Information Operations of Influence: Risks and Countermeasures

O G Leonova

Lomonosov Moscow State University, Moscow, Russian Federation,

email: politolga@gmail.com

Abstract. *The topic's pertinence.* Operations of information influence are aimed at interfering in a system of national elections, forming public opinion and destabilizing the socio-political situation in a country. *Goal setting:* identification of a risk system of information influence operations and systematizing possible countermeasures. *Theory.* The problem of elections system security has technical and political dimensions. Possible technical risks can be divided into three groups that are connected, firstly, with the security of the elections support system, secondly, with the security of the voting process, and, thirdly, with the vote counting process. Political risks cover corruption and information influence operations aiming, among other things, at disseminating misleading information. *Practice.* Technical risks of the elections procedure comprise unsanctioned access to databases; software "impermeability"; its quality; dependence of electronic devices on the Internet connection; a virus or a malfunction in a software that can automatically delete a person from a voting register; phishing technology etc. Misleading information technology and dissemination of falsified information cover personalization of information; information targeting; the creation of "interest targets"; "information baits" for consumers, "feedback loops", "filtering bubble" and "organic lift." *Propositions and conclusions.* There are three packages of information operations countermeasures. The first package consists of tasks for public information policy. The second package aims at cooperating with information users and consumers. The third package contains technical countermeasures to combat information influence operations.

1. Introduction

Cyber-security becomes more **pertinent** with every passing year as it affects even a national elections system and in the future, the number of interference attempts will only grow.

Today in most countries the elections process is based on the electronic system of voting and vote counting [30, 31]. Technological capabilities make it possible to disrupt elections, rig the results or at least to make them not credible, thus destabilizing the situation in a country.

By implementing cyber-attacks and information influence operations, external forces try to bias public opinion and even elections and their results [2, 3, 6, 21, 23]. This practice expands its scale and elections in Russia have also become the target for such attacks. For example, on March 18, 2018, the Central Electoral Committee of the Russian Federation was cyber-attacked during the presidential elections.

Unfortunately, today there are no perfectly secure systems that can eliminate risks of external interference in elections, and there is no 100% guaranteed cyber-security [29, 30].

Current electronic elections technologies have many weaknesses in all their elements and procedures [19]. This is why their security system must be fundamentally changed and taken to a whole new level soon.

At the moment, widespread usage of electronic elections systems made them more vulnerable to external actors. Information influence operations are aimed at forming a preliminary biased public opinion and destabilizing socio-political situation in a country [8, 9, 10, 12]. This makes it necessary to identify and assess risks during elections and the consequences of manipulating information consumers, systematize and summarize possible countermeasures against possible external information and technical influences proposed by the experts' community. This constitutes the **scientific merit** of the topic [5, 7, 11, 13, 20, 22, 24, 28]. A part of the article dedicated to practice makes use of the review, summary and filing of the publications in Russian and foreign journals as well as the documents provided by 'Net Politics and Digital and Cyberspace Policy Program' and the academic workshop 'Hacked Elections, Online Influence Operations, and the Threat to Democracy'.

The article uses content analysis and discourse analysis *methods*.

The risk system identification in information influence operations and the search for possible countermeasures seems to be **an important research goal**, and its solution without any doubt has a practical dimension to it as well.

2. Elections: risks and cyber-security issues

2.1Theory

Elections system security has ***two dimensions***, namely *technical and political.*

All possible **technical** risks in their turn can be divided into three groups that are connected; firstly, with the security of the elections support system, secondly, with the security of the voting process, and, thirdly, with the vote counting.

The main problem is that the elections system as a whole is a complicated process both technically and politically. Technically, it is based on integrity, "impermeability" and quality of the software that is used during the elections and in vote counting.

Politically, elections' success depends on their credibility [18]. If voters are made to doubt the transparency of the process, they will begin to doubt the results as well. Then the risks of disrupting the elections or of having a negative result caused by the negative emotional outrage of voters will increase manifold.

2.2 Practice

Let us consider *technological* risks in the elections process.

There are different *technologies for hacking the election process* [5, 6, 21, 23, 30, 31]. The most vulnerable elements of the modern electronic voting system are the following.

Risk No. 1: unauthorized access to the database. If such access happens during vote counting, it can compromise the results. This is also applicable to vote counting machines. In the past paper and punch cards were used, and votes were counted by people. After the electronic voting system was introduced, risks increased manifold.

Risk No. 2: current elections are too dependent on reliability and integrity ("impermeability", invulnerability to external influence) of the software. However, today there are no perfectly safe software programmes.

Risk No. 3 is also connected to the quality of the software. Somebody has yet to create a perfect software programme with no minor errors, no malfunctions, and proof against malware. That is why today the elections security and the credibility of their results depends on the quality of the software.

Risk No. 4: when a machine makes an audit trail, it is essential to secure it by cutting it off from the Internet and thus to protect it from external interference. However, quite often it is impossible. Firstly, many machines do not have a 'button' to block Wi-Fi signal locally. Secondly, without the Internet they will not be able to perform their primary functions, namely to read voting papers and to count votes.

Risk No. 5 is also technical. This is a virus or a deliberately planted error that automatically deletes a person from a voting register. This can happen before the elections or when a voter is in a voting booth and marks his choice in a voting paper. The voter himself or herself suspects nothing.

In developed countries, at the majority of voting stations, the register is stored on an electronic device. These devices are particularly vulnerable, especially if they are connected to Wi-Fi. As stated above, it is almost impossible to disconnect them. This is why errors or a big 'breach' in the database can occur at any moment. The only possible way to eliminate this risk is to have an emergency voting register on paper.

Risk No. 5. Unauthorized access to the database enables hackers either to destroy it or to manipulate the information in it. If it is vote counting, hackers can aim at rigging the results or even substituting the winner.

Risk No. 6 covers the phishing technology, a specific type of fraudulent activity on the Internet. For instance, intentionally hired agents or bots can send packages of phishing e-mails. If the addressee opens such a letter, he or she thus grants access to all their data, including log-ins and passwords. It makes it possible for anyone to vote in the addressee's name.

Other risks have nothing to do with technologies or electronics. They deal with *political and social factors.*

Risk No. 7. It is associated with common *corruption.* Someone who wants to be elected to an office (let us say on the regional or municipal level) can secretly buy voters. Others are willing to sell their votes for a particular (substantial or non-substantial) reward. No national elections system is secure against such corruption. Even before its delivery to a voting station voting equipment can be breached and reprogrammed to produce the desired outcome.

A candidate can also secure the support of professional hackers for a reward or other promises in case of their victory. It helps the candidate to double the chances of winning thanks not only to voters but also to real systemic support, including all information influence operations toolbox, from cyberattacks to software cracking.

Risk No. 8 is also not associated with machines and mechanisms, equipment or software tampering. It is enough to disseminate misleading information just before or on the day of the elections concerning a successful cyberattack, an interference of external forces into the electoral process, to foster voters' mistrust or even trigger panic and chaos. It is be enough to disrupt the electoral process.

2.3 Propositions and conclusions

Thus, risks are inherent to all the procedures of an electoral process and all the electoral system. Every element is vulnerable. There is still no security system that cannot be compromised. No software protects against such risks [19, 21].

Following countermeasures are implemented to protect the electoral system and prevent any interference: data transfer to a hard copy or another medium, strengthening the security of websites, additional check-ups and licensing of vote-counting machines, and so on; however, no measures are sufficient and can protect from risks.

In order to decrease these risks (but not to eliminate them), many experts suggest organizing risk-limiting audits [30]. This is a special procedure during which the results of electronic voting are compared with the results of manual vote counting. If the numbers are the same, then the elections have been secure and transparent. If the results differ dramatically, it may point to interference of external forces into the process.

That is why today it is so important to find and develop measures to reduce these risks [7, 11, 13]. The successful organization of the presidential elections in Russia in March 2018 shows that the risks of external technological interference can be diminished and political risks eliminated if the people are united and firm, if they understand national interests of the country and are responsible for the consequences of their choice.

Also, without any doubt, broad international cooperation, good practices exchange, the development of a joint package of countermeasures and international law to combat information influence operations are necessary to address these challenges efficiently, and this opinion is endorsed by foreign experts too [1, 14, 20, 22, 24, 27, 28].

3. Information influence operations

3.1 Theory

Political risks in the electoral process and their consequences are often the result of information influence operations. One of their goals is to disseminate misleading information among users [16, 25, 26, 30].

Misleading information is a mix of the truth, facts and false information (fraud), the truth and lies in a ratio of 80 to 20, with 80% of the truth and 20% of the false information. This ratio makes the information look truthful and makes it harder to distinguish between lies and facts [30].

3.2 Practice

As it is well known, the social media has a two-fold function: social service and business functions (making profit).

This two-fold goal determines its dual nature and makes it harder to implement countermeasures to combat flows of falsified information.

Recently they have been developing technologies to *personalise information even more*. They form targets of interest and set an information bait for a consumer that gives them many opportunities to conduct thoroughly planned information influence operations.

Today, selective *targeting* of information based on the analysis of vast amounts of a consumer's personal data is becoming more and more popular. The data about a person that has made at least one mouse click is meticulously stored and analysed (using, among others, the feedback loops technology). This helps to identify what content a user prefers, what interests him or her, attracts his or her attention and makes him or her a loyal customer.

Thus, a 'filter bubble' concept emerged: the platform shows a person only what he or she wants to see, read, and know. These platforms cannot be held accountable for disseminating false information. What is more, if it is in their economic interests and boosts gains (that are positively related to the number of the users' visits), they continue to disseminate false sensations, lies and conduct information influence operations.

They monitor users' reaction, and if it is positive, the operation goes on. The Internet platforms publish megabits of false content, and what attracts the most attention is promoted further. The more users are attracted by a piece of information, the more effective organic lift is: in the social media, thousands of subscribers begin to promote this information themselves so that it can become a viral information epidemic. For instance, in Russia, it was the information about 'a crying child' circulated in the social media.

It is easy to monitor users' reaction in the social media to those who want to create and promote fake news and pay for misleading information. Within a marketing strategy in the information and news market, it helps to target the intended audience more precisely. Direct impact on the interested segment guarantees that this information from now is going to be promoted by users themselves, which dramatically decreases the cost of the whole information operation.

Sooner or later, thanks to the hype in the social media this piece of news or misleading information is going to find its way into mass media. If experts eventually expose this fake news story or a hoax, it is going to affect users for a long time. It is well known that psychologically a person remembers information longer than its source, even if it is highly unreliable.

If this news story does not attract the media's attention, the information operation has still not failed. Its sponsors can use 'a conspiracy scenario' by accusing the mass media in deliberate (and paid for from abroad) silencing and hiding of important information that is going to attract additional attention and new consumers.

4.Propositions and conclusions

Countermeasures against information operations can be divided into three packages.

4.1 The first package consists of tasks for public information policy.

1. The primary role in digital information operations countermeasures technologies is played by a humanitarian component (social and cultural imperatives).

Today, most people do not share any set of values, do not know what to believe in, what values to uphold, what values are the most important for them. When a nation is not consolidated, when people do not know what can bring them together, what spiritual, political and social values they should defend together, the environment is favourable for conducting information operations.

That was what characterized Russia in the 1990s, though today when our traditional values and beliefs are being brought forward in politics and the situation has changed. That is why developing a clear ideology aimed at the defence of national interests and based on common universal values is the primary task within the information influence operation countermeasures system.

2. It is essential to develop an effective information influence operations *counter-strategy*.

First, it should help to create a technology for false information flows that assesses its potential threat to the state, its national interests and political, economic and social stability.

Second, it is vital that the creation of a false information flow (misleading information, fake news) be officially qualified as information cyber-terrorism.

Third, it is crucial to analyse how a country can respond to foreign actors' actions in the digital information space, namely to the propaganda of values that are alien and dangerous for the socio-cultural stability of a society (for instance, information activity of the ISIS), misleading information and promotion of certain views, ideas, and opinions.

Fourth, it is essential to develop an effective tactic to fight misleading information and attempts to influence people, that is, information consumers, through information.

3. It is pivotal to *invite experts to check and analyse accounts and posts* on the Internet. In the future, there is a need for an information policy that is going to help neutralize and even eliminate money (financial) stimuli to publish fake news.

4.2 The second package of information influence operations countermeasures aims at cooperating with information users and consumers.

The goal of developing information culture for users is pertinent.

[15] Today, the generation that is not accustomed to reading newspapers is especially active in the social media. That is why they are particularly vulnerable to misleading information and become an easy target for manipulators. It is essential to teach them to tell the truth from falsified information and to help them make an independent decision on whether to consume 'information garbage.' It is vital to teach them to be *responsible* for their information consumption behaviour, to search for news in other sources than the social media, in sources that guarantee its credibility, to understand the dire threat of falsehoods for them personally and to the society as a whole. *To make the right decisions* while consuming information is an important skill that must be developed from childhood.

It is preferable to introduce into the curriculum the technique of *information assessment* based on its credibility; to develop future users' skill in finding information's source and assess its impartiality and credibility; to distinguish official sources from agenda-driven business projects that only seek profit.

It is important to show to the younger generation how to assess information from the *ethical* point of view, to see whether it corresponds to traditional culture, values and civilizational codes of the country, whether it is a cultural and spiritual threat to the society.

4.3 The third package contains technical countermeasures to combat information influence operations.

Information influence operations are a source of considerable concern across the globe. For instance, participants of the educational workshop ‘The Hacked Elections, Online Influence Operations, and the Threat to Democracy symposium’ held on December 6, 2017 discussed technical measures to prevent misleading information and fake news dissemination [30]. Such techniques as labeling, rating, fake information blocking, and others were examined.

Nutrition *labels* for information. For instance, it has been proposed to mark 80% falsified information with a unique label. With such labels, it is no longer necessary to block misleading information, eliminate or forbid the source of its origin and development. The user themselves should decide whether to spend time on this 'information garbage.'

Information rating. This technique is close to the widespread practice of marking hotels, TV programmes, and books with stars. Today, this technology is being developed by Google. The lower information's rating, the less you should trust it.

Persons who define their platform's policy must be responsible for its content and architecture. It is time to change algorithms that give people news and events in a specific order taking into account and analyzing the consequences. Ethically motivated goals should prevail over financial gain that can be made by promoting fake news and false sensations. It is not about censorship of news content which would constitute a violation of the freedom of speech. A platform, or more precisely, people behind it, should make independent decisions on news design and refuse to transit fake news and information sharing in case this information is clearly falsified and can be a threat to the national security. Admittedly, there exist the problems of 'bots' (a platform's robots) but it can be solved in due time. An important task is to develop search engine optimization (SEO) for information search and users' search entries.

The possibility of *blocking or deleting information* that threatens the national security or social, economic or political stability. In this context, however, we face the issue of private property that also covers a given platform's policy and news content. That is why the law enforcement interference here is impossible and does not seem necessary. Nevertheless, the civil society can oppose the right to deceive people and to disseminate misleading information and fake news. Public opinion can to make platforms' owners use them to the detriment of national interests and information consumers.

Here, we can see two opposing trends. On the one hand, the market law of supply and demand regulates the news content of a platform. Demand for false sensations and fake sensational news is always going to be great among certain groups of consumers. On the other hand, self-regulation of content is very weakly motivated, and state interference into private business is impossible. However, the prospect of *public discredit* to platforms that house fake accounts and publish fake news is going to help them to make the right choice.

However, what can a state do to guarantee one's own security in information space? Is there an opportunity to somehow *regulate the activities of the social media* so that they cannot use their platforms to distribute misleading information and fake news? Among the measures discussed at the workshop are the following:

- informing and helping users to choose reliable information sources;
- an ability to correct fake news and expose misleading information;
- the development of user-friendly programmes that can help them to identify false accounts and information;
- active advertising of reliable information sources and resources;
- encouraging demand for official and unbiased information;
- engaging experts in checking falsehoods and exposing misleading information and refuting fake news (*fact checking*).

Today, the implementation of these proposals seems technically impossible, but the discussion of information influence operations countermeasures in itself and dynamic innovation progress provides hope that these technologies one day is going to see the light of day.

References

[1] Karbuzov D N 2017 Mobilizatsiya protestnoj aktivnosti pol'zovatelej sotsial'nykh medi v Rossii (2011-2017 gg.) *Sotsial'no-gumanitarnye znaniya* vol. 8 pp. 244-257.

[2] Rebrov A 2014 Vozdejstvie na massovoe soznanie v Internet-seti *Obozrevatel'* vol.9 pp. 75-81.

[3] Pozdnyakov A I, SHevtsov V S 2017 Metodologicheskaya osnova postroeniya teorii informatsionnogo protivoborstva *Sotsial'no-gumanitarnye znaniya* vol. 2 pp. 244-257.

[4] Shakhova N V 2017 Formirovanie informatsionnoj kul'tury v vysshej shkole *Sotsial'no-gumanitarnye znaniya* vol. 3 pp. 105-113.

[5] Combating Online Information Operations. 2017. URL: https://www.cfr.org/event/combating-online-information-operations

[6] Cyberwar 2006 *Netwar and the Revolution in Military Affairs.* Edited by Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright. New York: Palgrave Macmillan p. 246.

[7] *Malcolm and Carolyn Wiener* 2017 Cybersecurity Threats: How Vulnerable Is the United States? Annual Lecture on Science and Technology. URL: https://www.cfr.org/event/cybersecurity-threats-how-vulnerable-united-states

[8] *Networks and Netwars* 2001 The Future of Terror, Crime, and Militancy. Edited by John Arquilla and David Ronfeldt. Prepared for the Office of the Secretary of Defense. USA, National Defense Research Institute. Pittsburgh: RAND. p. 380 URL: https://www.rand.org/pubs/monograph_reports/MR1382.html

[9] *Stateless Attribution* 2017 Toward International Accountability in Cyberspace. Ed. by John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase. Santa Monica, Calif. Published by the RAND Corporation p. 57 URL: https://www.rand.org/pubs/research_reports/RR2081.html

[10] *Tactical Cyber* 2017 Building a Strategy for Cyber Support to Corps and Below. Ed. by Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, Drew Herrick. Santa Monica, Calif. Published by the RAND Corporation p. 83. URL: https://www.rand.org/pubs/research_reports/RR1600.html

[11] *The Daily Show and Philisophy* 2007 Moments of Zen in the Art of Fake News. Edited by Jason Holt. Australia: Blackwell Publishing Ltd. p. 258.

[12] *The Hacked Elections* 2017 Online Influence Operations, and the Threat to Democracy symposium. URL: https://www.cfr.org/hacked-elections-online-influence-operations-and-threat-democracy

[13] *The Standard of Good Practice for Information Security* 2007 Information Security Forum (ISF). URL: www.securityforum.org p. 25.