Paulina Krawczyk*
Jarosław Wiśnicki**

Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine

Abstract

This article seeks to identify social influence tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine. An attempt to analyse the creation and spread of information threats as a result of the actions taken by Russia in the ongoing conflict is dictated by the increasing impact of communication processes on global security. This article presents the role and impact of mass media on public awareness, revealing the mechanisms of forming public opinion.

Key words: information warfare, media, formation of public opinion

* Paulina Krawczyk, Faculty of National Security, War Studies Academy, Academic Centre for Cyber Security Policy, e-mail: p.krawczyk@akademia.mil.pl.
** Lt Col Jarosław Wiśnicki, Territorial Defence Forces Command, e-mail: jar.wisnicki@gmail.com.

Introduction

The purpose of this article is to attempt at identifying information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine. An attempt to analyse the creation and spread of information threats as a result of the actions taken by Russia in the ongoing conflict is dictated by the increasing impact of communication processes on global security. This article presents the role and impact of mass media on public awareness, revealing the mechanisms of forming public opinion. In approaching the topic of the work, the authors were guided primarily by the topicality of the analysed problem.

Social media

New media (traditional online media and social media) of the so-called non-governmental sector constitutes the information-technical and information-psychological space for the acquisition, processing and exchange of information. This multimedia reality bombards us with stimuli, strokes our senses and does not allow itself to be forgotten. It seduces us constantly with its attractiveness by intoxicating our cognitive zone. This action is in line with the concepts developed by Alexander Dugin, a Russian academic and politician, regarding network warfare. These agitation-propaganda and intelligence-organisation activities are carried out by non-state actors (in this case, by a network of various organisations linked to the Eurasian movement). Network technologies are understood broadly and apply to both real and virtual information spaces. Russian network structures are organised from the bottom up, and they are instructed, controlled and corrected from the top down, ensuring an airtight system. Strictly centralised, they operate according to the principles of network collectivism, within a common worldview matrix and according to executive instructions[1]. This type of activity is not a novelty, it is just a demonstration of the use of modern technology and communication solutions to introduce innovative activities in the infosphere. In this context, new means of communication, with a particular focus on social media, have

1 J. Darczewska, *Środki aktywne. Rosyjski towar eksportowy*, „Punkt Widzenia" 2017, no. 64, p. 51.

a fundamental impact on the time and space experienced by people, condemning audiences to navigate in a hyper-reality of constantly remediating messages. This is because the harder we focus on the content of the message, the less we recognise that we are stuck in a media web. Hence, it would be quite naïve of us to think that the worldview represented is our view or perhaps it is shaped by the media independently of our will.

The opportunities presented by social media are also used as a weapon in hybrid operations. The first in the area of using modern media is a broad analysis of the information environment. Studies apply, in a special manner, to social structures on the internet. Their composition, the topics covered, the purpose of the association, the activities conducted and the resonance on the net are among the main research domains. The second area is the target group vulnerability study since a lack of characterisation of these groups would make it impossible to shape their attitudes. The information left by users makes it easier for analysts to extract sensitive data. The analysis in these areas, deepened through the use of user preference recognition tools and micro-targeting, contributed to the planning of the information impact process and to the estimation of the necessary resources by the centre planning the impact operation in order to achieve the desired effect. This makes it possible to infiltrate all those communities that are indoctrinated with content favourable to the objectives of the social influence policy being pursued. Thus, it makes it clear that a potential attack, due to its complexity, cannot be carried out based on a previously prepared general outline of the objects of impact. Rather, it requires constant updating of data and continuous verification of methods and techniques of operation. The effectiveness of the analysis being carried out is maintained with the help of social media, which provides invaluable information for free.

The conduct of both active and passive actions in the area of information operations stems from the concept of conducting military operations, as developed in 2012–2013 by the Russian Federation. An important novelty in the assumptions of this concept is the wider spectrum of impact on the functional areas of the state such as politics, economy, society, and social and information structures with their infrastructure. The Russian concept provides for the use of simultaneity of impact on interconnected network-centric areas as a whole. It should be noted that this component of the adopted strategy should be considered the most original and requires the most attention.

This is evidenced by the conflict in Ukraine. Information activity makes the initiating element, which has been expanded to include elements

of energy warfare, an integrated operation where the two components are complementary to each other. In terms of information operations, Russia focused its activities, as it did during the 2014 conflict, on the impact of targeting the enemy population. Achieving the intent was to be possible through cascading intermediate goals. Success was seen in awakening the potential for protest in Ukrainian society. Success was expected to be achieved through cascading objectives essentially boiling down to, on the one hand, highlighting the unity of the two countries in terms of nationality, religion and culture, and, on the other hand, economic impact. The media offensive uses both traditional and completely new forms of impact while supporting the adopted narrative. These activities are closely coordinated with Moscow's broader objectives and operations.

Deepfake

In order to increase the information advantage, newer and newer techniques are being used to gain an advantage over the opponent using the element of surprise. One of them is deepfake. The term combines two issues: fakery and deep learning. The tool uses machine learning algorithms and facial recognition technology to digitally manipulate people's voices, bodies and faces. It was created, *inter alia*, for the purpose of reviving our favourite stage artists who are gone. Another area that uses the latest technology is for those who do not like to perform in front of a camera but can do so by having their own avatar. In addition, those who cannot speak will be able to restore their voice. The first material of this kind was created in 2017. Deepfake is a technology that uses artificial intelligence (AI) to create or edit video or image content to show something that never happened. The solution utilises algorithms called generative adversarial networks (GAN) based on two systems – the first one is the generator, and the second one is referred to as the discriminator. The generator identifies, analyses and learns patterns in datasets – for example, features that repeat in photos, videos or sounds as well as in facial expressions, intonation, tics, and eye movements – and then it creates a fake video clip. The discriminator then compares real and fake images and determines whether the clip is real or fake. Each time the discriminator accurately identifies a video clip as fake, it gives the generator a hint of what not to do when creating the next clip. The effectiveness of the use of this tool is evidenced by the video conference allegedly held with Leoid Volkov, Alexei Navalny's chief of staff.

As a result of the use of deepfake technology, it was a conversation with a character impersonating him. According to the daily newspaper *De Volkskrant*, the persons who took the bait included members of the lower house of the Dutch parliament, politicians from Lithuania, Latvia, Estonia and the United Kingdom[2]. If a person's speeches are properly crafted, it is possible to influence politics, destabilise the economy or even cause riots which may produce other dramatic consequences. Today, a well-done deepfake is the work of professionals but it is probable that in a few years, it will be possible to do it on our smartphones. However, it is important to point out that nowadays almost everyone can generate hyper-realistic images from delineation, like for instance human faces. The most modern models can already generate very realistic sounds to deceptively resemble specific people. This makes it possible, *inter alia*, to distort the truth when making speeches. Technologies with slightly weaker quality allow information to be intoxicated by using a generated voice during a phone call. As a result, impact activities using these tools are more and more difficult to detect and, consequently, the number of fakeries has increased exponentially. Therefore, the speed and diversity of content deformation should be seen as its greatest threat. As Marek Matacz writes „psychology works in favour of fakes". He refers to a study conducted by researchers at the Massachusetts Institute of Technology on false information posted on Twitter. Studies show that it is passed on to other users as much as 70% more often than real information. According to academics, as the author describes in his article, this is due to the illusory truth effect. This mechanism works in such a way that people are inclined to believe what seems familiar or coincides with their thinking. This can occur, for example, after repeated exposure to a given piece of information. Academics from Yale University in Connecticut have proven that reading a fake news headline just once later increased belief in its truthfulness. As it turns out, the illusory truth effect also occurs when the reliability of information is low, even when false reports are labelled as false and when they are inconsistent with the political ideology of the reader[3]. The large-scale detection of deepfakes requires scaled methods derived from multimedia models and computer vision. One of the tools used to help identify the risks associated with face morphing technology was the

2 *Wideorozmowa ze „współpracownikiem Nawalnego". Politycy z czterech krajów padli ofiarami deepfake'a*, https://tvn24.pl/swiat/deepfake-ktos-podszyl-sie-pod-leonida-wolkowa-wspolpracownika-aleksieja-nawalnego-5076773 [access: 28.05.2021].

3 M. Matacz, *Walka z deep-fake*, „Wiedza i Życie" 2021, no. 6.

program of the Defence Advanced Research Projects Agency (DARPA) called Media Forensics[4]. The development of technology forces a constant race with technology. Another activity is an initiative by Facebook and Microsoft Corp with the Partnership on AI coalition undertaking research work in the area of detecting and preventing the use of deepfakes. It is worth stressing that in 2019 the above body issued a statement of joint action against false content spread by the technology discussed herein. It is more than likely that because new technology affects wider and wider areas of social life, more and more actions will be undertaken to fight against the distortions of reality.

Fake news

Another important tool, which has been in use for a long time in various forms, is fake news. For hundreds of years, bad and sensational news allowed newspapers, radio and television stations to grab people's attention, thus attracting advertisers. We can find one of the sources in the American dictionary, Merriam Webster, according to which the etymology of the term dates back to the 19th century, citing headlines with this phrase from 1890. The term itself was popularised through the 2016 election campaign in the United States. And just a year later, the authors of the British Collins Dictionary named it their word of the year. One could venture a guess that this term has defined the last twelve months. The literature on the subject presents two approaches to the phenomenon it indicates: the media approach and the approach as part of the so-called active measures used in the course of hybrid warfare in Ukraine. It is worth noting that in the new realities of the global internet village, citizens, often unknowingly, are included in the distribution of content that builds into the accepted narrative.

Referring to the first approach, it would be appropriate to echo Manuel Castells, who wrote that we live with and through the media. World-renowned sociologist and social theorist Niklas Luhmann stated that we derive all information about the world from the media. The statement quoted above makes us aware of the importance of the media in constructing our consciousness. Therefore, paying attention to gossip's little brother as

4 M. Turek, *Media Forensics (MerFor)*, http://www.darpa.mil/program/media-forensics [access: 12.12.2021].

a tool used both to shape social attitudes and to manipulate public opinion to implement certain content is quite justifiable. Observations show that the primary source is online portals, which are characterised by a difficult process of verifying and controlling content. In turn, the medium and fertile ground for the spread of false content is social media. This results, as Stanislaw Krajski puts it, in the creation of a strange media mix that is the confusion of facts, opinions, interpretations and narratives, among which it is extremely easy to hide facts[5]. An analysis of the impact of this term leads to the conclusion that fake news is a technique used in many levels of social life, which was intended to be the main focus of Kremlin propaganda.

It is worth stressing that among the main channels spreading disinformation content in the ecosystem of Poland, engaging in support for the fighting in Ukraine, is the largest social media platform Telegram. This Russian app, founded by Pavel Durov, started as an instant messenger platform and has been adding social functions for the past few years, becoming more and more popular also in Poland. This is especially the case with migrants from the East and war refugees from Ukraine. Thanks to numerous network connections, it intoxicates the information environment by reinforcing Russian narrative lines according to the principles of Russian reflexive management theory. The main channels that make up a significant part of the Russian disinformation ecosystem are:

– „Kanał Informacyjny KJU", established on 12 October 2020;
– „Ciężka Artyleria", established on 10 April 2021;
– „Niezależny Dziennik Polityczny", established on 24 August 2021;
– „Nwk24.pl", established on 18 November 2021;
– „Syrenka.pl", established on 1 August 2021;
– „News Front Polska", established on 3 March 2022;
– „Ktoś", established on 30 October 2022;
– „Oko Cyklonu", established on 24 March 2022;
– „Olej w Głowie", established on 13 March this year, but commenced its activity on 6 April 2022;
– „Ruch Oporu", established on 4 March 2022;
– „News Factory", established on 15 March 2022 and „Ukraina w Ogniu"[6].

5 S. Krajski, *Masoneria polska 2021. Na skraju przepaści*, Warszawa 2021, p. 21.
6 K. Gil, *Raport. Jak działa rosyjska dezinformacja w aplikacji Telegram*, https://disinfodigest.pl/raport-jak-dziala-rosyjska-dezinformacja-w-aplikacji-telegram/ [access: 20.07.2022].

The components outlined above, which represent a small fraction of the Kremlin's disinformation web, facilitate information attacks. In addition, involving so many players makes it possible to avoid the restrictions imposed by media corporations or institutional requirements, thus gaining more and more possibilities to infect distributed information to influence public opinion.

The dynamics of the world developing on every level makes us realise that modern media mediatise our reality through complex technological and social processes. In other words, the weaponisation of information, using primarily new media as tools of articulation, is understood, in some simplistic terms, as a multifaceted set of practices through which people permanently reproduce individual and collective identities. Present-day functioning in the context of digital media is becoming increasingly important with the progressive commercialisation of the modern web. New media is not only a technology but also a set of market players with more and more powerful positions and specific objectives.

Conclusion

Non-military means of violence are becoming more and more important in supporting military action. Their arsenal consists of dysfunctional-disintegration activities in the informational, political, cultural, religious, economic or IT spheres. The main and all-time target of influence is human beings. Reckoning with the real threat, numerous states are setting up various agencies to fight it. Supranational consortia, which join the fight against disinformation, are trying to minimise its capabilities. Concerning Russia, which is fighting with Ukraine, some activities are undertaken to obstruct and condemn its actions in this regard. Civil companies such as Maxar Technologies, BlackSky and Planet, and the NGA agency are among those that are contributing to the efforts to reduce the intoxication of the information environment by making their satellites available. Thus, disinformation is immediately bared on an unprecedented scale. An example that condemns actions that distort the picture of reality is a UN Security Council statement. This document, signed by forty-five Member States including Poland, reads as follows: We condemn Russia for once again abusing its seat on the UN Security Council to spread disinformation. We reject Russia's continued efforts to distort history for its own political purposes and to promote hugely damaging false narratives and disinformation about neighbouring countries, including

by labelling others as „neo-fascists" and „neo-Nazis" without any basis[7]. Also noteworthy is the call, addressed to Russia in the last part of the document, to cease its hostile disinformation campaigns against Ukraine.

Bibliography

Darczewska J., *Środki aktywne. Rosyjski towar eksportowy*, „Punkt Widzenia" 2017, no. 64.

Wideorozmowa ze „współpracownikiem Nawalnego". Politycy z czterech krajów padli ofiarami deepfake'a, https://tvn24.pl/swiat/deepfake-ktos-podszyl-sie-pod-leonida-wolkowa-wspolpracownika-aleksieja-nawalnego-5076773 [access: 28.05.2021].

Matacz M., *Walka z deep-fake*, „Wiedza i Życie" 2021, no. 6.

Turek M., *Media Forensics (MerFor)*, http://www.darpa.mil/program/media-forensics [access: 12.12.2021].

Krajski S., *Masoneria polska 2021. Na skraju przepaści*, Warszawa 2021.

Gil K., *Raport. Jak działa rosyjska dezinformacja w aplikacji Telegram*, https://disinfodigest.pl/raport-jak-dziala-rosyjska-dezinformacja-w-aplikacji-telegram/ [access: 20.07.2022].

Rosja w rocznicę rzezi wołyńskiej oskarża Ukrainę na forum ONZ. Polska i 45 państw bojkotują posiedzenie, oprac. M. Zaremba, https://www.wprost.pl/polityka/10778995/rosja-w-rocznice-rzezi-wolynskiej-oskarza-ukraine-na-forum-onz-polska-i-45-panstw-bojkotuja-posiedzenie.html [access: 14.07.2022].

Narzędzia i techniki walki informacyjnej w kontekście operacji informacyjnych prowadzonych przez Federację Rosyjską podczas wojny w Ukrainie w 2022 roku

Streszczenie

W niniejszym artykule została podjęta próba zidentyfikowania narzędzi i technik wpływu społecznego w kontekście operacji informacyjnych prowadzonych przez Federację Rosyjską podczas wojny w Ukrainie w 2022 roku. Podjęcie analizy tworzenia i rozprzestrzeniania się zagrożeń informacyjnych w wyniku podejmowanych działań przez Rosję w trwającym konflikcie jest podyktowane coraz większym wpływem procesów komunikacyjnych na globalne bezpieczeństwo. Autorzy przedstawili wpływ i rolę mediów masowych na kształtowanie świadomości, odsłonili mechanizmy wpływania na opinię publiczną.

Słowa kluczowe: walka informacyjna, media, kreowanie opinii publicznej

7 *Rosja w rocznicę rzezi wołyńskiej oskarża Ukrainę na forum ONZ. Polska i 45 państw bojkotują posiedzenie*, oprac. M. Zaremba, https://www.wprost.pl/polityka/10778995/rosja-w-rocznice-rzezi-wolynskiej-oskarza-ukraine-na-forum-onz-polska-i-45-panstw-bojkotuja-posiedzenie.html [access: 14.07.2022].