INFORMATION POWER AND RUSSIA'S NATIONAL SECURITY OBJECTIVES

Kevin P. Riehle, University of Mississippi, Center for Intelligence and Security Studies, United States

Disclaimer: The views in this article are the author's and do not represent the opinions of any U.S. government agency.

Abstract

Russia's operations in the information domain are an integral part of Russia's interactions in the international environment. As one of Russia's levers of national power, information operations work in concert with all other levers of national power to achieve a defined list of Russia's national security objectives. Judging from pronouncements, policies, doctrine, and actions, it appears that Russia's objectives are: 1) Protect the Putin regime; 2) Control the post-Soviet space; 3) Counterweigh the unipolar actor in the world; 4) Portray Russia as an indispensable player in world affairs; and 5) Divide and disrupt the North Atlantic Treaty Organization (NATO) and the European Union (EU). Russian information operations can be traced through information themes directly to those Russian national security objectives. Some themes can address multiple objectives simultaneously, and the methods for communication can differ based on the target. However, Russian information operations are not standalone activities but work in concert with all other levers of national power to achieve Russia's overarching objectives.

Information Power and Russia's National Security Objectives

Russia's operations in the information domain are an integral part of Russia's interactions in the international environment. Those actions, both overt and covert, have gained a great amount of attention over the past few years. Ranging from hack-and-leak operations to propaganda spread through Russian government-sponsored media, to covert support to foreign political parties, Russia has become notorious for using the information domain to both enhance its own power and to denigrate the power of its adversaries. For Russia, information confrontation is as important as any other kind of confrontation.

But Russia's information operations are not a separate lever of national power, as is often described in the West (Fabian & Berzins, 2021; Jasper, 2020; Snegovaya, 2015). All of Russia's levers of national power—diplomatic,

information, military, economic, financial, intelligence, and law enforcement (DIMEFIL)—work in concert to achieve Russia's national security objectives. This is sometimes vaguely labeled "hybrid warfare" in the West, although Russia never uses that label to describe its own actions. Russian writers instead use "hybrid warfare" ("гибридная война") to refer only to what Western powers, especially the United States, do to Russia (Bartosh, 2016; Slipchenko, 2002; Tsygankov, 2015). In fact, Russia's harnessing of all its levers of national power, including information, to achieve its objectives is neither a newly emerging hybrid warfare concept, nor is it unique to Russia. All states choose how to mix and apply their levers of national power to achieve their objectives. However, Russia's centralized, authoritarian national decision-making process streamlines coordination across multiple levers toward a defined list of national security objectives, just as it has done since long before the hybrid warfare concept appeared.

Russian National Security Objectives

To understand Russian information power, or any of Russia's levers of national power for that matter, we first need to determine what Russia's overarching national security objectives are. What is Russia trying to achieve? Russia's actions in the information domain, as well as in any other domain, have a purpose—they are directed at advancing some objective. Judging from Russian pronouncements, formal policy documents, doctrine, and actions, it would appear that Russia has a discernable list of national security objectives:

1. Protect the Putin regime. Putin's personal security and the prolonging of his regime are the foremost national security concerns of the Russian Federation government. Russia applies all its levers of national power to achieve this objective, focusing heavily on controlling the domestic information environment and applying law enforcement and security tools to suppress opposition. This is evident in the use of Russia's security services to pursue and prosecute those who oppose Putin. The 2016 creation of the Russian National Guard ('Rosgvardiya') and the huge level of resources placed into it is also an indication of this priority. Rosgvardiya is made up of internal security troops and answers to the Presidential Administration, providing a tool for preventing any opposition to the Putin regime from forming either in the physical or virtual realms.
2. Control the post-Soviet space. The 2016 *Foreign Policy Concept of the Russian Federation* places special attention on the nominally (as Russia sees them) independent states that formerly made up the Soviet Union (The Ministry of Foreign Affairs of the Russian Federation, 2016). Moscow-

centric organizations, such as the Eurasian Economic Union and the Collective Security Treaty Organization, provide mechanisms for Russia to maintain control over the economic and security activities of its vassal states. Any effort by those states to reduce Moscow's influence is met with forceful Russian reactions across the whole DIMEFIL spectrum, focusing particularly on diplomatic, military, financial, and economic.

3. Counterweigh the unipolar actor in the world. Putin used the phrase "unipolar security model" in his now famous 2007 speech at the Munich Security Conference (Putin, 2007, para. 15). With that phrase, he was expressing his opinion that the United States imposes its will on the world. Russia uses all its DIMEFIL levers to reduce U.S. influence in the world, and as we shall see, the information lever is particularly prominent in this pursuit, along with intelligence. Russia's growing military and diplomatic collaboration with China is also at least partially designed to create a bloc to counter the unipolar actor.
4. Portray Russia as an indispensable player in world affairs. In contrast to how Russia portrays the unipolar actor, the Russian government trumpets what it characterizes as its military and diplomatic victories, such as in Crimea, Syria, Armenia/Azerbaijan, and in a global pandemic. Russia inserts itself into many world conflicts, claiming to be cleaning up what the unipolar actor has broken.
5. Divide and disrupt NATO and the European Union. Russia uses multiple DIMEFIL levers—military, diplomatic, economic, intelligence, and information—to portray NATO as a destabilizing factor in Europe and the EU as a tottering institution. Russia perceives NATO as a remnant of the Cold War world order and as a tool for the unipolar actor to control it. The EU's liberalist political philosophy often confronts Russia's aggressive self-interested actions, and Russia uses its levers of national power to cut the EU down at any opportunity.

Russia's actions, both internationally and domestically, can be tied directly to one or more of those overarching objectives.

The Information Lever

The information lever applies to some extent in all of those objectives. Russia has a consistent set of information themes that it communicates both overtly and covertly and through both domestic and international channels that align directly with its national security objectives. Those themes can be summarized as:

- Russia is a victim of a concerted, U.S.-led, anti-Russia campaign (США проплатили, 2021; Goncharuk, 2021; RIA Novosti, 2018; TASS, 2018; The Ministry of Foreign Affairs of the Russian Federation, 2021).
- Ukraine is a fascist, corrupt state (ARTV News, 2021; Izvestia, 2021b; Sokolov, 2021; Volkov, 2021).
- The United States creates instability in the world (Bartosh, 2018; Bartosh, 2021; Vesti, 2015).
- Russia bills itself as the savior of the world during World War II—any action that diminishes that is "Russophobia" (Krasheninnikov, 2019; Опубликована статья, 2021; RIA Novosti, 2020; Taran et al., 2020; TASS, 2019b).
- NATO is a threat to international security (*Посол РФ в Сараево*, 2018; NBC News, 2014; Reuters, 2014; RIA Novosti, 2022; Vedomosti, 2021).
- The European Union is on the verge of collapse (EurAsia Daily, 2021; RIA Novosti, 2015; TASS, 2019a; Vasilyeva, 2021).

Those themes reappear over and over again in various forms in Russia's information operations. They are often accompanied by operations using some other lever of national power, such as diplomatic or military. But the Russian information themes are not random. They derive from Russia's national security objectives, and one theme might address multiple objectives simultaneously.

For example, claiming that Russia is the victim of a concerted, U.S.-led, anti-Russia campaign supports the objectives of protecting the Putin regime, counterweighing the unipolar actor, and portraying Russia as an indispensable player in the world. Claims that Ukraine is a fascist state support the objective of controlling the post-Soviet space, counterweighing the unipolar actor, and dividing and disrupting NATO and the EU. The theme that the United States is the source of instability in the world is clearly directed at counterweighing the unipolar actor, but the theme of Russia being a savior of the world addresses both that objective and the objective of portraying Russia as an indispensable player in the world. NATO and EU themes are clearly aligned on the objective of dividing and disrupting NATO and the EU, but the NATO theme also addresses the objective of counterweighing the unipolar actor and portraying Russia as the indispensable alternative.

Counterweighing the United States is clearly a prominent national security objective in the information domain, as it is the target against which most of Russia's information themes are directed.

Figure 1

Alignment of Russian Information Themes to Russia's National Security Objectives

Exploitation of Information to Achieve Objectives

Russia uses its information lever differently in different countries. Russia's choice of how to employ its information lever depends on the nature of the target and where that target fits into Russia's national security objectives. The objectives remain the same, but the methods might differ based on the target. Often, operations against a single target can achieve multiple objectives simultaneously.

For example, Russia routinely labels Ukraine a fascist and corrupt state. It does this through relentless overt messaging, as well as through covert means. In the covert realm, Russia might launch intrusions into the Ukrainian Ministry of Defense e-mail server, as likely occurred in March 2014, when Russia was planning its annexation of Crimea. Once inside the server, Russia inserted fake inflammatory e-mails that portrayed Ukraine as the aggressor in the Russia-sponsored separatist insurgency in Eastern Ukraine, with the backing of a U.S. military attaché in Kiev. It then claimed that a hacker group intercepted the fake e-mails and revealed them publicly as if they were real (Rid, 2020; Smirnov, 2014). The operation was intended to denigrate Ukrainian sovereignty and tie it to an aggressive, Russophobic United States. Russia also likely provided information support to an anti-Ukrainian campaign during the 2016 referendum

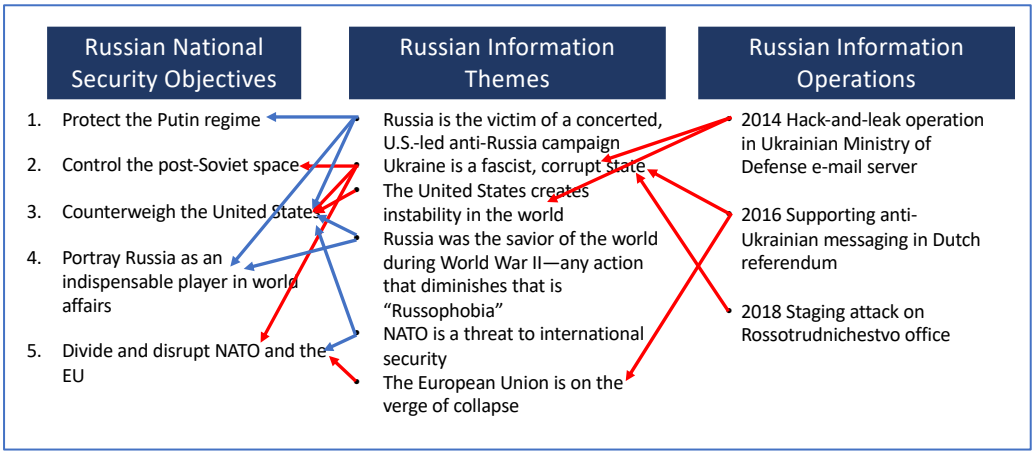
in the Netherlands on whether the Dutch parliament would ratify Ukraine's application for an EU Association Agreement. With Russian information support, anti-EU Dutch activists portrayed Ukraine as a corrupt, undemocratic state that did not deserve closer ties with the EU (Jankowicz, 2020, pp. 123–153). In another example, Russia also probably staged an attack on the office of the Russian organization, Rossotrudnichestvo, in Kiev in 2018, in which unknown intruders left Nazi markings on the walls but caused little other damage. Russian media then claimed the attack was perpetrated by a Ukrainian Nazi group (Russkiy Mir Foundation, 2018). Overt Russian press transformed the staged covert attack into an anti-Ukrainian information operation.

The primary objective of these efforts was to damage Ukraine's attempts to express its sovereignty and reduce its dependence on Russia. Because Ukraine's aspirations run directly counter to one of Russia's primary national security objectives—to control the post-Soviet space—it is worthy of whatever methods are available to prevent that from happening. The Russian government employs these information measures in tandem with other levers of national power, particularly military. Actions such as covert military operations to shut down electrical power generation capabilities in Ukraine in 2016 (Dragos 2017; Polityk, 2016), and the even more damaging NotPetya attack in 2017 (Dearden, 2017b; Griffin, 2017), show the use of the military lever in Russia's undeclared war with that country. Massing troops on the eastern Ukrainian border and claiming to be responding to Ukrainian "provocations," as is occurring in late 2021, demonstrates the use of information and military levers in concert.

But secondarily, those same information operations also address other Russian national security objectives. The e-mail hack-and-leak could be used to show how the United States is a destabilizing factor in the world by claiming U.S. backing of Ukraine's activities. The Netherlands operation could be used to divide and disrupt NATO and the EU by accentuating divisions within the EU regarding Ukraine's worthiness to receive an EU Association Agreement. While Ukraine is the primary target, the same operations can address several other targets simultaneously.

Figure 2

Tracing Russian Information Operations in Ukraine to Information Themes to National Security Objectives



In the other direction, Russia has provided information support to extreme right-wing parties in Europe, such as Spain's Vox Party, Hungary's Jobbik Party, and Austria's Freedom Party (Gricius, 2019; Wiederwald, 2019). All are firmly EU-skeptic and vocally favor Russia. The Russian government has invited representatives of these parties to Russia as special guests and public speakers, and the Russian government often treats them as being representative of their countries' populations, even though they are all relatively small minority parties. Russia has used the information domain to support those parties, both overtly through media placements and pro-Russia content, and possibly covertly via generating phantom tweets (Applebaum, 2019).

The primary national security objective that Russia achieves by supporting these and other right-wing political groups in Europe is to divide and disrupt NATO and the EU (Klasa, et al., 2019). These right-wing political groups are simultaneously staunchly anti-NATO and EU-skeptic and use their political power to advance those positions. But during the visits by members of these parties to Russia, they have often also given vocal support for Russia's Ukraine policy, and members of Hungary's Jobbik Party have participated as election monitors in Russian-sponsored so-called "elections" in eastern Ukraine (112 Ukraine, 2018a). Consequently, information support to these political groups secondarily addresses Russia's Ukraine-related themes and goals by rallying support against Ukrainian sovereignty over its own territory. EU and NATO may be the primary target, but Ukraine objectives can also be achieved simultaneously through the same activity.

Channels

Russia uses a variety of information channels to communicate these themes to achieve its objectives, ranging from overt press and diplomatic statements, to press statements supported by clandestinely acquired information, to covert placement of information without any tie back to Russia.

Russian Media Channels

Russia uses overt media channels when it has no intention of hiding the Russian hand behind the information activity. It may feed clandestinely collected information into overt broadcasts—it does not acknowledge the Russian collection of the information—but no attempt is made to hide the Russian hand in disseminating it.

For example, Russia routinely issues public criticism of U.S. and NATO military exercises and activities in Europe, calling them threatening, destabilizing, and a challenge to Russia—directly addressing several national security objectives (Izvestia, 2021d; Izvestia, 2021f; Izvestia, 2021g). Russia uses its criticism as justifications for actions using other levers of national power, such as large-scale military exercises on the border with NATO, military build-ups along the Ukrainian border, military and diplomatic support to Belarus, and military modernization across Russia (Izvestia, 2021c; Izvestia, 2021e). Russian media also spread narratives that blame the United States for COVID-19 and claim that COVID-19 will bring the end of the EU—similarly addressing multiple national security objectives (Emmott, 2020). These are accompanied by Russian diplomatic moves to support Russia's European allies while isolating countries that oppose Russian policies (AP News, 2021; Holroyd, 2021; Izvestia, 2021a; Portyakova, 2021; Reuters, 2020). These actions support all of Russia's national security objectives in some way or another.

Covert Channels

Russian covert actors have also created illicit channels (i.e., DCLeaks) to dump politically damaging or salacious material to leaker web sites (i.e., Wikileaks), or have created false flag actors that hide the Russian hand behind both the collection and dissemination of the information. These align closely with the Soviet Union's Cold War-era concept of "active measures", and often involve the theft and selective release of information or the falsification of information.

- In 2015, about a dozen U.S. congressmen received e-mails claiming to be from an organization called Patriot of Ukraine, saying that the Ukrainian military was corrupt and asking for the United States to replace Ukrainian military leaders with U.S. and NATO officers. The e-mails possibly originated with a GRU Unit 54777, which is responsible for psychological operations (112 Ukraine, 2018b; Troianovski et al., 2018).
- In 2016, Russian intelligence services conducted a hack-and-leak operation targeting Democratic National Committee and Hillary Clinton election campaign. The services created the leaker website DCLeaks to distribute the information. This became the most widely publicized covert Russian information operation in the post-Soviet era (Rid, 2020, pp. 383–385).
- In 2016 and 2018, Russian intelligence services conducted a hack-and-leak operation targeting the World Anti-Doping Agency, related to the banning of Russian athletes in reaction to a Russian-government sponsored athlete doping program (Cimpanu, 2020; *USA v. Aleksei Sergeyevich Morenets et al*., 2018; World Anti-Doping Agency, 2018). The leaks involved stolen information regarding non-Russian athletes who had obtained authorization to use various substances for health reasons, and Russian trumpeted the revelations as showing a Russophobic double standard. This was probably followed by the infamous Olympic Destroyer covert sabotage operation, which disabled the computer systems that ran the 2018 Seoul Korea Olympics (Greenberg, 2019).
- In 2017, Russian intelligence services conducted a hack-and-leak operation from the Emmanuel Macron campaign in France, in which Russia dumped material into leaker websites (Almasy, 2017; Dearden, 2017a).
- In 2017, a possibly GRU-linked illicit Twitter site called Anonymous Bulgaria disseminated likely Russian disinformation, including claims that the United States sent weapons to ISIS in Syria (Anonymous Bulgaria, 2015; Bellingcat Investigation Team, 2019).

The Russian government disclaims any responsibility for these actions, although investigations have led back to Russia in all of those cases. These operations supported multiple Russian national security objectives, including countering the unipolar actor, denigrating NATO and the EU, and controlling the post-Soviet space.

Non-Russian Overt Media Channels

Russian information operations insert politically damaging or divisive information into non-Russian media sites, such as newspapers and social media sites, to exploit existing dissention or create confusion. In some cases, the media sites are prominent, such as Facebook or Twitter, and draw a great amount of attention. In other cases, the media sites are obscure and attract little attention themselves but offer Russian media the opportunity to cite them as supposedly corroborating sources to further disseminate the information. This method is similar to the infamous Operation Infektion AIDS active measures operation of the 1980s, in which the KGB inserted a Soviet disinformation narrative into a non-Russian media channel initially—a small newspaper in India—and then later broadcast it via Soviet news media (Boghardt, 2009).

- In 2014 and 2015, Russia launched a disinformation campaign in reaction to the shootdown of Malaysian Airlines flight 17 over Ukraine. The campaign involved multiple conflicting explanations disseminated over multiple channels, many of which were obscure, but which were subsequently echoed in Russian media (Nest, 2015; Shandra, 2016). The objective was to confuse the issue and point fingers away from Russia. Russia applied its law enforcement lever in 2017 in parallel with this information campaign, according to Ukrainian media, by arresting a Russian army colonel who may have been able to provide information about the crash, thus eliminating him as a possible witness for the Dutch investigation of the incident (Дело MH17: ФСБ, 2017).
- In 2015 and 2016, a Russian group purchased Facebook and Twitter ads in the lead-up to the U.S. election. The ads portrayed inflammatory messages, many of which supported multiple sides of the same divisive political issue in the United States (Shane & Goel, 2017; U.S. House of Representatives Permanent Select Committee on Intelligence, n.d.).
- In 2017, reports arose alleging that German soldiers raped a teenager in Lithuania; there was no truth to the inflammatory allegations, but they were disseminated via e-mail nevertheless (Deutsche Welle, 2017a; Deutsche Welle, 2017b).

These actions supported the national security objectives of portraying Russia as a responsible world actor, countering the unipolar actor, and denigrating NATO. An item may start in one channel and then be reinforced in the others. For example, information about U.S. political campaigns leaked through illicit channels was later reinforced through Russian media channels and fed to non-

Russian media. Regardless of the channel, the information operations can be linked to one of Russia's primary themes, and thus directly to Russian national security objectives. Additionally, actions related to other levers of national power, including diplomatic, military, and law enforcement, occurred alongside several of these information operations to achieve the same national security objective.

Conclusion

Russia uses its information lever aggressively to achieve its national security objectives, and individual information operations can address multiple objectives simultaneously. However, Russia's actions in the information domain are just one of Russia's DIMEFIL levers. Although Russia's information operations have attracted a great amount of attention, they do not act alone. Russian diplomatic activity has addressed many of the same information themes, Russia has justified its military aggressiveness based on narratives regarding NATO and U.S. actions, and Russian covert sabotage operations have occurred in the same space as information activities. Rather than some novel hybrid warfare concept, Russia simply marshals and coordinate all its levers, including information, toward a defined list of national security objectives. As an authoritarian state with a highly centralized and personalized national security decision making process, it is easier for Russia to do that than it is for democratic states that have multiple competing constituencies.

References

112 Ukraine (2018a, November 13). *Member of Hungarian party Jobbik was observer at Donbas elections.* https://112.international/conflict-in-eastern-ukraine/member-of-hungarian-party-jobbik-was-observer-at-donbas-elections-34121.html

112 Ukraine. (2018b, December 29). *Russia's GRU sends letters to U.S. politicians on behalf of 'patriot of Ukraine' organization.* https://112.international/politics/russias-gru-sends-messages-to-american-politicians-on-behalf-of-ukrainian-patriots-35580.html

Almasy, S. (2017, May 6). *Emmanuel Macron's French presidential campaign hacked*. CNN. https://www.cnn.com/2017/05/05/europe/france-election-macron-hack-allegation/index.html

Anonymous Bulgaria. (2015, February 21). *US 'easing into' war with Syria using ISIS boogeyman.* https://anonybulgaria.wordpress.com/2015/02/21/us-easing-into-war-with-syria-using-isis-boogeyman/

AP News. (2021, May 6). *Slovakia becomes 2nd EU country to approve Russia's Sputnik.* https://apnews.com/article/russia-europe-slovakia-coronavirus-pandemic-government-and-politics-009327bd95f9ecbbe62ee73d45aafa73

Applebaum, A. (2019, May 2). Want to build a far-right movement? Spain's Vox Party shows how. *The Washington Post*. https://www.washingtonpost.com/graphics/2019/opinions/spains-far-right-vox-party-shot-from-social-media-into-parliament-overnight-how/

ARTV News. (2021, August 25). *Фашизм главная идея украинских националистов [Fascism is the main idea of Ukrainian nationalists].* https://artv-news.ru/stati/86489.html[1]

[1] ARTV News is a news blog associated with the unrecognized Luhansk and Donetsk separatist governments. This article was retransmitted as "IA Regnum. (2021, August 25). *'1488': обыкновенный фашизм на Украине ['1488': Normal Fascism in Ukraine].* https://regnum.ru/news/polit/3353041.html. IA Regnum is run by Yuliya Krizhanskaya, a former leader in the pro-Putin United Russia political party.

Bartosh, A. (2016). Hybrid warfare as a possible catalyst of a global conflict. *Security Issues*, 4, 41-53. 10.7256/2409-7543.2016.4.19958

Bartosh, A. (2018, April 10). *Вашингтон ставит на 'управляемый хаос' [Washington bets of 'controlled chaos'].* Nezavisimaya Gazeta. https://www.ng.ru/armies/2018-04-10/8_7208_washington.html

Bartosh, A. (2021, January 14). *О гибридной агрессии и необходимой обороне [On hybrid aggression and necessary defense].* Nezavisimaya Gazeta. https://nvo.ng.ru/gpolit/2021-01-14/8_1124_challenge.html

Bellingcat Investigation Team. (2019, November 23). *The dreadful eight: GRU's unit 29155 and the 2015 poisoning of Emilian Gebrev.* https://www.bellingcat.com/news/uk-and-europe/2019/11/23/the-dreadful-eight-grus-unit-29155-and-the-2015-poisoning-of-emilian-gebrev/

Boghardt, T. (2009, December). Operation Infektion: Soviet bloc intelligence and its AIDS disinformation campaign. *Studies in Intelligence, 53*(4), 1-24. https://digitallibrary.tsu.ge/book/2019/september/books/Soviet-Bloc-Intelligence-and-Its-AIDS.pdf

США проплатили антироссийскую кампанию в западных СМИ ради введения новых санкций [USA paid for the anti-Russian Western media campaign to introduce new sanctions]. (2021, December 11). Ekonomika Segodnya. https://rueconomics.ru/556333-ssha-proplatili-antirossiiskuyu-kampaniyu-v-zapadnykh-smi-radi-vvedeniya-novykh-sankcii

Cimpanu, C. (2020, May 5). *German authorities charge Russian hacker for 2015 bundestag hack.* Zero Day. https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/

Dearden, L. (2017a, May 6). *Emmanuel Macron email leaks linked to Russian-backed hackers who attacked Democratic National Committee.* Independent. https://www.independent.co.uk/news/world/europe/emmanuel-macron-leaks-hack-en-marche-cyber-attack-russia-dnc-marine-le-pen-election-france-latest-a7721796.html

Dearden, L. (2017b, June 27). *Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers: Russian energy firms and Danish shipping company also hit by hackers.* Independent. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html

Deutsche Welle. (2017a, February 16). *NATO: Russia targeted German army with fake news campaign.* https://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978

Deutsche Welle. (2017b, February 17). *Lithuanian authorities launch investigation into fake German rape story.* https://www.dw.com/en/lithuanian-authorities-launch-investigation-into-fake-german-rape-story/a-37608180

Dragos. (2017). *Crashoverride analysis of the threat to electric grid operations.* https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

Emmott, R. (2020, March 18). *Russia deploying Coronavirus disinformation to sow panic in West, EU document says.* Reuters. https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F

EurAsia Daily. (2021, March 10). *Daily express: ЕС разваливается из-за своей вакцинной стратегии [Daily express: The EU is collapsing because of its vaccination strategy].* https://eadaily.com/ru/news/2021/03/10/daily-express-es-razvalivaetsya-iz-za-svoey-vakcinnoy-strategii

Fabian, S. & Berzins, J. (2021, April 12). *Striking the right balance: How Russian information operations in the Baltic states should inform us strategy in great power competition.* Modern War Institute. https://mwi.usma.edu/striking-the-right-balance-how-russian-information-operations-in-the-baltic-states-should-inform-us-strategy-in-great-power-competition/

Goncharuk, D. (2021, December 21). *Путин: Россия ждет от США юридических гарантий по безопасности [Putin: Russia is expecting from the USA legal guarantees of security].* Rossiyskaya Gazeta.

https://rg.ru/2021/12/21/putin-rossiia-zhdet-ot-ssha-iuridicheskih-garantij-po-bezopasnosti.html

Greenberg, A. (2019, October 17). *The untold story of the 2018 Olympics cyberattack, the most deceptive hack in history.* Wired. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

Gricius, G. (2019, June 10). *Hungary's relationship with Russia poses a risk for Europe.* Global Security Review. https://globalsecurityreview.com/hungarys-growing-relationship-russia/

Griffin, A. (2017, June 27). *'Petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack, monitoring is now being performed manually, Ukrainian authorities said*. Independent. https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

Holroyd, M. (2021, March 2). *Slovakia's Prime Minister steps down amid Sputnik V vaccine scandal.* Euronews. https://www.euronews.com/2021/03/28/slovakia-s-prime-minister-to-step-down-amid-sputnik-v-vaccine-scandal

Izvestia. (2021a, May 11). Словакия в ближайшие дни начнет прививать своих граждан 'Спутником V' [Slovakia will begin soon to inoculate its citizens with 'Sputnik V']. https://iz.ru/1162102/2021-05-11/slovakiia-v-blizhaishie-dni-nachnet-privivat-zhitelei-sputnikom-v

Izvestia. (2021b, July 12). *Путин указал на оправдание нацизма властями Украины [Putin pointed to Ukrainian authorities' justification for Naziism]*. https://iz.ru/1192058/2021-07-12/putin-ukazal-na-opravdanie-natcizma-vlastiami-ukrainy

Izvestia. (2021c, November 1). *Путин предупредил о реакции России на попытки сломать стратегический паритет [Putin warned of Russia's reaction to attempts to break strategic parity].* https://iz.ru/1243858/2021-11-01/putin-predupredil-o-reaktcii-rossii-na-popytki-slomat-strategicheskii-paritet

Izvestia. (2021d, November 13). *Путин назвал учения США в Черном море вызовом для РФ [Putin called US exercises in the Black Sea a challenge for Russia]*. https://iz.ru/1249395/2021-11-13/putin-nazval-ucheniia-ssha-v-chernom-more-vyzovom-dlia-rf

Izvestia. (2021e, November 15). *Лукашенко обсудил с Путиным маневры кораблей НАТО в Черном море [Lukashenko and Putin discuss NATO ship maneuvers in the Black Sea]*. https://iz.ru/1249900/2021-11-15/lukashenko-obsudil-s-putinym-manevry-korablei-nato-v-chernom-more

Izvestia. (2021f, November 21). Захарова указала на провокационное поведение НАТО [Zakharova pointed to NATO's provocative behavior]. https://iz.ru/1253292/video/nato-provotciruet-rf-zatem-srazu-prosit-uspokoitsia

Izvestia. (2021g, November 28). *Посол РФ оценил размещение военных Британии в ФРГ [RF ambassador appraises the deployment of British forces to Germany]*. https://iz.ru/1256423/2021-11-28/posol-rf-otcenil-razmeshchenie-voennykh-britanii-v-frg

Jankowicz, N. (2020). *How to lose the information war.* Bloomsbury Publishing.

Jasper, S. (2020). *Russian cyber operations: Coding the boundaries of conflict.* Georgetown University Press.

Klasa, A. (2019, May 22). *Russia's long arm reaches to the right in Europe.* Financial Times. https://www.ft.com/content/48c4bfa6-7ca2-11e9-81d2-f785092ab560

Krasheninnikov, F. (2019, December 25). *Великая победа владимира Путина [Vladimir Putin's great victory]*. Vedomosti.ru. https://www.vedomosti.ru/opinion/columns/2019/12/25/819633-velikaya-pobeda

The Ministry of Foreign Affairs of the Russian Federation. (2016, December 1). *Foreign policy concept of the Russian Federation*. https://www.mid.ru/en/foreign_policy/fundamental_documents/1538901/

Посол РФ в Сараево заявил, что стабильность на Балканах нельзя обеспечить расширением НАТО [RF ambassador in Sarajevo stated that expanding NATO cannot provide stability in the Balkans]. (2018, October 18). Interfax. https://www.interfax.ru/world/797787

NBC News. (2014, September 4). *Russia's Lavrov warns Ukraine against joining NATO, slams U.S.* https://www.nbcnews.com/storyline/ukraine-crisis/russias-lavrov-warns-ukraine-against-joining-nato-slams-u-s-n195396.

Дело MH17: ФСБ изолировала ключевого свидетеля [MH17 Case: The FSB isolated a key witness]. (2017, July 5). For.ua. https://for-ua.com/article/1138404

Nest, D. (2015, September 7). *10 outrageous ways Russian media covered the crash of MH17.* Listverse. https://listverse.com/2015/09/07/10-outrageous-ways-russian-media-covered-the-crash-of-mh17/

Опубликована статья Путина к 80-летию начала Великой Отечественной войны [Putin's article commemorating the 80th anniversary of the beginning of the Great Patriotic War was published]. (2021, June 22). Lenta.ru. https://lenta.ru/news/2021/06/22/Guerra/

Polityuk, P. (2016, December 20). *Ukraine investigates suspected cyber attack on Kiev power grid.* Reuters. https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF

Portyakova, N. (2021, October 21). *Ориентация—Запад: Чехия собралась пересмотреть отношения с Россией [Orientation-west: Chechia is reconsidering its relations with Russia]*. Izvestia. https://iz.ru/1238871/nataliia-portiakova/orientatciia-zapad-chekhiia-sobralas-peresmotret-otnosheniia-s-rossiei

Putin, V. (2007, February 10). *Выступление и дискуссия на Мюнхенской конференции по вопросам политики безопасности* [Speech and discussion]. Munich Conference on Security Policy, Munich, Germany. http://kremlin.ru/events/president/transcripts/24034

Reuters. (2014, April 17). *Putin says annexation of Crimea partly a response to NATO enlargement.* https://www.reuters.com/article/us-russia-putin-

nato/putin-says-annexation-of-crimea-partly-a-response-to-nato-enlargement-idUSBREA3G22A20140417

Reuters. (2020, March 22). *Russian army to send Coronavirus help to Italy after Putin phone call.* https://www.reuters.com/article/us-health-coronavirus-russia-italy/russian-army-to-send-coronavirus-help-to-italy-after-putin-phone-call-idUSKBN219081

RIA Novosti. (2015, October 21). *Легран: Европейский союз разваливается, причем опасными темпами [Legrain: The European Union is falling apart, and at a dangerous pace].* https://ria.ru/20151021/1305587606.html

RIA Novosti. (2018, April 20). *Антироссийская кампания в США выдыхается, заявил Лавров [USA's anti-Russia campaign fizzles out, declared Lavrov].* https://ria.ru/20180420/1519044831.html.

RIA Novosti. (2020, February 23) Путин: Россия не позволит искажать историю Великой Отечественной войны [Putin: Russian will not allow distortions of the history of the Great Patriotic War]. https://ria.ru/20200223/1565121055.html

RIA Novosti. (2022, January 8). *Посол России в США назвал НАТО рудиментом холодной войны [Ambassador of Russia in the USA called NATO the foundation of the Cold War].* https://ria.ru/20220108/nato-1766920712.html

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Russkiy Mir Foundation. (2018, February 19). *OSCE confirms the Ukrainian radicals' attack on Rossotrudnichestvo in Kiev.* https://russkiymir.ru/en/news/237995/

Shandra, A. (2016, July 18). *The most comprehensive guide ever to MH17 conspiracies.* Stopfake. https://www.stopfake.org/en/the-most-comprehensive-guide-ever-to-mh17-conspiracies/

Shane, S., & Goel, V. (2017, September 6). 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

Slipchenko, V. (2002, December). Новые Формы Борьбы: В Наступившем Веке Роль Информации в Бесконтактныйх Войнах Будет Лишь Возрастать [New forms of war: In the coming century, the role of information in non-contact war will increase]. *Armeyskiy Sbornik*, *12*, 30-32.

Smirnov, A. (2014). *Глобальная Безопасность в Цифровую Эпоху: Стратагемы Для России [Global security in the cyber epoch: Stratagems for Russia]*. International Institute for the Study of Global Security.

Snegovaya, M. (2015). *Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare.* Institute for the Study of War. https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Sokolov, Maksim. (2021, May 26). *Украина и фашизм [Ukraine and Fascism]*. RIA Novosti. https://ria.ru/20140901/1022273164

Taran, I, Medvedeva, A., & Rumyantseva, A. (2020, January 20). *'Сплочены русофобией': почему страны Восточной Европы всё чаще обвиняют Россию в 'переписывании истории ['United by Russofobia': Why do Western European countries increasingly blame Russia for 'rewriting history]*. RT. https://russian.rt.com/world/article/712672-rossiya-perepisyvanie-istorii-pribaltika-polsha

TASS. (2018, June 10). *Посол в США: антироссийская кампания в информационном поле отразилась на выходцах из РФ [Ambassador to the USA: The anti-Russia campaign has affected people from the Russian Federation]*. https://tass.ru/politika/5281341

TASS. (2019a, February 21). *Лавров заявил, что Евросоюз 'заразился бациллой американской вседозволенности' [Lavrov stated that the European Union 'has become infected with the disease of American permissiveness]*. https://tass.ru/politika/6144436/amp

TASS. (2019b, July 8). *Путин объявил 2020-й Годом памяти и славы в ознаменование 75-летия Победы [Putin declared 2020 a year of remembrance and glory in marking the 75th anniversary of the victory]*. https://tass.ru/obschestvo/6642848

The Ministry of Foreign Affairs of the Russian Federation. (2021, September 14). *Об антироссийской кампании в германских СМИ [About the anti-Russian campaign in German media]*. https://archive.mid.ru/nedostovernie-publikacii/-/asset_publisher/nTzOQTrrCFd0/content/id/4858005

Troianovski, A., Nakashima, E., & Harris, S. (2018, December 28). How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. *Washington Post*. https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html

Tsygankov, P. A. (ed.). (2015). *Гибридные войны' в хаотизирующемся мире XXI века ['Hybrid warfare' in a chaotic world of the XXI century]*. Moscow University Press.

U.S. House of Representatives Permanent Select Committee on Intelligence. (n.d.). *Exposing Russia's effort to sow discord online: The internet research agency and advertisements.* https://intelligence.house.gov/social-media-content/

USA v. Aleksei Sergeyevich Morenets et al., 18 U.S. 371 (2018). https://nsarchive.gwu.edu/document/17596-united-states-v-alexei-sergeyevich-morenets-et

Vasilyeva, M. (2021, November 17). *Взлет падений: в ЕС усиливают меры безопасности из-за COVID [The rise of the falls: EU increases security measures due to COVID]*. Izvestia. https://iz.ru/1250759/mariia-vasileva/vzlet-padenii-v-es-usilivaiut-mery-bezopasnosti-iz-za-covid

Vedomosti. (2021, December 17). Россия опубликовала свои предложения НАТО о безопасности [Russia published its proposals to NATO on stability].

https://www.vedomosti.ru/politics/articles/2021/12/17/901302-rossiya-opublikovala-bezopasnosti

Vesti. (2015, December 15). *Управляемый хаос выходит из-под контроля США [Controlled chaos is getting out of USA's control].* https://www.vesti.ru/article/1748122

Volkov, P. (2021, February 27). *Есть ли на Украине фашизм? [Is there Fascism in Ukraine?].* Ukraina.ru. https://ukraina.ru/exclusive/20210227/1030683630.html[2]

Wiederwald, R. (2019, May 21). *Austria's far-right FPÖ party under scrutiny for ties to Russia.* Deutsche Welle. https://www.dw.com/en/austrias-far-right-fp%C3%B6-party-under-scrutiny-for-ties-to-russia/a-48822539

World Anti-Doping Agency. (2016, September 13). *WADA confirms attack by Russian cyber espionage group.* https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group

Author Biography

Kevin Riehle is an associate professor at the University of Mississippi, Center for Intelligence and Security Studies. He spent over 30 years in the U.S. government as a counterintelligence analyst studying foreign intelligence services, finishing his government career as an associate professor of strategic intelligence at the National Intelligence University. He received a PhD in War Studies from King's College London, an MS of Strategic Intelligence from the Joint Military Intelligence College, and a BA in Russian and Political Science from Brigham Young University. In 2020, he published *Soviet Defectors: Revelations of Renegade Intelligence Officers, 1924-1954*. A second book, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present*, will be published by the National Intelligence Press in late 2021. His articles have also appeared in the *Intelligence and National Security*, *International Journal of Intelligence and CounterIntelligence*, *Cold War History*, and *Journal of Intelligence History*.

[2] Ukraine.ru is run by Iskander Khasimov, a political consultant associated with Russia-supported former Ukrainian president, Viktor Yushchenko.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/