ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

Publisher
http://jssidoi.org/esc/home

ON DISINFORMATION AS A HYBRID THREAT SPREAD THROUGH SOCIAL NETWORKS*

Radoslav Ivančík [1], Pavel Nečas [2]*

[1] *Academy of the Police Force, Department of Informatics and Management, Sklabinská 1, 835 17 Bratislava, Slovakia*
[2] *Matej Bel Univesity, Department of Security Studies, Kuzmányho 1, 974 01 Banská Bystrica, Slovakia*

E-mails:[1] *radoslav.ivancik@akademiapz.sk* ; [2*] *pavel.necas@umb.sk (Corresponding author)*

Received 25 April 2022; accepted 18 August 2022; published 30 September 2022

Abstract. Disinformation today poses a serious hybrid threat, the severity of which is exacerbated by the dynamic development and massive use of social networks. The development of the Internet, connectivity and information and communication technologies has caused that information are disseminated 24 hours a day, 7 days a week. In the history of mankind, it has never been easier to receive, search and spread. However, this progress has many positives and many negatives. In the avalanche of information that comes to us on a daily basis, it is undoubtedly very difficult to distinguish which information is true, objective, based on real events and, conversely, which information is misleading, distorted or completely fabricated, created in order to obtain economic, political or other profit. Many non-state actors, but also, unfortunately, state actors, have begun to use this fact to disseminate false information to advance their financial, political, or power interests. Information, resp. disinformation has become a weapon and social networks, which are an excellent tool for spreading disinformation in today's modern information society, have become a battleground for hostile hybrid activities performed on the target audience in the so called Gray zone between peace and war.

Keywords: Disinformation; sustainability; social networks; hybrid threats; Internet; technologies

Reference to this paper should be made as follows: Ivančík, R., Nečas, P. 2022. On disinformation as a hybrid threat spread through social networks. *Entrepreneurship and Sustainability Issues*, 10(1), 344-357. http://doi.org/10.9770/jesi.2022.10.1(18)

JEL Classifications: O33, Z00

Additional disciplines: information and communication; political sciences; sociology

1. Introduction

In the first two decades of the new millennium, the way of life and functioning of all areas of contemporary human society, from political, through social, economic, technological to security, has changed significantly in connection with the spread and increasing use of information and communication technologies. With the

* *This work was supported by the Agency for the Support of Research and Development on the basis of Contract no. APVV-20-0334.*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

constantly increasing “internetization” and “informatization” of society, rapid development, and massive use not only of technologies, but also of various information and communication systems, means and tools and the related dynamic advent of new media, a new range of options how to search, receive, create, and spread information has emerged. At the same time, however, a new, relatively wide range of opportunities have emerged, such as modern technology, tools, or the media, to misuse and disseminate misleading, false information through them in order to influence people's actions and make political, economic or other profits. The misuse of modern technologies, means, and media and the dissemination of such information thus poses a very dangerous threat, which may be part of hybrid threats, resp. part of a hybrid war.

The primary goal of the authors, using relevant methods of qualitative theoretical interdisciplinary scientific research (especially analytical-synthetic methods, qualitative, content and comparative analysis, methods of theoretical generalization of knowledge, as well as methods of document study and other research methods), is to contribute to a scientific and professional discussion on the issues of the dissemination of disinformation, as a tool for hybrid warfare and hybrid threats and the roles that social networks play.

2. Theoretical basis for the study of hybrid warfare and hybrid threats

The terms hybrid threats and hybrid warfare are the subject of several publications, studies, or articles in which foreign or domestic authors deal with hybrid threats or hybrid warfare in general or focus their individual aspects in their research. For this reason, it is possible to come across several definitions. One of them states *"the term hybrid threat refers to an activity carried out by state or non-state actors whose purpose is to undermine or damage a target by a combination of open and covert military and non-military means"* (Hybrid CoE, 2022:9).

Glenn defines hybrid threats as *"an enemy who simultaneously and adaptably uses various combinations of political, economic, social and information means as well as conventional, irregular, catastrophic, terrorist and subversive criminal methods of fighting"* (Glenn, 2009:2). According to Hoffman, *"hybrid threats include a range of conventional and unconventional ways of fighting and irregular tactics, as well as criminal and terrorist acts, which include unrestricted violence, coercion, social unrest and disruption"* (Hoffman, 2007:14).

Hybrid warfare can be understood as "a wide range of hostile activities in which the role of the military component is rather small, as political, informational, economic and psychological influence becomes the main means of waging war. Such methods help to achieve significant results: the territorial, political and economic losses of the enemy, the chaos and disruption of the system of exercise of state power and the weakening of the morale of society" (Manko & Mikhieiev, 2018). Hybrid warfare can also be understood as *"a set of lethal and non-lethal means that a state or non-state actor uses to assert his interests against the will of another actor. At the same time, hybrid warfare combines several methods of fighting: classic military operations, operations in cyberspace or cyber-attacks, espionage, dissemination of false information in order to influence the public opinion of the enemy, etc."* (Danyk et al., 2017:12).

Another definition states, *“A hybrid war is an armed conflict waged by a combination of non-military and military means in order to force the enemy to take steps that it would not take on its own. The state is at least one side of the conflict. Non-military means in the form of information and psychological operations, propaganda, economic sanctions, embargoes, criminal activities, terrorist activities and other subversive activities of a similar nature play a key role in achieving the objectives of the war. These activities are conducted against the whole society, especially against its political structures, state administration and self-government bodies, the state economy, the morality of the population and the armed forces"* (Kříž et al., 2015:8).

It can also be said that *“in the case of hybrid warfare, it is a way of waging a modern armed conflict. A conflict that does not begin with a shot and not with a declaration of war at all. The conflict that the attacked company*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

initially does not know has been attacked and is at war. It is a dynamic combination of military, political, diplomatic, economic, humanitarian, diverse, terrorist, and criminal activities carried out by state and non-state actors, regular and irregular formations, using propaganda and the implementation of information, cyber and psychological operations" (Ivančík, 2016:148)

In connection with the hybrid war, the information war is mentioned quite often. In her case, it is a general term encompassing several types of combat management, which have certain characteristics in common. As the name implies, the emphasis is on the information that is taken in this type of conflict (war) as a key element necessary to achieve victory. Different authors explain the concept of information warfare in different ways, and therefore, as in the case of hybrid warfare, in the case of information warfare, it is possible to meet with several definitions in the professional literature (Ivančík, 2021).

One of the most general and probably also the simplest and at the same time most frequently used definitions characterizes the information war as *"the struggle for control over the enemy's information activities and the effort to save their own"* (Bayer, 2006:36). Another, more comprehensive definition says: *"Information warfare is a wide range of activities whose tool or goal is information and information technology. These activities include, for example, the dissemination of disinformation, psychological operations, and cyber-attacks – disruption of communication networks and intrusion into them in order to obtain strategic information. These activities can take place in peacetime without having to prevent any conflict at all. The main goal of the information war is not to weaken the enemy from the outside, but to weaken, disorient and destabilize him from the inside"* (Halpin et al., 2006:79).

The information war is also understood as an ideological influence of the adversary, while a wide range of tools are used for this purpose, such as disinformation or propaganda, or diplomacy, military coercion, etc. It can therefore be characterized as a *"concept aimed at gaining information dominance"* (Ivančík, 2021:140). Information dominance is defined as *"the ability to gather, process, and disseminate information while exploiting or suppressing the adversary's efforts to do the same"* (US DoD, 2000:26). It is clear from the above definitions that information warfare is a narrower term than hybrid warfare.

3. Disinformation as a hybrid threat phenomenon

Disinformation, as follows from the above, is an integral part of hybrid threats, as the purpose of their use in hybrid war is to act on the enemy to weaken, disorient, destabilize, disrupt its political structures, the functioning of state and non-state bodies, its security, defence, economy, the ability to respond to threats, and to influence public opinion and morality of the population.

In close connection with the concept of disinformation, it is necessary to take a closer look at other concepts such as false news and propaganda. These two terms are quite often confused or used as synonyms in the public debate. Some authors consider false reports to be all reports that are not based on facts but are nevertheless published as truthful reports (Allcott & Gentzkow, 2017) or reports that deny the principles of quality and objective journalism (Baym, 2005). Other authors, in turn, distinguish between media that spread false news and so-called political media that regulate news in such a way that they try to set the political agenda of a related political party or movement (Vargo et al., 2017).

Silverman, on the other hand, claims that fake news is news that is not based on truth and is created mainly for financial gain. Motivation to make a profit is crucial, because in the absence of a financial motive, it is according to him propaganda (Silverman, 2016). Propaganda can then be characterized as the dissemination of false reports,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

which are not produced for the purpose of economic profit but are information that is to force them to think or act in a certain way. It is mostly associated with political, religious, or ideological goals.

The term disinformation covers both groups of false reports, whether it is the spread of propaganda or false reports published in order to attract the readers' attention and thus increase the profits from the sale of advertising (Andrassy & Grega, 2015; Korauš & Kelemen, 2018). The starting point is the definition of the concept of disinformation, prepared and presented by an independent group of experts for false reports and online disinformation. According to this expert group: *"Disinformation is all forms of false, fraudulent, untrue and misleading reports that are created, presented and disseminated with the intent to cause public damage or profit"* (European Commission, 2018a:10). However, this definition of the term does not include unintentional errors of information or political satire.

A similar definition can be found in the Short Dictionary of Hybrid Threats (2022:11) of the National Security Office of the Slovak Republic: *"Disinformation is verifiably false, misleading or manipulative information that is intentionally created, presented and disseminated with the unequivocal intent to deceive or mislead, cause harm or secure any profit (for example, economic or political). Disinformation often contains an element that is clearly true, which adds to its credibility and can thus complicate its detection. Disinformation does not include unintentional errors in news, satire, and parody, nor one-sided reports and comments, which are thus clearly marked."*

Other definitions found in the relevant dictionaries are also used quite often. For example, in the Oxford Dictionary (2021), disinformation is briefly defined as *"intentionally providing false information"*, in the Cambridge Dictionary (2021) as *"false information disseminated to deceive people"*, and in the MacMillan Dictionary (2021) as *"false information to persuade people to believe something that actually is not true"*.

Although information about disinformation appears in some media as a new security threat, this is not the case. Disinformation is not an achievement of the 21st century or today's information society. As early as the 6th century BC, Chinese general and thinker Sun Tzu[†] wrote in his Art of War about the strategy of indirect combat using lies and false, fraudulent reports. Textbook examples of the use of disinformation in practice can also be found in ancient Greece from the Greco-Persian wars, when, for example, the Athenian duke Temistocles defeated the Persian king Xerxes in some battles with the help of false messages sent from seemingly escaped slaves.

Another good example of the use of disinformation from ancient times can be the strategy used by the Mongol conqueror Genghis Khan. Before the attack, he sent spies into enemy territory, who infiltrated the population and spread false reports about the approaching huge and cruel Mongol army. In this way, he tried to weaken and demoralize the enemy in advance and gain an advantage. As confirmed, this tactic was successful as he was able to win multiple battles in which the enemy was outnumbered. Of course, the creation and spread of various disinformation has also been used successfully in other, well-known, or lesser-known wars and armed conflicts, including the two largest - in World War I and World War II.

What has changed in the first two decades of the third millennium is the means used to spread disinformation. With the development and increasing availability of the Internet and the closely related mass use of social networks, it is much easier to create and disseminate information that is tailored to individual users, as well as narratives in which events, facts and their interpretation are subject to a certain purpose (political, ideological,

[†] Sun Tzu (in the 6th century BC) was a Chinese general, philosopher, strategist, and tactician whose work The Art of War had a great influence on Eastern and Western military thinking, and many famous dukes were inspired by this work. He is still studied at many military academies. The general, also known as Master Sun, focuses on alternatives to battle, such as robbery, delay, the use of spies, lies and false, fraudulent information, or the creation and maintenance of alliances.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

religious, etc.), and are served to the public. Social networks have created a new space in which people form opinions about what is happening around them – about various events, personalities, processes, policies, etc. At the same time, it is a space in which it is relatively easy to give people various distorted, fabricated, untrue information or information taken out of context, and thus influence them in the desired direction.

The spread of disinformation is considered a hybrid security threat, mainly because it undermines citizens' trust in democratic institutions and processes and spreads a hateful ideology. Several authors agree that a large number of disinformation and disinformation websites present and spread especially right-wing ideology. We could observe this phenomenon, for example, in elections in several European countries, when disinformation sites in various countries supported far-right candidates and spread disinformation about their opponents, migrants, etc. In the Netherlands, it was Geert Wilders, in France Marine Le Pen, and in Germany, it was representatives of the Alternative for Germany party. From the point of view of the spread of violent propaganda, the dominant actor is primarily the Islamic State, which is extremely effective in spreading narratives on social networks (Prier, 2017).

An example of a state actor who uses disinformation extensively for his political purposes is Russia, for example in spreading disinformation in the context of the conflict in Ukraine (Danyk et al., 2017) or in spreading disinformation and propaganda in the Baltic countries and Scandinavia (Aro, 2016). Several mechanisms used by Russian propaganda are also relatively well mapped, either in influencing democratic processes in Western countries or in disseminating disinformation and using paid debates. The spread of Russian propaganda is a problem identified not only in individual European countries, but also at the level of the European Union ("EU") as a whole. According to the EU Strategic Communication Report, Russian propaganda concerns the spread of several meta-narratives in combination with conspiracy theories. According to the report, the underlying meta-narratives vary greatly over time, but the constant is the presentation of the West on the one hand as an aggressive and expansive entity, on the other hand as an entity on the verge of collapse. Russia Today and Sputnik are considered the most significant disseminators of disinformation. Local media networks and friendly think tanks in target countries are also used to spread disinformation (Kovanič, 2017).

Disinformation, as mentioned above, poses a hybrid security threat because it can affect democratic processes in countries. In the United States, several inquiries are still under way to clarify the role played by the spread of disinformation on social media in the 2016 and 2020 presidential elections. There are also reasonable suspicions that some of the UK population who voted to leave the EU did so on the basis of various false information disseminated primarily through social networks. The result of the referendum was close, 52% in favour and 48% against leaving the EU, so it can be assumed that false information played a very important, if not decisive, role. For example, it is proven that, among other politicians, the current Prime Minister Johnson or MEP Farage deceived their own people (TA3, 2017).

In addition, disinformation undermines the credibility of traditional information channels. Today, it is very easy to create a site that looks like a serious news server, but its real goal is to spread disinformation, either for the benefit of advertising or for political, ideological or religious reasons. Such websites often spread various conspiracy theories and do not follow the principles of serious journalism. By presenting themselves as credible media, they undermine people's trust in classic, serious news.

4. Development of disinformation spread

As mentioned above, the spread of disinformation is not a phenomenon that originated in the 21st century. In fact, this phenomenon is practically as old as humanity itself. However, what has changed dramatically is the way disinformation is spread. This is due to the already mentioned progress in the introduction and use of fast internet, the deepening informatization of society, the massive use of information and communication technologies, systems, and tools, and finally the fact that virtually every user has unrestricted access to information 24 hours a

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

day, 7 days of the week. However, this progress brings with it, in addition to many positives, also several negatives, such as those in the form of receiving and disseminating disinformation

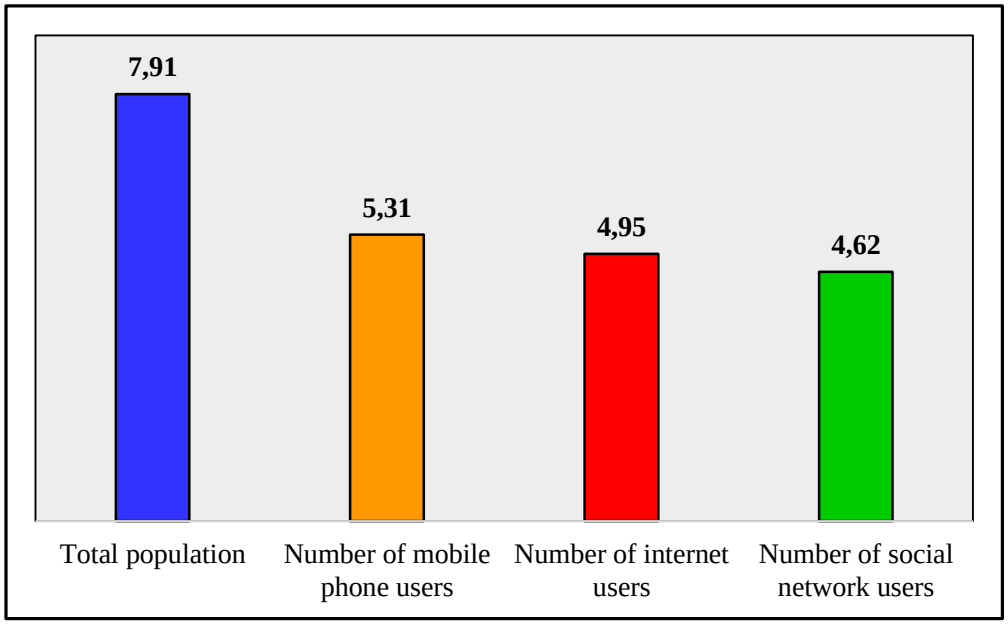

Figure 1. Overview of mobile phone, internet, and social network users in 2022 worldwide (in billions)
Source: DataReportal, 2022

The development of the Internet and the use of social networks, which are an excellent tool for disseminating, have a great deal of credit for the fact that disinformation is considered to be an increasing and more urgent security problem. Social networks bring together huge numbers of people from different parts of the world and allow them to communicate and exchange information with each other. Today, about 5.31 billion people use the mobile phone, representing more than two-thirds (67.1%) of the world's population, about 4.95 billion people use the Internet, more than three-fifths (62.5%) of the world's population, and active users of social networks amount to about 4.62 billion, which represents a share of the total population of the planet at 58.4% (Fig. 1). Up to 95% of their users use social networks via their mobile phones.

The dynamic growth of internet and social network users is evidenced by the fact that the number of internet users worldwide has increased by more than one third (36%) in the last five years. While in 2017 about 3.64 billion people used the Internet, in 2022 it was about 4.95 billion. The growth of social network users is even more dynamic, as it increased by almost two thirds (by 65.6%) in the evaluated years. While in 2017 about 2.79 billion people used social networks, in 2022 it is already about 4.62 billion (Fig. 2). Of these, one user spends an average of 2 hours and 27 minutes a day on social networks and uses an average of 7.5 different social networks per month (DataReportal, 2022).

The world's most popular social network is Facebook, which in January 2022 was used by about 2.91 billion active users, second is YouTube with 2.56 billion active users and third is WhatsApp, which is currently actively used by about two billion people. Other popular social networks that have more than one billion active users include Instagram, WeChat, TikTok and Messenger, and to the social networks with more than half a billion active users belong Douyin, QQ, Sina Weibo, Kuaishou, Snapchat and Telegram boast (Fig. 3).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

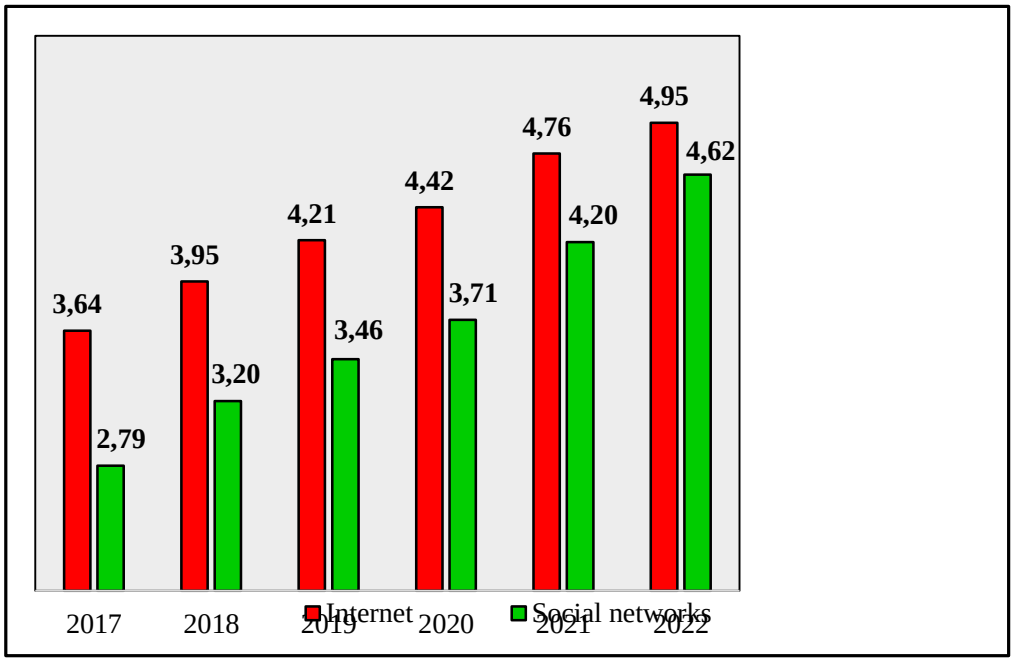

Figure 2. Overview of the growth of Internet and social network users in the years 2017 to 2022 (in billions)
Source: DataReportal, 2022

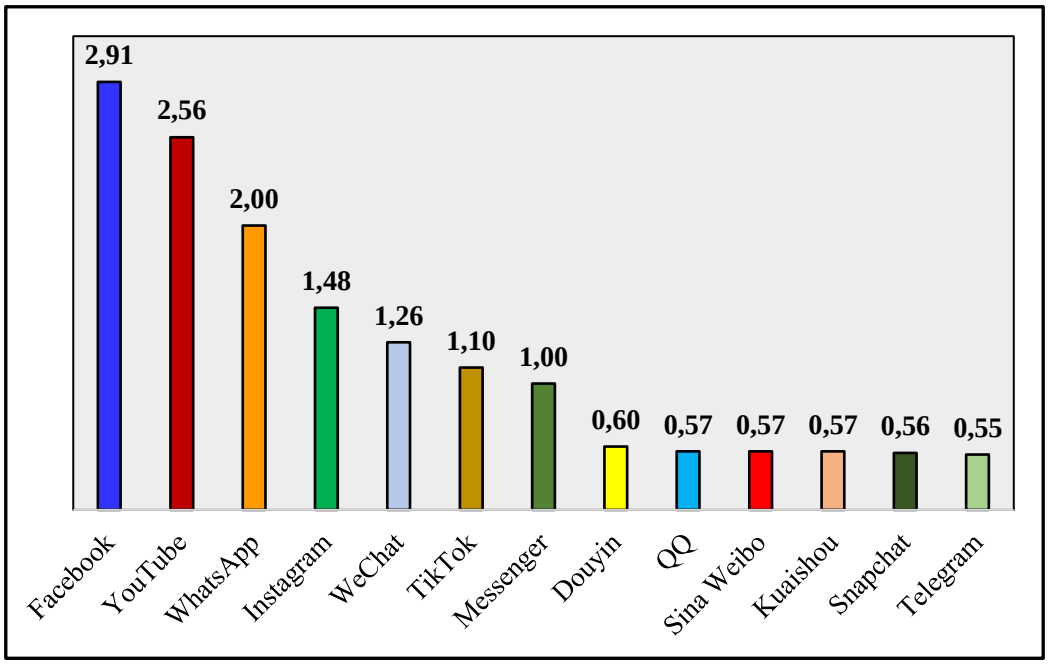

Figure 3. Overview of social networks with the largest number of active users in 2022 (in billions)
Source: DataReportal, 2022

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

The almost unlimited reach, combined with the high speed of information flow, low costs, and availability 24/7, creates ideal conditions for disinformation to spread virally (Bialy, 2017). Although traditional news media are still the primary source of information for most people, the fact that more and more people use social networks, especially as a source to follow new events in the world and at home, exacerbates the threat posed by the disinformation on social networks. In addition, social networks create social bubbles. This means that people tend to connect on social networks with people with a similar worldview, which in turn creates the so-called closed homophilic groups, where their individual members confirm each other in their opinions (Prier, 2017). As a result, people gradually lose sight of the wider context and think critically about the arguments used in such groups. The problem arises especially when disinformation begins to spread in the groups in question.

All the above factors have made social networks a tool for mobilizing, disseminating various narratives, conducting hybrid operations and, in some cases, even conducting combat operations in the real world. Both state and non-state actors are increasingly using social networks as a tool to influence the behaviour, attitudes, moods, and opinions of their target group. This trend is called the weaponization of social networks, which means that they are turning into a battlefield where the target group is attacked through disinformation (Bialy, 2017).

Social network users are often unaware of the risk involved and have full confidence in the online environment. They believe that when they control the circle of people who have access to their content, they also have control over the information that comes to them. Disinformation is most often spread through two social networks – Facebook and Twitter.

As mentioned above, Facebook is the largest and most popular social network in the world and is therefore the main target of virtually all disinformation campaigns. Unlike Twitter, Facebook is based on much more personal contact between users, because they themselves decide who becomes their friend and thus gain access to their content. Users then usually approach the information that their Facebook contacts disseminate uncritically, and since they consider it trustworthy, they usually do not verify this information further. Another way in which disinformation can reach a Facebook user is through posts published by various Facebook sites.

The user chooses them based on his own decision, usually when:
- the site clearly disseminates disinformation from the beginning, but the user sympathizes with this type of message and shares the site's views,
- the site initially produces neutral content that the user identifies with, decides to follow, but in the next phase the site begins to spread disinformation, in order to influence the attitudes, opinions and values of the user, who did not initially sympathize with this type of information (Biteniece et al., 2017).

The greatest credit for the dissemination of disinformation goes to those contributions which, thanks to the algorithm used, become viral. Facebook basically offers three operations options that can be used to wage a hybrid war:
- targeted collection of personal data of users[‡], which are later used to disseminate disinformation, the content of which is adapted to the user's preferences,
- content production,
- artificial distribution of content (usually done by machines, not real users).

Although Twitter is not as popular as Facebook, it currently has about 436 million active users (DataReportal, 2022), but it is still becoming one of the main targets, especially for political manipulation, as it is widely used

[‡] This was the case with the Cambridge Analytica scandal, which collected personal data from hundreds of thousands of users. Thanks to the data obtained, it was then able to personalize the content of the information she provided to the users. Cambridge Analytica provided data for political campaigns in various countries around the world. There are currently suspicions that this was not an isolated case, and that other state or non-state actors may be operating in this way (The Guardian, 2022).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

mainly by Western politicians, traditional media, and world thinkers. With a feature that allows you to track individual topics in the form of threads, it is becoming an increasingly common source of daily news for many people, especially in the United States and Western Europe. Unlike Facebook, Twitter offers less personal contact between individual users. In most cases, users who follow each other's content don't know each other personally, and the content they add to Twitter is less personal than Facebook.

The purpose of Twitter is primarily to publish opinions on individual topics. The length of one post is currently limited to 280 characters,[§] which automatically means that posts have the character of short statements. As the limited number of characters does not allow arguments to be developed and sources to support individual claims, such contributions do not give rise to caution to users; on the contrary, they consider them credible. The so-called trolls[**] and fake profiles in the form of boots[††]. The dissemination of disinformation most often takes place in such a way that a number of contributions are automatically generated for one specific topic, which will receive this topic in the so-called trends that are visible to all Twitter users (Biteniece et al., 2017).

5. Tools of disinformation dissemination

Disinformation is spread on social networks in several ways. Among the most used today are the use of:
- hybrid internet trolls,
- automatic boots with artificial intelligence,
- algorithms for creating so-called echo effect.

5.1 Use of hybrid internet trolls

One of the basic means for disseminating disinformation on social networks is the use of so-called Internet trolls that aim to spread or destroy a narrative. The operation of Internet trolls is not directly related to the development of social networks. The first cases of Internet trolls appeared in discussions on various websites and blogs before the emergence of social networks. Originally, it was about labelling users who were extremely aggressive in their views and hiding behind the anonymity that the Internet was already providing at the time Hannan (2018). These trolls were characterized by a very vulgar language.

Gradually, as social networks became more popular and became more and more weaponized[‡‡], the behaviour of trolls on social networks also changed. Some experts refer to such Internet trolls as hybrid trolls. In their case, they are a kind of fighters in the media, who are mostly hired by state or non-state actors who, in addition to spreading disinformation, spread the narratives of their employers (tenants) and, conversely, try to destroy the enemy's narrative. To this end, they produce a large number of contributions in which they use various manipulation techniques. Hybrid trolls are aggressive and often vulgarly insult their opponents, discouraging them and other readers or discussants who do not share the opinion of the trolls from further discussion (Aro, 2016).

[§] In one contribution, it was possible to write a text with a maximum of 140 characters before 2017. In 2017, a change came when the limit rose to 280 characters, but even such a range was not enough for many users. Therefore, Twitter has made it possible to split a longer post into several parts, which is displayed as a separate thread. It seems that soon it will be possible to post texts on Twitter without a limit on the number of characters. It will offer a new content format "Twitter Articles".

[**] A troll is an Internet user who, with his comments and behavior on the Internet, deliberately provokes others or distracts the discussion from the original topic (Short Dictionary of Hybrid Threats, 2022).

[††] A bot is a computer program that autonomously performs automated tasks on the Internet, e.g., simulation of human communication in communication with the customer (chatbot). Bot can be misused to spread messages on social networks, attacks on Internet services or increase the number of responses to a specific post - the so-called Likes (Short Dictionary of Hybrid Threats, 2022).

[‡‡] In the weaponization of the social network, the target group is attacked by hostile information, members of the target group are mobilized, and information operations are conducted in order to influence the behaviour, attitudes, moods and opinions of the target group (Short Dictionary of Hybrid Threats, 2022).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

Russia in particular uses hybrid internet trolls to spread disinformation. Ongoing investigations suggest that there is a headquarters in St. Petersburg, which is estimated to have about four hundred such hybrid trolls, whose main job is to conduct trolls on social networks. Former headquarters employees say that people take turns here in twelve-hour shifts and their monthly earnings are around a thousand US dollars. There are about twenty people working in one room, following well-defined scenarios and instructions. Each room is supervised by three editors who are authorized to impose fines if the set daily contribution limits are not reached, or the contributions are not governed by an established manual (Prier, 2017; Bialy, 2017; Aro, 2016).

5.2 Use of bots and artificial intelligence

The second, very often used tool for disseminating disinformation is the use of so-called bots (Bialy, 2017). Bot is something that pretends to be a real social user, but it's computer software that is programmed to automatically create and distribute some kind of posts at regular intervals. With these contributions, he then tries to flood the public space on social networks and thus promote his narrative. Bots try to behave like real people, so they often use artificial intelligence to imitate human behaviour. It is currently estimated that bots account for approximately 5 to 15% of all users on Twitter, with a similar ratio estimated for the largest social network Facebook, where bots account for about 5 to 11% of all users (Biteniece et al., 2017).

The use of bots was very popular, especially before the US presidential election in 2016. It is estimated that in the key period between spring and autumn 2016, up to 30% of all messages sent in the United States via social networks were not created by human users but by bots (Bialy, 2017). As indicated above, the bots are mainly used on Twitter and Facebook. According to research, up to 20% of contributions belonging to the Islamic State are automatically generated by bots. Even more worrying is the findings of the North Atlantic Alliance's Centre of Excellence for Strategic Communications.[§§] According to their reports, in Poland and the Baltic countries, up to 70% of all Russian-language contributions that talk about NATO are the work of boots (Biteniece et al., 2017).

5.3 Misuse of algorithms

The third relatively frequently used tool for disseminating disinformation is the misuse of algorithms that work on social networks. These are algorithms that recommend different posts to social network users based on their behaviour on the social network. They also consider posts posted by their acquaintances and posts read by users of sites and groups of which they are members. Algorithms push users that are viral, that reach a large number of shares, and so-called likes. This creates the so-called echo effect. Just one click on an article and the social network will automatically start offering other articles with similar topics to the user. That is, if a user clicks on a hoax or fake message once because of the article's title, the social network will automatically start subtracting other similar articles and posts. Also based on this aspect, disinformation actors try to focus on breath-taking and emotionally sensitive topics in order to force users to click on their message or post with a shocking headline. The algorithms used monitor all articles and contributions and based on this, evaluate the frequency of occurrence of

[§§] The Center of Excellence for Strategic Communications is a NATO-accredited international military organization that is not part of NATO's command structure and is not subordinate to any other NATO body. Based in Riga, Latvia, it contributes to improving strategic communication capabilities within the Alliance and Allied countries. Strategic communication is an integral part of the Alliance's political and military objectives, so it is increasingly important for the Alliance to communicate in an appropriate, timely, accurate and sensitive manner about its evolving tasks, objectives and missions. The Centre's mission is to make a concrete contribution to the strategic communication capabilities of NATO, NATO Allies and NATO Partners. Its strength is built by transnational and cross-sectoral actors from the civil and military, private and academic sectors and using modern technologies, virtual tools for analysis, research and decision-making. At the heart of NATO's StratCom COE is a diverse group of international experts with military, governmental and academic backgrounds - trainers, educators, analysts, and researchers. For more details see: NATO. 2022. NATO Center of Excellence for Strategic Communications, 2022

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

individual words. The ones with the highest frequency are then marked as trends, which are displayed to all users Prier, 2017). The combined efforts of trolls, boots and users are used to create trends. By artificially and collectively distributing a large number of posts, the algorithms are able to evaluate that the topic is popular among users and then automatically offer the posts to other users.

Conclusions

Social networks are one of the most dynamically developing communication and information platforms. Over the course of a few years, they have undergone many significant changes. From small, scattered local community websites, they have evolved to consolidated companies with global reach and influence. Social networks have also been part of the leap into the world of mobile technologies, which have a huge impact on human behaviour, including patterns of social network use. Over time, users' motivations to engage in social media discussions have also changed. The initial, purely "social" motivation was gradually replaced by other motivations, such as the search for information, the provision of which brought social platforms much closer to the traditional media. In this information environment, a dramatic change has gradually taken place, which can be called the weaponization of social networks, which means the transformation of social networks into a battlefield in which hostile hybrid activities take place on the target audience in the Gray zone[***] between peace and war.

Due to their exceptional characteristics, such as global reach, high availability, low costs, huge volume and speed of information exchange, and to some extent the anonymity of users, social networks are attractive to several actors with hostile agendas. Paradoxically, what was a great advantage became a visible weakness. Platforms, which were born "social", have become the site of a large number of activities that are clearly anti-social in nature. Therefore, in our opinion, it is justified to call social networks a battleground in which there is an intense struggle for people's hearts and minds. It is a battlefield where you can observe various military and non-military strategies and tactics and the use of tools such as disinformation, propaganda, false reports, conspiracy theories, threats against opponents, mobilization of supporters, coordination of actions and activities, etc. The dynamic development of technology plays an important role here, making all these activities simpler and more efficient. Robots and various applications help or even replace human actors to a large extent, and content (news, information) is becoming more and more attractive due to the development of multimedia.

In this context, the question arises as to what the democratic world can take, what measures it can take to deal effectively and efficiently with hostile activities on social networks and hybrid threats in general, as adversaries do not follow the same legal rules and ethical principles as democratic societies and do not share democratic values. Moreover, while adversaries are cunning, fast, flexible, and adaptable given the specific nature of their organizations and their establishment, democratic countries, and institutions are obliged to follow specific procedures with lengthy decision-making processes. Social networks, as it turns out, are therefore a very powerful and effective tool for manipulating the population on a mass scale. Their current mass use facilitates the dissemination of disinformation to state and non-state actors more than ever before. That is why it is very important not only to continue research in this area, but to deepen it even more. The achieved research results should contribute to the impossibility to use, resp. to abuse social networks as a hybrid weapon to influence people's thinking and behaviour and to jeopardize the democratic processes taking place in developed democracies.

[***] The Gray zone is an area where hybrid warfare is taking place, taking advantage of the ambiguity of national and international law. These are activities of one state that are detrimental to another state, but legally they are not acts of war. This is the so-called acts below the border of armed conflict (Short Dictionary of Hybrid Threats, 2022).

References:

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31 (2), 211-236. https://doi.org/10.3386/w23089

Andrassy, V., & Grega, M. (2015). Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. *Košická bezpečnostná revue*, 5 (2), 11-18. ISSN 1338-4880.

Aro, J. (2016). The Cyberspace War: Propaganda and Trolling as Warfare Tools. *European View*, 15(1), 121-132. http://dx.doi.org/10.1007/s12290-016-0395-5

Bayer, M. (2006). Strategic Information Warfare: An introduction. *Cyberwar, Netwar and the Revolution in Military Affairs*, 32-48. https://doi.org/10.1057/9780230625839_3

Baym, G. (2005). The daily show: discursive integration and the reinvention of political journalism. *Political Communication*, 22 (3), 259–276. https://doi.org/10.1080/10584600591006492

Bennett, L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33 (2), 122-139. http://dx.doi.org/10.1177/0267323118760317

Biały, B. (2017). Social Media - From Social Exchange to Battlefield. *The Cyber Defense Review*, 2 (2), 69-90. Retrieved May 9, 2022, from https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Social%20Media%20From%20Social%20Exchange_Bialy.pdf?ver=2018-07-31-093711-437

Biteniece, N., Bertolin, G., Agarwal, N., Bandeli, K. K., & Sedova, K. (2017). *Digital Hydra: Security Implications of False Information Online*. Riga: NATO Strategic Communications Centre of Excellence

Cambridge Dictionary. (2021). Disinformation. Retrieved May 6, 2022, from https://dictionary.cambridge.org/dictionary/english/disinformation

Davison, W. P. (1971). Some Trends in International Propaganda. *The Annals of the American Academy of Political and Social Science*, 1-13. https://doi.org/10.1177/000271627139800102

DataReportal. (2022). Global Digital Overview. Retrieved May 15, 2022, from https://datareportal.com/reports/digital-2021-global-overview-report

European Commission. (2018). Final report of the High-Level Expert Group on Fake News and Online Disinformation. Brussels: European Commission. Retrieved May 12, 2022, from https://www.ecsite.eu/activities-and-services/resources/final-report-high-level-expert-group-fake-news-and-online

European Parliament. (2016). Report on EU strategic communication to counteract propaganda against it by third parties. In *European Parliament*. Brussels: European Commission. Retrieved May 12, 2022, from https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html

European Union External Action. (2021). *Questions and Answers about the East StratCom Task Force*. Brussels: European Union External Action. Retrieved May 12, 2022, from https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

Glenn, R. W. (2009). Thoughts on Hybrid Conflict. *Small Wars Journal*. Retrieved May 13, 2022, from https://www.smallwarsjournal.com/blog/188-glenn.pdf

Griscioli, G. (2016). *Intelligence. The Hybrid War*. Roma: Aracne

Halpin, E., Trevorrow, P., Webb, D., & Wright, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs*. London: Palgrave McMillan https://doi.org/10.1057/9780230625839

Hannan, J. (2018). Trolling ourselves to death? Social media and post-truth politics. *European Journal of Communication*, 33(2), 214-226. http://dx.doi.org/10.1177/0267323118760323

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies*, Retrieved May 8, 2022, from https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hybrid Centre of Excellence. (2022). Hybrid Threats. Retrieved May 8, 2022, from https://www.hybridcoe.fi/hybrid-threats/

Ivančík, R. (2016). Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. *Medzinárodné vzťahy*, 14(2), 130-156. Retrieved May 3, 2022, from https://fmv.euba.sk/www_write/files/dokumenty/veda-vyskum/medzinarodne-vztahy/archiv/2016/2/mv_2016_2_130-156_ivancik.pdf

Ivančík, R. (2021). Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. *Politické vedy*, 24(1), 135-152. https://doi.org/10.24040/politickevedy.2021.24.1.135-152

Jurčák, V. (2020). Súčasné pohľady na definovanie pojmov hybridná hrozba a hybridná vojna. *Hodnoty trestného práva, kriminalistiky, kriminológie, forenzných a bezpečnostných vied v teórii a praxis*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 753-769.

Korauš, A., & Kelemen P. (2018). Protection of persons and property in terms of cybersecurity. *Ekonomické, politické a právne otázky medzinárodných vzťahov*, 18(1), 234-244. Retrieved May 7, 2022, from https://fmv.euba.sk/www_write/files/Virt_zborník.pdf

Kovanič, M. (2017). Dezinformácie a ruská propaganda ako bezpečnostné hrozby. *Bezpečnostní teorie a praxe*, 2,121-132. ISSN 1801-8211.

Krátky slovník hybridných hrozieb. (2022). *Dezinformácia*. Retrieved May 6, 2022, from https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html

MacMillan Dictionary. (2021). *Disinformation*. Retrieved May 6, 2022, from https://www.macmillandictionary.com/dictionary/british/disinformation

Manko, O., & Mikhieiev, Y. (2018). Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. Connections. *Information & Security: An International Journal*, 41, 11-20. https://doi.org/10.11610/isij.4107

Miller, M. (2015). *Hybrid Warfare: Preparing for Future Conflict*. Montgomery: Air War College https://doi.org/10.21236/ADA618902

NATO. (2022). *NATO Strategic Communications Centre of Excellence*. Retrieved May 8, 2022, from https://connections-qj.org/article/defining-concept-hybrid-warfare-based-analysis-russias-aggression-against-ukraine https://www.stratcomcoe.org/about-strategic-communications

Oxford Learner´s Dictionary. (2021). *Disinformation*. Retrieved May 6, 2022, from https://www.oxfordlearnersdictionaries.com/definition/english/disinformation?q=disinformation

Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11 (4), 50-85. Retrieved May 9, 2022, from https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf

Silverman, C. (2016). This analysis shows how viral fake election news stories outperformed real news on Facebook. *BuzzFeed.News* Retrieved May 10, 2022, from https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

The Guardian. (2022). *The Cambridge Analaytica Files*. Retrieved May 10, 2022 from https://www.theguardian.com/news/series/cambridge-analytica-files

US DoD. (2000). *United States Department of Defense: Joint Vision 2020*. Washington: United States Government Printing Office. May 12, 2022, from https://www.hsdl.org/?abstract&did=446826

Vargo, C. J., & Guo, L., & Amazeen, M. A. (2017). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*, 20 (5), 2028-2049. http://dx.doi.org/10.1177/1461444817712086

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 1 (September)
http://doi.org/10.9770/jesi.2022.10.1(18)

Funding: This work was supported by the Agency for the Support of Research and Development on the basis of Contract no. APVV-20-0334.

Author Contributions: The authors contributed equally; they have read and agreed to the published version of the manuscript.

Radoslav IVANČÍK
ORCID ID: 0000-0003-2233-1014

Pavel NEČAS
ORCID ID: 0000-0001-7743-0453