UA: UKRAINE ANALYTICA

Issue 1(11), 2018

- **DISINFORMATION CAMPAIGNS**
- **FAKE NEWS**
- **INFLUENCE OPERATIONS**

UA: UKRAINE ANALYTICA

Issue 1 (11), 2018

Propaganda

Editors
Dr. Hanna Shelest
Dr. Mykola Kapitonenko

Publisher:
Published by NGO "Promotion of Intercultural Cooperation" (Ukraine), Centre of International Studies (Ukraine), with the financial support of the Representation of the Friedrich Ebert Foundation in Ukraine, and the Black Sea Trust.

UA: Ukraine Analytica is the first Ukrainian analytical journal in English on International Relations, Politics and Economics. The journal is aimed for experts, diplomats, academics, students interested in the international relations and Ukraine in particular.

Contacts:
website: http://ukraine-analytica.org/
e-mail: Ukraine_analytica@ukr.net
Facebook: https://www.facebook.com/ukraineanalytica
Twitter: https://twitter.com/UA_Analytica

ISSN 2518-7481

500 copies

BOARD OF ADVISERS

TABLE OF CONTENTS

FACING THE RUSSIAN SCHOOL OF SOFT POWER

Tony Jensen
Independent expert, Sweden

This article addresses the nature of the use of influence operations by the federal government of the Russian Federation's as well as ways for detecting and countering such operations. This has been done via a qualitative study of the concept, the Russian government's use, and principles for countering influence operations. The article concludes that the operations appear to be guided by a coercive reimagining of the concept of soft power. It also argues for the need to address the operations on multiple interconnected levels that include the promotion of transparent and responsive communication.

Introduction

Information is the core knowledge that actors can use to interpret an issue. In order to not fall prey to pitfalls such as misinformation and disinformation (inadvertently spread false information and deliberately spread false information, respectively), actors attempt to digest information before accepting it as a part of their perceptions. However, even if information is deemed to be correct, using it as a basis for one's decisions can still be detrimental to the actor's interests. This is because decisions are commonly made without all the facts related to any given issue. By selectively presenting information, foreign actors can therefore tip the scale in another party's decision-making process towards something that the influencing actor (IA) prefers.[1]

These aspects are common occurrences in influence operations, but the latter, the selective presenting of information, has oftentimes been overlooked in discussions regarding the concept. This is despite the prominence that influence operations hold in current debates. While many attempts to influence foreign audiences have been discussed, many others have been left out. Instead, most discussions on the subject simply focus on what they are instead of what an actor can do about it. This, in turn, suggests a need to broaden the debate and focus on how actors can understand, detect, and counter influence operations. Due to the prominence that the federal government of the Russian Federation's (FGRF) actions hold in the contemporary discourse, this article explores the FGRF's use of influence operations, these operations' nature, as

[1] B. Whaley, J. Busby, *Detecting Deception: Practice, Practitioners, and Theory, "Trends in Organized Crime",* Fall 2000, p. 83.

M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, Artech House: Norwood - Massachusetts 2007, p. 63.

R.H. Stolfi, *Barbarossa: German Grand Deception and the Achievement of Strategic and Tactical Surprise against the Soviet Union, 1940-1941*, [in:] D.C. Daniel, K.L. Herbig (eds.), Strategic Military Deception, Pergamon Press: New York - New York 1981, p. 197.

well as ways to detect and counter them. The questions the article sought to answer are:

- What is the nature of the FGRF's use of influence operations?
- How can actors detect and counter the FGRF's influence operations?

These questions have been addressed via a summary of general aspects of information operations, followed by a presentation of principles for countering such operations as well as the FGRF's use of influence operations. These principles have been used to guide the analysis of how the FGRF's influence operations can be countered both proactively as well as after the fact.

Influence Operations

Influence operations are commonly defined by the manner of an actor's coordinated use of resources in order to promote its interests by altering the attitudes, actions, and decisions of a target audience (TA).[2] These attitudes, actions, and decisions in turn are the product of how an actor perceives and reacts to the information environments in which it and its dependencies operate. By utilising one's diplomatic, cultural, military, informational, and economic capabilities to alter these environments, an influencing actor may alter the perceptions of a TA and its dependencies, thereby reshaping how they interpret and address a given situation.[3]

For these efforts to be successful, the operations need to penetrate the target audience's filters: barriers such as previous knowledge and perceptions.[4] To penetrate these filters, alterations of the information environment commonly need to be, at least in part, based on truth. Doing so increases both the alterations' persuasive qualities and their ability to pass scrutiny.[5] By factoring in trust, time constraints, power dynamics, playing on prior knowledge, biases, and exploiting prolonged exposures to similar information as aspects of the operations, the IA can further increase the odds for the alterations to pass scrutiny.[6]

---

2 E.V. Larson (ed.), *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, Rand Arroyo Center: Santa Monica - California 2009, p. 2.

3 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security,* Artech House: Norwood - Massachusetts 2007, p. 55.

4 T.L. Thomas, *Russia's Reflexive Control Theory and the Military*, "Journal of Slavic Military Studies", June 2004, p. 241.

5 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, Artech House: Norwood - Massachusetts 2007, p. 59.

6 Armed Forces Headquarters, *PM Vilseledning, kortversion av AL studie 6: Ett sätt att dölja det sanna och framhäva det falka: En öppen sammanfattning av studien VILSELEDNING (Memorandum Deception, A Short Version of Army Command's Study 6: A Way to Mask the Truth and Emphasise What Is False: A Open Summary of the DECEPTION Study)*, Swedish Armed Forces: Stockholm 1997, p. 19.

M.I. Handel, *Intelligence and Deception*, "Journal of Strategic Studies", March 1982, p. 139.

M.L. Jaitner, H. Kantola, *Applying Principles of Reflexive Control in Information and Cyber Operations*, "Journal of Information Warfare", Fall 2016, p. 29.

J.B. Bruce, M. Bennett, *Foreign Denial and Deception: Analytical Imperatives*, [in:] R.Z. George, J.B. Bruce (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations,* Georgetown University Press: Washington - District of Columbia, pp. 127-128.

R.J. Heuer Jr., *Strategic Deception and Counterdeception: A Cognitive Process Approach*, "International Studies Quarterly", June 1981, p. 298.

S. Macdonald, *Propaganda and Information Warfare in the Twenty-first Century: Altered Images and Deception Operations*, Routledge: London 2006, p. 84.

U.K. Ecker, S. Lewandowsky, O. Fenton, K. Martin, *Do People Keep Believing because They Want to? Preexisting Attitudes and the Continued Influence of Misinformation,* "Memory & Cognition", February 2014, p. 303.

The trust aspect is connected to both the communication channel used to deliver the alterations as well as the source that is perceived to be delivering them. If the TA trusts the perceived source and the communication channels, the TA is more likely to accept the alterations.[7]

The prime target audience for a state actor's operations tends to be another state's decision makers.[8] This is because influencing them is commonly synonymous with the greatest potential payoff. As decision makers are inclined to seek both the approval and input of others as part of their decision making process, IAs may use these as attack vectors in their operations.[9] Approval may be sought from a state's population while input is typically gathered from bureaucrats that serve in the government. By acting upon these lesser TAs, the IAs may separate themselves from their primary TA but still act upon them.[10] This in turn grants them another way to mask the source of the alterations and thereby minimise the prime target audience's ability to discover the IAs' involvement and intentions.

An example of how this can be achieved can be seen in how an IA may use media outlets in order to affect public opinion and the opinion of bureaucrats. These outlets do not necessarily have to be controlled by the IA or be under its direct influence. Instead, they may become unwitting agents of the IA of their own will. This can be achieved by exploiting journalists' dependence on outside expertise, the need of many journalists to present what is perceived as the other sides of an issue, or their ideological inclinations.[11] The former allows the IA to directly shape and reinforce the message if the IA holds influence over the consulted expert.[12] In turn, information transmitted by the IA or its proxies is not necessarily complete or truthful in its entirety. What is important is that the information is convincing enough to pass through the respective recipients' filters and for them to appropriate it.

If all of this is done correctly, the influencing actor should be able to transmit both the motives and the reasons that cause the target audience to act, or not, in a manner that goes against the TA's interests but is in

---

7 D. Lerner, *Is International Pursuasion Sociologically Feasible*, [in:] D.C. Pollock (ed.), *The Art and Science of Psychological Operations: Case Studies of Military Application*. Vol. I, American Institutes for Research: Washington - District of Columbia 1976, p. 48.

M. Cohn, *Getting Psyched: Putting Psychology to Work to Shorten Conflicts and Save Lives, [in:] M.J. Weller (ed.), Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare*, Institute of World Politics Press: Washington - District of Columbia 2008, 231.

8 R.J. Heuer Jr., *Strategic Deception and Counterdeception: A Cognitive Process Approach*, "International Studies Quarterly", June 1981, p. 294.

E.V. Larson (ed.), *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, Rand Arroyo Center: Santa Monica - California 2009, pp. 44-45.

9 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, Artech House: Norwood - Massachusetts 2007, p. 96.

10 G. Sjöstedt, *Desinformation, vilseledning och nationell säkerhet: en problembeskrivning (Disinformation, Deception and National Security: A Problem Description)*, Board for Psychological Defence: Stockholm 1988, pp. 9-10.

L. Bittman, *The KGB and Soviet Disinformation: An Insider's View*, Pergamon-Brassey's: Washington - District of Columbia 1985, p. 52.

11 L. Bittman, *The Use of Disinformation by Democracies*, "International Journal of Intelligence and Counterintelligence", Summer 1990, p. 248.

E.S. Herman, N. Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, Pantheon Books: New York 2002, p. 2.

12 S. Macdonald, *Propaganda and Information Warfare in the Twenty-first Century: Altered Images and Deception Operations*, Routledge: London 2006, pp. 35-36.

accordance with the interests of the IA.[13] This is commonly referred to as reflexive control and can be seen as the highest level of success of an influence operation. Lesser results, such as making the TA act on the altered information (but not in the desired way) and conditioning the TA, can still be considered a success.[14] Examples of lesser results include further polarisation of a state's political climate or casting doubts on the state's institutions.

Principles for Countering Influence Operations

In order for an actor to detect and counter influence operations, he/she needs to possess at least two things: a mental awareness for the possibility of him/her or others becoming a target audience, as well as the structural capabilities to expose and understand these operations.[15] The former acts as the actor's first line of defence by permitting influence operations to be recognised. If the actor lacks the awareness of the possibility that it may become affected, its susceptibility to influence operations is greatly increased.[16] Awareness, however, only offers some protection and may, at worst, even be a burden by creating overly cautious attitudes.[17] It therefore needs to be coupled with means of evaluating changes in the information environment. Once suspected influence operations have been identified, the actor can, via intelligence collection and analysis, expose them. The actor can, through the exposing process, discern what the IA wants to make the TA believe as well as what action the influencing actor desires the target audience to take. The same tools can also allow the actor to gain an understanding of the aims of the operations as well as capabilities of the IA.[18]

For this to work, actors and their dependencies should possess knowledge of how a potential IA may act and how their respective weaknesses may be exploited. The actor should also understand potential weaknesses associated with the information environment they operate in and the communication channels they use.

By knowing what kind of expectations target audience has, how these expectations came about, what the influencing actor knows and does not know, and what the actor expects to see, an actor can further its understanding of why the actor has these perceptions and how they can be exploited.[19] This can include making the actor aware of how their biases can be exploited and reinforced by the IA.[20] As notions based on an actor's biases are resistant to change, even if they are proven false,[21] actors need to constantly evaluate why they hold a certain perception.[22] Doing so can increase their ability to act even if they have been influenced by another party.

---

13 T.L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness*, Foreign Military Studies Office: Fort Leavenworth - Kansas 2011, p. 132.

14 D.C. Daniel, K.L. Herbig, *Propositions on Military Deception*, "Journal of Strategic Studies", March 1982, p. 157.

15 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, Artech House: Norwood - Massachusetts 2007, p. 144.

16 B. Whaley, *Stratagem: Deception and Surprise in War*, Artech House: Boston 2007, pp. 74-75.

17 R.J. Heuer Jr., *Strategic Deception and Counterdeception: A Cognitive Process Approach*, "International Studies Quarterly", June 1981, pp. 319-320.

18 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 144.

19 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 176.

20 R.J. Heuer Jr., *Strategic Deception and Counterdeception: A Cognitive Process Approach*, "International Studies Quarterly", June 1981, p. 315.

21 U.K. Ecker, S. Lewandowsky, O. Fenton, K. Martin, *Do People Keep Believing because They Want to? Preexisting Attitudes and the Continued Influence of Misinformation*, "Memory & Cognition", February 2014, p. 293.

22 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 175.

Since the information environment acts as the primary base for an actor's perceptions, actors should strive to understand how the environment develops. To do this, the actor has to continuously monitor and analyse the information environment for changes to the environment as well as changes in the conduct of other actors. An important aspect in such commitments includes efforts that seek answers to why these changes have come about. To do this, the actor needs to be able to see an event from the perspective of others. Being able to do so can allow the actor to see why other actors act the way they do and what their intentions may be.[23] This in turn requires understanding other actors' doctrines, resources, capabilities, and general aims as well as an awareness of the changing nature of these factors.[24] No actor lives in a bubble or is frozen in time.

For example, an influencing actor may decide to posture and exaggerate their capabilities and intentions in order to deter a TA from acting in a certain manner.[25] This reaction may come about as a reaction to a change in the target audience's goals and interests. If the TA in such a situation knows the IA's true capabilities and motives, then the TA may still be able to act. This is because the target audience then has the means to accurately assess the consequences of acting and can determine if the costs outweigh the benefits.

To accurately do this, actors have to consider the sources of the information they receive as well as the risks associated with the communications channels they use. This is because most of the information that an actor receives tends to come from outside actors as well as the actor's dependencies. Since actors have less control over the information that is delivered and produced by secondary or third parties, but nonetheless rely on them to understand the information environment, the actors need be on guard for notions that may act against their interests. Actors should therefore question and rigorously scrutinize information that reaches them before accepting it.[26]

Since the information environment acts as the primary base for an actor's perceptions, actors should strive to understand how the environment develops

The Federal Government of the Russian Federation's Use of Influence Operations

A number of developments of note have occurred in the FGRF since the mid-2000s and early 2010s that affect how it conducts its foreign policy. Prominent ones include the notion of being trapped in a permanent conflict with outside actors, the use of information warfare as one of the primary means to achieve the FGRF's interests, and the expansion and reinterpretation of the concept of soft power.

The former two are reflected in contemporary Russian military thought. Aspects of it include the holistic and simultaneous use of all of the state's available means in an information and culture war that is transitional – existing through times of both peace and conflict with the ability to achieve the state's goals independently

23 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 178 & 179.

24 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 177.

25 M.I. Handel, *War, Strategy and Intelligence*, Cass: London 1989, p. 314.

26 M. Bennet, E. Waltz, *Counterdeception Principles and Applications for National Security*, p. 180.

or in coordination with the state's other efforts.[27] The open use of force has been relegated to the later stages of a conflict.[28] Instead, conflicts are to be dominated by information and psychological warfare.[29] These approaches aim to break down actors, thereby limiting their ability to function and granting the FGRF a strategic advantage.[30]

These changes in the Russian military thought have also come to be reflected in the FGRF's views on the concept of soft power: from being a concept that emphasises the attraction of other actors as a means to gain influence over them,[31] to a concept that includes the use of coercion as a way to gain the same influence. Soft power has as such evolved into something that can be used to interfere with a state's internal affairs and destabilise its political environment in order to promote a foreign actor's interests.[32]

These notions are largely reflected in many of the FGRF's attempts to influence other actors. As a prelude to what later became the FGRF's invasion of Ukraine and continued intervention in the same, both Estonia and Georgia became targets of influence campaigns from the FGRF. This included, in the case of the former, the exploitation of grievances that members of the Russian minority in Estonia held with regards to the Estonian government,[33] thereby destabilising the political situation in Estonia and placing pressure on the Estonian government. The operations also included a negative portrayal of the Estonian government in Russophone media outlets (both in Estonia and in Russia)[34] and aggressive demonstrations outside of the Estonian embassy in Moscow by members of a Russian non-governmental organisation promoted by the FGRF (commonly referred to as Nashi, "Ours").[35] These were followed by riots in Tallinn (with rioters consisting in part of members of Nashi),[36] as well as large scale cyber-attacks against Estonian institutions.[37] While many sources of the cyber-attacks could be traced to Russia, the Estonian government could not definitively say that the FGRF was behind them.[38]

---

27 P.A. Mattson, *Russian Military Thinking – A New Generation of Warfare*, "Journal on Baltic Security", June 2015, p.66.

U. Franke, *War by Non-military Means: Understanding Russian Information Warfare*, Swedish Defence Research Agency: Stockholm 2015, p. 40.

28 V. Gerisimov, *Ценность науки в предвидении (The Value of Science Is in Foresight)*, "Military-Industrial Courier", February 2013, p. 2.

29 S. Chekinov, S. Bogdanov, *The Nature and Content of a New-Generation War*, "Military Thought", April 2013, p.16.

30 J. Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, National Defence Academy of Latvia: Riga 2014, p. 5.

31 J.S. Nye Jr., *Soft Power: The Means to Success in World Politics*, Public Affairs: New York - New York 2004, p. x.

32 *Concept of the Foreign Policy of the Russian Federation*, "Ministry of Foreign Affairs of the Russian Federation", 18 February 2013 [http://www.mid.ru access: 20 February 2018].

33 *Annual Review 2007,* Estonian Internal Security Service: Tallinn 2008, p. 13.

34 E. Lucas, P. Pomerantsev, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda*, Center for European Policy Analysis/Legatum Institute: London/Washington - District of Columbia 2016, p. 22.

35 M. van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism*, Rowman & Littlefield: Lanham - Maryland 2014, Chapter 8 (E-book).

36 M. van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism*, Rowman & Littlefield: Lanham - Maryland 2014, Chapter 8 (E-book).

37 E. Lucas, P. Pomerantsev, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda.* Center for European Policy Analysis/Legatum Institute: London/Washington - District of Columbia 2016, p. 23.

38 A. Soldatov, I. Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB*, PublicAffairs: New York - New York 2010, Chapter 18 (E-book).

A.J. Selhorst, *Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine,* "Militaire Spectator", April 2016, pp. 154-155.

Following the riots, a delegation consisting of parliamentarians from the ruling party in Russia travelled to Tallinn. Before arriving, they made calls for the resignation of the Estonian government.[39]

The Estonian Internal Security Service attributed much of the polarisation of the political climate in Estonia to the differences in the country's ethnic communities' information environment.[40] The Estonian Internal Security Service also identified attempts by the Russian media outlets to distort the presentation of events, as well as attempts by the members of the FGRF's diplomatic corps and intelligence services to influence the Russian minority in Estonia.[41]

These influence campaigns resulted in the creation of a new concept, that of the Russian world. It officially started as a concept for promoting the Russian language and culture aboard but later it came to be intertwined with the FGRF's claimed right to intervene in other states in order to protect compatriots and citizens of the Russian Federation living abroad.[42] People considered to be compatriots are to a large extent former citizens of the Soviet Union who are in favour of spiritual and cultural ties with the Russian Federation.[43] This policy was put into full effect during the FGRF's occupation of the Crimean peninsula, but, just as forms of the policy can be traced to the events in Estonia, it can also be traced to the Russo-Georgian War. The FGRF had prior to its conflict with Georgia eased the citizenship requirements for Abkhazians and South Ossetians, thereby creating a majority "Russian" community in their respective regions.[44] Their protection was cited as one of the reasons for the FGRF's intervention in Georgia.[45]

Prior to the FGRF's intervention, the prime minister of Russia directly approached the president of Georgia whereby the latter was informed of the FGRF's intention to intervene in Georgia. The reasons cited then were Tbilisi's NATO aspirations as well as the newly declared independence of Kosovo.[46] This was later followed by a build-up of the FGRF's armed forces both inside Georgia and along its border, minor clashes between Georgian, Abkhaz, and South Ossetian forcers, distortions of events in Russian media outlets, and cyber-attacks against infrastructure that limited the Georgian government's ability to communicate and to coordinate its efforts.[47]

---

39 *Николай Ковалев: эстонское правительство должно уйти в отставку (Nikolai Kovalev: The Estonian Government Should Resign)*, "RIA Novosti", 7 June 2008 [http://www.ria.ru access: 20 February 2018].

40 *Annual Review 2007*, Estonian Internal Security Service: Tallinn 2008, p. 13.

41 *Annual Review 2007*, Estonian Internal Security Service: Tallinn 2008, pp. 8, 13, 15.

42 *Conference of Russian Ambassadors and Permanent Representatives*, "Official Internet Resources of the President of Russia", 1 July 2014 [http://www.en.kremlin.ru access: 20 February 2018].

K. Pynnöniemi, A. Rácz, *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, Finnish Institute of International Affairs: Helsinki 2016, p. 94.

43 *О государственной политике Российской Федерации в отношении соотечественников за рубежом (On the Russian Federation's State Policy Toward Compatriots Living Abroad)*, "Официальный интернет-портал правовой информации" (Official Internet Portal for Legal Information), 10 July 2013 [http://www.pravo.gov.ru access: 20 February 2018].

44 K. Natoli, *Weaponizing Nationality: An Analysis of Russia's Passport Policy in Georgia*, "Boston University International Law Journal", Summer 2010, pp. 391-392.

45 M. van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism*, Rowman & Littlefield: Lanham - Maryland 2014, Chapter 13 (E-book).

46 R.D. Asmus, *A Little War that Shook the World: Georgia, Russia, and the Future of the West*, Palgrave Macmillan: Basingstoke 2010, pp. 105-107.

47 A.J. Selhorst, *Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine*, "Militaire Spectator", April 2016, pp. 155-156.

> ***Efforts in the electronic and information realms, including the use of social media, appear to have grown in salience as means for the FGRF to spread its alterations.***

This, combined with Tbilisi's diplomatic options going from bad to worse, convinced the Georgian government that they needed to pre-empt the FGRF's coming actions. Doing otherwise was perceived by the government as something that would end their ability to rule Georgia.[48] By initiating the armed conflict, the FGRF would claim that the Georgian government was the aggressor in the conflict.

The Russia's use of power pressure, distortion of the media coverage of events, and use of ethno-cultural arguments have largely, with some tweaks, continued throughout its conflict with Ukraine and the related influence operations. The largest differences, however, can be traced to how the FGRF attempted to, and with some success been able to, steer the narrative regarding its involvement in the conflict. Examples of this can be seen in how many foreign media outlets came to repeat, at least in part, the FGRF's and its proxies' description of the conflict's development, thereby casting doubt on what actually transpired and resulting in the promotion of the FGRF's interests.[49]

Efforts in the electronic and information realms, including the use of social media, appear to have grown in salience as means for the FGRF to spread its alterations. While the extent and effects of the FGRF's involvement in the United States presidential election is still under investigation, government intelligence agencies have determined that the FGRF did indeed attempt to steer the election via a mixed overt-covert influence campaign. These efforts appear to have included the support of the FGRF's preferred presidential candidate, the release of unlawfully acquired internal documents, and attempts to polarise the political climate by the online promotion of controversial or divisive organisations and topics.[50] Similar trends can be seen in other countries as well. Examples include attempts to infiltrate foreign media outlets as well as the support of foreign parties and groups whose interests align with the FGRF's.[51]

Analysis and Recommendations

The nature of the FGRF's use of influence operations seems largely to be defined by their holistic, coordinated, and coercive use of soft power. The use of soft power

---

48 R.D. Asmus, *A Little War that Shook the World: Georgia, Russia, and the Future of the West*, Palgrave Macmillan: Basingstoke 2010, p. 50.

49 K. Pynnöniemi, A. Rácz, *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, Finnish Institute of International Affairs: Helsinki 2016, pp. 137, 171 196.

50 *Assessing Russian Activities and Intentions in Recent US Elections*, Office of the Director of National Intelligence: Washington - District of Columbia 2017, p. ii.

An Ex St. Petersburg 'Troll' Speaks out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency, "Meduza", 15 October 2017 [http://www.meduza.io access: 20 February 2018].

V. Sauter, *Video and Transcript: Press Conference by Senators Richard Burr and Mark Warner of SSCI on the Russia Probe*, "Lawfare", 4 October 2017 [http://www.lawfareblog.com access: 20 February 2018].

51 A. Polyakova, M. Laruelle, S. Meister, N. Barnett, *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom*, The Atlantic Council: Washington - District of Columbia 2016, pp. 3-4.

S. Meister, J. Puglierin, *Perception and Exploitation: Russia's Non-Military Influence in Europe*, "German Council on Foreign Relations", October 2015, p. 5.

Annual Report of the Security Information Service for 2015, Security Information Service: Prague 2016, p. 9.

resources is then, when necessary, complemented by capabilities that traditionally fall outside of the concept of soft power. These include the threat of the use of armed force in order to put power pressure on the TA and its dependencies. Direct use of force is discouraged in the Russian military thought in favour of information and psychological warfare.

The Russian influence operations are conducted both before and during a conflict as well as in times of peace. Their focus often seems to be on the exploiting of divisions in foreign states, the promotion of groups and parties whose policies align with the FGRF's, and the steering of the narrative towards what is deemed beneficial to the FGRF's interests. Prominent means to achieve these goals include traditional media outlets controlled by the FGRF as well as ones over which the FGRF can gain influence. The use of social media has, in turn, come to gain prominence.

Due to the FGRF's influence operations' holistic nature, any response to them needs to be equally comprehensive. As the operations act on multiple target audiences, both primary and lesser ones, any actor must prepare all of its dependencies for the possibility of them being targets of influence operations. This is necessary in order to increase the actor's general ability to detect the operations and also in order to increase the actor's ability to resist to them.

By promoting healthy scepticism and a code of good conduct amongst citizens, private corporations, and government agencies, an actor can achieve much of this. Such a conduct should include transparent and responsive delivery of information – in particular concerning sourcing. This is in order to combat the spread of inaccuracies, uncertainty, as well as foster trust between parties. This promotion of awareness, good conduct, and scepticism should come natural and occur at all levels. Examples for implementing such solutions include adding them to school curriculums and training new employees especially in targeted fields.

Special attention should be placed on the creation of trust and cooperation among the media outlets, the government, and government institutions. The reasoning for this is threefold: these outlets can aid in the detection of falsehoods and correct them, they constitute a large part of the information environment and act as some of its more prominent communication channels, and they are some of the most interesting targets for an IA. If one can foster trust and cooperation, approaching outlets in cases where they may have been compromised should be made easier. A healthy relationship can also increase a government's ability to penetrate influence operations that limit the information environment or saturate it.

As a part of the private-public cooperation effort and promotion of good conduct, governments could encourage the use and creation of fact-checking organisations and special fact-checking editors or ombudsmen. Such fact-checking organisations may in part be run, or supported, by the government, as governments already possess much of the needed infrastructure to provide such organisations with relevant information through their agencies.

Governments should furthermore strive to lessen the divisions and grievances that exist within the state. This is not only good policy, but given the FGRF's history of exploiting their existence, efforts to reduce these divisions and grievances should be made a priority. In cases where groups already have been compromised, as was seen in the case of Estonia where groups had entirely different information environments, governments need to go even further in their integration efforts. This can include the creation of media outlets

tailored specifically to the compromised group, working directly with civil society, and working directly with prominent groups in these communities.

Most governments already have the infrastructure that monitors and analyses developments in various information environments and their respective channels. However, few possess the infrastructure and command structures needed for coordinating and reviewing the above mentioned endeavours. Most of them more or less need to be decentralised. This is because centralised organisations tend to have a hard time to fully grasp the problems of the periphery. But, if all of these efforts were decentralised, the risk would increase for wasting resources as the same issue might be addressed multiple times. Centralised institutions for coordinating and reviewing counter influence efforts, as well as creating new ways to address developments in the field, should therefore be preferred and encouraged. Additionally, such organisations offer the ability to collect information and spread it quickly to relevant parties. However, in doing so, one should take a number of precautions so that one does not grant an audience to what otherwise would see little to no penetration.

Tony Jensen, *currently unaffiliated, is a former student at Gothenburg University and the Swedish Defence University. He has participated in a number of international conferences on international relations and security policy. His specialisation is the use of deception and influence operations as a means to further an actor's interests. The main focus of his research has been Russian activities in its near abroad.*
