Russian Interference in Foreign Elections: Threats and Countermeasures

Davit Kutidze[1]

In the modern world, concomitant with the rapid expansion of the speed and reach of news dissemination, information operations have become integral to warfare. Hostile nations often utilize information to influence the mindsets of people and thereby interfere in the affairs of other countries. Elections are one of the primary targets of malign influence because they provide fertile ground for manipulating public opinion. This challenge became particularly evident for Western society during the 2016 US Presidential Elections, when coordinated Russian interference was identified.[2] While the Russian Federation is not the sole malign actor employing such activities to discredit undesirable subjects and, in general, undermine the concept of elections and weaken democratic institutions, scholars believe that Russia has institutionalized such methods at a high level.[3]

It's challenging to determine whether and to what extent the Russian Federation might intervene in Georgia's 2024 parliamentary elections. However, given the continuous spread of Kremlin propaganda in Georgia, aimed at negatively influencing[4] the aspirations of the vast majority of Georgian nationals to join Euro-Atlantic structures, the threat of interference naturally persists. Just a few days ago, US Secretary of State Antony Blinken also highlighted this threat within a global context, which includes concerns about Georgia, and identified attempts by Russia and China to promote disinformation as a primary challenge. As stated by Secretary Blinken, "Nearly half the people of the world are going to be going to the polls this year – this is an extraordinary election year in country after country – but citizens and candidates will face a flood of falsehoods that suffocate serious civic debate".[5]

Given the aforementioned circumstances, it is paramount to learn from past experiences and analyze Russian malign influence over the electoral processes in different countries to better inform

[1] Research Institute Gnomon Wise, University of Georgia, e-mail: d.kutidze@ug.edu.ge
[2] Mueller, R. S. (Special Counsel). (2019). Report on The Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice. Accessible at: https://bit.ly/3ItHonm
[3] Marek N. et al. (2020). From Consensus to Conflict Understanding Foreign Measures Targeting U.S. Elections. RAND Corporation. Accessible at: https://www.rand.org/pubs/research_reports/RRA704-1.html
[4] Government of Georgia (2021) Ordinance №482 – On approval of Georgia's National Cybersecurity Strategy and its action plan. Accessible at: https://matsne.gov.ge/ka/document/view/5263611?publication=0
[5] Antony Blinken – "2024 is a special election year in many countries across the world. Democracies should to more to fight disinformation. 1tv.ge. Accessible at: https://bit.ly/3Pyka3R

Georgian citizens about this challenge. Additionally, it is crucial to highlight the countermeasures that more experienced and stronger countries than Georgia have employed to safeguard their elections from Russia's information warfare.

As previously mentioned, discussions about Russia's malign influence have intensified since the 2016 US presidential elections. The special counsel investigation launched later confirmed that the Russian government interfered massively and systematically in the 2016 US presidential elections. Evidence of meddling operations began to emerge in mid-2016, with hacking attacks and the networks behind those attacks being identified. The report of the special counsel says: Russia interfered in the 2016 presidential election principally through two operations. First, a Russian entity carried out a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton. Second, a Russian intelligence service conducted computer-intrusion operations against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents".[6]

The special counsel's report mentions the organization founded by the Russian oligarch Yevgeniy Prigozhin—the Internet Research Agency (IRA)—which exploited social media profiles and interest groups to sow discord within the US political system. This campaign, to a certain extent, was a continuation of a general program developed in 2014-2015 with the purpose of damaging the US electoral process. It is clear from the report that one of the major aims of the operation was to polarize society to the maximum possible extent. In addition, to gain access to a wider audience, according to Facebook's data, the IRA purchased over 3,500 ads and paid nearly USD 100,000 for them. Furthermore, there were coordinated campaigns on Twitter as well to manipulate public opinion.

Scholars analyze Russia's election interference through theoretical lenses to understand its main features. According to Posard et al. (2020), modern Russia employs theoretical grounds and approaches that were tested as early as the Soviet era, particularly reflexive control theory. Unlike game theory, reflexive control theory does not argue that individuals act rationally; it claims that with relevant efforts from outside, it is possible to change their views. Additionally, this gives rise to a paradigm where people are either together or against each other, and they are either passive or act aggressively. Scholars believe that in the modern era, this approach can be used in two ways: 1. Information efforts are aimed at altering people's perceptions and do not change a group's fundamental structure. For instance, reflexive control

[6] Mueller, R. S. (Special Counsel). (2019). Report on The Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice. Via link: https:/bit.ly/3ItHonm

does not seek to convince people in political party A that they are in conflict with people from political party B; it assumes that the conflict already exists. Its aim is to increase the degree of this confrontation; 2. The second feature of reflexive control theory is to spark responses among the targets. It views the world as a dichotomy between conflict and cooperation. Successful information attempts sow deep divisions between groups of people and generate perceptions of "us" and "them," which in turn spark strong reactions among individuals. The eventual aim is to reduce the probability of groups of people finding common ground to address important societal matters.[7]

Based on abovementioned theoretical approach, Posard et al. (2020) underline the four main objectives for Russia's meddling in the US presidential elections: 1. Polarize and disrupt societal cohesion by exacerbating important and divisive issues, such as race, social class, and gender. 2. Undermine public confidence in democratic institutions and processes. 3. Spread confusion, generate exhaustion, and create apathy. 4. Gain strategic influence over U.S. political decision-making and public opinion.[8]

Aaltola's (2017) work also identifies five main steps of malign information interference of the foreign countries. Drawing on experience of different western countries, the author concludes that abovementioned five features have more or less universal application. These features are as follows: 1. using disinformation to amplify suspicions and divisions, undermine trust in democratic institutions; 2. stealing sensitive and leakable data (for instance, by hacking attacks against websites and email addresses), ultimately aiming to disrupt election processes; 3. leaking the stolen data via supposed 'hacktivists'; 4. whitewashing the leaked data through the professional media, that is, pushing these issues into media spotlight (such type of information naturally attracts media attention); 5. secret colluding in order to synchronize election efforts when a specific candidate, party or other groups create background and covert links with a foreign state to change the election dynamic.[9]

It is noteworthy that the Russian Federation's attempts to use the aforementioned manipulative methods for interference in the elections of foreign countries are well-known to the leading European states. Brattberg and Maurer (2018) studied cases in five European countries—Netherlands, France, UK, Germany, and Sweden (based on examples of elections held in these countries in 2017-2018)—where

[7] Posard, Marek N., Marta Kepe, Hilary Reininger, James V. Marrone, Todd C. Helmus, and Jordan R. Reimer. (2020). From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections. RAND Corporation. Via link: https://www.rand.org/pubs/research_reports/RRA704-1.html

[8] Ibid. Accessible at: https://www.rand.org/pubs/research_reports/RRA704-1.html

[9] Aaltola, M. (2017). Democracy's Eleventh Hour – Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling. The Finnish Institute of International Affairs. Briefing Paper 226. Via link: https://storage.googleapis.com/upi-live/2017/11/bp226_democracys_eleventh_hour.pdf

Russia's malign information interferences were also identified. The strategic objectives remained unchanged here as well and mirrored the basic features of the abovementioned reflexive control approach: 1. Influencing voter preferences in favor of a specific candidate or party. 2. Undermining trust in democratic institutions and electoral processes in societies, delegitimizing elections, and causing apathy among the people.[10]

The accumulated experience regarding malign Russian information influence, its methods of implementation, and objectives has enabled scholars and policymakers to formulate relevant countermeasures. Naturally, these countermeasures are not identical, given the specific contexts of different countries. However, since Russia's information interference in foreign countries' elections often bears a similar trademark, the responses tend to be more or less alike. Therefore, it is important to study this experience.

The 2017 French presidential elections are considered a successful example of countering Russian information warfare. Vilmer and Conley (2018)[11] offer insights from this experience along with respective recommendations. Firstly, the authors underline that France was keenly aware of the mistakes made in the US in 2016 and, through strong coordination among administrative bodies (such as the National Commission for the Control of the Electoral Campaign, National Cybersecurity Agency, etc.), succeeded in maintaining public trust in electoral processes. Proactively informing the public about disinformation and the risks of cyber-attacks also played a crucial role in this process. Additionally, from the outset of the election campaign, the government demonstrated clear readiness to combat malign information interference. A 2,600-strong group of "cyber-warriors" was established within the Ministry of Defense. Furthermore, the French government, through public and private communication channels, warned the Russian side that attempts to meddle in the elections would be met with a strong response. As part of countering disinformation, the French government increased pressure on social media platforms at the communication level to take more robust measures to identify and neutralize false accounts. Transparency and timely reaction against cyber-attacks were crucial aspects – all such attempts identified by relevant agencies were made available to the public.

[10] Brattberg, E. and Maurer, T. (2018). Five European Experiences with Russian Election Interference. *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace. pp. 5-28. *JSTOR*, http://www.jstor.org/stable/resrep21009.6

[11] Jean-Baptiste Jeangène Vilmer and Heather A. Conley. (2018). Successfully Countering Russian Electoral Interference. Center for Strategic & International Studies (CSIS). Via link: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Given France's 2017 election experience, another intriguing aspect is that Emmanuel Macron's campaign team, anticipating hacking attacks, deliberately falsified its own electronic correspondence and documents, often making their content appear absurd. By deploying this so-called false flag, they aimed to inundate hackers' working field with false information, causing confusion and slowing down their efforts.[12]

Brattberg and Maurer (2018) offer some key recommendations in their study to safeguard democratic electoral process from Russia's malign influence.[13] The authors particularly emphasize the importance of transforming the electoral system into critical government infrastructure and strengthening all institutions connected to the process. Additionally, they believe it is necessary for the government to regularly investigate flaws in the system and spare no efforts to address them. The scholars pay particular attention to transparent communication with the public, including issuing public statements regarding specific threats and raising voters' awareness. Within this context, they emphasize the need for cooperation with both traditional and social media, as well as with fact-checking organizations. Brattberg and Maurer (2018) also highlight various legislative regulations that need to be adopted to safeguard elections, though they note that it is essential for all parties subject to these laws to be involved in drafting such regulations. The last recommendation concerns international cooperation, and the authors identify the following organizations as driving forces behind such collaboration.

***

Review of investigation reports and academic literature reveals that the Russian Federation has meddled in the elections of numerous democratic countries multiple times. The main objectives of Russian meddling are as follows: 1. Influencing voter preferences in favor of a specific candidate or country, which is mostly implemented by discrediting undesirable subjects and conducting extremely negative campaigns against them; 2. Undermining trust in democratic institutions and the electoral process in societies, delegitimizing elections, and fostering apathy among the people. The latter serves as a certain insurance for the first objective because if the Kremlin fails to help a preferred candidate win the elections, it at least damages a target country's democratic environment—shrinking the space for

[12] Ibid. Accessible at: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

[13] Brattberg, E. and Maurer, T. (2018). Five European Experiences with Russian Election Interference. *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace. pp. 5-28. *JSTOR*, http://www.jstor.org/stable/resrep21009.6

constructive debates, fueling polarization, sowing fear and confusion, and causing instability in this manner.

There are active debates within political and academic circles about countermeasures to safeguard democratic elections from Kremlin's malign information interference. Given the experience in this regard, it is important first that the government recognizes the risks while relevant institutions or society are mobilized. Additionally, scholars believe that it is necessary to transform the electoral system into critical government infrastructure. Furthermore, the government should regularly investigate flaws and ensure their eradication. The scholars pay particular attention to transparent communication with the public, including issuing public statements regarding specific attacks and raising general awareness among voters. Strong cooperation with traditional and social media, as well as with fact-checking organizations, is emphasized within this context.