Advances in Social Science, Education and Humanities Research, Volume 489
Proceedings of the International Conference Digital Age: Traditions, Modernity and Innovations (ICDATMI 2020)

Arab Spring Revolutions and Digital Technologies: Implications for Russia

Ruslan Shangaraev
Associate Professor
Dept. of Public Administration in Foreign Policy Activity
Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russia
shang143@mail.ru

Olga Timakova
Assistant Professor
Dept. of Political Theory and Political Philosophy
Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russia
olga.timakova12@gmail.com

***Abstract*—Ensuring information security in modern Russia is a complex process directly affected by most internal and external factors. The political conditions in which this process takes place determine its specificity. The negative impact of digital technologies such as social networks is confirmed by the catastrophic events taking place in the Middle East and North Africa since 2011 and collectively called the Arab Spring revolutions. The purpose of the study is to ascertaine the impact of social networks on the state's national security based on the case of the Arab Spring. Based on the conclusions, the authors will highlight the implications for ensuring Russia's national security in current conditions. Social networks are the primary source of information for the population of most states and have become one of the main channels of disinformation and propaganda, is the main tool for influencing the consciousness of a large number of people, since through their platforms citizens not only receive political information but also form their political beliefs and have a chance to influence the course of the political process of the state.**

Keywords—Middle East and North Africa, Russia, Arab Spring, USA, Social Media, information security, strategic interests, national security

I. INTRODUCTION

The formation of the information society creates a new problem for science – developing new methods, technologies, and procedures for researching information security as an integral part of national security as a whole. Everything that relates to ensuring information security creates tasks and possible solutions of a theoretical and methodological nature.

Public relations are inseparable from information and its technical components. Information resources and technologies have entered the structure of economic instruments, and themselves have become objects of the global market and, over time, become a mechanism through which one can influence the tools of political governance in all its manifestations.

The development of information technologies in the 21st century has presented humanity with a platform for free communication and interaction – the Internet. More than one billion people are users of the Internet, which at the present stage is not only one of the primary means of communication, but also serves as the foremost source of information and its dissemination. The main means of social communication are services such as "Skype", "Facebook", "LinkedIn", "Twitter", "Vkontakte", etc. [1, 5630], and not only news agencies or official Internet resources, but also alternative sources of information, such as Wikipedia [2], sites with unverified content or only groups and communities on social networks, or chats and apps that facilitate communication, discussion, exchange and dissemination of various ideas.

Social media has significant potential as a channel for disseminating information and providing opportunities for content replication. It is worth recognizing that social networks have gone beyond just interpersonal communication or exchanging pictures, music, or video files. They influence the domestic and foreign policies of states, the worldview of people, become a method of public diplomacy, and a way of spreading extremist ideas, which indirectly or directly affects the national security of the Russian Federation. In the course of the study, this phenomenon would be examined, and its impact on the Russian national security would be determined.

II. METHODS

The comparative analysis is seen as the most appropriate method, allowing to present the mechanisms of manipulating society through social networks and methods of preventing and countering information security threats.

- First of all, a comparison will be made of the use of digital technology and social networks to destabilize the political situation and security in the country and the region.

- The second point for comparison will be foreign states' experience in responding to the threats and challenges that the destructive influence of social media and other technologies brings with it.
- A separate issue will be carried out to study the interaction of the world's states with technological giants – developers of social networking applications.

Apps claiming to encrypt data such as WhatsApp and Telegram are insecure. Information obtained through social networks and messengers can help the intelligence agencies of foreign states. Firstly, it is not known how correctly they will use this information, and secondly, whether it will leak from them. Edward Snowden, a former employee of the US National Security Agency, believes that texting in messengers is too risky, especially for government officials, and advised officials not to use such applications. At the same time, in an interview with France Inter radio station, Snowden did not dare to advise on the safety of smartphones and computers, noting that the struggle of ordinary people with foreign intelligence services will, in any case, be unequal. IT expert Alexander Baulin said that "Snowden told us a long time ago that, for example, the United States has a large system for tracking users' electronic communications. Furthermore, in this regard, the coding of information transmission cannot be saved because companies promise to issue it at the request of government agencies". Mikhail Kondrashin, Technical Director of Trend Micro in Russia and the CIS, in turn, states that: "All systems that we considered safe at some point are vulnerable" [3].

Facebook also admitted the wiretapping – the social network paid third-party companies to decrypt users' voice messages, including intimate content. Representatives of the company itself claim that contractors eavesdropped on messages to improve the work of neural algorithms on the social network. In 2019, a class-action lawsuit was filed in the United States for illegal surveillance against Apple – the corporation was convicted of decrypting and processing messages received by the voice assistant Siri. Apple, like Facebook, claims that the data has been anonymized [4]. All social networks and instant messengers work approximately according to the same principle: there is a server on which the software is installed, users connect to it, all text and sound messages, photos, videos pass through this server. It should be admitted that the range of application of such information is quite extensive, but certainly, we are not talking about training a neural network after the data has left you, no matter what form – video, voice, or text – what happens next is almost impossible to track. All the information on the Internet can be used for provocation to organize all kinds of destructive movements, including protest ones.

III. Results

No one can deny that based on messengers and other social networks, manipulative mechanisms for organizing large masses of people, and effectively managing them at a distance have been studied and improved [5, 866]. An example is the technology of organized meetings of people – "flash mob" – the organizer of which is an individual or a group of people and is a mass action, often a protest, aimed at achieving some goal and organized synchronously in a number of cities and towns of the country.

It is noteworthy that many experts assess the "Twitter revolution" in Egypt as a kind of flash mob that brought more than a million people out onto the streets of cities [6]. Many analysts, the participants in the riots themselves and the world community as a whole, note the importance of social networks' role in organizing the Arab Spring. It was a series of spontaneous mass protests and coups in the Middle East and North Africa since 2011 [7].

Since the second half of the twentieth century, "color revolutions" have become a quite common tool for achieving geopolitical goals - one of the tools of hybrid wars implemented by foreign states with the use of special services and other shadow mechanisms for actual interference in the internal affairs of independent states. The beneficiaries of such a technology to achieve their goals often take as a basis the methods of speculation and incitement of the internal problems of the state, to mobilize the most active part of society for the subsequent organization and conduct of protests against the legitimate authorities in order to overthrow them and bring loyal political forces to power. On the one hand, states should not bring contradictions in society to a high degree of tension, and on the other hand, the risks and implementation of such technologies are a kind of test for the authorities, which in such situations should show their maturity and strength, general viability in the face of both internal and external threats.

The problems of "color revolutions" in the modern conditions are becoming extremely acute and vital. This is due not only to the fact that the events in Belarus, Ukraine, Armenia or Moldova, upon detailed examination, exactly repeat the scenario of the "color revolutions" in North Africa and the Middle East, in particular the revolution in Egypt, which indicates non-randomness of these events. The reason is that the traditional tools for transforming political regimes, which are customary for the world community, are being replaced by a new generation of more subtle tools that combine forceful methods of influence with technologies of manipulative control of the mass consciousness and mass behavior of the broad masses of the civilian population.

The most affected by the revolution and the most striking negative example of the results of the revolution with the support of foreign states can be named Syria and Libya, which before the events were economically and socially prosperous countries with a high standard of living for the region, and the results of the revolution were: the destruction of the institution of the state, the shattering of the country to separate warring regions under the control of bandit formations, the placement of terrorist training camps and secret prisons on the territory of the state, the smuggling and plundering of the state's natural resources, the transformation of the country's territory into an arena of struggle between various states.

The revolutionary events that took place in the countries of the Commonwealth of Independent States are interesting primarily because they are based on technologies that are in many ways relevant for Russia and events on the internal

political agenda similar to the possible scenarios potentially implemented in Russia. The difficulty in their independent interpretation is that, on the one hand, the old elites allowed a loss of support for a significant part of the population, thereby providing opportunities for the implementation of revolutionary scenarios, and on the other hand, with a more thorough analysis of the events that took place, it is possible to trace the influence and management of the events from abroad – by external forces interested in the geopolitical weakening of the positions of Russia and the reorientation of state policies towards Western countries.

The popularity and comprehensiveness of the information and social networks have inevitably led to the abuse of their capabilities and use for destructive purposes. Over the past few years, the number of various cyberattacks made on the Internet resources and servers of state and socially significant objects, recruiting via social networks, or organizing mass demonstrations (even virtual) has increased several times.

Thus, hackers “Gforce Pakistan” and an unknown loner “Dodi” disabled the largest provider in Israel “NetVision”, through which 70% of the population of this country go to the Internet. Israeli hackers calling themselves the “Israeli Internet Underground”, in turn, hacked the GulfNews, a well-known information site in the Arab world, which, in particular, contained information in support of the actions of radical Palestinians [8]. Do not forget that in 2013, in the other hemisphere resulting from computer infection, the information systems of drilling platforms in the Gulf of Mexico were disabled, which put the facilities at risk of flooding [9].

IV. Discussion

It should be noted that many states are building information security and protection systems. For more than one year, the American and Chinese armies have in their composition units that take an active part, both in the protection of information and in intelligence activities, and special operations. Because to the hacking of the computer systems of the military department, the Chinese hackers managed to gain access to secret developments of the latest weapons, including the blueprints of the Patriot anti-aircraft missile system, the newest version of the Aegis multifunctional missile defense system, the F-18 fighter, the Black Hawk helicopter and the F-35 attack aircraft [10].

In the United States itself, a discussion is underway around the PRISM (Program for Robotics, Intelligence Sensing and Mechatronics) intelligence system, through which the FBI and the National Security Agency get direct access to the servers of such popular services like Microsoft, Google, Skype, Facebook, Apple, and YouTube – such conclusions can be drawn from the presentation to NSA analysts, which got on the world web [11]. According to the information contained in it, PRISM allows general monitoring of resources and, in a short time, access to e-mails of any user suspected of illegal activity.

According to the TV program Vesti, Russian special services also use PRISM. Many believe that the increased interest of the authorities in social networks is associated with a manifold increase in the number of so-called "trolls" – engaged commentators whose purpose is to create the appearance of support or, conversely, indignation about a significant event or initiative. However, by influencing the statistics of monitoring systems, trolls, as a rule, cannot seriously influence public opinion, since their comments are often anonymous or made from fake pages, which significantly reduces user confidence in them [12].

The Russian Federation organized and approved a state system to detect, prevent, and eliminate computer attacks on Russian information resources, cyber systems, and information and telecommunication networks in Russia and diplomatic missions and consular offices abroad [13]. It is worth noting that in the United States, a similar directive has existed since 2013. With its help, the country's cybersecurity system was developed and created, and methods to reduce the risk from a wide range of cyber-attacks on essential government infrastructure facilities [14].

As part of the Russian defense department, a similar structure of "information operations troops" also functions, which ensures the protection of Russian military command and control systems from attacks by cyber terrorists and, in every possible way protects the data passing through them from a potential enemy [15].

Under the auspices of the Ministry of Internal Affairs of Russia, there is Department “K” – a unit whose purpose is to fight against crimes in the field of information technology, and the illegal circulation of radio-electronic means and special technical means. It is a part of the Bureau of Special Technical Measures of the Ministry of Internal Affairs of the Russian Federation [16].

V. Conclusion

Thus, the Russian government recognized that information security is an urgent problem of our time of a global nature, and it will grow steadily as information technology develops and spreads.

It can be stated that social networks are becoming the leading source of information for the population of most states and have become one of the main channels of disinformation and propaganda, have become the main tool for influencing the consciousness of a large number of people, since through their platforms citizens not only receive political information but and form their political convictions and have a chance to influence the course of the process related to state policy. Thus, instead of mainly attacking military or economic infrastructure, cyber operations now target people within society, affecting their worldview as well as behavior and diminishing trust in government and state institutions. In this regard, information security protection is becoming a priority task for every country in our time.

References

[1] R. Schroeder, “The Globalization of On-Screen Sociability: Social Media and Tethered Togetherness,” in International Journal of Communication, 2016, vol. 10, pp. 5626-5643.

[2] D. Chaffey, "Global Social Media Research Summary 2020," in Smart Insights Website, April 17th, 2020. URL: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (accessed July 18th, 2020).

[3] Z. Doffman, "WhatsApp And Telegram Flaw Exposes Personal Media to Hackers," in Forbes online, July 16th, 2019. URL: https://www.forbes.com/sites/zakdoffman/2019/07/16/whatsapptelegram-issue-has-put-a-billion-users-at-risk-check-your-settings-now/#725e9405ab88 (accessed July 26th, 2020).

[4] Z. Doffman, "Why You Should Stop Using Facebook Messenger," in Forbes online, July 25th, 2020. URL: https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/#cc9050669ada (accessed July 26th, 2020).

[5] M. Adamov, R. Shangaraev, "Information Communications as Method of Digital Diplomacy in US Foreign Policy," in Issues of National and Federal Relations, 2019, vol. 9, issue 6(51), pp. 865-871.

[6] A. Abo el-Fetouh, "July is the month for coups," in Middle East Monitor Website, July 27th, 2020. URL: https://www.middleeastmonitor.com/20200727-july-is-the-month-for-coups/ (accessed July 30th, 2020).

[7] S. Anderson, "Fractures Lands: How the Arab World Came Apart," in New York Times online, January 19th, 2018. URL: https://www.nytimes.com/interactive/2016/08/11/magazine/isis-middle-east-arab-spring-fractured-lands.html?mtrref=www.google.com&gwh=CCD6E0BCE12AD052A22FDBBCE402C69A&gwt=pay&assetType=REGIWALL (accessed July 10th, 2020).

[8] GForce Pakistan official group, on Facebook Website. URL: https://www.facebook.com/GForce.Pakistan/ (accessed July 29th, 2020).

[9] Z. Shauk, "Malware on oil rig computers raises security fears," in Houston Chronicle online, February 22d, 2013. URL: https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php?t=1b259d62f3b05374ef&t=1b259d62f3&t=1b259d62f3 (accessed July 14th, 2020).

[10] G. Ingersoll, "Chinese Hackers Stole Plans for Dozens of Critical US Weapons Systems," in Business Insider online, May 28th, 2013. URL: https://www.businessinsider.com/china-hacked-us-military-weapons-systems-2013-5 (accessed July 13th, 2020).

[11] M. Hosenball, "Warrant not Always Needed for 'Indavertent' NSA Surveillance of Americans: US Court," Reuters online, December 19th, 2019. URL: https://www.reuters.com/article/us-usa-courts-surveillance/warrant-not-always-needed-for-inadvertent-nsa-surveillance-of-americans-u-s-court-idUSKBN1YN02U (accessed July 21st, 2020).

[12] "USA Launched Staff Recruitment for Cyber Forces," in VestiRu Website, October 3d, 2009. URL: http://www.vesti.ru/doc.html?id=318470 (accessed July 10th, 2020).

[13] "Decree of the President of the Russian Federation of January 15th, 2013 №31s 'On Creation of State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks on Information Resources of the Russian Federation," in Russian Newspaper online, January 18th, 2013. URL: https://rg.ru/2013/01/18/komp-ataki-site-dok.html (accessed July 20th, 2020).

[14] E. Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," in Washington Post online, November 14th, 2012. URL: https://www.washingtonpost.com (accessed July 26th, 2020).

[15] "Russia Creates Cyber Forces," in VestiRu Website, May 12th, 2014. URL: http://www.vesti.ru/doc.html?id=1573024 (accessed July 10th, 2020).

[16] Ministry of Internal Affairs of the Russian Federation Official Website. URL: https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (accessed July 22d, 2020).