Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Typhon's Song: Examining Russia's Employment of COVID-19 Disinformation to Generate Disruptive Effects

Matthew A. Lauder
DRDC – Toronto Research Centre

Small Wars Journal

Online article
https://smallwarsjournal.com/jrnl/art/typhons-song-examining-russias-employment-covid-19-disinformation-generate-disruptive

Date of Publication from Ext Publisher: December 2020

Defence Research and Development Canada

External Literature (N)
DRDC-RDDC-2021-N002
January 2021

CAN UNCLASSIFIED

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Typhon's[i] Song: Examining Russia's Employment of COVID-19 Disinformation to Generate Disruptive Effects

Matthew A. Lauder
Defence Scientist, Defence Research and Development Canada

Abstract

The emergence of the coronavirus disease (COVID-19) and a lack of clear and definitive information and guidance by public health organizations and national and regional governments, coupled with heightened collective anxiety, created the perfect storm for the promulgation of disinformation and other manipulative and deceitful content. The Russian government has been one of the most prolific offenders, seeking to generate disruptive effects in targeted countries. This article examines the mechanics of how the Russian government generates disruptive effects through COVID-19 disinformation, as well as discussing implications for NATO and its partners.

Biography

Matthew A. Lauder, CD, BA (Hons.), MA, MPhil is a Defence Scientist and Group Leader of the Influence Group in the Intelligence, Influence and Collaboration Section at Defence R&D Canada. Matthew is involved in three broad areas of activity, including the design and execution of research projects in support of information and irregular warfare force development, supporting operations through adversary intent analysis, and supporting professional military education, specifically in the areas of information operations, psychological operations, special warfare, targeting and intelligence. Matthew also served as an infantry officer for more than 12 years in The Argyll and Sutherland Highlanders of Canada (Princess Louise's).

The emergence of the coronavirus disease (COVID-19) and the ensuing pandemic, along with a lack of clear and definitive information and guidance by public health organizations as well as national and regional governments (in some cases trivializing the disease and minimizing its lethal potential) coupled with heightened collective anxiety, offers a unique opportunity – basically, the perfect storm – for the promulgation of disinformation and other manipulative and deceitful content, such as conspiracy theories (often referred to as an 'infodemic') (Richtel, 2020; Beaumont, Borger & Boffey 2020). The Russian government is one of the most prolific offenders (Broad, 2020), taking advantage of collective anxiety and uncertainty to advance a myriad of false narratives and disinformation about COVID-19, including linking it to a long-running disinformation campaign about the US military developing bioweapons in a network of secret laboratories in former Soviet countries (Gamberini & Moddie, 2020). The Russian government also exploited COVID-19 in numerous attempts to generate deliberate and tailored disruptive effects, such as inciting violence against state authorities and fracturing military partnerships, specifically North Atlantic Treaty Organization (NATO) countries and its allies in Europe.

The objective of this paper is to examine the mechanics of how the Russian government generates disruptive effects through COVID-19 disinformation campaigns, as well as to identify and discuss implications for NATO and its partners. To achieve this objective, this paper is divided into three sections. The first section offers a grounded perspective[ii] of the structure of Russian information confrontation as well as the entities and sociotechnical mechanisms utilized to engage and manipulate target audiences. The second section examines three case studies (Ukraine, Lithuania and Latvia) in which the Russian government employed COVID-19 disinformation for the purposes of generating deliberate and tailored disruptive effects in targeted countries. The last section discusses several observations about Russian information confrontation and the implications to NATO and its allies, as well as offering some practical recommendations to respond to Russian information confrontation.

Russian Information Confrontation

Since the mid-1990s, the Russian government has engaged in numerous cycles of defence and security revitalization. As a part of this renewal program, the Russian government has made significant investments in and evolved its information confrontation capability.[iii] Based on lessons learned from a series of conflicts, as well as perceived US and NATO information warfare force developments, this revitalization included revising underpinning theories and concepts, reorganizing operational structures and responsibilities, implementing new strategic policies and doctrine and incorporating new information technology (Sukhankin, 2020) as well as developing and fielding new tactics, techniques and procedures (TTPs). In addition, the Russian government has shown itself to be highly agile by decentralizing and outsourcing responsibility to devise, plan and execute informational campaigns to a variety of non-state actors, including private businesses, media conglomerates, private military contractors (PMCs), non-governmental organizations (NGOs), motorcycle clubs, criminal organizations, patriotic groups and religious organizations – in other words, any outward or publicly-facing entity that operates at arms-length from and provides deniability for the Russian government (Lauder, 2019a). The end result is a highly diversified, decentralized and matrixed approach to information confrontation, one that goes beyond a whole-of-government (WOG) approach and fully embraces a whole-of-society (WOS) approach, with little hierarchy and exceedingly high capacity to operate, as well as a proclivity to ignore political risk.

Core Characteristic of the Russian Defence Perspective

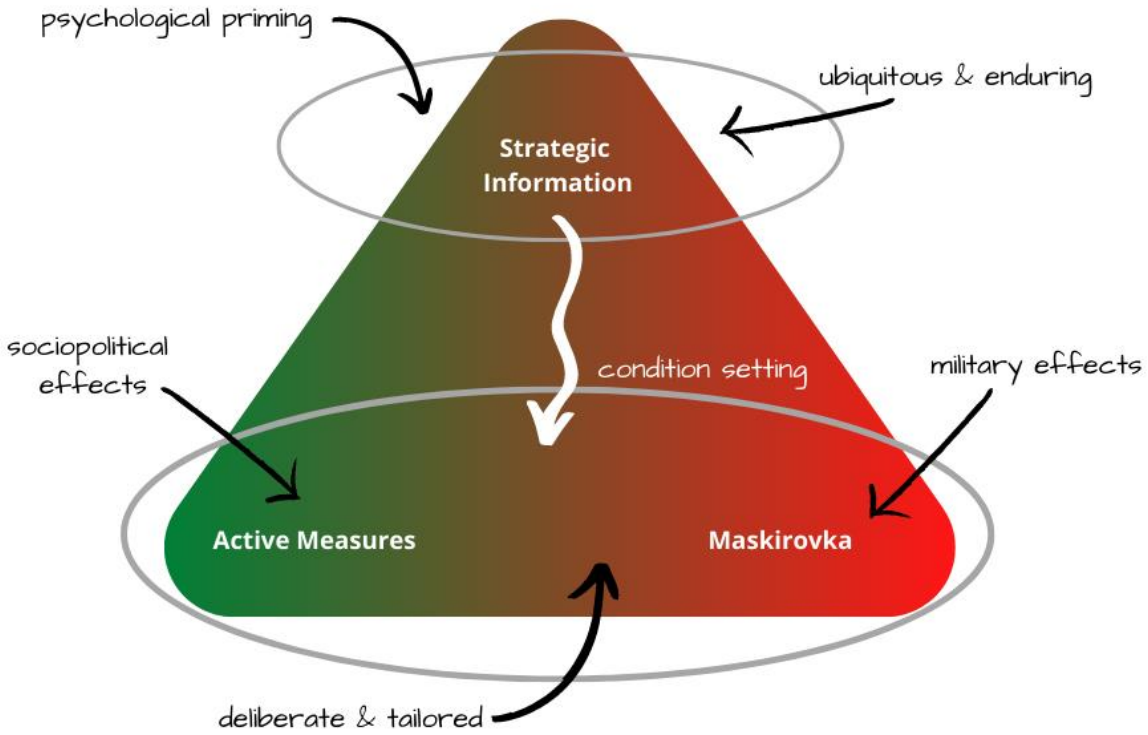
Before proceeding with an examination of Russian information confrontation and to help frame the discussion, an outline of main components of Russia's defense perspective is required. Based on an analysis of Russian military operations over the last twenty years, as well as a close reading of strategic doctrine and various military theorists and capability proponents (e.g., Sergei Shoigu, Valery Gerasimov, Konstantine Sivkov, Igor Panarin, etc.), Russia's defence perspective is underpinned by six core characteristics (Lauder, 2019a). In essence, these characteristics define how the Russian government perceives, understands and responds to the evolving nature of interstate conflict, in particular the role of externally conducted information warfare. The six characteristics include:

1. Maintaining traditional Russian cultural and national identity;
2. Countering threats to the integrity of the domestic information space;
3. Protecting Russian citizens and compatriots against internal and external threats, as well as ethno-linguistic populations abroad;
4. Maintaining the principle of first strike and pre-emptive action, including in the information space;
5. Defending against evolving asymmetric (including informational, political, etc.) approaches to contemporary interstate conflict; and,
6. Empowering and utilizing a whole-of-society approach, including the application of non-military means, for both offensive and defensive action.

Forms of Russian Information Confrontation

In contrast to the Cold War in which the Soviet Union employed two relatively distinct forms of psychological warfare (i.e., maskirovka and active measures), the Russian government recently developed and implemented an overarching concept of information confrontation that is robust, comprehensive, overlapping and applicable at all levels of conflict. At least for discussion purposes, however, Russian information confrontation can be divided into three, subtly distinct but complementary, conceptual forms; that of (a) maskirovka, (b) active measures, and (c) strategic information, also referred to as strategic propaganda and strategic deception, as illustrated in Figure 1.[iv]

Figure 1
Forms of Russian Information Confrontation



Maskirovka is generally applied to generate deliberate and tailored military effects against an enemy, such as disrupting an enemy's command and control (C2), misleading the enemy about the location and movement of Russian forces, or undermining the morale of enemy soldiers.[v] Maskirovka can also be applied against the civilian population, but done so to generate an effect within an adversary's defence or security structures or to achieve a military objective. During the Cold War, the GRU (*Glavnoye razvedyvatel'noye upravleniye* or the Main Intelligence Directorate) was responsible for the design and execution of maskirovka. However, recent military operations in Ukraine and Syria suggest numerous entities are involved in generating military effects, including the FSB *(Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii,* or the Federal Security Service) (Lauder, 2019a).[vi] Moreover, outsourced non-state assets, such as the Night Wolves and the Wagner Group, plan and conduct maskirovka, either in support of discrete tactical military activities (e.g., armed raids) or as a part a broader, combined force effort to achieve operational-level military objectives (e.g., the annexation of Crimea or the invasion of Donbass) (Lauder, 2019b).

In contrast, active measures are applied against a target nation's civilian population or political, cultural and business elites.[vii] As a general rule, the objective of active measures is to generate deliberate and tailored effects in the socio-political realm, such as undermining public trust in democratic institutions or confidence in election results. Alternatively, active measures can be used to shape the development or undermine the implementation of a state's foreign or

domestic policies in order for Russia to gain a geopolitical or economic advantage over its state competitors. Like that of the Soviet era, the efficacy of active measures is most often realized through the integration and aggregation of a number of activities rather than through a single or discrete effort. While active measures during the Cold War were largely considered to be the remit of the KGB, recent operations indicate numerous state and non-state entities are involved in the design and conduct of active measures campaigns, including – but not limited to – the GRU and the Ministry of Foreign Affairs (MFA), as well as various grassroots media outlets, non-profit organizations, hacker groups and criminal organizations (Lauder, 2019a). While active measures were traditionally focused on the operational and strategic levels, recent activities have also shown active measures can be utilized at the tactical level (e.g., attempts to undermine or eliminate local politicians and social justice advocates, encouraging localized riots and looting to undermine civilian security services, etc.).

Strategic information are ubiquitous and enduring high-level information activities designed to set conditions for more tailored psychological interventions, such as maskirovka and active measures.[viii] The purpose of strategic information activities is not to generate an effect per se, but rather to broadly disseminate narratives to *psychologically prime* target audiences, increasing susceptibility to more tailored interventions. In other words, strategic information serves a "pre-propaganda" function, effectively conditioning target audience to be receptive to maskirovka and action measures (Siriwardane, 2020).

Like that of maskirovka and active measures, various Russian state and non-state entities are responsible for the design and execution of strategic information, including state agencies (e.g., Ministry of Foreign Affairs, etc.), state-owned news media agencies (RT, Sputnik, TASS, etc.), privately-owned but state aligned news media agencies and conglomerates (e.g., Internet Research Agency [also known as Glavset and the Federal News Agency, or FAN)], Vesti News, etc.), and religious organizations (Russian Orthodox Church), as well as non-profit agencies and private companies, including Russkiy Mir and various subsidiaries of the Nightwolves (Lauder, 2019a; 2019b).

Two points regarding the general forms of Russian information confrontation should be noted. First, there are no clear lines of ownership or responsibility for information confrontation. Historically, the GRU owned the tactical and operational space for the purposes of conducting maskirovka, whereas the KGB owned the operational and strategic space, and was responsible for the design, execution and management of active measures, largely under the direction of the Secretariate of the Communist Part of the Soviet Union (CPSU) (Lauder, 2019a). However, in the contemporary context, the entire information space is muddled and a whole host of agencies independently design and execute information confrontation on behalf of the Russian government (Galeotti, 2017). In practice, it appears the Russian government utilizes whatever assets, capabilities and resources it has at its disposal to conduct information confrontation and generate psychological and behavioural effects, regardless as to the level of conflict or target audience. Second and very much an adjunct to the first point is that non-state actors have proven to be particularly valuable and effective, and this increasingly relied upon, in the planning and conduct of information confrontation, not only in terms of successfully generating effects but

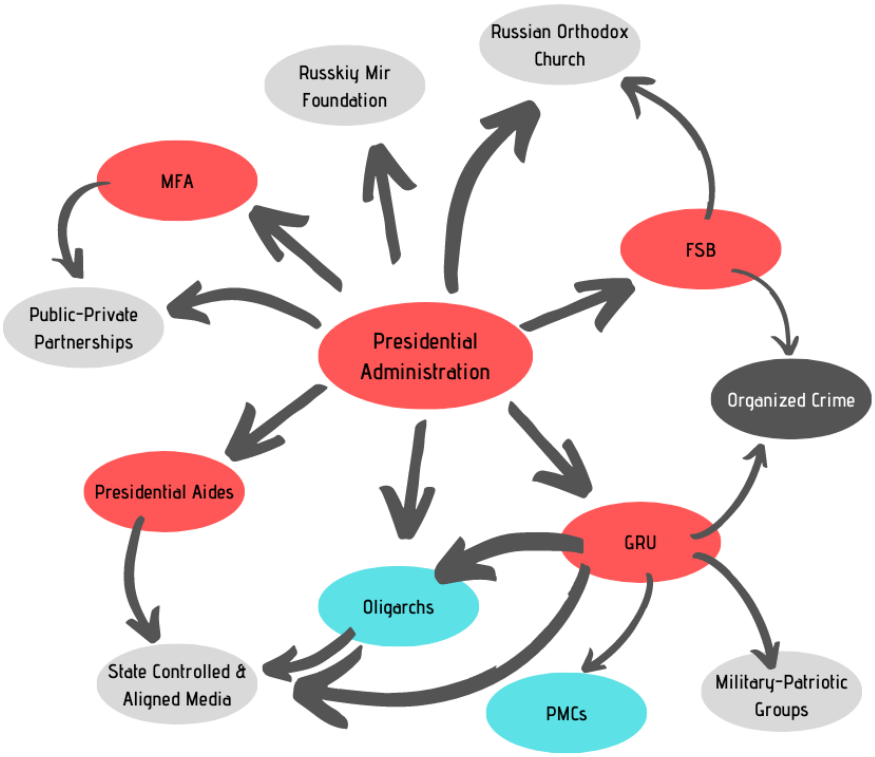
also for maintaining plausible deniability for the Russian government. As such, it is expected the use of non-state actors by the Russian government will increase in future interstate conflict.

Information Confrontation Entities

Although the psychological warfare employed by the Soviet Union was robust and comprehensive, with involvement by state and non-state actors (typically front groups, proxies and other controlled assets), there were generally clear lines of responsibility for the GRU and KGB. Moreover, the C2 for psychological warfare was largely hierarchical, with direction and – most critically – approval from higher state entities, such as the CPSU. Overall, the approach employed by the Soviet Union was highly centralized and bureaucratic, with planning occurring at higher levels of government and execution a departmental responsibility. This was done for a variety of reasons, the foremost being that psychological warfare efforts directly contributed to the achievement to geopolitical objectives.

In contrast, contemporary Russian information confrontation appears to have eliminated the requirement for strict hierarchical control, and the design, planning and execution of activities is now highly decentralized. From the limited information available in the public domain, it appears that there is no C2 administered by the Presidential Administration or other central body but rather expressions of intent or objectives to be achieved, or what can be referred to as command aspirations (Lauder, 2019a; Galeotti, 2017; Ouellet, 2020). While this approach requires the embracement of political risk it also nurtures multifarious messaging efforts, including contradictory content and narratives (Branford, 2017). In addition to official and state entities, a significant and growing number of semi-official, arms-length and non-state actors actively participate in information confrontation campaigns at the behest of the Russian government. As noted in Figure 2, for example, these organizations include public-private enterprises, military-patriotic organizations, criminal organizations, media conglomerates, and as well as private businesses, cultural associations and religious organizations (Lauder, 2019b). While some of these organizations have tenuous links to the Russian government, including receiving indirect financial support or strategic direction through aides or interlocutors (e.g., Nightwolves, Internet Research Agency, etc.), many are at a distance, with little or no apparent connection to the government and appear to operate autonomously (Lauder, 2019b). In some cases, such as the Nightwolves, the Wagner Group or the Russian Orthodox Church, key proxies receive expressions of strategic intent directly from the Presidential Administration (Lauder, 2018a, 2019a, 2019b). This is due to personal relationships between the leaders of these organizations and Putin (e.g., Yevgeny Prigozhin, Alexander Zaldostanov, etc.). In other cases, information confrontation conducted by non-state actors are coordinated or facilitated by state entities, such as – but not limited to – the GRU or the FSB (Lauder, 2019b).

Figure 2:
Entities involved in Russian Information Confrontation



Note: This is a high-level, simplified account of the main entities or types of organizations involved in Russian information confrontation for the purposes of illustrating the breadth of entities as well as the interrelationships. Red denotes government departments, grey denotes a non-profit or arms-length entities, blue denotes private organizations/networks or commercial enterprises and black denotes organized crime or illegal/black-market entities. Arrows indicate a connection but not necessarily a command and control (C2) relationship.

Sociotechnical Model of Engagement and Manipulation

Successful information confrontation is not merely a matter of disseminating messages; rather, and most critically, the content of the message or narrative must be meaningful to, and also serve to mobilize, the intended target audience (i.e., it must serve a sensemaking function). To accomplish a high degree of resonance with the target audience, information confrontation leverages, to varying degrees depending upon the form of the activity, the perception to be shaped and the behaviour to be elicited, eight interrelated and theoretically grounded sociotechnical mechanisms. Referred to as the *Barrage Model* and as noted in Figure 3 (Lauder, 2018b), the eight mechanisms include:

1. *Emotional appeal:* Sometimes referred to as emotional elicitation, messages are designed to elicit and exploit a highly emotional response (such as fear, anger or surprise), the

purpose of which is to short-circuit or bypass rational thought and encourage action (Gross & Levenson, 1995). Although individual susceptibility to emotional appeal varies significantly, an increased state of emotional arousal is generally achieved through the use of messages loaded with provocative language or ad hominin attacks (MacFarquhar, 2016). Moreover, research indicates that, when people engage in retrospection, the emotional response tends to be more memorable than the content of the original message (Tolz & Chatterje-Doody, 2018). As a result, subjects or issues are quickly associated with certain powerful emotional responses (e.g., political issue X made me really angry, etc.), which could help distort future perception and undermine decision-making or prompt a certain behaviour (Lamia, 2012);

2. *Belief formation:* People tend to search for and consume information that confirms, rather than challenges or contradicts, one's existing beliefs (Grayling, 2011). In essence, rather than searching for well-grounded and logical explanations, people search for confirmatory information in order to rationalize and justify existing beliefs, and also to ensure consistency and reliability of the beliefs and actions over time (Grayling, 2011). Research indicates that beliefs form first, and then rationalizations follow, including the search for confirmatory information from likeminded and ideologically aligned and consistent sources (Shermer, 2011). Moreover, research indicates that the presentation of countervailing information has the opposite effect (commonly referred to as the back-fire effect) than intended (Shermer, 2011); that is, rather than correcting the erroneous beliefs and encouraging an attitudinal shift, the presentation of contradictory information actually reinforces and hardens the individual's commitment to existing beliefs (i.e., ideological entrenchment);
3. *Stereotypes and conspiratorial language:* Several studies indicate the use of stereotypes and conspiratorial language serves as a cognitive heuristic, meant to simplify and impose order on complex explanations or contradictory information, and generally functions to reduce mental effort for decision-making (Tolz & Chatterje-Doody, Rudman & Glick, 2008; Uscinski & Enders, 2020). In essence, people look for easy or simple explanations during periods of heightened or increased anxiety and uncertainty, and these convenient explanations are often found in conspiratorial thinking and stereotypes;
4. *Filter bubbles:* Is a state of informational and cognitive isolation or marginalization as a result of algorithmic and computational models that customize and curate information retrieval based on a user's search history, personal details and other online behaviours (likes, dislikes, shares, etc.), as well as the financial and promotional interests or requirements of the software application being employed to facilitate the information search (Bakshy, Messing & Adamic, 2015). As a result of using search engines over time, a user will become increasing informationally isolated and fragmented (Hosanagar, 2016), receiving increasingly narrow bands of information, which most often confirm rather than challenge the user's pre-existing beliefs;
5. *Echo chambers:* Conceptually interwoven with belief formation and filter bubbles, echo chambers can be described as enclosed digital information environments in which existing beliefs are reinforced and amplified (Grimes, 2017). Also referred to virtual cliques and digital enclaves, echo chambers are created and maintained by people so that they can participate in a like-minded and ideologically aligned community (Hoggan, 2016;

Lauder, 2018b). Several scholars have criticized echo chambers for encouraging and creating ideological safe-havens for bias and extremist beliefs and – more generally – for skewing and damaging understanding (Grimes, 2017; Lauder, 2018b);

6. *Ingroup bias:* Also known as intergroup bias, this concept is closely associated with filter bubbles, echo chambers and conspiratorial language and can be understood as a pattern of behaviour favouring one's group (ingroup) over that of other groups (outgroups) (Tajfel & Turner, 2001). One of the leading explanations of ingroup bias can be found in *Social Identity Theory*, which proposes that identity-based favouritism, and claims of ingroup exclusivity, is utilized to enhance one's self-esteem. In studies conducted by Henri Tajfel and John Turner (2001), it was determined that by having a positive impression of members of the ingroup, individuals are able to enhance their self-esteem and sense of self-importance and efficacy as members of or being associated with that group. Critically, ingroup bias can be employed for social and political mobilization. However, this often comes at the expense of the identified or perceived outgroup, including but not limited to discriminatory and other antisocial behaviour, such as targeted violence against members of outgroups (Tajfel & Turner, 2004).
7. *Information saturation:* The objective of information saturation is to support the other mechanisms by overwhelming the information space with messaging and supplanting and pushing-out external and countervailing information sources. This is typically achieved through a three-pronged approach of message repetition (frequently disseminated), pervasiveness (across multiple means) and persistence (disseminated across prolonged period of time) (Lauder, 2018b). Closely associated with confirmation bias, this approach leverages the *illusory truth effect*, which is the tendency to believe false information if repeated (Weiss, 1969; Clifton, 2017, Paul & Matthews, 2016; Fazio, Payne, Brashier & Marsh, 2015);
8. *Creeping normality:* Is both a process and the culminating effect of all the mechanisms working in tandem. Sometimes referred to a *gradualism*, *death by a thousand cuts* and the *tyranny of bad decisions*, and predicated on theories of social, economic and environmental decline, creeping normality is the phenomenon of accepting as normal a major or significant alteration (which would have been rejected outright) if that alteration occurred slowly, through unremarkable and otherwise inconspicuous increments of change (Diamond, 2011). In other words, if the change remains below the threshold of collective awareness, it will be accepted as normal (Diamond, 2011). Through this process, and if properly manipulated, a protagonist may reverse significant advancements of a society or, alternatively, push it towards potential collapse.

Three points should be noted about the Barrage Model. First, the model has been developed using a grounded approach, in particular how information confrontation is operationalized and the resulting effects. The Barrage Model, however, requires further validation and refinement and, as such, should be considered a working framework for understanding the mechanics of information confrontation. Second, the model also takes into consideration the evolving nature of information confrontation, specifically earlier methods (pre-2016) that focused on pervasive and unmitigated dissemination of messages to a variety of target audiences, what Paul and Matthews (2016) referred to as the "firehose of falsehood," without much concern for resonance

and adapted a more deliberate and curated approach focusing on establishing deeper and more meaningful relationships by organically building (or coopting) and exploiting vulnerable communities (Thompson & Lapowsky, 2018). Central in Russia's revised approach to information confrontation is the appearance of information source authenticity, specifically that the disseminator belongs to the community being exploited. In addition, this approach is less about promoting explicitly pro-Russian messages but rather amplifying regional social and political discord and promoting calls to action, such as violent protests (Sebenius, 2020). In some cases, the Russian government, through a third-party, hires local interlocutors and franchises message dissemination, providing an additional layer of authenticity as well as deniability (Alba, 2020). Third, this is a general model; that is, it reflects the employment of traditional and new media, as well as other technical and non-technical means of delivery, and across all levels of conflict. As such, not all aspects of the Barrage Model are or need to be utilized in a particular information activity. Rather, specific components are leveraged based upon the nuances and idiosyncrasies of the target audience and the behavioural effect to be generated.

Figure 3
The Barrage Model

Case Studies of Disruptive Effects Generation using COVID-19 Disinformation

The purpose of this section is to highlight and discuss specific cases of COVID-19 disinformation activities resulting in disruption, damage or subversion or cases in which a suspected state actor (i.e., Russia) attempted to generate disruptive political and social effects through the employment of COVID-19 disinformation activities. The analytical focus of this section is on the tactics employed and effects generated, specifically at the tactical and operational levels.

Novi Sanzhary COVID-19 Riots

With a population of less than 10,000 people, Novi Sanzhary is a small town approximately 335 kms east of Kiev in central Ukraine. On 18 February 2020, a plane carrying evacuees from China (45 Ukrainians and 27 foreign nationals, including flight personnel) arrived in Kharkiv, Ukraine. However, as soon as the plane landed, rumours started to spread on social media that the passengers were infected and in the process of being transferred to an unidentified medical facility (Miller, 2020b). In response to the rumours, the Ukrainian government confirmed the arrival of the plane, but indicated that the passengers had been tested prior to departure and that no infections or positive COVID-19 tests were reported. Ukrainian government

representatives confirmed that all the passengers would be transferred to a national guard medical centre located in Novi Sanchary and placed in a 14-day quarantine as a precautionary measure.

Following the government announcement, however, additional disinformation about the evacuees was posted and shared across multiple social media platforms, including Viber, Facebook and Instagram (Miller, 2020b). Moreover, local politicians and residents asserted they were not informed of the evacuees prior to the arrival of the plane and complained of a lack of information from the central government officials in Kiev. Angered by the situation, local residents in Novi Sanzhary started to mobilize on 19 February using social media and constructed barricades to block the arrival of the evacuees at the medical clinic. Local residents also gathered and protested at the city centre. Later that day, dedicated channels on various social media platforms were created which disseminated dire warnings of "countless deaths" and spread disinformation about the evacuees, as well as to encourage local residents to take action, including confronting soldiers and setting fire to the hospital (Miller, 2020; Velichko, 2020). Some of the social media channels also suggested local residents watch online broadcasts about the situation from NASH TV, a station own by a pro-Russian politician, as well as other online pro-Russian broadcasters (Velichko, 2020). In some cases, the administrators of social media channels did not conceal their Russian identities and overtly promoted a pro-Russian narrative and provided links to Russian news media outlets.

Dozens of police officers and security personnel, including members of the National Guard, arrived in Novi Sanchary by the morning of 20 February 2020. However, rather than alleviating concerns, the arrival of the security services actually heightened tensions and, at least to local residents, served as confirmation of the rumours the evacuees were infected. Increasing the level of collective anxiety, a spoofed health advisory (which was sent to the entire contact list of the Ministry of Health) confirming that at least five of the evacuees were positive with COVID-19 was released from what appeared to have been the Ukrainian Health Ministry email address (Peters, 2020). While government officials declared the email to have been spoofed, rumours of the infections still took hold and, along with paid agents provocateurs on the ground inciting violence, the situation in Novi Sanzhary reached a tipping point (Velichko, 2020). As the buses carrying the evacuees arrived in Novi Sanzhary, several hundred local residents manned barricades and set fires in an attempt to block their progress. In response, police in riot gear attempted to push the protesters back and clear a path for the buses, using armoured personnel carriers to move vehicles blocking the road (Miller, 2020b). The situation quickly degenerated into violent clashes, with local residents throwing stones and other projectiles at the passing buses (Melkozerova & Parafeniuk, 2020). Aggravating the situation and adding to the uncertainty, additional disinformation was released by at least one news media outlet suggesting the staff at the medical centre resigned in protest over concerns about a lack of proper equipment and training.

Later that day, and in an attempt to defuse the situations, Oleksiy Honcharuk, the Ukrainian prime minister, arrived in town, along with Arsen Avakov and Zoryana Skaletska, the interior and health ministers, respectively. However, the appearance of national political officials as well as

public statements, including a Facebook post by Ukrainian President Zelensky pleading for calm, did nothing to reassure the local residents. By the time the riots subsided, at least nine police officers and one civilian were injured, and 24 people arrested. Both Honcharuk and Skaletska were subsequently dismissed from their government positions.

Campaign to Fracture NATO-Lithuania Relationship

Unlike Novi Sanzhary, which was an attempt to promote civil disobedience and undermine national governance, the campaign targeting Lithuania was designed to fracture a multilateral relationship between the host country and NATO, largely by aggravating and leveraging the local population. The first incident occurred on 31 January 2020 when operatives hacked into the content management system of a Lithuanian news media website and posted a story claiming a US army officer deployed on the NATO mission in Lithuania was taken to the hospital with COVID-19 (Tucker, 2020). The fabricated article indicated the US officer was in serious condition with a variety of symptoms including fever, cough, shortness of breath and other respiratory issues. The article also claimed the commanding officer of the US Battalion declined to inform Lithuanian authorities of the infection, and that health authorities were scrambling to identify local residents whom may have come into contact with the infected US officer. In addition, actual photos and names of US military personnel were used in the fabricated article, which were likely gleaned from official unit social media accounts (Saldziunas, 2020a). While the story only appeared on the news media portal for approximately 10 minutes before being removed, the incident gained significant and widespread media attention and was reported by other news media outlets. Likely to ensure widespread dissemination, the fabricated news story was simultaneously posted to several blogs, one of which purports to be about daily life in the deployed US unit (this blog posts in English and has been used on several occasions to disseminate disinformation about the US military presence in Lithuania).

On 20 March 2020, another fake story was posted on a Baltic web-based news portal, this time claiming that Exercise DEFENDER-Europe 20, a US-led, multinational military exercise that was (in actuality) recently scaled back due to COVID-19, would take place in secret (Tucker, 2020). The fake news article referenced previously published fake news stories regarding the coronavirus, including an article appearing in early March claiming the infection rate in Lithuania had significantly increased, as well as a fabricated email sent to the editorial office of a news media website purporting to be from the Lithuanian Minister of Defence and asking US military commanders not to cancel the exercise because of its economic benefit to the country. The email also noted that information about the exercise would not be provided to the media in order to avoid creating public hysteria (Saldziunas, 2020b). At the same time, the perpetrators of the disinformation effort emailed similar details to several news media outlets and also created information releases on popular social media platforms using a variety of fake accounts. Other fabricated emails were sent to allied NATO military forces, as well as NATO headquarters staff.

Although not focused on the NATO presence, the fake news story was quickly follow-up by two more disinformation activities. On 21 March 2020, *Eurasia Daily*, a Russian language media outlet, published an article claiming the Lithuanian government was planning to use the

pandemic to shutdown pro-Russian media outlets. Two days later, *Eurasia Daily* published another claiming the Lithuanian strategic food reserves had been intentionally destroyed prior to the pandemic and that farmers were unable to plant seeds to support the 2020 harvest, suggesting the national food supply chain was dangerously close to collapse (Tucker, 2020). The disinformation was ostensibly designed to agitate the Russian ethno-linguistic community but also to increase collective anxiety and encourage the general Lithuanian public to question the credibility of the government, especially during an international emergency.

Approximately a month later, another series of disinformation-based attacks took place, this time directly targeting Lithuania's relationship with NATO. On 20 April 2020 (and leveraging a disinformation campaign targeting the NATO mission in Latvia), an article was published on a Russian language news media website serving the Baltic region claiming that several hundred Lithuanian soldiers were or had been in isolation, and that at least 10 members of the NATO battalion had tested positive for COVID-19. The next day, on 21 April 2020, a spoofed email seemingly originating from Jens Stoltenberg, the Secretary General of NATO, was sent to the Lithuanian Minister of National Defence, with copies simultaneously sent to Lithuanian news media outlets and numerous emails of NATO Headquarters and other NATO mission staff, indicating that NATO was removing immediately all troops from Lithuania due to the pandemic (Vandiver, 2020). Although the email was quickly and publicly refuted by the Lithuanian government, several media outlets published articles detailing the alleged troop withdrawal by NATO.[ix]

Campaign to Fracture Canada-Latvia Relationship

The NATO mission in Latvia has also been targeted by Russian COVID-19 disinformation activities and, like that of Lithuania, the effort seems to be focused on creating a rift between the host nation and NATO by amplifying and exploiting anxiety on part of the local population. On 20 April 2020, *Baltic Voice,* a Russian language news media outlet operating the Baltic region, published an article claiming that more than 20 members of the NATO mission in Latvia were infected, and that most of the those infected were Canadian troops who recently arrived from the garrison in at Canadian Forces Base (CFB) Edmonton. According to the article, health concerns were first raised by the family and friends of deployed Canadian soldiers on social media (Staff Writer, 2020a). The article also quoted the Canadian commander (using the real name and photo of the Canadian commander), who confirmed that 21 Canadian soldiers tested positive, and that he first became aware of the infections at least a month earlier – implying that both Canadian and Latvian military leadership intentionally concealed the infections from the public. The interview with the Canadian commander did not happen; rather, it was a fabrication. The article, however, did leverage legitimate (i.e., real) reporting from the *Baltic News Service* (BNS) from a 17 April 2020 article in which the Lithuanian government released information about isolation and infections amongst military personnel. The article also criticized the NATO mission for not only putting the public at risk but also for ignoring public health restrictions, which the general population are obligated to follow (Jakubauskas, 2020).

Two days later, an article authored by Edgars Palladis about the infections appeared in *The Duran*, an online sensationalist news outlet known for disseminating far-right and pro-Russian propaganda that is operated by former employees of *RT*, a Russian state-controlled news organization with significant global presence. The article, which links back to and copied of the text of the article that appeared in the *Baltic Voice* on 20 April, claimed the infection rate amongst NATO members has significantly increased and suggested the infections are not limited to military bases, as NATO troops continued to conduct exercises across Latvia and many members live off-base. The article also pointed out that NATO military activities continued despite Latvia implementing public health measures, including restrictions on social gathering, and argued the military is a "waste of taxpayer money (Palladis, 2020)."

Concerned that rumours about the infection rates amongst NATO military members had the. Potential to create a rift between the Latvian population and the NATO mission, the Latvian government responded to the Palladis article (that appeared in *The Duran*) in two articles and a press release. In the first article, published on 23 April 2020 in *SARGS.LV* (an online popular news publication by the Ministry of Defence), government representatives dismissed the rumour of NATO soldier infections and claimed Palladis is a false online persona or pseudonym used by a professional pro-Russian agitator and it not a real journalist (Mandiant, 2020).[x] The article also identified numerous errors in the article posted on *The Duran*, including inconsistent information, false quotes and erroneous graphics, and provides an official quote from the Canadian commander who stated the information and quote used in the original article were fabricated (Staff Writer, 2020b April 23). In the second article appearing on 25 April, representatives from the Ministry of Defence exposed the questionable origin and the myriad of connections of *The Duran* to the Russian government. The article also identified and explained how the original article was a part of a Russian disinformation operation, and how the author attempted to amplify the rumour by promoting it through more reputable and well-known writers and online platforms. Lastly, the article identified how the author had conducted a series of other disinformation activities, such as targeting the 2017 French Presidential election (Staff Writer, 2020c). The press release, which appeared on 27 April on the Ministry of Defence website, restated many of the concerns identified in the *SARG.LV* articles and declared *The Duran* article to be a fabrication. The press release also stated *The Duran* had been involved in previous disinformation activities, including writing erroneous stories about the spoofed email from NATO Secretary General to the Lithuanian government (Staff Writer, 2020d).[xi]

Why the Difference?

The question remains, why did the COVID-19 disinformation activities in Ukraine degenerate into violence and disorder, whereas similar information confrontation activities in Latvia and Lithuania failed to generate disruptive effects? Although a detailed examination is beyond the remit of this paper, two reasons appear to have made the difference. The first is widespread confidence of the Latvian and Lithuanian public in their government and democratic institutions, whereas in Ukraine there is a general lack of trust in the central government, in particular the Ministry of Health (Miller, 2020a). The second is the employment of agents provocateurs on the ground to help amplify and direct the anger of the civilian population towards state authorities.

While it is possible that a situation could naturally reach a tipping point and descend into violence, in particular when two antagonistic groups come into close proximity, the presence of agents provocateurs appears to significantly increase the likelihood a protest or similar demonstrative activity will culminate in violence. (Agents provocateurs were used extensively by the Russian government in eastern Ukraine in 2014 as well as in Estonia during the Bronze Night riots in 2007 [Lauder, 2019b]).

Observations, Implications and Recommendations

Based upon the case studies, as well as a close examination of Russian information confrontation theory, doctrine and operations since the mid-1990s, the following observations, implications and recommendations have been identified:

Observations:

1. The strategic guidance for the effects to be generated may be centralized but the design and execution of activities is almost entirely decentralized. In other words, information confrontation appears to be a highly decentralized set of activities that are planned and executed by a range of state and non-state assets. There is little evidence to suggest or indicate the Russian government utilizes a hierarchical C2 system for information confrontation (which the Soviet Union employed during the Cold War), and no indication the Russian government is concerned about potential information fratricide or the effects of contradictory information being released to target audiences;
2. There is increased emphasis on outsourcing or contracting out. That is, non-state actors, such as – but not limited to – private businesses, NGOs, organized crime, patriotic groups, biker gangs as well as highly-motivated civilian agitators and agents provocateurs, have served as a force-multiplier for the Russian government. More critically, non-state actors are both disposable and deniable, which appears to be a core principle in how Russia projects power in the contemporary operating environment, in particular as a central component of a broad political warfare strategy (Lauder, 2019a);
3. It appears the Russian government has shifted its dissemination strategy and rather than broad and wide-ranging activities (i.e., messaging to everyone) it has narrowed its overall approach and engages specific target audiences (in some cases creating and maintain discussion groups and other types of peer networks or affinity groups), in particular those that agree with or who's beliefs are generally consistent with the messaging. This qualitative adaptation in message dissemination occurred over the last few years, starting just prior to the US Presidential election in 2016. As such, the audiences engaged by the Russian government are likely ideologically out-of-reach of or generally not receptive to Western government messaging efforts;
4. Activities are rarely done in isolation and are generally complementary in nature. As such, information confrontation appears to be layered, occurring at and generating effects across all levels of conflict. This is by intention and has led not only to the blurring of traditional conceptual divides between levels of conflict (e.g., between tactical,

operational and strategic levels) but also the blurring of lines of responsibility (Lauder, 2019a);
5. While some analysts refer to the current context as the post-truth era or the "normalization of lying (Skillen, 2019)," it appears that truth is no longer relevant in the contemporary operating environment; rather, truth (i.e., people's perception and construction of reality) appears to be malleable and manageable, or what can be referred to as managed reality (Lauder, 2019a).

Implications and Recommendations:

1. Facts and truth may not be sufficient to alter or change the beliefs of the audiences being targeted by Russian information confrontation. According to recent research, the presentation of countervailing information or counter arguments may have the opposite effect of what is intended, essentially reinforcing the beliefs and pushing the audience further into informational isolation (i.e., the backfire effect). As a result, fact-checking websites and similar counter-messaging efforts may be a waste of resources and actually do more harm than good, in so far as convincing the audience they adhere to faulty beliefs. Alternative approaches to effectively changing people's minds, in particular through long-term engagement focused on building trust will need to be investigated and operationalized; and,
2. The sheer volume and frequency of messaging emanating from the Russian government and its proxies makes it extremely difficult and incredibly resource intensive to counter. Coupled with the lack of access to certain audiences, due to filter bubbles, echo chambers and being informationally isolated, the best strategy may be to maintain information outreach to and reinforce ideologically supportive/friendly audiences vice trying to convince unsupportive or irreconcilable audience their beliefs are faulty. In addition, since resources are extremely limited, a risk assessment framework needs to be developed to identify when it is most desirable, valuable and effective to respond to Russian information confrontation across both supportive and unsupportive audiences.

Summary

The emergence of the coronavirus and a lack of clear and definitive information and guidance by public health organizations and national and regional governments, coupled with heightened collective anxiety, has created the perfect storm for the promulgation of disinformation and other manipulative and deceitful content. The Russian government is one of the most prolific offenders and has taken advantage of the anxiety and uncertainty to advance a myriad of false narratives and disinformation about COVID-19 to generate deliberate and tailored disruptive effects, such as inciting violence against government authorities and fracturing military partnerships, specifically the relationship between the host country and NATO.

While the Russia government has a long history of conducting psychological warfare, dating back to the early days of the Cold War, since the mid-1990s it has engaged in several iterations of defence and security renewal. Based on lessons learned from operations (e.g., Chechnya, Estonia,

Georgia, Ukraine, etc.), as well as perceived US and NATO information warfare force developments, the Russian government has modernized its approach, which includes integrating information technology as well as developing new sociotechnical approaches to engaging and exploiting target audiences. Russia's new approach can be summed up as decentralized, matrixed, complementary, theoretically grounded and high-volume while at the same time tailored, deliberate and ambiguous in its origins. As a result, the Russian government has demonstrated a clear capacity, capability and desire to generate disruptive effects, in particular by amplifying and exploiting uncertainty and anxiety regarding the pandemic. A cursory examination of three case studies suggests two factors are necessary for the generation of disruptive effects. First, a lack of public confidence in government and democratic institutions. Second, employment of agents provocateurs to help amplify and direct the anger of the civilian population towards state authorities.

References

Alba, D. (2020, March 29). How Russia's troll farm is changing tactics before the fall election. *The New York Times*. https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html

Bakshy, E., Messing, S. and Adamic, L. (2015). Exposure to ideologically divisive news and opinion on Facebook. *Science*. 348(6239). http://science.sciencemag.org/content/348/6239/1130#BIBL,

Beaumont, P. Borger, J. & Boffey, D. (2020, April 24). Malicious forces creating 'perfect storm' of coronavirus disinformation. *The Guardian*. https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-state-led-disinformation

Branford, B. (2017, March 30). Information warfare: Is Russia really interfering in European states? *BBC News*. https://www.bbc.com/news/world-europe-39401637

Broad, W.J. (2020, April 13). Putin's long war against American science. *The New York Times*. https://www.nytimes.com/2020/04/13/science/putin-russia-disinformation-health-coronavirus.html

Clifton, D. (2017, August 3). A Chilling Theory on Trump's Nonstop Lies: His duplicity bears a disturbing resemblance to Putin-style propaganda. *Mother Jones*. https://www.motherjones.com/politics/2017/08/trump-nonstop-lies

Diamond, J. (2011). *Collapse: How Societies Choose to Fail or Succeed* (revised). Penguin Books.

Fazio, L.K., Payne, B.K. Brashier, N.M. & Marsh, E.J. (2015). Knowledge does not protect against illusory truth. *Journal of Experimental Psychology.* 144(5). https://doi.apa.org/doiLanding?doi=10.1037%2Fxge0000098

Galeotti, M. (2017, September 1). Controlling chaos: How Russia manages its political war in Europe. *European Council of Foreign Relations.* *https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/*

Gamberini, S.J. & Moddie, A. (2020, April 6). The virus of disinformation: Echoes of past bioweapons accusations in today's Covid-19 conspiracy theories. *War on the Rocks*. https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/

Grayling, A. (2011, June 23). Psychology: How we form beliefs. *Nature*. 474.

Grimes, D. (2017, December 4). Echo chambers are dangerous—we must try to break free of our online bubbles. *The Guardian*. https://www.theguardian.com/science/blog/2017/dec/04/echo-chambers-are-dangerous-we-must-try-to-break-free-of-our-online-bubbles

Gross, J. and Levenson, R. (1995). Emotion elicitation using films. *Journal of Cognition and Emotion*. 9(1), 87–108. https://pdfs.semanticscholar.org/8d06/090b74b1cd4c54bc6c149507bfda6533f80f.pdf

Hoggan, J. (2016, March 31). How Propaganda (Actually) Works. *Huffington Post*. https://www.huffingtonpost.com/james-hoggan/how-propaganda-actually-w_b_9584138.html

Hosanagar, K. (2016, November 25). Blame the Echo Chamber on Facebook: But Blame Yourself, Too. *Wired.* https://www.wired.com/2016/11/facebook-echo-chamber/

Jakubauskas, R. (2020, April 17). There are eight people with coronavirus in the army and about 200 soldiers in isolation. *BNS*. https://www.bns.lt/topic/1912/news/61092239/

Lauder, M.A. (2018a). 'Wolves of the Russian spring': An examination of the Nightwolves as a proxy for the Russian government. *Canadian Military Journal, 18(3).* *http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf*

Lauder, M.A. (2018b). *Analysis of the Russian Strategic Information campaign during the Skripal diplomatic crisis.* Defence Research and Development Canada.

Lauder, M.A. (2019a, May). *Gunshots by computers: An examination of Russian information confrontation in doctrine, theory and practice*. Defence Research and Development Canada.

Lauder, M.A. (2019b, Fall). Limits of control: Examining the employment of proxies by the Russian Federation in political warfare. *Journal of Future Conflict*. 1(1). https://www.queensu.ca/psychology/sites/webpublish.queensu.ca.psycwww/files/files/Journal%20of%20Future%20Conflict/Issue%201%20Fall%202019/Matthew_Lauder-Limits_of_Control-Examining_the_Employment_of_Proxies_by_the_Russian_Federation_in_Political_Warfare.pdf

Lamia, C.C. (2012, March 6). Emotional memories: When people and events remain with you. *Psychology Today*. https://www.psychologytoday.com/ca/blog/intense-emotions-and-strong-feelings/201203/emotional-memories-when-people-and-events-remain

MacFarquhar, N. (2016, August 28). A Powerful Russian Weapon: The Spread of False Stories. *The New York Times*. https://www.nytimes.com/2016/08/29/world/europe/russia-swedendisinformation.html

Mandiant. (2020). '*Ghostwriter' influence campaign: Unknown actors leverage website compromises and fabricated content to push narrative aligned with Russian security interests*. https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html

Melkozerova, V., & Parafeniuk, O. (2020, March 3). How coronavirus disinformation caused chaos in a small Ukrainian town. *NBC News*. https://www.nbcnews.com/news/world/how-coronavirus-disinformation-caused-chaos-small-ukrainian-town-n1146936

Miller, C. (2020a, February 20). A viral email about coronavirus had people smashing buses and blocking hospitals. *BuzzFeed*. https://www.buzzfeednews.com/article/christopherm51/coronavirus-ukraine-china

Miller, C. (2020b, March 9). A small town was torn apart by coronavirus rumors. *BuzzFeed*. https://www.buzzfeednews.com/article/christopherm51/coronavirus-riots-social-media-ukraine

Ouellet, E. (2020, March). *Russian command dynamics – A sociological primer*. Defence Research and Development Canada.

Palladis, E. (2020, April 22). 20 Canadian soldiers test positive in Latvia. *The Duran*. https://theduran.com/20-canadian-soldiers-tested-positive-in-latvia/

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

Peters, J. (2020, February 21). Coronavirus email hoax led to violent protests in Ukraine. *The Verge*. https://www.theverge.com/2020/2/21/21147969/coronavirus-misinformation-protests-ukraine-evacuees

Richtel, M. (2020, February 6). W.H.O. fights pandemic besides coronavirus: An 'infodemic'. *The New York Times*. https://www.nytimes.com/2020/02/06/health/coronavirus-misinformation-social-media.html

Rudman, L. & Glick, P. (2008). *The Social Psychology of Gender: How Power and Intimacy Shape Gender Relations*. New York: The Guildford Press.

Saldziunas, V. (2020a, January 31). Coronavirus panic was sown by hackers: They targeted US troops in Lithuania. *Delfi*. https://www.delfi.lt/news/daily/demaskuok/panika-del-koronaviruso-seja-ir-isilauzeliai-nusitaike-i-jav-karius-lietuvoje.d?id=83419671

Saldziunas, V. (2020b, March 20). Scammers use coronavirus: Impersonating officials allegedly concealing information. *Delfi*. https://www.delfi.lt/news/daily/demaskuok/sukciai-naudojasi-koronavirusu-apsimete-pareigunais-baugina-apie-neva-slepiama-informacija.d?id=83829475

Sebenius, A. (2020, March 09). Russian internet trolls are apparently switching strategies for 2020 U.S. elections. *Time*. https://time.com/5548544/russian-internet-trolls-strategies-2020-elections/

Shermer, M. (2011, July 1). The believing brain: Why science is the only way out of belief-dependent realism. *Scientific American*. https://www.scientificamerican.com/article/the-believing-brain/

Siriwardane, V. (2020, May 15). How Russian trolls are adapting Cold War propaganda techniques. *Brookings*. https://tinyurl.com/y3j3366g

Skillen, D. (2019). Post-truth and normalised lies in Russia. In E. Polanska & C. Beckett (Eds). *Public service broadcasting and media systems in troubled European democracies.* Palgrace Macmillan. https://doi.org/10.1007/978-3-030-02710-0_16

Staff Writer. (2020a, April 20). Several troops had to be sent into isolation. *Baltijas Balss*. https://bb.lv/statja/covid-19/2020/04/20/neskolko-voennoslujaschih-nato-prishlos-otpravit-v-izolyaciyu

Staff Writer. (2020b, April 23). False news is being directed against NATO soldiers in Latvia, announcing the mass illness of Covid-19. *SARGS.LV*. https://www.sargs.lv/lv/latvija/2020-04-23/pret-nato-karaviriem-latvija-vers-viltus-zinas-vestot-par-masveida-saslimsanu-ar?fbclid=IwAR154JDfxDGDaWstr-GGsy%E2%80%A6

Staff Writer. (2020c, April 25). The fake news portal that attacked NATO soldiers has also affected the French Presidential Election. *SARGS.LV*. https://www.sargs.lv/lv/latvija/2020-04-25/nato-karaviriem-uzbrukusais-viltus-zinu-portals-ietekmejis-ari-francijas?fbclid=IwAR1Xe8lI3wW1ZvooEJVuc2ZgLp77L%E2%80%A6

Staff Writer. (2020d, April 27). *Artis Pabriks: Attempts to attack information space with deceptive messages area a sign of potential adversary's inferiority complex.* Ministry of Defence of the Republic of Latvia. https://www.mod.gov.lv/en/news/artis-pabriks-attempts-attack-information-space-deceptive-messages-are-sign-potential

Sukhankin, S. (2020, April 1). Covid-19 as a tool of information confrontation: Russia's approach. *The School of Public Policy Publications*. http://dx.doi.org/10.11575/sppp.v13i0.70113

Tajfel, H., & Turner, J. (2001). An integrative theory of intergroup conflict. In M. A. Hogg & D. Abrams (Eds.), *Key readings in social psychology. Intergroup relations: Essential readings* (p. 94–109). Psychology Press.

Tajfel, H., & Turner, J. C. (2004). *The Social Identity Theory of Intergroup Behavior.* In J. T. Jost & J. Sidanius (Eds.), *Key readings in social psychology. Political psychology: Key readings* (p. 276–293). Psychology Press. https://doi.org/10.4324/9780203505984-16

Thompson, N. & Lapowsky, I. (2018, December 17). How Russian trolls used meme warfare to divide America. *Wired*. https://www.wired.com/story/russia-ira-propaganda-senate-report/

Tolz, V. and Chatterje-Doody, P. (2018, April 5). Four Things You Need To Know About Russian Media Manipulation Strategies. *The Conversation*. https://theconversation.com/four-things-you-need-to-know-about-russian-media-manipulation-strategies-94307

Tucker, P. (2020, 26 March). Russia pushing coronavirus lies as part of anti-NATO influence ops in Europe. *Defense One*. https://www.defenseone.com/technology/2020/03/russia-pushing-coronavirus-lies-part-anti-nato-influence-ops-europe/164140/

Uscinski, J. & Enders, A.M. (2020, April 30). The coronavirus conspiracy boom. *The Atlantic*. https://www.theatlantic.com/health/archive/2020/04/what-can-coronavirus-tell-us-about-conspiracy-theories/610894/

Vandiver, J. (2020, April 23). Coronavirus pandemic leads to spike in disinformation directed at US, NATO in Europe. *Military.com.* https://www.military.com/daily-news/2020/04/23/coronavirus-pandemic-leads-spike-disinformation-directed-us-nato-europe.html

Velichko, L. (2020, 28 February). Masters of panic: A pro-Russian network in Ukraine organized a riot in Novi Sanzhary. *Texty*. https://texty.org.ua/articles/100356/specoperaciya-imeni-portnova-ta-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-hto-za-cym-stoyit/

Weiss, R. (1969). Repetition of Persuasion. *Psychological Reports*. 25(2). https://doi.org/10.2466%2Fpr0.1969.25.2.669

Endnotes

[i] From Greek mythology, Typhon was described as an immensely powerful and lawless beast, having a head of over a hundred snakes that shot fire and generated a terrible and debilitating noise. Typhon attempted to overthrow Zeus in a failed bid to gain control over the cosmos.

[ii] A grounded approach implies the development of theories and concepts based on the collection and analysis of data and information. This is one of the methods used in adversarial intent analysis, which is defined as the employment of scientific knowledge and the rigorous application of scientific methodologies, including empirical research, to develop and apply analytical techniques, models and tools to discern malicious and hostile intent in targets, and to conduct forensic examinations of, and provide advice to defeat, adversary information and special warfare capabilities, strategies and tactics.

[iii] The Russian government along with many Russian military theorists and capability proponents (e.g., General V. Gerasimov), often use the term information confrontation to denote information activities conducted by the Russian government in support of the achievement of geopolitical objectives. Since information confrontation is a relatively new term, I will use the term psychological warfare when referring to information capabilities and tactics employed during the Soviet era.

[iv] Although the terms maskirovka, active measures (both legacy terms) and strategic information are not used by the Russian government, I believe there is analytical utility in dividing information confrontation into three complementary and overlapping conceptual categories, as it provides a more nuanced appreciation of how the Russia government operationalizes and conducts activities in the information space.

[v] Maskirovka, or operational masking (i.e., military deception), can be defined as activities conducted by, or on the behest of, the Russian government to obfuscate Russian military or paramilitary activity and conceal Russian government intent or cause confusion amongst and undermine the operational effectiveness of the enemy.

[vi] The Russian federal security agency is the primary successor of the KGB (*Komitet Gosudarstvennoy Bezopasnosti*, or the Committee for State Security).

[vii] Albeit a working definition, active measures can be defined as activities conducted by, or on the behest of, the Russian government designed to generate tailored effects and support the achievement of geopolitical objectives through psychological and political manipulation.

[viii] Strategic information campaigns can be defined as activities conducted by, or on the behest of, the Russian government in which mass media and new media resources to disseminate pro-Russian and anti-Western messaging and related narratives to broad audiences.

[ix] According to Lithuanian government officials, there were more than 800 incidents of false information targeting Lithuania about the coronavirus released using a range means (social media, email, news media, etc.) between February and mid-April 2020.

[x] Mandiant Solutions, a cyber security company that also writes publicly accessible threat assessments, identified 14 cases of news media-based disinformation activities conducted by fake personas since 2017 targeting NATO military forces in Poland, Lithuania and Latvia (Mandiant, 2020).

[xi] It should be noted that none of the releases from the Latvian Ministry of Defence identified or addressed the earlier article appearing in the *Baltic Voice* but rather focused on Palladis and *The Duran*.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

Small Wars Journal
Small Wars Foundation
1350 Beverly Rd, Ste 115-224
McLean, VA. USA 22101-3633

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Typhon's Song: Examining Russia's Employment of COVID-19 Disinformation to Generate Disruptive Effects

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Lauder, M. A.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
December 2020	23	52

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

External Literature (N)

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Toronto Research Centre
Defence Research and Development Canada
1133 Sheppard Avenue West
Toronto, Ontario M3K 2C9
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
05cc	

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2021-N002	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Russia; Disinformation; Active Measures; Political Warfare; COVID-19; Information Warfare

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

The emergence of the coronavirus disease (COVID-19) and a lack of clear and definitive information and guidance by public health organizations and national and regional governments, coupled with heightened collective anxiety, created the perfect storm for the promulgation of disinformation and other manipulative and deceitful content. The Russian government has been one of the most prolific offenders, seeking to generate disruptive effects in targeted countries. This article examines the mechanics of how the Russian government generates disruptive effects through COVID-19 disinformation, as well as discussing implications for NATO and its partners.

L'émergence de la maladie à coronavirus (COVID-19) et le manque d'informations et de conseils clairs et définitifs de la part des organisations de santé publique et des gouvernements nationaux et régionaux, associés à une anxiété collective accrue, ont créé la tempête parfaite pour la promulgation de la désinformation et d'autres manipulations et contenu trompeur. Le gouvernement russe a été l'un des délinquants les plus prolifiques, cherchant à générer des effets perturbateurs dans les pays ciblés. Cet article examine les mécanismes de la façon dont le gouvernement russe génère des effets perturbateurs grâce à la désinformation COVID-19, ainsi que les implications pour l'OTAN et ses partenaires.