RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

MAIN DIRECTIONS OF THE RUSSIAN INFORMATION WARFARE AND ITS RESULTS IN LIGHT OF THE 2018 GEORGIAN PRESIDENTIAL ELECTIONS

ANDRIA GOTSIRIDZE

115

EXPERT OPINION

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

EXPERT OPINION

ANDRIA GOTSIRIDZE

MAIN DIRECTIONS OF THE RUSSIAN INFORMATION WARFARE AND ITS RESULTS IN LIGHT OF THE 2018 GEORGIAN PRESIDENTIAL ELECTIONS

115

2019

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 978-9941-8-0961-3

Information warfare («Информационное противоборство»), the main outcome of which is the formation of a particular mentality and the manipulation of behaviours within its target audience, is one of Russia's tools for ensuring its domination in the world arena. This aspect of Russian strategy implies a fight against Western society and is based on Soviet tactics of psychological warfare. The result – "information dominance" («информационное превосходство») – implies control over information and the technical facilities for its dissemination, often leading to cyber-attacks in support of psychological operations. The goal of such cyber activity is to compromise networks subject to interest. Depending on the strategic or technical aim, information obtained this way may be used for intimidation, blackmail, discreditation or falsification. Often, in order to introduce the desired narrative or to create the relevant attitudes, informational content obtained through cyber-espionage is disseminated as if accidentally by mass media or social networks.

Disseminated content – a mixture of true and false information – targets confused and demoralized audiences for the purpose of influencing them, typically local citizens, various groups of residents of other countries and the political elite of Russia and other countries – this depending on the set aims of said dissemination.

Russia consistently aims to achieve an informational advantage, for which it technically processes information and controls its content. This is why the concept papers and doctrines of Russia do not contain the term "cyber-security", but rather "informational security". Russian websites, TV and radio programmes (like Russia Today and Sputnik News), bots, trolls, optimized search engines and others, represent an important instrument for the dissemination of propagandistic content and "information warfare". Buying over western journalists is also a common practice. In the opinion of a reputed American expert, "Distributed Denial of Services (DDoS) attacks, advanced (cyber) exploitation techniques and Russia Today television are all related tools of information warfare."[1].

In recent years, the main direction of the Russian informational warfare and its integral element – destructive cyber-operations – have been aimed at attacking state democratic institutions and systems and the discreditation of political figures and governance forms. For this purpose, a number of secret organizations have been established and false flag and other covert operations conducted. Kremlin-founded and financed or outsourced hacker organizations conduct extensive cyber-operations in full observance

of state interests – DDoS attacks, complex cyber-espionage acts and smear campaigns. Materials compromising political figures and institutions are often published "independently" (for instance, on WikiLeaks), which ensures the anonymity of the source.

In order to meddle with the elections of Western countries, and in cyber-operations used to obtain compromising materials, two hacker groups are associated with the operations of the Russian special services: APT 28 (Fancy Bear)[2] and APT 29 (Cosy Bear)[3]. In addition to well-known cyber-attacks, these are responsible for hacking the US Democratic National Committee server and the illegal acquisition of information thereof (the so-called DNC hack). The "DNC hack" is considered as interference in the US elections and served the purpose of weakening trust in the democratic institution and compromising a specific presidential candidate, all of which was sanctioned at the highest levels of the Russian government[4].

APT 28 is responsible for stealing information from the defence sector of European countries and for the cyber-intelligence campaigns of 2008-2014 against Georgian public structures and journalists. APT 29 is connected to the leakage of non-confidential information belonging to the US Department of State, White House, Pentagon and other public agencies. Both APT 29 and APT 28 are linked to the "DNC hack": according to existing data, APT 29 had access to the communication facilities of the Democratic Party, as well as its electronic communication and chats, for almost a year[5]. The tradition of disseminating ammunition on undesirable candidates or putting out damaging disinformation against them dates back to the Cold War. As to the use of cyber-operations for interference with elections, Russia created a precedent during the Ukraine conflict in 2014, conducting a massive attack on the election infrastructure of Ukraine.

An action plan exists which is aimed at the stimulation and manipulation of election processes in countries of interest. Long before elections, sensitive information is obtained from information systems by cyber-espionage or is collected from open sources in accordance with certain selected topics, and later used to discredit political figures or institutions. At the same time, trolls introduce false information via false profiles. In their blogs, they raise certain topics of the Russian narrative, disseminating false information which facilitates the formation of the desired public opinion. This process is facilitated by so-called "useful idiots" who provide voluminous comments on such posts.

In early 2010s, during "Arab Spring" Revolutions and Internet-organized anti-Putin protests against electoral fraud, Kremlin got the impression, that the Internet and social networks could be a direct threat to the Russian ruling elite's stability. Therefore, government control over the information space has become more stringent for the benefit of internal political stability. Following the election experience the Kremlin intensified use of trolls to influence domestic policy;

Recently, in order to remove anti-Russian information and narrative from Social Networks, troll technologies have been used at the international level in Ukraine, Georgia, Western Europe, and the USA.

In 2012, the hacktivist group "Anonymous" published evidence that professional trolls were being funded by the Russian government to discredit anti-Russian information, disseminate Kremlin messages online and form pro-Kremlin attitudes[6]. Specifically, the trolls were being paid to comment on anti-Russian articles, dislike videos against the regime, and manage false online profiles for the persecution of anti-Russian opinions in social media. Trolls often use multiple online platforms and blogs. However, the Russian trolling goal is to convince the audience of the "truth" of the Kremlin and to overload media with false content, creating doubt and fear of instability and prevent the use of a democratic internet space.

Attacks on the US and European Elections

In 2014, following the cyber-attack on the Ukrainian election systems, cyber-operations were used (with varying degrees of success) in the presidential elections in the US and France, and in the Bundestag elections of Germany. A US Intelligence Community-prepared analysis revealed the possibility of Russia applying the abovementioned technologies in the elections of the US partner countries in order to increase its global influence[7]. American experts had come to similar conclusions[8].

Based on that analysis, Russian interference in elections served the purpose of not only denigrating the candidates, but also discrediting democratic processes and the election institution in general. The image of the winning-candidate is created to look as if Russia supports him/her, and that prevents the community from uniting around the overall national goal; Russia, in its turn, benefits from this.

Head of the Federal Office for the Protection of the Constitution (the domestic security agency of Germany), Hans-Georg Maassen (2012-2018), went even further and questioned Russian support to any US presidential candidate or candidate in the 2016 Bundestag elections[9]. According to his agency's report, the main goal of the attacks was the long-term discreditation of democratic institutions and weakening of support to any state leader, which helps Russia in the implementation of its geo-political interests. The Open Report[10] of the abovementioned German agency focuses on the German elections and related threats coming from hacker groups affiliated with Russia. According to Maassen, in the German elections, Russia's disinformation campaign goals were not to support any specific party, but rather reduce faith in Germany's democratic institution and to minimize internal political support for the future Chancellor; just like in case with the US, this being beneficial for Russia's foreign policy[11].

During the German elections, just as in the US, compromising and other sensitive information had been stolen by hackers from cyber networks much earlier: in Germany, it happened in 2015 during cyber-attacks on the Bundestag networks, and in the US, from communication networks of the democratic party- almost one year before the elections.

The Georgia Case

If we take into consideration the level of Russia's interest in Georgia's internal politics, state and private sector network insecurity, and the capacity of Russia's destructive cyber-actors to penetrate such networks, then, naturally, the importance of the Russian narrative in the Georgian presidential elections, and Russian influence overall, should also be seriously considered. It is a well-known fact that Kremlin-related actors, including APT 28, had unauthorized access to both Georgian state and private communication networks. As a result, a large amount of sensitive information was for years leaked from Georgia and put into the hands of the Russian Special Services[12]. As to the Georgian elections, in addition to the existence of illegally obtained compromising materials about the candidates, statements from the supporting political forces on sensitive topics, which were available via open sources and social networks, made very good content for dissemination.

The Russian "information warfare" project achieved its goal in Georgia. Notwithstanding the final winner of the Georgian elections, such activities brought benefit to the Kremlin in several different directions, resulting in a clear number of threats to the Georgian state:

- By pedalling hidden or open connections with Russia and disseminating relevant content, both candidates were strongly discredited. According to the established image, an elected president in Georgia is perceived either as one governed by Russia or as one who can be easily manipulated by it. This leads to the loss of internal political support. To further strengthen such an image, Russian officials made public statements at the government level to this end. A president, on losing internal political support, will be deprived of the prevarication and power to run flexible policies in negotiations on the de-occupation of the country's occupied territories;
- The win of the candidate whose image is associated with the occupants and their support further deepens **antagonistic attitudes and facilitates the formation of a large group of protestors**. The 2018 campaign, run in such a way, led to the formation of an antagonistic opposition (40-50% of voters) towards the elected president (notwithstanding personal preferences). Considering these circumstances, the majority of attention during the presidency will not be paid to issues of state significance but rather to efforts spent to avoid confrontation;
- The perception, that a president and commander-in-chief is associated with Russia creates the feeling in society that the ruling circles in Georgia can be controlled by loyalty to the Kremlin forces; which, in turn, facilitates the dangerous process of the formation of pro-Russian elites;
- **The growth of loyalty to the Kremlin, as well as to the usurpation and discreditation of the national idea,** was promoted by mass actions of protest before the 2nd round of the Georgian elections, organized by clearly pro-Russian political forces under the aegis of the consolidation of the nation. It may well have been a signal of some sort for Russia on the preparedness of Georgian **pro-Russian political forces to participate in the governance of the country**. In addition, such actions deepened the perception that the candidates (and eventual elected president) were supported by pro-Russian political forces; and that **a niche of the national forces is occupied by pro-Russian persons**;

- The issue of initiating the 2008 war, as well as the so-called "bringing to justice" of Georgian military servants by the international court, was raised in a fully self-defeating context by the Georgian state. Later, international communication networks spread information on the topic of the tragedy of April 9th [13], insulting national feelings. Trolls and "useful idiots" responded to it with multiple comments, and the wave of dividing propaganda touched many reputed groups, including military servants, veterans, the Church, and others;
- The information space is yet again buzzing with topics regarding the "start of the war" and the EU court investigation into it, fascism and Nazi regimes, lustration, etc. The publication of these topics on the one hand facilitates the processes of social division and complicates the consolidation of issues of state significance; and, on the other hand, damages the international image of the country, ultimately proving **extremely negative from both a domestic and international point of view;**
- From 2012, the assessments of international observers and strategic partners for the first time began criticizing the Georgian election system and processes[14]; with negative comment released about the election campaigns, unequal distribution of resources in favour of only one party and bribing of voters. Such assessments[15] will not be left without attention by Georgia's adversary - especially if the problem worsens prior to the upcoming parliamentary elections and if Euro-Atlantic integration is put off further, which, ultimately, will be blamed on an insufficient level of democracy and not on Russia's veto in NATO[16],[17]. This factor will ease any sense of guilt felt by countries which are sceptical about Georgia's Euro-Atlantic integration, as their scepticism is influenced by Russia. Such events will lead to political or economic instability, which is one of the key goals of information warfare;
- The use of social networks and cyber space for subversive activities, especially in relations with neighbours and/or partners, is one direction of Russia's information warfare. The aim of such actions is usually to reduce trust in strategic partners or neighbouring countries, spoiling their relationship, which ultimately affects military, political, humanitarian and other cooperation and support in case of aggression. For that, comments made by both 2018 Georgian

presidential candidates on incidents and expressions related to those regions of Georgia populated by national minorities or partner state representatives were highlighted and exacerbated. The "traditional," often simple, dispute between the neighbouring countries was made to be viewed in the context of negative inter-state or international relations and traditionally sensitive issues were underlined. The comments, shown in a negative context, were replicated in social networks and then discussed by trolls and "useful idiots". Ultimately, a simple issue was expanded to the level of international or inter-state.

Thus, unlike the US Presidential elections, where in addition to the discreditation of democratic processes and the election system, Russia obviously acted by compromising and discrediting one of the presidential candidates, in the Georgian presidential elections, Russian interests were concentrated on the maximum discreditation of both candidates in order for the elected president to be unable to count on the support of domestic political forces in matters of state significance; and, first of all, on matters of de-occupation and Euro-Atlantic Integration. In addition, from a propagandistic point of view, the main goal of this extremely negatively-charged campaign was to focus on society itself, the opinion of which on sensitive state matters needed to be divided. During the presidential campaign, pro-Russian political forces became very active and tried to unite the people around them for the national idea.

Significant propagandistic resources were spent on creating the perception that both the presidential candidates, and in particular the president-elect, were supported by Russia, which on the one hand generated antagonistic attitudes among a large group of voters, and on the other, resulted in the formation of a pro-Russian elite. Such trends require attention since any change of perception in favour of Russia may become a precondition for a conventional attack.

Counter-measures

It is important to discuss counter-measures which will help prevent Russia's meddling in elections and minimize the resulting negative impact of said attacks. Countries with developed cyber-capacity and/or strong military potential can easily develop such counter-measures. France and Germany, who dealt with the Russian interference in their elections better than the USA, achieved a preventive result in their own

form of counter-measures.[18] The Minister of Defence of France publicly announced the creation of a powerful cyber-security body and, when there was interference from Russia, publicly spoke about the cyber-attacks and the resultant response[19]. Later, the country's Minister of Affairs added that France would not tolerate any type of election interference from any state, be it Russia or any other country. We can also clearly read a warming and an indication at counter-measures in the statement of the Head of the Counter-intelligence Agency of Germany, in which he clearly outed Russia's preparation of a disinformation campaign and that a psychological operation had been sanctioned by the highest political authority of Russia.[20] Georgia is deprived of the possibility of making such statements, and even more, it cannot act as, due to unequal power and the aggressive nature of Russia, such rhetoric bears great risk. As such, Georgia needs to seek solutions internally.

It is important to create a cyber defence mechanism that can prevent the information-psychological outcome of destructive cyber operations, in addition to the technical effects of computer network attacks. In particular, we recommend:

- Engagement in various activities of cyber-security organizations to minimalize the negative effect of attacks, in particular, the identification of threats, study of threat sources and informing relevant target groups about the potential threat and destructive actors;
- Increasing awareness, for which it is necessary to regularly conduct pro-active campaigns with media representatives, political parties and other participants of the election process. It is important to inform all stakeholders in advance about the destructive cyber-actions of Russia, possible channels, possible results and effective defence measures;
- A policy of timely publicity and transparency with regard to attacks. Often, for the sake of reputation, the incurred damage, which becomes the basis for propagandistic content preparation and distribution, is not publicized.
- Neutralizing the negative effects of disinformation by using social media more actively. In this regard, it is important to integrate the civic platform – the participation of non-criminal activists and their voluntary engagement in cyber-defence activities – in cyber-defence.

- The temporary or permanent blockage of propagandistic channels (in this case, RT and Sputnik) at the legislative level (even if it is a one-time normative act), seen to work quite effectively when based on the case of the French presidential elections.
- The categorization of information and the introduction of safe usage of information technologies by public services or political actors. In transmitting open, confidential or sensitive information, we will not be able to avoid the need to diversify information channels, and, in some instances, it may be necessary to completely remove such information from a network.

References

1. D. J. Smith, 'How Russia Harnesses Cyberwarfare,' Defence Dossier, American Foreign Policy Council, Issue 4, August 2012, p. 8, 11.12.2018
2. Fancy Bear (I.e. APT 28, Sofacy, Pawn Strom), cyber-actor of Russian origin acts as of mid-2000s and is responsible for cyber-activities conducted in air space, defence and energy spheres, state and media-sector. Area of attacks is broad and includes the USA, Western Europe, Iran, Japan, Georgia, Malaysia and S. Korea. It is known for cyber-attacks on defence sector and other military settings/facilities, which served the interests of the general staff of the Main Intelligence Service of Russia "GRU". Attacks on the German Bundestag and French TV5 Monde are also linked to Fancy Bear. In addition to the above fact of cyber-espionage, it became famous for organized phishing scams.
3. Cosy Bear (i.e. Cosy Duke or APT 29) is a Russian hacker group which recently conducted cyber-attacks on the White House, State Department and United Staff of the US. In addition to the above, the group's goals are the defence and energy sectors, financial and insurance areas, pharmaceutical and technological research, and media and analytical centres. Attacks on Europe, China, Brazil, Mexico, Japan, Turkey and Central Asia are described. It is known for the "Spear Phishing" technique used for phishing attacks.
4. Intelligence Community Assessment. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017.
5. www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
6. www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi
7. Intelligence Community Assessment. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017.
8. In describing a Russian hacker organization's actions in the French Presidential elections, D. Smith concludes: "Russia is indeed conducting a broad integrated strategy to attack western democratic processes. Let us see what unfolds before and after the May 7 French presidential run-off election, but Pawn Storm is more than a French affair." See D. Smith. Pawn Storm: More than a French Affair; www.cyberlightglobal.com/insight-blog/
9. www.express.co.uk/news/world/993893/Russia-German-election-Merkel.
10. Bundesministerium des Inners. Verfassungsschutzberricht 2016. SPIONAGE UND SONSTIGE NACHRICHTENDIENSTLICHE AKTIVITÄTEN.
11. www.dw.com/ru/берлин-знает-чего-ждать-от-хакеров-из-рф-во-время-выборов/a-39540359

12. Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

13. The **April 9 tragedy** refers to the events in Tbilisi, within the Georgian Soviet Socialist Republic, on April 9, 1989, when an anti-Soviet demonstration was dispersed by the Soviet Army, resulting in 21 deaths and hundreds of injuries.

14. www.state.gov/r/pa/prs/ps/2018/11/287714.htm

15. www.amerikiskhma.com/a/interview-with-rasa-jukneviciene/4671137.