MIDDLE EUROPEAN SCIENTIFIC BULLETIN

Volume 44, Issue 4 | 2024
ISSN: 2694-9970

https://cejsr.academicjournal.io/index.php/journal/

Article

Intelligence Character of Information War in the Digital Age

Ana Jikia[1], Davit Kukhalashvili[2]

1. Caucasus International University Faculty of Social Sciences Political Science Ph.D PhD student of the program
2. Caucasus International University Faculty of Social Sciences Associate Professor

Abstract: Social media and information warfare are explicitly relevant in ensuring the operativeness and scope of intelligence processes, which makes social media an object of intelligence and counter-intelligence activities because its use for hostile intelligence purposes is a significant threat to the political stability of the state. As for the information war, it's used under the cover of intelligence services and serves the interests of the country which carries out the intelligence process to form the desired public opinion in the target country and the international arena.

Keywords: cyber security, intelligence, media, security, counter-intelligence

1. Introduction

Intelligence Character of Information War in the Digital Age

From ancient times, we find elements of information war in the governance processes of states. It was used both within the states and outside its borders. The information war had target objects, methods, and means of spreading information, and everything served the interests of its implementer country.

We can find early cases of information warfare in ancient civilizations, where it was actively used both to initiate conflicts and in the ongoing processes. Signs of intelligence propaganda and disinformation were recorded during this war. For this period, spreading rumors, and using false signals to demoralize the target country's government, armed forces, and the enemy was an important factor.

It should be noted that the invention of the printing press by Johannes Gutenberg in the 15th-16th centuries contributed to the strengthening of propaganda, the purpose of which was the formation of religious views and political ideologies according to the state's interest.

In the 20th century, before and during the First and the Second World Wars, there was a large-scale use of intelligence propaganda within one's own countries and on international public opinion to influence strategic interests, form alliances, expand their influence, and demoralize the opponent. Such means as posters, radio broadcasts, and newspapers played an important role in achieving this result.

During the "Cold War" period, to achieve the desired results, the states fighting for dominance in the international arena used psychological operations (PsyOps) on a large scale in different geographical areas, within which intelligence propaganda and the spread of intelligence misinformation played a special role. Through this process, it became possible to ensure the demoralization of specific authorities, organizations, individuals, and groups of persons, the undermining of existing institutions, and their involvement in internal and external military actions of the country.

Citation: Ana Jikia, Davit Kukhalashvili, Intelligence Character of Information War in the Digital Age. Middle European Scientific Bulletin 2024, 44(3), 1-4.

Received: 4th July 2024
Revised: 11th Aug 2024
Accepted: 28th Aug 2024
Published: 4th Sep 2024

In the modern epoch, digital technologies have revolutionized information dissemination, access, and positive outcomes. Without them, the further existence of the world is unthinkable. In addition to the positive result, significant threats are expected from it, including intelligence organizations conducting information war against the target country. The tactics and methodology of this type of war have significantly developed in parallel with historical processes and have been adapted along with technological progress.

The advent of the Internet and digital technologies has brought a significant change in the art of information warfare. State and non-state actors have begun using cyber attacks, hacking, and disinformation campaigns to target facilities including critical infrastructure, influence elections, and spread false narratives on social media platforms. Precedents of this type of war, large-scale development, and use of social media are recorded in the 21st century. For example, the Russian Federation's alleged interference in the US elections through intelligence activities (2016) ["New report of the US Senate". Radio Freedom. Information was retrieved from: https://www.radiotavisupleba.ge/a/30076742.html] and the spread of misinformation during the COVID-19 pandemic.

The creation of new tools to manipulate information during the growth of artificial intelligence has made the possibility of a damaging impact on the provision of state security even higher. For example, Deepfake technology, which can create audio and video content similar to the real one, which differs from the real one, simplifies the probability of influencing the target objects in terms of effectively producing disinformation campaigns of an intelligence nature.

It should be noted that the technology of conducting information warfare is characterized by rapid development. It combines with technological progress and geopolitical changes, which, along with receiving certain benefits for states, creates a significant problem in terms of organizing various categories of threats.

Information War: A New Battlefield

In the modern era, the structure of warfare has transformed. The evolution of technology and communication tools has ushered in a new era where conflicts are no longer confined to the physical battlefield. Information warfare has become as intense as physical battles. Here, both the state and non-state actors and various subjects are actively participating by their intelligence strategies, which makes this war especially intense. In this process, controlled information will again play an important role as a powerful weapon on the battlefield of the future. The development and availability of digital platforms are contributing factors to the increase in intelligence capabilities of information warfare, which is evidenced by such results as disruption of social unity, manipulation of target groups (government, individuals, groups of people, organizations), critical damage to infrastructure by cyber-attacks, provoking social unrest, destabilization of political institutions and others.

Therefore, along with the benefits, both the development and availability of digital platforms can be considered a significant threat to national security.

Cyber Attacks and Espionage

Cyber-attacks are the most important component of information warfare because with this process it is possible to disable the target objects of intelligence activities. Accordingly, both employees and spies of the intelligence service organizing the actions may be working under hackers and cybercriminals. The fact that there are objects of intelligence influence and penetration, including government networks, and private institutions, which steal intelligence data, the disruption of the infrastructure important to the state, and the disruption of the system is useful to support the expressed opinions.

To support the above-mentioned opinions, let's review the information available in the open source, [,,the Senate presented a preliminary report on Russian interference in the US elections. American Voice. Information was retrieved from: https://www.amerikiskhma.com/a/senate-intelligence-report/4056564.html] about the Russian Federation's alleged interference in the 2016 United States presidential election. The analysis of the actions indicates that there is an organization with signs of political intelligence (7 years have passed since the above event, but the influence of Russian interference on the outcome of the elections is still a matter of debate), including from the

point of view of conducting information warfare. The use of such methods as cyber-attacks, hacking of e-mails of target objects, dissemination of disinformation, obtaining important information for political intelligence, and manipulation of social media are used for the execution of intelligence goals. By using this method, it is achieved to create division and tension in the society of the target country. It is important to note that on the part of the USA, such response intelligence and counter-intelligence organizations to this act, such as the use of appropriate sanctions against the Russian Federation.

Analysis of open-source information includes signs of political intelligence. Political consulting firm Cambridge Analytica collected data from millions of Facebook users without their consent. They used this data to create fake profiles and target political ads during the 2016 US presidential election and the Brexit referendum. The scandal highlighted the misuse of personal data for political intelligence purposes to manipulate voters' behavior and influence election results.

The Intelligence Value of Traditional and Social Media

The intelligence value of traditional and social media is determined by the following factors:

- **Its vulnerability to the spread of intelligence propaganda** (including for manipulation of public opinion of the target state, for discrediting-neutralization of undesirable views, etc.)
- **Its vulnerability to the spread of intelligence disinformation** (target object of the state authorities, the population, information without objection, immature sharing to have the desired effect, etc.)
- **Its vulnerability in terms of creating a psychological portrait of an intelligence nature favorable for recruitment and perfect dissemination of information** (Social media platforms, including Facebook, and Twitter);
- **Its vulnerability to media bias of an intelligence nature** (formation of the opinion desired by the spying country in the target state through biased, selective coverage);

Conclusion

In the intelligence organization, the use of printed material within the framework of information war is of particular importance for the formation of religious beliefs and political ideologies to the advantage of the intelligence country, to the detriment of the target state;

The large-scale use of intelligence-type propaganda of posters, radio broadcasts, and newspapers creates favorable conditions for influencing the strategic interest of the country and international public opinion, forming alliances, expanding their influence, and demoralizing the opponent;

Within the framework of intelligence propaganda in psychological operations on the part of the states, spreading disinformation is a means of ensuring demoralization of the target country's authorities, organizations, individuals, and groups of individuals, encouraging recruitment, undermining existing institutions, and engaging in internal and external hostilities of the country;

The use of cyber-attacks, hacking, and disinformation campaigns by intelligence organizations through the Internet and digital technologies to target objects, including critical infrastructure, to influence elections and to ensure the spread of false narratives on social media platforms is particularly important;

The development and availability of digital platforms should be seen as both a benefit and a threat to national security.

The development and availability of digital platforms are contributing factors to the increase in intelligence capabilities of information warfare, which can achieve the following results: disruption of social cohesion, manipulation of target groups (governments, individuals, groups of individuals, organizations), critical damage to infrastructure by cyber-attacks, provoking social unrest, destabilization of political institutions, etc).

Cyber-attacks are the most important component of information warfare because with this process it is possible to disable the target objects of intelligence activities. Both employees of the intelligence service organizing the actions and spies may be working under hackers and cybercriminals.

During the cyber-attack during the information war of intelligence information, the used methods are the following: hacking the e-mails of the target objects, spreading disinformation, and obtaining important information for political intelligence. The objects of impact-penetration of cyber-

attacks are represented by: government networks, and private institutions.

The intelligence importance of traditional and social media is determined by their vulnerability, the creation of a psychological portrait of an intelligence nature favorable for intelligence propaganda, disinformation, and recruitment through media bias.

References

- Awan, I., & Blakemore, B. (2020). Cyberhate in the context of international relations. *Journal of International Relations and Development, 23*(2), 197–211.
- Chesterman, S. (2021). *We, the robots?: Regulating artificial intelligence and the limits of the law*. Cambridge University Press.
- Heickero, R. (2017). *Cyber terrorism: An examination of the concepts and policy implications*. RAND Corporation.
- Herrmann, R. K. (2019). *Intelligence power in peace and war*. Cambridge University Press.
- Kulkhalashvili, D. (2021). *Aspects of information warfare and lobbying, intelligence and counter-intelligence activities*. Tbilisi.
- Marsoz, J. (2021). *Terrorism and media: A guide for journalists (Georgian edition)*. Tbilisi.
- Puyvelde, D. (2019). *Intelligence and national security: A strategic approach*. Oxford University Press.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt.
- Zegart, A. B. (2021). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.