RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

MILITARY CYBER OPERATIONS AS A RUSSIAN WEAPON TO CHANGE THE POLITICAL AGENDA IN EUROPEAN COUNTRIES

MAMUKA KIRKITADZE

149

EXPERT OPINION

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

MAMUKA KIRKITADZE

MILITARY CYBER OPERATIONS AS A RUSSIAN WEAPON TO CHANGE THE POLITICAL AGENDA IN EUROPEAN COUNTRIES

149

2020

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN 978-9941-8-2772-3

Introduction

In recent years, cyber operations have become an effective means of achieving political, economic and military goals for Russia. It is a weapon used by Putin's regime to suppress opposition leaders within the country and influence foreign states in the international arena.

Cyber-attacks and espionage are seen in Moscow as components of war. This was clearly reflected in a 2013 report by the Chief of General Staff, Valery Gerasimov,[1] in which he spoke about the importance of non-military, hybrid methods for achieving political and strategic goals.

It can be said that cyber espionage is not a new discipline for Russia. During the Soviet era, the USSR State Security Committee (Комите́т госуда́рственной безопа́сности СССР), known as the KGB, actively used high-tech equipment, in intelligence operations against the West. After the collapse of the Soviet Union, the KGB's signals intelligence (SIGINT) functions were distributed to various Russian intelligence services and adapted to modern information technologies.

Currently, one can see a lot of cyber units that serve different purposes in the Kremlin's intelligence services. Particularly active in this regard is the main division of the General Staff of the Armed Forces (Гла́вное управле́ние Генера́льного шта́ба Вооружённых Сил Росси́йской Федера́ции), the GRU, which is responsible for the military intelligence and operation of the military special forces. The main purpose of the division is to provide military intelligence to senior Russian government officials; in particular, the Minister of Defense and the Chief of General Staff as well as to ensure Russia's military, economic and technological security. The GRU also carries out covert espionage, intelligence and sabotage operations using kinetic and digital means. The hacker groups Sofacy/Fancy Bear[2] and Sandworm,[3] operating under its umbrella, have repeatedly been criticized by the international community.

The following incidents allow us to analyze how Russia uses the hacker groups affiliated with the GRU intelligence service to promote its desired policies in European countries.

Czech Republic

Diplomatic relations between the Czech Republic and Russia have been at a low point multiple times; however, the atmosphere between the two countries has significantly deteriorated in recent years.

In 2020, the square in front of the Russian embassy in Prague was renamed after the murdered Russian opposition leader, Boris Nemtsov. An alley named after another Kremlin critic, Russian journalist Anna Politkovskaya, was opened near the embassy.

The "provocative actions" in the capital of the Czech Republic have provoked the Kremlin's outrage but Moscow's dissatisfaction was truly triggered by the dismantling of a monument of the Soviet military marshal, Ivan Konev. This has raised tensions between the two countries to the highest point since the end of the Cold War. An unsuccessful attempt by the Russian Defense Minister, Sergei Shoigu, to return the statue of the Soviet marshal to the homeland was followed by retaliatory actions from the Kremlin.

A large-scale cyber-attack was carried out against Czech hospitals and the airport a few days after the monument was dismantled. According to the Slovak Internet Security Company (ESET),[4] a Russian trail was found behind the attack.

It is noteworthy that similar types of cyber-attacks have occurred numerous times in the past. According to a 2017 report by the Czech Security Information Service (BIS), two Kremlin-linked cyber espionage groups, Turla and APT28, ran a cyber-espionage operation on the websites of the Ministry of Foreign Affairs and Ministry of Defense as well as the Czech Army in 2016-2017.5

Cyber aggression in the Czech Republic invokes a kind of déjà vu. Precisely, the dismantling of a Soviet monument in Estonia was followed by a large-scale, coordinated cyber-attack campaign by Russia in 2007. It lasted for three weeks and caused serious economic damage to the country.

For Moscow, the Soviet Union and every little detail connected to it are associated with historical greatness and so it is not surprising that it responds to the "insult" of "symbols of military glory" with retaliatory, punitive actions.

Montenegro

Russia began to actively interfere in Montenegro's internal affairs after the country expressed its readiness to join the North Atlantic Alliance.[6] For the Kremlin, Podgorica has always been an area of interest while for NATO the incorporation of Montenegro into its ranks can be understood as a strategic move. Clearly, a country with an army of just 2,000 men[7] militarily

has a minimal benefit to NATO although strategically, the admission of this small Balkan country into the North Atlantic Alliance gives full control over the Adriatic Sea. This is even more relevant when the rest of the Adriatic countries - Albania, Croatia and Italy - are already members of NATO.

For the Kremlin, the operations orchestrated by the GRU played a crucial role in bringing a pro-Russian government to power in Montenegro and altering the country's North Atlantic path.

Three days before parliamentary elections, GRU operators launched low-tech but effective cyber-attacks on Montenegro's media outlets, major telecoms, election NGOs and government websites. It served to disrupt the election and divert the country from the path toward the North Atlantic Alliance.[8]

In addition to manipulating Montenegro's political and social environment through cyber means, the Kremlin also sought to discredit the elections and win over the opposition, political groups and clerics through financial means.[9] The case also involved GRU operators who allegedly planned to attack the parliament, assassinate the prime minister and stage civil unrest but Montenegrin law enforcement officers were able to arrest them promptly.[10] A Montenegrin court sentenced up to 20 people to prison for a coup d'état in 2019, including two Russian citizens - Eduard Shishmakov and Vladimir Popov - who were sentenced to 15 years in prison in absentia. The investigation established that Shishmakov and Popov were GRU intelligence officers who, after a failed coup, left Montenegro with the help of Serbian officials.[11]

Denmark

If we look at the risk assessment reports of the Danish Defense Intelligence Service (DDIS) for the last ten years, we will see that among the threats to Copenhagen emanating from Russia, cyber-attacks and intelligence operations are one of the leading ones that can have a serious impact on the country's national security. Denmark, as one of the founding members of the North Atlantic Alliance, has always been an area of interest for Russia.

The radar of the Kremlin intelligence service actively started to track Copenhagen in 2014 when Denmark expressed readiness to join NATO's missile defense system.[12] Unsurprisingly, this decision angered Russia.

Mikhail Vanin, Russia's ambassador at the time and resorting to the usual tactic from the playbook - threat - tried to force the Danes to reconsider their decision. He noted that if Copenhagen were to join NATO's missile defense system, Danish ships stationed in the Baltic Sea would become targets for Russian nuclear missiles.[13]

Despite the Russian threat, Denmark became part of the NATO missile defense architecture; however, a few weeks after the threat, the Kremlin tried to exert influence through cyber channels. For two years, the GRU intelligence cyber unit, the APT28, illegally accessed the e-mail addresses of the staff of the Danish Foreign and Defense Ministry with the aim of acquiring documents related to the North Atlantic Alliance as well as blackmailing and recruiting ministry staff.[14]

Poland

The discussion about the expansion of NATO bases in Poland became a sufficient reason for the GRU to begin the illegal monitoring of the Polish government and defense sector in the summer of 2014.

In a decision made at the NATO Wales Summit, the number of NATO Response Force (NRF) units has been increased in Poland to contain aggression from Russia. The summit also set up the Very High Readiness Joint Task Force which can mobilize and deploy in a conventional war within days from making the appropriate decision.[15] In response, hackers affiliated with the Russian intelligence service illegally penetrated up to ten Polish government websites in order to gain information.

In doing so, Russia's main goal was to monitor and assess threats emanating from the NATO troops stationed in Eastern Europe. This was largely carried out with the involvement of cyber operations.[16]

The Kremlin's reaction was similar when Poland declared readiness to station an American base in the country with an increased contingent in order to curb Russian aggression.[17] In response to a sudden announcement by official Warsaw, Russian intelligence services illegally accessed networks and infected Polish government websites with malware, including the websites of the Ministry of Foreign Affairs and Finance. Moreover, according to the Polish security services, hackers affiliated with the Kremlin illegally penetrated the website of the Polish Elite Military Academy and posted a letter with discriminations against the USA.[18] The fake letter was actively

covered by the Russian state news media. This malicious campaign was aimed at straining relations between Europe's main strategic partners, the United States and Poland.

Ukraine

As in the case of other post-Soviet countries, Russia has always considered Ukraine as its sphere of influence and is actively trying to influence the country's domestic and foreign policy to date.

The protests in Ukraine, which began in 2014, ended with the ouster of a pro-Kremlin president, Viktor Yanukovych, and the scheduling of an early presidential election. This was a clear defeat for Russia.

While the fate of the "Revolution of Dignity" was still being decided at the Maidan, a part of Ukraine - the Crimean Peninsula - faced the threat of military aggression. The 35,000 member Russian army which, among others, included units of the elite special forces of the GRU intelligence service stormed the Crimean regional parliament within a few days and raised the Russian flag over the building. The military occupation of the Ukrainian peninsula ended with an illegitimate referendum on March 16 and the declaration of Crimea as Russian territory.

The epilogue of the annexation of Crimea by the Kremlin was a cyber-attack perpetrated against the elections of May 25. Four days before the vote, a hacker group affiliated with the GRU (CyberBerkut) attacked the infrastructure of Ukraine's electoral system and began deleting crucial files.[19] The election administration was able to repair the damage in time before the start of the voting procedure. On election day, however, the cyber divisions of the intelligence services still managed to gain unauthorized access to the election website.[20] Citizens entering the site saw a picture of ultra-right candidate, Dimitri Yarosh, reporting he had won the presidential election. The Russian state media used this fact and actively began to provide false information to the public.

Although the 2014 incident failed to affect the outcome of the election, Russia had at least partially achieved its goal. According to the Ambassador of the NATO Cyber Center, Kenneth Geers, the purpose of the operations carried out by the Kremlin was to disrupt and discredit the election process.[21]

The annexation of Crimea by Russia and the attempts to influence elections through the information attacks turned out to be just the beginning for Ukraine. The Kremlin has actively started using Ukraine as a cyber-laboratory and has managed to successfully undermine Kyiv's critical infrastructure several times.[22]

The use of the post-Soviet countries as guinea pigs is not new for the Kremlin. The sense of impunity allows Russia to actively test both kinetic and new cyber capabilities on neighboring countries which, in the long run, is aimed at discrediting the West.

Georgia

The United States House of Representatives approved a bipartisan act in support of Georgia on October 22, 2019 which aims to support the country's independence, sovereignty and territorial integrity.[23] The Georgia Support Act obliges the US president to impose sanctions on anyone involved in the human rights abuse and attempts on the life of Georgian citizens in the Russian-occupied Abkhazia and the Tskhinvali region. The document also includes assistance to Georgia in the field of cyber security.[24]

Six days after the adoption of the Support Act on October 28, 2019, a large-scale cyber-attack was carried out in Georgia targeting the websites, servers and other operational systems of the Presidential Administration, the judiciary, various municipal councils and non-governmental and media organizations. Several TV stations stopped broadcasting as a result of the cyber-attack.[25]

A joint investigation with the help of international partners has revealed that the elite cyber group of the General Staff of the Armed Forces of the Russian Federation, Sandworm, was behind the cyber-attack. This group is the author of a number of destructive cyber-operations.[26] The attack caused an unprecedented response from the international community.[27]

Almost a year after the October cyber aggression on September 1, 2020, a cyber-attack was carried out against the computer system of the Ministry of Health. According to the Ministry of Internal Affairs of Georgia,[28] the cyber-attack was aimed at illegally obtaining and using important information related to medical documentation and pandemic management stored in the databases of the ministry's central office and its structural units, including the Disease Control and Richard Lugar Public Health Research

Center. According to the Ministry of Internal Affairs, the special services of one foreign state was behind the cyber-attack.

It should be noted that since its very opening, the research center named after the US Senator, Richard Lugar, in Georgia became the subject of criticism and deliberate disinformation by the Kremlin. People close to Russian official circles still openly criticize the work of the laboratory, accusing the United States and Georgia of sometimes making biological weapons and at other times spreading dangerous viruses. The September cyber-attack "strangely" coincided with a comment by Duma MP, Yuri Shvitkin, on the poisoning of the Russian opposition leader, Alexei Navalny. According to the MP, Russia supposedly does not produce the nerve agent of the Novichok group and poisonous substances of a similar group are created in America and Georgia; in particular, in the Lugar laboratory.[29]

Documents up to 14GB in size illegally obtained as a result of the cyber-attack were posted on a foreign website and are still available to Internet users. According to the Ministry of Internal Affairs, along with the aforementioned files, falsified documents were also uploaded; these documents were intentionally fabricated.

It is noteworthy that the author of the posted, illegally obtained materials bears distinctive national signs and symbols. In particular, the user has the flag of the National Awakening Movement of South Azerbaijan (SANAM) operating in Baku as a profile picture and with the chosen name - Bakililar (from Baku) - emphasizing origin. Such an action might be a part of a so-called false flag operation which is often used to cover tracks and redirect attention. One also cannot rule out the possibility that such actions on the part of a state which is hostile to Georgia aim at straining relations with one of our strategic partner countries in the region - Azerbaijan.

Based on the facts, we can assume that the September cyber-attack was carried out by elite cyber groups linked to the Russian special services and aimed at reinforcing the Kremlin-invented Lugar myth, intimidating, confusing and sowing distrust in the public.

The two large-scale cyber-attacks on Georgia in a short period of time may as well have been caused by other factors.

What did Russia Try to Achieve?

The destructive cyber-attacks, orchestrated by the northern neighbor, were aimed at violating Georgia's national security as well as sowing discontent in society by impeding the functioning of various governmental and non-governmental organizations and, most importantly, testing the ground before the elections.

Interference and influence in the domestic policies of other countries has become a commonplace for the Kremlin in recent years. The Kremlin has already been incriminated in interfering in the elections of several countries, including Britain,[30] France,[31] Germany,[32] the Netherlands,[33] Austria,[34] Belarus,[35] Bulgaria,[36] Norway[37] and the United States.[38]

According to a member of European Parliament, Viola von Cramon, it would be a miracle if Russia does not try to interfere in the October elections as this is its usual behavior.[39] The newly appointed US Ambassador to Georgia, Kelly Degnan, also made a number of comments on Georgia's upcoming elections noting that Russia will probably try to interfere in the Georgian elections.[40] The fact that Georgia is moving towards a proportional electoral system increases the likelihood of Russian interference in the elections.

The 2020 report of the Estonian Intelligence Service also touched upon the Georgian elections. It states that the US presidential and Georgian parliamentary elections will become the subject of Russia's interest. According to the report, it is important for official Moscow to get the desired result in the elections and in doing so it will try to support a candidate who radically opposes Western politics.[41]

What Should We Expect in October?

The Kremlin will probably try its best to influence the elections in October through various channels. This could be cyber aggression on the website of the Central Election Commission of Georgia or the previously and already

well employed method of creating an informational vacuum in society by interfering with the broadcasting of media channels or the support of candidates loyal to the Kremlin with propaganda methods through social media.

One should highly anticipate more activity from the Kremlin-run Internet Research Agency (Агентство интернет-исследований), the same Russian troll factory in Georgian Internet space. Its main purpose is to spread false information adapted to the Kremlin's narrative on social networks. The individuals affiliated with this organization are attacking politicians, parties and civil society representatives they deem as unacceptable. They are able to sway public opinion through social networks and covertly or explicitly spread messages which are favorable for the Kremlin throughout society.

In parallel with the increased pre-election cyber activities, the incidents of the abduction of Georgian citizens from the occupation line and illegal borderization are also expected to increase. In addition, one should anticipate intensified military exercises of the Russian army on the territory of the occupied Abkhazia and Samachablo which the Kremlin uses to try to inflame a sense of fear and insecurity among the Georgian population.

It is also noteworthy that in parallel with the Georgian parliamentary elections, our main strategic partner, the United States, will try to elect a new president. Clearly, America will concentrate more on its internal affairs and the attention of our European partners will also be more focused on the Trump-Biden duel rather than on Georgia. Given this fact, Russia will certainly have a sense of impunity and try to harm Georgia as much as possible through subversive digital aggression or other means. It will try to divide society by harmful actions and regain exclusive control over our country's domestic and foreign policy.

Conclusion

After the end of the Cold War and the collapse of the Soviet Union, the Kremlin, largely through the involvement of intelligence services, has been actively seeking to regain a leading position in the international arena. Today, the Russian Federation is one of those few countries that have successfully integrated cyber elements into the military component. A clear example of this is the formation of elite cyber divisions within the intelligence services which play an important role in shaping Russia's foreign and domestic policy.

Regardless of geopolitical standing or status, Russia is actively campaigning to discredit undesirable countries or individuals with the help of intelligence operations. The fact is that for the Kremlin, most post-Soviet countries are a kind of testing ground where successful trials of both military and information-propaganda tactics are conducted. This, in the long run, is aimed at demolishing Western democratic order.

Given the current situation, it is essential for the Georgian government to adequately assess the threats posed by Russia and cooperate closely with strategic partners. It is also necessary to make the most out of every opportunity in order to mitigate the threat to the democratic development of our country and membership of Euro-Atlantic structures. These are the only correct alternatives for building a democratic and secure country.

References

1. Герасимов Валерий, Ценность науки в предвидении, February 26, 2013. Еженедельник ВПК. www.vpk-news.ru/articles/14632
2. CrowdStrike, February 12, 2019. Who is FANCY BEAR (APT 28)? www.crowdstrike.com/blog/who-is-fancy-bear
3. *Vanity Fair*, October 29, 2019. INSIDE THE DISCOVERY OF SANDWORM, THE WORLD'S MOST DANGEROUS HACKERS. www.vanityfair.com/news/2019/10/the-discovery-of-sandworm-the-worlds-most-dangerous-hackers
4. "Russian Hackers May be Behind Cyber Attacks on Czech Hospitals, says ESET," April 22, 2020. https://news.expats.cz/weekly-czech-news/russian-hackers-may-be-behind-cyber-attacks-on-czech-hospitals-says-eset/
5. ZDNet, "Czech Republic Blames Russia for Multiple Government Network Hacks," December 3, 2018. www.zdnet.com/article/czech-republic-blames-russia-for-multiple-government-network-hacks/
6. European Western Balkans, December 28, 2016. "Path to NATO: The Case of Montenegro." https://europeanwesternbalkans.com/2016/12/28/path-to-nato-the-case-of-montenegro
7. The GlobalFirepower. "Montenegro Military Strength 2020." www.globalfirepower.com/country-military-strength-detail.asp?country_id=montenegro
8. Georgi Gotev, *Euractiv*, October 17, 2016. "Montenegro Hit by Cyber-attacks on Election Day." www.euractiv.com/section/global-europe/news/montenegro-hit-by-cyber-attacks-on-election-day/
9. Heather A. Conly, May 14, 2019. "Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics." Center for Strategic and International Studies. www.csis.org/analysis/russian-malign-influence-montenegro
10. Andrew E. Kramer and Joseph Orovic, May 9, 2019. "Two Suspected Russian Agents Among 14 Convicted in Montenegro Coup Plot." *New York Times*. www.nytimes.com/2019/05/09/world/europe/montenegro-coup-plot-gru.html
11. AP News, May 9, 2019, "2 Russian Spies Sentenced in Montenegro in Coup Attempt." https://apnews.com/9782460f2ca943cca88b628405033c2c
12. *The Local*, August 22, 2014, "Denmark Will Join Nato's Missile Defense System." www.thelocal.dk/20140822/denmark-will-join-natos-missile-defense-system
13. Teis Jense, March 22, 2015, "Russia Threatens to Aim Nuclear Missiles at Denmark Ships if It Joins NATO Shield." www.reuters.com/article/us-denmark-russia/russia-threatens-to-aim-nuclear-missiles-at-denmark-ships-if-it-joins-nato-shield-idUSKBN0MI0ML20150322
14. Neil MacFarquhar, April 24, 2017. "Denmark Says 'Key Elements' of Russian Government Hacked Defense Ministry." www.nytimes.com/2017/04/24/world/europe/russia-denmark-hacking-cyberattack-defense-ministry.html

15. Government of Poland, Poland in NATO - More Than 20 Years. www.gov.pl/web/national-defence/poland-in-nato-20-years

16. A Trend Micro Research Paper, 2016, "Operation Pawn Storm Using Decoys to Evade Detection," www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

17. Harriet Alexander, 2018. "Poland Asks Donald Trump to Establish Permanent US Military Base to Counter Russian Aggression." www.telegraph.co.uk/news/2018/05/30/poland-asks-donald-trump-establish-permanent-us-military-base/

18. Sean Lyngaas, 2020, Cyberscoop, "Poland Implicates Russia in Cyberattack, Info Op Aimed at Undercutting U.S. Relations." www.cyberscoop.com/poland-cyberattack-russia-us-military/

19. Mark Clayton, 2014, "Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers." www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

20. Gabe Joselow, 2016, "Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past." www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246

21. *Ibid*.

22. Andy Greenberg, 2017, Wired, "How an Entire Nation Became Russia's Test Lab for Cyberwar." www.wired.com/story/russian-hackers-attack-ukraine/

23. U.S. Congress, 2020, H.R.598 - Georgia Support Act, www.congress.gov/bill/116th-congress/house-bill/598/text?q=%7B%22search%22%3A%5B%22H.R.598+Georgia+Support+act%22%5D%7D&r=1&s=2#HE7A4D682814743F9BFC51B27090FBBA2

24. *Ibid*.

25. BBC, 2019, "Georgia Hit by Massive Cyber-attack." www.bbc.com/news/technology-50207192

26. *Interpressnews*, 2020, "Foreign Ministry: On 28 October, a Large Scale Cyber-attack was Carried Out by Main Division of the General Staff of the Armed Forces of Russia." www.interpressnews.ge/en/article/105913-foreign-ministry-on-28-october-a-large-scale-cyber-attack-was-carried-out-by-main-division-of-the-general-staff-of-the-armed-forces-of-russia

27. *Civil.ge*, 2020, "At UN Security Council, Estonia, UK, U.S. Condemn Russian Cyberattack on Georgia." https://civil.ge/archives/341090

28. Ministry of Internal Affairs of Georgia, Statement of the Ministry Of Internal Affairs of Georgia, September 3, 2020. https://police.ge/en/saqartvelos-shinagan-saqmeta-saministros-gantskhadeba/13926

29. РИА Новости, Депутат напомнил о лабораториях по изготовлению «Новичка» в Грузии и США, October 2, 2020 https://ria.ru/20200902/novichok-1576642485.html

30. Kate Holton, Guy Faulconbridge, 2017, Reuters, "UK Investigates Brexit Campaign Funding amid Speculation of Russian Meddling." www.reuters.com/article/us-britain-eu-investigation/uk-investigates-brexit-campaign-funding-amid-speculation-of-russian-meddling-idUSKBN1D157I

31. Ken Gude, 2017, Center for American Progress, “Russia’s 5th Column,” www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-colum/

32. *Financial Times*, “Nationalist AfD Make Historic Breakthrough in German Elections.” www.ft.com/content/d18213e0-a105-11e7-b797-b61809486fe2

33. Andrew Higgins, 2017, *New York Times*, “Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote.” www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html?mcubz=1

34. *DW*, “‘Putin’s Friends’ in Austria’s Right-wing FPÖ Achieve Strong Election Result.” www.dw.com/en/putins-friends-in-austrias-right-wing-fp%C3%B6-achieve-strong-election-result/a-40960928

35. Andrei Makhovsky, 2020, *Reuters*, “Belarus Accuses Russia of Election Meddling, Seeks Talks with Putin.” www.reuters.com/article/us-belarus-election-meddling/belarus-accuses-russia-of-election-meddling-seeks-talks-with-putin-idUSKBN23W1J0

36. *RFE/RL*, 2016, “Bulgaria Faces Uncertainty After Election of Pro-Russia President.” www.rferl.org/a/bulgaria-president-radev-pro-russia/28114949.html

37. *NTB/The Local*, 2017, “Norway’s Labour Party was Hacked by Russia: Report.” www.thelocal.no/20170203/norways-labour-party-was-hacked-by-russia-report

38. Abigail Abrams, 2019, Time, “What We Know So Far About Russia’s 2016 Meddling.” https://time.com/5565991/russia-influence-2016-election/

39. *On.ge*, 2020, სასწაული იქნება, რუსეთმა ამ არჩევნებში ჩარევა რომ არ სცადოს, ეს მათი ჩვეულებრივი ქცევაა – ევროპარლამენტარი

40. *On.ge*, 2020 არ მაქვს კონკრეტული მტკიცებულებები, თუმცა რუსეთი ალბათ შეეცდება საქართველოს არჩევნებში ჩარევას – დეგნანი

41. International Security and Estonia 2020, www.valisluureamet.ee/pdf/raport-2020-en.pdf