-second-day-of-russia-hearings/

Lauder, M. (2017). *Leveraging proxy agents: The night wolves and other examples of Russia out-sourcing activity to criminal and grey-market enterprises* [Paper presentation]. 2017 Adversarial Intent Symposium: Putin's Russia—The Weaponization of Society, Kingston, ON, 11 October 2017.

Lipton, E., Sanger, D., & Shane, S. (2016, 13 December). The perfect weapon: How Russian cyberpower invaded the U.S. *New York Times*. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-DCCC.html

Lucas, E., & Nimmo, B. (2015). CEPA info war paper no. 1: Information warfare—what is it and how to win it. *Center for European Policy Analysis*. Retrieved 4 October 2017 from http://cepa.org/files/?id_plik=1896

Lucas, E., & Pomerantsev, P. (2016). *Winning the information war: Techniques and counter-strategies to Russian propaganda in central and eastern Europe.* Center for European Policy Analysis. https://cepa.ecms.pl/files/?id_plik=2773

MacFarquhar, N. (2016, 28 August). A powerful Russian weapon: The spread of false stories. *New York Times*. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

MacFarquhar, N. (2018a, 18 February). Inside the Russian troll factory: Zombies and a breakneck pace. *New York Times*. https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html

MacFarquhar, N. (2018b, 18 February). Russian trolls were sloppy, but indictment still 'points at the Kremlin." *New York Times*. https://www.nytimes.com/2018/02/17/world/europe/russia-indictment-trolls-putin.html

MacFarquhar, N. (2018c, 16 February). Yevgeny Prigozhin, Russian oligarch indicted by US, is known as "Putin's cook." *New York Times*. https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html

McCabe, D. (2017, 1 November). What Facebook, Google, and Twitter told the Senate Intel Committee. *Axios*. https://www.axios.com/what-facebook-google-and-twitter-told-the-senate-intel-committee-1513306593-acf2d8d6-3459-45c5-963b-482e42071d52.html

McClintock, B. (2017, 21 July). Russian information warfare: A reality that needs a response. *RAND Blog*. https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html

Mueller, R. (2018, 16 February). Grand Jury for the District of Columbia indictment against Internet Research Agency, et al. *US Department of Justice*. https://www.justice.gov/file/1035477/download

Nanji, S. (2017, 19 October). Facebook's Canadian "election integrity" plan puts much of the responsibility on political players. *Toronto Star*. https://www.thestar.com/news/gta/2017/10/19/facebooks-canadian-election-integrity-plan-puts-much-of-the-responsibility-on-political-players.html

Nimmo, B. (2015, 19 May). Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it. *StopFake.org*. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

Nimmo, B. (2016). CEPA information warfare paper no. 2: Sputnik—propaganda in a new orbit. *Center for European Policy Analysis*. Retrieved 4 October 2017 from http://cepa.org/files/?id_plik=2083

ODNI (Office of the Director of National Intelligence). (2017, 6 January). *Assessing Russian activities and intentions in recent US elections: The analytic process and cyber incident attribution*. National Intelligence Council. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Oliker, O. (2016, 7 January). Unpacking Russia's new national security strategy. *Center for Strategic and International Studies*. https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy

O'Sullivan, D. (2017, 2 November). Seen any of these before? You may have been targeted by Russian ads on Facebook. *CNN Money*. http://money.cnn.com/2017/11/01/media/russian-facebook-ads-release-house-intelligence-committee/index.html

Paul, C., & Matthews, M. (2016). *The Russian "firehose of falsehood" propaganda model*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

Paul, C., & Courtney, W. (2016, 13 September). Russian propaganda is pervasive, and America is behind the power curve in countering it. *RAND Blog*. https://www.rand.org/blog/2016/09/russian-propaganda-is-pervasive-and-america-is-behind.html

Perlroth, N., Wines, M., & Rosenberg, M. (2017, 1 September). Russian election hacking efforts, wider than previously known, draw little scrutiny. *New York Times*. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=5&pgtype=collection

Polyakova, A., Laruelle, M., Meister, S., & Barnett, N. (2016). *The Kremlin's Trojan Horses: Russian influence in France, Germany, and the United Kingdom*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2016/11/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf

Pomerantsev, P. (2014, 11 December). Russia's ideology: There is no truth. *New York Times*. https://www.nytimes.com/2014/12/12/opinion/russias-ideology-there-is-no-truth.html?_r=1

Popken, B. (2017, 30 October). What to expect when Facebook, Google, and Twitter testify on election meddling. *NBC News*. https://www.nbcnews.com/business/business-news/what-expect-when-facebook-google-twitter-testify-election-meddling-n815631

Porotsky, S. (2017a, 27 August). Cambridge Analytica: The darker side of big data. *Global Security*. https://globalsecurityreview.com/cambridge-analytica-darker-side-big-data/

Porotsky, S. (2017b, 27 August). Cold War 2.0: Russian information warfare. *Global Security*. https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/

Porotsky, S. (2017c, 27 August). Facebook, compromised: How Russia manipulated US voters. *Global Security*. https://globalsecurityreview.com/russia-manipulated-u-s-voters-social-media/

Presidential election results: Donald J. Trump wins. (2017, 9 August). *New York Times*. https://www.nytimes.com/elections/results/president

Raju, M., Byers, D., & Bash, D. (2017, 4 October). Russian-linked Facebook ads targeted Michigan and Wisconsin. *CNN News*. http://www.cnn.com/2017/10/03/politics/russian-facebook-ads-michigan-wisconsin/index.html

Rasmussen, R.C. (2015, 26 November). Cutting through the fog: Reflexive control and Russian STRATCOM in Ukraine. *Center for International Maritime Security*. http://cimsec.org/cutting-fog-reflexive-control-russian-stratcom-ukraine/20156

Rumer, E. (2017, 30 March). Russian active measures and influence campaigns [Testimony]. *US Senate Select Committee on Intelligence*. http://carnegieendowment.org/2017/03/30/russian-active-measures-and-influence-campaigns-pub-68438

Russian Federation. (2014). *Russian military doctrine*. Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. Retrieved 21 September 2017, from https://rusemb.org.uk/press/2029

Russian Federation. (2015). *Russian national security strategy*. Russian Federation president, edict 683. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Russian Twitter accounts promoted Brexit ahead of EU referendum: Times newspaper. (2017, 15 November). *Reuters*. https://www.reuters.com/article/us-britain-eu-russia/

russian-twitter-accounts-promoted-brexit-ahead-of-eu-referendum-times-newspaper-idUSKBN1DF0ZR

Rutenberg, J. (2017, 13 September). RT, Sputnik, and Russia's new theory of war. *New York Times*. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html?action=click&contentCollection=Politics&module=Trending&version=Full&region=Marginalia&pgtype=article

Satter, R., & Vasilyeva, N. (2018, 20 February). Russia troll farm more strange than Mueller's indictment says, according to insiders. *Global News*. https://globalnews.ca/news/4036331/russia-troll-farm-strange-muellers-indictment/

Scannell, K., Shortell, D., & Stracqualursi, V. (2018, 17 February). Mueller indicts 13 Russian nationals over 2016 election interference. *CNN News*. https://www.cnn.com/2018/02/16/politics/mueller-russia-indictments-election-interference/index.html

Schwirtzsept, M. (2017, 21 September). German election mystery: Why no Russian meddling? *New York Times*. https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html

Seetharaman, D. (2017a, 30 October). Russian-backed Facebook accounts staged events around divisive issues. *Wall Street Journal*. https://www.wsj.com/articles/russian-backed-facebook-accounts-organized-events-on-all-sides-of-polarizing-issues-1509355801

Seetharaman, D. (2017b, 31 October). Tech executives testify in Senate hearing on Russian election activity. *Wall Street Journal*. https://www.wsj.com/livecoverage/senate-judiciary-hearing-tech-executives-russia-campaign/card/1509476733

Shane, S. (2017, 7 September). The fake Americans Russia created to influence the election. *New York Times*. https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

Shane, S., & Goel, V. (2017, 6 September). Fake Russian Facebook accounts bought $100,000 in political ads. *New York Times*. https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

Shinal, J. (2018, 25 January). Facebook admits to the Senate that it recommended Russian propaganda to some users. *CNBC News*. https://www.cnbc.com/2018/01/25/facebook-tells-senate-its-software-recommended-russian-propaganda.html

Skaskiw, R. (2017, 27 March). Nine lessons of Russian propaganda. *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/nine-lessons-of-russian-propaganda

Smith, D. (2017, 31 October). Angry Al Franken hammers Facebook lawyer at hearing over Russian ads. *The Guardian*. https://www.theguardian.com/us-news/2017/oct/31/facebook-russia-ads-senate-hearing-al-franken

Solon, O., & Siddiqui, S. (2017, 31 October). Russia-backed Facebook posts "reached 126m Americans" during US election. *The Guardian*. https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million

Stelzenmüller, C. (2017, 28 June). The impact of Russian interference on Germany's 2017 elections. *Brookings Institution*. https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

Stewart, B. (2017, 15 December). More than just hacks: Russia's "hybrid warfare" has been targeting western Europe for months. *CBC News*. http://www.cbc.ca/news/world/russia-cyber-warfare-election-hack-1.3896613

Stretch, C. (2017, 31 October). Testimony of Colin Stretch, general counsel, Facebook. *US Senate Committee on the Judiciary Subcommittee on Crime and Terrorism*. https://www.judiciary.senate.gov/download/10-31-17-stretch-testimony

Stretch, C. (2018, January 8). Facebook's response to US Senate Intelligence Committee [Testimony]. *U.S. Senate Select Committee on Intelligence*. https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf

Šuplata, M., & Nič, M. (2016, 31 August). Summary—Russia's information war in central Europe: New trends and counter-measures. *GlobSec*. https://www.globsec.org/publications/russias-information-war-central-europe-new-trends-counter-measures/

Synovitz, R. (2017, 17 January). Europe bracing against risk of Russian "influence operations." *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/europe-russian-influence-operations/28236212.html

Taylor, A. (2017, 28 August). Putin saw the Panama Papers as a personal attack and may have wanted revenge, Russian authors say. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2017/08/28/putin-saw-the-panama-papers-as-a-personal-attack-and-may-have-wanted-revenge-russian-authors-say/?utm_term=.69e78ec6cd3b

Taylor, A. (2018, 18 February). The Russian journalist who helped uncover election interference is confounded by the Mueller indictments. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2018/02/18/the-russian-journalist-who-helped-uncover-election-meddling-is-confounded-by-the-mueller-indictments/?utm_term=.02bb5ea6f423

Thomas, T. (2010). Russia's reflexive control theory and the military. *Journal of Slavic Military Studies, 17*(2), 237–56. http://www.tandfonline.com/doi/pdf/10.1080/13518040490450529?needAccess=true

Thomas, T. (2016). The evolution of Russian military thought: Integrating hybrid, new-generation, and new-type thinking. *Journal of Slavic Military Studies, 29*(4), 554–75. http://www.tandfonline.com/doi/pdf/10.1080/13518046.2016.1232541?needAccess=true

Tomášek, J. (2015, 13 October). Countering Kremlin's information war. *GlobSec*. https://www.globsec.org/publications/countering-kremlins-information-war/

Vowell, J. B. (2016, 30 October). Maskirovka: From Russia, with deception. *Real Clear Defense*. https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html

Walker, K. (n.d.). Responses to questions for the record for Mr. Kent Walker, senior vice president and general counsel, Google [Testimony]. *US Senate Select Committee on Intelligence*. https://www.intelligence.senate.gov/sites/default/files/documents/Google%20Response%20to%20Committee%20QFRs.pdf

Waltzman, R. (2017, 27 April). The weaponization of information: The need for cognitive security [Testimony]. *US Senate Committee on Armed Services Subcommittee on Cybersecurity*. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

Watts, C. (2017, 30 March). Disinformation: A primer in Russian active measures and influence campaigns [Statement]. *US Senate Select Committee on Intelligence*. https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf

Watts, C., & Weisburd, A. (2016, 8 June). How Russia dominates your Twitter feed to promote lies (and, Trump, too). *Daily Beast*. http://www.thedailybeast.com/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too

Weisburd, A., Watts, C., & Berger, J. M. (2016, 6 November). Trolling for Trump: How Russia is trying to destroy our democracy. *War on the Rocks*. https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/

Wherry, A. (2017, 19 October). Facebook launches "election integrity initiative" to fight hacking and fake news. *CBC News*. http://www.cbc.ca/news/politics/facebook-election-hacking-fake-news-1.4362002