Russia as an Information Superpower

Vera Michlin-Shapir, David Siman-Tov, and Nufar Shaashua[1]

In recent years, there has been much research and political attention directed to the campaign to influence cognition through the manipulation of content, especially in light of the accelerated development of information technologies.[2] This article looks at Russia, which has drawn considerable attention as a case study of political media influence operations. The article reviews conceptual, organizational, and operational aspects (principles, methods, tools, and modus operandi), while emphasizing the element of content. In addition, it explores several recent proven instances that included Russian influence efforts, and draws patterns that characterize Russia's action in this field.

Literature Review

Since 2008, the Russian regime has invested considerable efforts in rebuilding Russia's military capabilities.[3] However, aware of the ongoing

1 Dr. Vera Michlin-Shapir is a researcher on Russia at INSS, David Siman-Tov is a researcher on intelligence, cyber challenges, and cognitive warfare at INSS, and Nufar Shaashua is a former intern at INSS.

2 See the INSS publications on this topic: Zvi Magen, "The Battle over Consciousness," in *The Delegitimization Phenomenon: Challenges and Responses*, eds. Einav Yogev and Gallia Lindenstrauss, Memorandum No. 164 (Tel Aviv: Institute for National Security Studies, 2017), pp. 93-98; Yotam Rosner and David Siman-Tov, "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion," *INSS Insight* No. 1031, March 8, 2018; Gabi Siboni and Gal Perl Finkel, "The IDF's Cognitive Effort: Supplementing the Kinetic Effort," *INSS Insight* No. 1028, March 1, 2018.

3 Scott Boston, Michael Johnson, Nathan Beauchamp-Mustafaga, and Yvonne K. Crane, *Assessing the Conventional Force Imbalance in Europe: Implications for*

gap between Russia's conventional capabilities and those of the "collective West" (NATO in general and the United States in particular), it invests considerable resources in an attempt to develop tools and methods that offset its inferiority. These include asymmetric measures, including a doctrine on the use of non-military means. In effect, this is a doctrine based on the indirect warfare approach, which has existed since the days of the Soviet Union.[4] According to this doctrine, one must consistently look for the enemy's weak points and attack them by means of fast, constant maneuvering, in order to surprise the enemy. Against this background, the Kremlin has exploited the sense of crisis in the West, the increasing opposition to globalization, and the rise of nationalism, populism, and ultra-nationalism, and looked for weak links, in the hope of identifying tensions between Western countries and rifts within the respective societies. Attacking these tensions and rifts is meant to undermine intergovernmental organizations, such as NATO and the European Union, which are seen by Russia as a threat, as well as the institutions and societies of specific countries, such as Ukraine or Germany.

Russia has adapted its traditional approaches to the current era, which is shaped heavily by economic, geopolitical, and technological processes of globalization that blur international borders, both physically (the movement of goods, capital, and people) and technologically (the flow of information and knowledge). Within this framework, Russia has also adapted its historic Soviet doctrine of indirect warfare to the information age, and plays with new tools and according to new rules of the game, in order to fulfill both novel and traditional objectives.

According to published Russian doctrines, activity in the information realm is an integral part of regular governmental activity.[5] The "information struggle" is defined in Russian Defense Ministry documents in the following manner:

> A struggle between two or more countries in the information realm with the aim of damaging information systems, processes,

---

Countering Russian Local Superiority (Santa Monica, CA: RAND Corp., 2018), http://bit.ly/2U6AFoY.

4 Ulrik Franke, *War by Non-Military Means, Understanding Russian Information Warfare* (Stockholm: Totalförsvarets Forskningsinstitut – FOI, 2015).

5 Ibid.

> or resources, critical or other infrastructure, in order to undermine political, economic, and social systems, undermine the society and state by massive psychological influence of the public, and place pressure on the [attacked] state to make decisions that suit the interests of the attacker…it shall be used before using other means in order to achieve the state's objectives without the use of kinetic force, and in order to positively influence the reaction of the international system if and when the struggle becomes conventional.[6]

Sergey Chekinov and Sergey Bogdanov, former senior officers in the Russian army, note that one of the main advantages of activity in this realm of warfare is the ability to deny it, thanks to the nature of the technological and communications network, in which one can operate covertly and with a small footprint, and the relative difficulty of proving the identity of the attacker, unless he/it chooses to reveal himself.[7]

The strategic and academic discourse in the West refers extensively to Russian activity in the information realm, including political influence operations. Many researchers connect Russian activity in the field of cognition with what is called the "hybrid warfare doctrine" or "new generation warfare." Their studies often refer in part to a speech by General Valery Gerasimov, Chief of the General Staff of the Armed Forces of Russia, who in 2013 referred to the "new kind of warfare" as warfare based on the understanding that in the age of digital communication, the human brain increasingly becomes the battlefield of the future. As a result, he believes that the focus should be on human cognition, making the use of kinetic means only one part of the overall struggle.[8]

The "hybrid warfare doctrine," as it is described in the West, includes a combination of psychological measures and electronic and cyber warfare in a comprehensive systemic attempt that becomes a force multiplier to ensure

---

6 "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," Ministry of Defense of the Russian Federation, 2011 [in Russian].

7 Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 12-23.

8 V. Gerasimov, "The Value of Science in Forecasting," V*oenno Promyshlennyi Kur'e*r 8, no. 476 (2013) [in Russian].

victory in a future war. The information struggle takes place in wartime, during phases of conflict escalation, and during times of peace, and continues regardless of the nature of the relations between the countries.[9]

Researcher Mark Galeotti noted that researchers in the West need to rethink whether the Russian information warfare in reality bears the characteristics of a formal doctrine.[10] Another researcher, Keir Giles, claims that the current Russian approach to information warfare is not new, but is based on Russian military thinking since the Second World War and the Cold War. In his opinion, this is an adaptation of traditional Soviet doctrines of warfare and political subversion (known as active measures) to the current era. Giles claims that the Kremlin sees information simultaneously as a tool, a means, a goal, and a theater of operation, and thus its activity in this sphere relates both to processing digital information and to processing information in the human brain.[11]

We agree with Galeotti and Giles and believe that Russia's activity is not necessarily part of a formal doctrine, but rather an adaptation of traditional methods of action to the era of digital communication and information. In our opinion, this approach allows for better understanding of Russian modus operandi in the field of cognition and national security.

Russia's Cognitive Operations in Various Arenas

There are several geographical arenas in which Russia conducts campaigns to influence political cognition: the internal Russian arena, the arena of the Commonwealth of Independent States, the Western arena (which also includes the East European countries that have joined the European Union and NATO), and the arena of the Middle East and Africa (not addressed in this article).[12] As a rule, in these arenas Russia works to achieve several overarching objectives in the field of cognition: maintaining its own regime

9 Keir Giles, *Handbook of Russian Information Warfare* (NATO Defense College, Research Division, 2016).

10 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018.

11 Giles, *Handbook of Russian Information Warfare*.

12 The RAND Corporation made a similar division into arenas: Todd C. Helmus, Elizabeth Bodine-Baron, and Andrew Radin, *Russian Social Media Influence* (Santa Monica, CA: RAND Corp., 2018), http://bit.ly/2SWcw7S.

stability; influencing the policies of foreign governments in ways that benefit Russian interests as they are perceived by the Kremlin; and undermining citizens' trust and confidence in government leaders and institutions in target countries, in order to harm the legitimacy of liberal democracy and disrupt relations between target countries and third countries.[13] The Russian regime conducts cognitive campaigns with different messages and tools that are tailored to each arena.

Early in the 21st century, the regime decided to manage Russia's domestic political arena as a cognition theater, and has continued this approach ever since. In this framework, the Kremlin retook control of Russian media networks that were privatized and those established in the 1990s, and began to use them to convey self-serving political messages. There are three significant interests that the regime seeks to advance and thereby also advance its interests in other arenas: maintaining Putin's rule; strengthening the state's control over internal affairs, dubbed "sovereign democracy" (or as it is called in the West, an "illiberal democracy"); and demonstrating its great power status in the external arena. This is often achieved by weakening and denigrating (by disseminating negative, embarrassing, or false information, often known in Russian as *kompromat*) opposition figures who advance liberal ideas or other notions that challenge the regime (e.g., nationalist extremists).[14]

Russia's main interest regarding the former Soviet Union is to maintain the Russian sphere of political and economic influence and retain the rule of pro-Russian elites who do not challenge the Russian form of government. The Color Revolutions in Georgia (2003) and Ukraine (2004) challenged the Russian regime with the loss of political-economic influence, the penetration of liberal ideas into the post-Soviet political sphere, and the possibility of undermining the "sovereign democracy"; they were also a military threat vis-à-vis the expansion of NATO. In these countries, the Kremlin fosters relations with Russian-speaking communities, which are considered supportive of Russia. Sometimes, cognitive influence over these groups occurs in part

13 Pynnöniemi Patri and András Rácz, "Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine," FIIA Report 45 (2016).

14 For further reading on the topic of the use of denigration measures in the Russian arena, which is considered a very common tool and not only by the regime, see Alina V. Ledeneva, *How Russia Really Works? The Informal Practices that Shaped Post-Soviet Politics and Business* (Ithaca: Cornell University Press, 2006).

by fanning the flames of tensions between Russian speakers and the general population, which is considered more critical of Russia.[15] Other times, this occurs by weakening confidence in government institutions and leaders in those countries in order to cast doubt on democratization processes underway and liberal ideology in general, and to undermine the relations between these countries and Western countries and intergovernmental organizations.

The Kremlin has three main interests in relation to the West. First, it seeks to demonstrate Russia's strength as a great power in the ongoing power struggle with the West in general and with the United States in particular. In other words, Russia seeks parity with the West and resists what is seen by the Kremlin as American subversion in Russia's internal arena aimed at toppling the regime. Second, it seeks to undermine the foundations of the European Union and weaken the NATO alliance, whose spread eastward is seen by Russia as a military threat; and third, it aims to erode democratic institutions and mechanisms in the West by exploiting the structural weaknesses of capitalism and democracy.[16] In these countries, Russia fosters relations with political groups that challenge liberal-democratic regimes (such as extreme right wing groups, religious groups, or even extreme leftist groups) and uses their assistance to change the public's cognition and undermine citizens' confidence in state institutions and in the democratic system. In addition, Russia attempts to undermine the relations between NATO and European Union states and Western intergovernmental institutions.

The Russian "Information Community"

The cognitive campaign that Russia wages internally and externally includes overt and covert efforts in the traditional and new media (social media); they involve content attacks, as well as technological attacks. Russia's activity in these spheres is carried out by a variety of official, semi-official, and unofficial actors, which side by side make up the "information community." This community can be divided into two main spheres: the military sphere (including Military Intelligence – GRU, the Federal Security Service – FSB,

15 Helmus, Bodine-Baron, and Radin, *Russian Social Media Influence*.

16 William C. Wohlforth and Vladislav M. Zubok, "An Abiding Antagonism: Realism, Idealism, and the Mirage of Western-Russian Partnership after the Cold War," *International Politics* (2017): 1-15.

and the Foreign Intelligence Service – SVR), and the governmental-civilian sphere.

The Military Sphere

In 2012, the Russian Ministry of Defense published its "Cybernetic Strategy."[17] The new strategy, which was approved by President Putin, expands the powers of Russia's security and intelligence organizations in cyberspace. In 2008, after the war with Georgia, Russia's military intelligence became the last of the organizations to join the Russian information community. At that time, as part of changes to Russian operational doctrines, the Russian Defense Minister made initial attempts to integrate the field of information warfare within military activity and to create military departments that would carry out attacks to accompany military actions.

In 2013, the Russian government announced the establishment of information units in the Russian army, which would include hackers, journalists, media strategists, psychological operations experts, and linguists. The emphasis was placed on language skills, to create the ability to communicate with large and diverse target audiences.[18] These units seem to have begun operating between 2013 and 2017. In February 2017, Russian Defense Minister Sergey Shoygu announced that a propaganda department had been established within the army, which would join the information operations division.[19]

The organizations that make up the "military sphere" use diverse media to achieve cognition-related objectives. The most basic tool is the human communication group in Russia and in the target countries. This group includes ordinary people, "concerned citizens," experts, statesmen, and celebrities, who are interviewed and refute Western messages or, alternatively, support Russian narratives. This framework likewise activates pro-Russian organizations, pro-Russian parties, activists, and lobbyists. When the Russians

---

17 "Conceptual Outlooks on the Activity of the Armed Forces of the Russian Federation in the Information Sphere," Ministersvo Oborony Rossiyskoy Federatsii, 2011 [in Russian]; Oren Dotan, "Cyber Bullying: How Russia Uses Hackers and Broadcasts Global Cyberattacks," *Walla*, July 21, 2016, http://bit.ly/2TdF6kB [in Hebrew].

18 Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington: Center for Naval Analyses, 2017).

19 Demian Sharkov, "Russia Announces 'Information Operations' Troops with 'Counter-Propaganda' Remit," *Newsweek*, February 22, 2017, http://bit.ly/2GXQpXM.

operate in countries that are home to communities of Russian immigrants (for example, Germany), they try to galvanize these communities as part of the information struggle, and do so by spreading rumors in the local community.

Social media has also become a very important tool in the hands of the military sphere of Russia's information community. At a relatively early stage, Russia adopted advanced technological tools toward these objectives, and unlike most Western countries, which are cautious about using such tools − as their activity could be seen as undemocratic and because their impact is unclear − has learned through trial and error how to use them and utilize them extensively against strategic targets.[20] Keir Giles estimates that inter alia the Russian army's propaganda unit carries out psychological and influence operations in traditional and new and online media – social networks, the press, and other media.[21]

Reports by many security companies in the world point to signs on the internet starting in 2013, that indicate the activity of a unit identified as belonging to GRU, known in the West as APT28 (Advanced Persistent Threat) or "Fancy Bear." According to these reports, APT28 focuses on foreign security agencies and government ministries.[22] For example, it attacked the Georgian Foreign Ministry and its footprint was clearly identified.

During the US presidential election race in 2016, American researchers identified another group also belonging to Russian military intelligence – APT29 – which is known as "Cozy Bear."[23] The indictment by special prosecutor Robert Mueller, who was appointed to investigate Russia's intervention in the US presidential elections, revealed that these groups belong to units 26165 (the cyberwarfare unit) and 74455 of GRU, and described in detail their practices and their synergetic use of three spheres

---

20 Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *Journal of Slavic Military Studies* 27, no. 1 (2014): 101-30; Giles, *Handbook of Russian Information Warfare*.

21 Keir Giles, *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (Chatham House, Russia and Eurasia Programme, 2016).

22 "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye, Inc*., 2014; Eric Lipton, David Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016.

23 Connell and Vogler, *Russia's Approach to Cyber Warfare*.

– technological (hacking), psychological (exposing information via third party sites and fictional identities), and espionage-related (collecting sensitive information on official figures).[24]

It was reported recently that GRU (together with FSB), funds and operates "cadet classes" at public schools in Moscow, whose purpose is to foster and improve the mathematical and technological skills of potential recruits.[25] Within this framework, unit 25165, mentioned in Mueller's indictment, developed a curriculum at several public schools over the past few years. In addition, it was revealed that there are a number of leading organizations that operate under unit 54777, responsible for psychological warfare in the Russian army, that are officially funded by government grants, but covertly run by the GRU. Two of the most important organizations that operate under this unit are the InfoRos news agency and the Russian Diaspora Institute.

The Governmental Sphere and the Civilian Sphere

The governmental sphere of the Russian information community consists of governmental bodies and private companies that are recruited both overtly and covertly by the government and security organizations. Actors are mainly active in the cognitive-psychological sphere (cognitive operations), and sometimes also in the technological sphere (cyberattacks). The private companies that are part of this sphere include the Internet Research Agency, which is connected to the regime but is not part of the chain of command of military and governmental bodies. According to the US Justice Department indictments and a detailed report submitted to the Senate, this company conducted an extensive cognitive operation to influence internal politics in the United States.[26]

---

24 United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin and co., Criminal No. (18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.), July 13, 2018, US Department of Justice Website, http://bit.ly/2XjTtmJ.

25 A. Troianovski and E. Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West, *Washington Post*, December 28, 2018.

26 United States of America v. Internet Research Agency LLC and Co., Criminal No. (18 U.S.C. §§ 2, 371, 1349, 1028A), February 16, 2018, US Department of Justice Website, http://bit.ly/2NoIL9M; Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, *The IRA, Social Media, and Political Polarization*

In addition, "hacktivists" work within Russia's governmental and civilian sphere – hackers who carry out relatively complex offensive actions, along with patriotic pro-Russian civilians, who volunteer to advance Russia's national interests when the goal of the activity is compatible with their worldview. It is not clear to what extent the hacktivists can be effective in influence operations without assistance from the state. For example, the attack on the internet in Estonia (2007), which occurred during a diplomatic and cognitive struggle that Russia conducted against the intention of the Estonian authorities to remove the "bronze soldier" statue in memory of the Soviet soldiers during the Second World War, was attributed at a certain stage to "activists" from the Nashi (Ours!) youth movement, who claimed responsibility for the event. The Estonian government did not accept this version and claimed that the attack was complex and carried out by the Russian government, and that the involvement of the hacktivists in it was apparently marginal.[27]

These actors also used online and new media, and the Justice Department indictments identified the Internet Research Agency's use of trolls and bots.[28] "Bots" are artificial digital entities that collect information and carry out activities on the internet by imitating human users. The use of bots on the internet takes place in social media, blogs, forums, and internet communities. "Trolls" are people who operate and manage fake profiles on the internet (also via blogs, social media, forums, and so on). Each troll can maintain several profiles and several digital identities. The trolls that the Russians operate write comments on anti-Russian news sites and articles, maintain pro-Russian blogs, report on anti-Russian statuses and videos on YouTube and social networks, flood these networks with posts supportive of Russia, and in addition respond to anti-Russian posts in order to shift the discussion to one that suits the Russian narrative. The purpose of the use of bots is to

---

in the United States, 2012-2018 (University of Oxford, Project on Computational Propaganda, 2018); "The Disinformation Report," New Knowledge, December 17, 2018, http://bit.ly/2E6pIgk.

27 Joshua Keating, "Who Was behind the Estonia Cyber Attacks?" *Foreign Policy*, December 7, 2010, http://bit.ly/2U5d33V.

28 United States of America v. Internet Research Agency LLC and Co., Criminal No. (18 U.S.C. §§ 2, 371, 1349, 1028A).

"strengthen" the posts uploaded by trolls (with "likes," shares, and built-in responses).[29]

In addition, there have been reports of the use of fake news sites and landing pages,[30] and fictitious users, both journalists and news sites, have disseminated misinformation and received extensive publicity.[31] Russia uses mechanisms to distribute messages that are customized to various targets. This involves the distribution of paid advertisements or information on social media, based on algorithms of big data analysis that studies the characteristics of specific targets and sends them messages with the goal of capitalizing on their personal weak points that are recognized by the systems and motivating them to act. The distribution of messages takes place through text messages sent to personal cell phones, emails, and personal messages on social media.[32]

Likewise acting in the Russian governmental-civilian sphere are federal media bodies and agencies that constitute an important part of Russia's information struggle. These agencies and bodies operate openly and disseminate information that serves the Kremlin through articles, television coverage, citation of sources, and the creation of "external" content, such as movies and TV series that convey particular messages. Russian federal TV stations broadcast on cable and satellite networks to countries around the world and relay messages that suit Kremlin ideology to Russian-speaking populations in those countries. Russia also operates the broadcasting corporation Rossiya Segodnya (Russia Today) for its purposes, which includes Radio Sputnik and the news agency RIA Novosti, which broadcast in a large number of languages throughout the world. In addition, the government media network RT broadcasts in five languages, and two different content networks broadcast in English (one is aimed at the UK, and the other at the United States).

---

29 Keir Giles, "Putin's Troll Factories," *World Today* 71 (Chatham House, 2015).

30 A "landing page" is a dedicated web page that looks like part of a site, but is in fact a single page but sometimes looks like part of a well-known site, even though they are not connected. Phony news sites are similar to leading global news sites, with a similar domain name and almost identical appearance to the original site.

31 Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case," CSIS, 2017.

32 Giles, "Putin's Troll Factories."

The traditional institutional media group disseminates information that is convenient for Russia in the form of news reports, talk shows, movies, TV series, documents and "special reports," newsletters, and printed materials. All are distributed in a variety of ways, or posted on bulletin boards. The media networks that are under the control of the Russian administration (RT and Sputnik) disseminate the initial information, repeating it, simplifying it, and framing it as part of events taking place around the world in a manner that is convenient for Russia. In addition, these networks have disseminated information that was stolen through hacking carried out by the Russian military sphere. In doing so, the networks have caused the foreign media to take an interest in the information and repeat it in their reports, contributing to the propagation of the Russian narrative. Figure 1 charts the structure of the Russian information community.

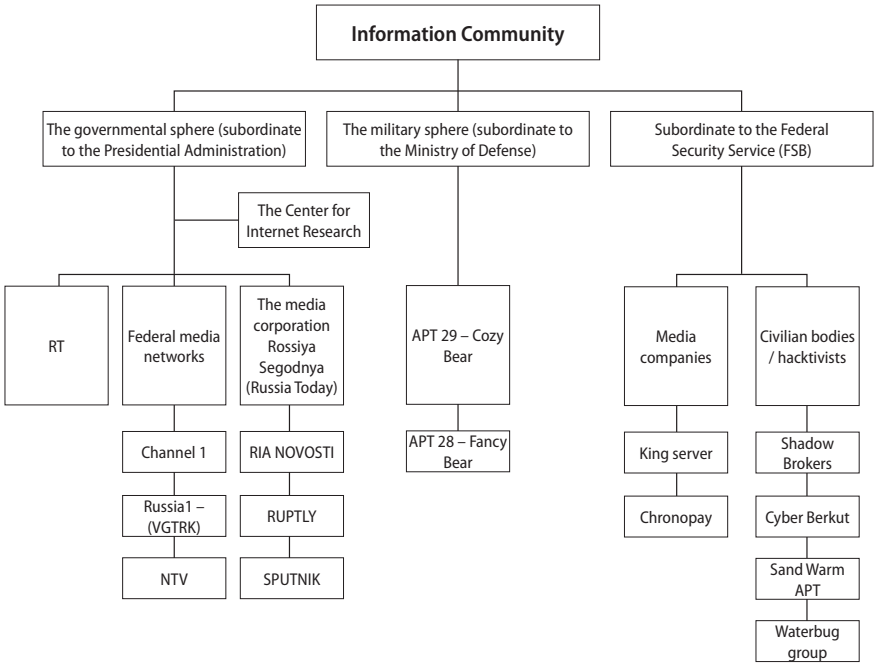

Figure 1: The Russian Information Community[33]

33 The diagram does not include all of the bodies that belong to the Russian information community, but maps its general architecture.

Two clear interests drive the Russian approach behind the decision to activate actors from the governmental and civilian sectors, and they are compatible with Russia's attempts to adapt its traditional methods of indirect warfare to the era of digital media and information: first, the desire to maintain ambiguity and plausible deniability regarding the Kremlin's direct involvement in the Russian cognitive campaign; and second, the relatively cheap cost of these means of warfare.

The Use of Force: Primary Modus Operandi

An analysis of political influence operations attributed to Russia shows the modus operandi of the Russian information community as it utilizes its cognition capabilities and the new tools at its disposal. The analysis indicates a number of patterns: appealing to emotions and sowing doubt among the target audience; aiming at a diverse target audience using diverse messages, and constantly looking for the adversary's social weaknesses. Often, several types of activity can be seen in a single influence operation. Indeed, in the Russian influence operations that we are aware of, a mix of several types has been identified.

The Emotional Element and Undermining Confidence

One of the most prominent characteristics of the Russian activity is the appeal to emotions. The purpose is to influence the cognition of the other side, from the most senior statesman to the citizens of the target country.[34] The appeal to emotion influences decision making, whether it is deciding whom to vote for or a strategic-diplomatic decision by a certain senior official. The feelings sparked are often meant to create doubts and sow confusion, with the aim of influencing an individual to take a certain action or to refrain from a different one.[35] The emotional effort includes attempts to instill the sense that news organizations in the world are not credible, and therefore one must doubt every figure or piece of information they present.

---

34 Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corp., 2017).

35 Nigel Inkster, "Information Warfare and the US Presidential Election," *Survival* 58, no. 5 (2016): 23-32.

This perspective can also be seen in the motto of the Russian governmental media network RT – "question more."

Reports by Ukrainian civilians describe how the information that Russia disseminated during the occupation of the Crimean Peninsula undermined their certainty of an objective truth.[36] Indeed, the Russian method of operation in annexing the Peninsula in March 2014 created a sense of confusion and raised doubts about whether Russia was even involved in the critical hours at the outset of the operation, as for many hours people wearing unidentified uniforms, later nicknamed "little green men," took action on the ground. The Russian media coverage of the annexation aimed to evoke positive emotions toward Russia's actions and to cause viewers to doubt claims by the West of its illegality.

At home Russian media networks are active not only in the effort to glorify the regime's achievements, but work to undermine the public's confidence in its political competitors. In Russian international coverage they too aim not necessarily to promote the Russian narrative, but to offer an alternative and cover the information from a different angle, ostensibly in order to present "the full picture." Underlying this aim is the assumption that doing so can undermine the truths told from a liberal perspective that the public is exposed to on Western international news networks. Creating doubt is based on the assumption that Western governments lack the means to systematically refute the coverage on Russian networks, and on the assessment that the moment doubt is introduced, it is hard to convince the target audience of factual truths, and these doubts compose another possible version of reality. In this way, Russian influence operations erode the hegemony of Western-liberal news coverage and challenge the West on its home turf – international satellite and internet media.

One example of this is the documentary film by RT on the downing of Malaysian Airlines Flight 17 over eastern Ukraine in July 2014.[37] En route from Amsterdam to Kuala Lumpur with 298 passengers and crew on board, many of them Dutch citizens, the plane was downed over a region in which pro-Russian separatists were active, and led to negative coverage of Russia in

36 Peter Pomerantsev, "Inside the Kremlin's Hall of Mirrors," *The Guardian*, April 5, 2015, http://bit.ly/2BNNWvm.

37 RT Documentary, "MH-17: The Untold Story. Exploring Possible Causes of the Tragedy," *YouTube*, October 22, 2014, http://bit.ly/2tA8T8U.

the Western media. Blame was directed at Russia for supporting the separatist groups in Ukraine and providing them with advanced weapon systems. The RT network chose a media approach that encouraged doubting the Western version, which held that the Buk air defense system, given by Russia to the Ukrainian separatists, is what shot down the Malaysian plane. Not only did the Russian network undermine the factual basis of the accusations against Russia; it also created a parallel narrative whereby there was Ukrainian Air Force military activity over Ukraine at the time of the incident, which could have caused the plane's fall. RT did not try to refute the claims against Russia or to substantiate its claims regarding Ukrainian responsibility for the tragedy. RT did not strive to create its own narrative of the events, but to present another possibility, and focused on gaps in the Western version, in order to cast doubt on Russia being at fault for the event. In later coverage of the same event, RT focused on the version whereby the investigation into the incident is not conclusive, thus attempting to exonerate Russia due to the existence of reasonable doubt.

Target Audiences and Social Weaknesses

Aiming at a diverse variety of groups shows that the Russian information community undertakes in-depth social research on target populations. In addition to the civilian population, Russian information operatives direct their messages at leaders and public opinion shapers, and in military campaigns, also at commanders and soldiers. Russia's political influence operations are customized to the various targets, with the message itself directed at a weakness that characterizes each of the target populations. In order to succeed in customizing the attacks to these weaknesses at the right times, intelligence work is required, and this takes place constantly in order to identify the particular weaknesses to be targeted by the attack.

A clear example of the approach of aiming at a variety of target audiences can be seen in the number of political influence operations that the Russians have carried out over the past few years in various places, including Germany. Russia has recognized Germany's importance in intergovernmental European mechanisms, especially in the European Union. Russia also seems to have recognized that Chancellor Angela Merkel's policy regarding the refugees has agitated much of the German population, and saw this as an opportunity. Even before the decision to operate in Germany, Russia worked to consolidate its

relations with pro-Russian elements and candidates for the German political and establishment sphere, in order to expand its influence and its power, and in order to improve its information-gathering in the internal arena.[38]

An example of exploiting the weakness of public opinion in Germany was the way Russia likely used the events surrounding a Russian-speaking girl who lived in Germany, 13-year-old Liza, whose parents reported to the Berlin police that she was missing. She returned home 30 hours later and told her parents that she was kidnapped and raped by three immigrants, but it quickly became clear that this was not the case. Nonetheless, Russian federal television networks began intensive broadcasts on YouTube and on social media in order to spread the girl's initial version, while casting doubt on the credibility of the response by German authorities (who ostensibly silenced the story) and blaming Chancellor Merkel's immigration policy. Following this, demonstrations were organized in Germany, building on the local Russian-speaking community, joined by additional social groups. The demonstrations received media coverage, and the girl's story went viral and flooded the German media. Russia continued to claim that the police version that was publicized, including evidence that contradicts the girl's version, aimed to cover up Germany's inability to cope with the refugee problem – an issue that Russia recognized as a political vulnerability of the German government. In the end, the girl's story became a central issue in the discourse in Germany and caused considerable tensions within the German government, and undermined public confidence in the Merkel government.[39]

Diversity and the Distribution of Content

As a direct continuation of the ongoing search for social weaknesses among the public, the Kremlin sees great importance in the scope and diversity of the content distributed, as well as the continuity of activity. A study conducted by NATO claims that Russia aspires to flood the internet with information relating to the narrative that it wants to instill, including unnecessary and irrelevant information, in order to maximize its distribution. In addition, it has an interest in blurring the relevant facts and replacing them with

38 Stefan Meister, "The Lisa Case: Germany as a Target for Russian Disinformation," *NATO Review*, 2016.

39 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017.

"alternative facts."[40] In effect, Russia optimally adapts its types of activity for the era of online communication.

Historian Yuval Noah Harari emphasizes that in the world of internet communication and the information technology revolution, the most effective way to impose censorship is to flood the information arena – "today, censorship works not by blocking access to information, but by concealing it in enormous amounts of irrelevant information."[41] Proof of this type of activity can be seen in the testimony of two former employees at the Russian troll organization.[42] The two related how each day they received a new list of tasks, which was updated according to events and included detailed explanations of possible responses and links to designated content. The goal was to create new content each day that would be distributed on the internet and serve the Russian narrative.

Russia ensures that each campaign includes the use of several parallel channels to distribute messages, including official media, informal media, and social media. These are sometimes operated simultaneously by actors from both the military sphere and the governmental-civilian sphere. An example of the variety of sources distributing the content and the continuity of activity can be seen in the Russian intervention in the US presidential elections in 2016, when Russia used tools from all three of the groups. Each day additional information was disseminated, some of new information and some information that was already available on the internet.

The US Department of Justice stated that Russian intelligence operated the Guccifer 2.0 Twitter account, which posted content that came from hacking the Democratic Party headquarters. The account shared tweets by other users, among them those issued by trolls operated by Russia, including manipulated content on events in the United States surrounding the elections. It also responded to accusations against it and created an ongoing, lively

40 "Russian Information Campaign against Ukrainian State and Defense Forces," NATO Strategic Communications Centre of Excellence, 2017.

41 Yuval Noah Harari, "In a World Deluged by Irrelevant Information, Clarity is Power," Penguin Books, August 20, 2018, http://bit.ly/2IxxWUm.

42 Shaun Walker, "Salutin' Putin: Inside a Russian Troll House," *The Guardian*, April 2, 2015.

discourse supportive of Donald Trump, and came out against Democratic candidate Hillary Clinton.[43]

The US presidential elections also revealed the variety of platforms that Russia used: manipulated content was distributed on Twitter, Facebook, written media, live YouTube videos, and Russian-funded television networks. Later, after the information received attention, it appeared in all foreign media networks, including American networks. British media researcher Stephen Hutchings recognized this Russian pattern of activity, but also noted that the Russian system of message creation, which is meant to influence political consciousness, is highly decentralized and does not necessarily convey a coordinated, coherent doctrine.[44]

Conclusion

This article presents Russia's political-cognitive efforts, and surveys the Russian information community that operates in military, governmental, and civilian spheres. Russia's information community is a diverse professional community that enables sophisticated activities in all geographical arenas of activity that are relevant to Russia, using a variety of technological spheres of activity. The information tools that Russia uses rely both on online media and on traditional and human communication, via military and governmental-civilian actors. The efforts that Russia invests in the realm of influencing cognition, through the information community and with the help of new information technology tools, have increased its confidence in its ability to operate in this sphere around the world.

In this way, Russia attempts to overcome what it sees as its structural inferiority in the conventional and economic spheres, compared to other superpowers. Thus, it situates itself as an information superpower that aspires to control the new tools of warfare offered in the knowledge and information era. This is multi-dimensional control, from the ability to disrupt the functioning of communications systems and computers, to advanced espionage capabilities and the manipulation of content. The control of

---

43 "Kremlin Troll Tells All About Influencing U.S. Elections," *Moscow Times*, October 16, 2017, http://bit.ly/2VkxWbT.

44 Stephen Hutchings, "We must Rethink Russia's Propaganda Machine in Order to Reset the Dynamic that Drives It," London School of Economics blog, April 4, 2018, http://bit.ly/2SjhMgN.

information could provide an answer to the question: what is a superpower in the era of knowledge and information? Russia's activities in the realm of information are in effect an expression of the new superpower status that it has helped create.

Yet Russia's efforts to become an information superpower indicate a mixed balance sheet. In effect, there is no unequivocal proof of the effectiveness of the use of information as a strategic tool. This is a tool that poses two main problems for its users: difficulty measuring success (it is more than likely that some activity has only limited influence); even when an influence operation seemingly succeeds, the level of success in achieving strategic objectives is still in doubt. Russia's intervention in the US presidential elections illustrates this problem. For example, even if we assume that it is true that Russia conducted a large scale influence operation with the goal of helping Donald Trump's election as president, and that this operation did indeed play a significant role in his election as president, it is still an open question whether Russia achieved its objectives in this way. In effect, its increased intervention in the American information arena exposed President Trump to unprecedented criticism and pushed him into a political situation that does not enable him to improve relations between the United States and Russia – which was a prominent campaign promise.

Thus at least for now, information warfare is a new tool that creates opportunities in the international arena, but its level of effectiveness and its ability to achieve political objectives are still in doubt. The Russian case should also warn us against any exclusive overreliance on information warfare as a tool in international relations, as long as its level of credibility and the consequences of its use have not yet been fully clarified.