Countering fake information as a guarantee of state information security

Andrii V. Svintsytskyi · Oleksandr H. Semeniuk · Olena S. Ufimtseva · Yurii B. Irkha · Serhii V. Suslin

Accepted: 22 June 2022 / Published online: 23 July 2022
© The Author(s), under exclusive licence to Springer Nature Limited 2022

Abstract
The article focuses on the notion of fake information as a tool of psychological influence in the context of hybrid wars. Works of the prominent academicians in the area of manipulation studies constitute the theoretical framework of this research. Empirical research methods such as observation, comparison, generalization and expert evaluation are used. First of all, types and methods of psychological influences used by mass media and social networks with a view to manipulate public opinions are distinguished. Moreover, the impact of emotions on the critical perception of the news is highlighted. The indicators of manipulative influence are defined in order to resist them. Besides, the ways of creating and distributing false information are described. In addition, the development of fakes identification mechanisms is considered a priority for the governmental and other public institutions. This is illustrated by a range of technologies developed to automatically detect fake news. Apart from that, the degrees of the information reliability are explored. Furthermore, structural elements of fake messages, which include the source and the message itself, are discussed. Misinformation of the public, promotion of certain opinions, encouragement of aggressive actions and instalment of doubts are singled out as the main tasks of fake information. Additionally, stages of countering fakes are distinguished. Finally, the specific features of the forensic expertise procedure are determined in order to provide information security in Ukraine. The research demonstrates the importance of an efficient security system, which would identify fake information and limit its propagation.

Keywords Fake information · Manipulation · Propaganda · Hybrid war · Forensic expertise
Introduction

In modern society, all spheres of life operate on the basis of a developed information structure. The security of the state, society and person in today’s conditions directly depends on the quality of the national information resource. That is why fake information, penetrating into all spheres of life, causes significant damage to their interests, provokes conflicts and generally undermines public confidence in government. The spread of unreliable information in order to mislead the enemy dates back to ancient times. A prominent Chinese strategist and thinker, Sun Tzu (Forbes 2014), wrote: “War is a way of deception. Therefore, even if you are capable, show your opponent your incapability. When you have to put your forces into battle, go inactive. When the goal is close, show it as far; when it is really far away, give the impression that it is close”.

At one time, Napoleon Bonaparte was a master of disinformation, which he skilfully used through the press to achieve his military goals. “Four newspapers can do more harm to the enemy than an army of a hundred thousand” (Timofeev 2007) is the catchphrase of the French emperor. At the same time, Napoleon perfectly understood the delicacy of publishing false information, which must have its own logic, rhythm and look as reliable as possible. In a letter from Fouché in November 1808, he made recommendations for the use of the press in the field of disinformation: “It should be well done, it should be allegedly the result of a common opinion, go from all sides and be the work of a dozen of well-combined articles in different newspapers” (Timofeev 2007).

Many modern methods and techniques of propaganda were developed by the Nazis during World War II. Thus, the Minister of Public Education and Propaganda of the Third Reich (1933–1945) Joseph Goebbels is credited with the following quote: “Propaganda should affect the senses more than the mind” (Reuters 2020), and therefore be bright and visible. Indeed, the greater the emotional colour of the message, the better it will achieve its goal. In addition, emotions interfere with the intellectual analysis of the news. Thus, another quote is worth mentioning: “so that the crowd has no doubts, the ‘messages’ should be primitive, without details, at the level of an unequivocal slogan: the worst enemy of propaganda is intellectualism” (Reuters 2020). In modern conditions, the dissemination of false information has acquired new methods and techniques. First of all, this is due to globalization and open access to modern information technologies that provide social communication of the general population and the dissemination of information among them. For example, in social networks, messenger channels, news websites and more.

Information technology has given a person a real opportunity not only to “read, see and hear”, but also to be “read, seen and heard”. Virtually everyone who has a smartphone, Internet access, an account on social networks has the opportunity not only to consume, but also to generate, modify, create and distribute information in unlimited quantities. However, fakes are increasingly becoming an instrument of information and psychological influence on the enemy during the so-called “hybrid wars”, when it is necessary to replace the objective ideas of the
target population about the nature of the conflict with those “information phan-
toms” needed by the aggressor. For example, the Open Source Communications, Analytics Research (OSCAR) Development Centre at Cardiff University prepared a report according to which Russia uses trolls to comment the articles on the websites of the British and American media. British scientists revealed almost 250 cases. In addition, they noted that the “opinions” of these trolls are used to form a distorted picture through the Russian media. In other words, the Russian media presents the statement of the troll of “Russian origin” under the publication in the Western media with the title of his or her own article, and therefore, it already takes the form of the official opinion of the Western media. For example, there is a news article in Russian with a certain bias, which claims that “the British think X or Y” and points to broad support for Russian policy by Western citizens (Corera 2021).

There is a much larger scale of the spread of Russian fakes in Ukraine. This is quite natural, given the Russian-Ukrainian military confrontation. At the same time, despite a certain destructive impact of Russia’s information and psychological operations against Ukraine even before the armed conflict and their intensification during the war, the Ukrainian authorities have only recently begun considering this problem seriously. Given that Russia is currently waging an information war not only against Ukraine, but also against the EU, Great Britain, and the United States, creating an effective system to counter fakes is an important task for the entire progressive world. For example, on December 8, The Times reported that several hundred fake accounts created on behalf of the “yellow vest” movement called for the forcible overthrow of President of France Emmanuel Macron. According to the newspaper, these accounts were registered in Russia (Blakely 2018). In addition, an information attack by Kremlin bots on France was reported by Bloomberg in a publication dated December 8 (updated December 9). In the last week, the focus of about 600 accounts on Twitter, promoting pro-Kremlin views, turned out to be protests of "yellow vests", writes Bloomberg (Matlack and Williams 2018).

On January 6, 2021, during the seizure of the Capitol building in the United States, false information about the illegitimacy of the US presidential election calls to storm the parliament building, while organized and instructed groups of people were spread on social networks. In particular, Renee DiResta, a researcher at the Stanford Internet Observatory, which studies online communities, claims that the violence that day was the result of online movements operating on closed social networks, where people believed allegations of vote rigging and election theft from Mr. Trump (Frenkel 2021). The main role was played by the social network Parler (Munn 2021). In August 2021, protests against Covid-19 restrictions took place near the Lithuanian Seimas. At the same time, fake messages were spread on social networks and in certain media, claiming that the protests were “speeches based on the migrant crisis” (DELFI 2021; Information resistance 2021).

These examples show that the main purpose of fake messages is to sow doubt and convince the audience of the truth of the information provided. Their task is to misinform the population; to promote one’s own vision of the situation; shake the position of the individual and make him doubt; to encourage certain aggressive actions; to convince the audience using fictional facts, etc. At the same time, fake
recognition requires sophisticated tools that the average consumer does not have. Given the rapid pace of such disinformation attacks and the danger they pose to the information sovereignty of the state, it is extremely important to form a powerful and effective information security system, conduct research in this area and develop a strategic concept and tactics to combat information threats. And the development of tools and mechanisms that will identify fake information and limit its dissemination should be a priority for public authorities and non-governmental institutions.

Research methods are chosen by taking into account the goals and objectives of the scientific article. In particular, the process of data collection for this scientific work was carried out in the most authoritative international scientometric databases Scopus and Web of Science using Google search engine and publicly available application software. With the help of bibliographic and abstract databases, scientific publications by scientists from different countries, who studied the problems of detecting fakes and developing tools to combat them, were collected and analysed. The data were downloaded from public Internet pages and can be accessed by every user. The study used methods of qualitative analysis; in particular, qualitative thematic analysis was used to interpret the data collected from textual sources. Empirical research methods (observation, comparison, generalization and expert evaluation) were also used.

The notion of manipulative influence: its indicators, types and methods

The authors reviewed the literature on the research topic, which included the most famous and authoritative scientific works. It should be noted that topical issues of detecting fake information in the media, assessing the impact of such messages on social network users and developing tools to counter the spread of inaccurate information in the global media space have been studied by both domestic and foreign scientists. In particular, the essence of manipulative influence on people’s consciousness with the help of the media was studied Pocheptsov (2015), Bard and Soderqvist (2004), Sheinov (2006), Schiller (1980). The essence of the phenomenon of “fake news” as a kind of misinformation is noted by Gelfert (2018). However, in his opinion, there are also important specific differences between misinformation and fakes.

An article by scientists at Nanyang Technological University of Singapore (Tandoc et al. 2018) outlines a typology of fake news. Based on a review of 34 academic articles that used the term between 2003 and 2017, the authors defined six ways to identify fake news in previous research as follows: news satire, news parody, news fiction, photo manipulation, advertising, public relations and propaganda (Tandoc et al. 2018). Scholars Allcott and Gentzkow (2017) presented a modern view on the impact of social media and fake news on the 2016 US presidential election. The authors discuss the role of fake news in Donald Trump’s election. The article proposes a model of the fake news media market, presents data on the distribution of fake news and its detection on the eve of the election, as well as the impact on voter turnout and other factors, including segregation on social networks and people’s ability to recognize false news (Allcott and Gentzkow 2017).
A significant contribution to the study of the problem of detecting fakes is a scientific paper (Conroy et al. 2015) entitled “Automatic fraud detection: methods of finding fake news”. This article provides an overview of modern technologies that facilitate the search and detection of fake news and “a typology of several types of methods for assessing truthfulness, which fall into two main categories—approaches of a linguistic cue (with machine learning) and approaches to network analysis, and offers an innovative hybrid approach that combines linguistic cue and machine learning with networked behaviour data” (Conroy et al. 2015). It is worth mentioning the publication of Spanish experts (Figueira and Oliveira 2017) on the available technical capabilities of automatic detection of fake news by using technologies in the form of algorithms (text mining, machine learning, etc.), equipment for working with big data, access to big data for learning algorithms. The authors note that suddenly all major companies such as Amazon, IBM, Google, Facebook, Twitter, Baidu, Yahoo and Microsoft made their code open and accessible to everyone. For example, Google provided the use of part of its own technology Deep Learning TensorFlow AI free of charge for commercial customers (Figueira and Oliveira 2017). According to a scientist from Croatia (Biloš 2019), the term “fake news” is often defined as a deliberate presentation of false or misleading statements in order to manipulate the cognitive processes of the audience. The author’s article is based on the approach of meta-analysis and description of the current state of scientific research on the phenomenon of fake news in the context of disinformation activities on the Internet (Biloš 2019).

According to research by Massachusetts Institute of Technology experts who studied more than 126,000 fake news (published on Twitter between 2006 and 2017), fake news spreads six times faster than “real” information from reliable sources. In addition, for fake news, the probability of reposts is 70% higher (Vosoughi et al. 2018). It should be noted that during the study of the results of scientific research and analytical materials, it was concluded that fakes are used as an effective means of manipulating public consciousness. Therefore, such manipulative influence is characterized by the following indicators: (a) it is carried out purposefully and covertly; (b) contains algorithms for programming both thinking and perception of reality by the object and its behaviour; (c) includes methods and techniques by which it has a purposeful effect on the human psyche. The information flows permeated with fakes fall on the mass consciousness, depriving the consumer of mass media of the opportunity to process them qualitatively, leaving him or her only a passive role, which becomes a prerequisite for manipulative influence.

Countering fakes, as one of the independent varieties and at the same time components of information and psychological operations (hereinafter—IPsO), is a multifaceted process. The purpose of the IPsO is psychological influence—active purposeful activity to obtain the necessary information or change the psyche or behaviour of the object (individual or group of people). Purposefulness presupposes that the subject of influence has a certain goal and is aware of it, and his actions are guided by the idea of what the object of influence should become, how his behaviour should change. Otherwise, the result of applying one method or another becomes unpredictable (Sopilko 2021).
Psychological influence is not a homogeneous phenomenon; it is of different types and can be exercised by different methods. Usually the following types of psychological influence are singled out. Informational and psychological influence (it is also called information-propaganda, ideological), is the influence by means of words, information, which main purpose is to form certain ideological (social) ideas, views, ideas, beliefs, and at the same time it causes positive or negative emotions, feelings and even violent psychological reactions in large social groups or masses of people. Psychogenic effects, which may be the result of physical influence on the brain of an individual, resulting in a violation of normal neuropsychological activity (for example, a person suffers a brain injury, as a result of which he loses the ability to think rationally, memory loss, etc.; or it is affected by factors such as sound, lighting, temperature and other factors that change his psyche due to certain physiological reactions), or the shocking impact of environmental conditions or events (such as pictures of mass destruction, numerous casualties, etc.) on human consciousness, resulting in person’s inability to act rationally, experiencing affect or depression, panicking, etc. (Sheinov 2006).

Psychoanalytic (psychocorrectional) effect is the impact on the human subconscious by therapeutic means, especially in a state of hypnosis or deep sleep. Neurolinguistic influence (neurolinguistic programming) is a type of psychological influence that changes people’s motivation by introducing special linguistic programmes into their consciousness. It is possible to compose messages texts in the media in such a way and in such a form (content) that they cause certain reactions of the psyche and behaviour of people. Psychotropic effects involve the use of drugs, chemicals or biological substances to affect the psyche of people in order to achieve changes in their behaviour. Some of the main methods of psychological influence are the following (Irkha 2021):

(1) Persuasion. It is carried out in verbal form and is based on logic, while the influence on feelings and emotions is of secondary importance. Both parties are active, i.e. the process of persuasion is an explicit or implicit discussion, the purpose of which is to achieve the unity of opinion.

(2) Suggestion. As one of the parties is active, the other must take what is said as critically as possible. Suggestion is unproven and unsubstantiated, thus, the person who carries it out (authority, prestige, etc.) is of great importance. It is carried out in a categorical verbal form. The lack of time and mental state of the object of influence is crucial.

(3) Infection. Psychological influence on the personality in the process of communication and interaction, which conveys certain moods, motivations not through consciousness and intellect, but through the emotional sphere. This is an influence based on the unconscious tendency of people (especially in a group) to emotional influence in condition of a direct contact. A mass way of integrating group activities arises in large crowds of people such as in stadiums, concert halls, rallies.

(4) Manipulation. Hidden influence, the fact of which should not be noticed by the object of manipulation. The success of manipulation is guaranteed when the object of manipulation believes that everything happens naturally and inevitably.
(5) Fashion. A form of standardized mass behaviour of people that occurs spontaneously under the influence of moods, tastes, hobbies that dominate society. Its features include the fact that it is manifested in all spheres of public life, economics, politics, art, life, sports, and so on.

(6) Rumours. Reports from one or more people about unconfirmed events. As a rule, they concern the phenomena important for a certain social group or person, affect the needs and interests relevant to them. The expectation of satisfying the need for information is the main motive for the perception and reproduction of what is heard.

During the IPsO, the information disseminated can be of varying degrees of reliability, from completely fake to completely true. Usually, completely fictional news is constructed in such a way that it is difficult to verify (that is, there is no choice, but to "take the bare word"), or the time of its "life" will be relatively short. Partially fake information is more durable. In this case, some of the facts do take place, but others do not. For example, a news item refers to an actually existing official document, but the content of that document in the news item is distorted. Sometimes the IPsO provides completely truthful information, but the emotional emphasis is on only one part of it (Sopilko 2021).

For example, in October 2021, the Armed Forces of Ukraine for the first time used the Bayraktar UAV to destroy the D-30 howitzer of illegal military formations in the east of the country. “From 2:25 pm to 3:15 pm, a battery of D-30 howitzers of the Russian terrorist forces fired at the positions of the Joint Forces near the settlement of Granitne. The General Staff reported that two servicemen of the Armed Forces of Ukraine were wounded during the shelling, one of them was killed” (Donik 2021). It was on one of these howitzers that the Bayraktar UAV missile was fired. Commenting on the described incident, the Russian media focussed on Ukraine’s use of UAVs as the violation of Minsk agreements. At the same time, the howitzer battery fire on the positions of the Armed Forces, which is also a violation of the Minsk agreements and which led to the use of the Bayraktar UAV, is not mentioned at all (Shestak 2021).

Quite true and undistorted information can also be disseminated during the IPsO. Most often, this applies to compromising information. The publication of compromising material in the media, on social networks or in any other way can significantly shake the positions of those involved in compromising events. The spread of fake news as a form of IPsO can have several types of psychological impact at the same time. First of all, this is informational and psychological influence, because the main content of fake news is information. Informational and psychological influence is often accompanied by psychogenic impact as a consequence of the shock effect on the human consciousness of the events described in the fake news. Under the influence of shock, a person’s consciousness largely loses the ability to think rationally and critically perceive a fake. Neurolinguistic influence is also possible, but its effectiveness looks much less (Pocheptsov 2015). As for the choice of methods of influence, this largely depends on the target audience. What matters is, first of all, awareness of the problem, the ability to think critically, the degree of trust in the source of information, etc.
Structural elements of fake information

Researching fake messages, the following structural elements can be distinguished: the source of false information and the message itself, which in turn contains information and emotional components (Nizovtsev 2021). Let’s take a closer look at these elements. Thus, the first element is a source of false information. Most often this is a so-called bot—a fake (i.e. not related to a real person) account with a fictional avatar (i.e. someone else’s photo or a neutral plot is captured on the avatar—a cat, a dog, a flower, etc.), on whose behalf certain messages are published. Bots spread fake information through Internet resources (social networks, micro-blogging services, etc.). Usually the bot writes the right comments at the right time under the right post, but sometimes it publishes certain fake news itself. From a technical point of view, such a fake account on social networks can be managed by a program, which is usually also called a bot—abbreviated from “robot”. In addition, a fake account or multiple accounts can be managed simultaneously by a person—a troll or a bots’ owner. It is clear that the activity of a fake account under human control is the most effective. On the other hand, quality work requires resources (especially time), which limits the number of such bots. As a result, a combination of software-controlled bots and human-controlled bots (troll) is usually used. In this case, the troll usually posts fake news, and software bots do a simpler job, such as commenting and “liking”.

Single boots are a rather rare phenomenon. As a rule, a significant number of bots are used simultaneously. The computer complex that manages them is called a bot farm. The basis of the bot farm is specialized software that can be installed on a desktop computer or laptop. This program automatically supports authorization (receives SMS messages or incoming calls and transmits this information as intended), generates messages from pre-formed templates and publishes them in the appropriate comments. To connect SIM cards, authorizing accounts via SMS messages is required. So, a so-called SIM bank is usually used—a specialized device that allows to simultaneously connect a significant number of SIM cards (for example, “GoIP SMB128” supports simultaneous connection to 128 SIM cards, and “OpenVox Simbank-320”—in accordance with 320 SIM cards). Digital emulation of previously read SIM cards can also be used. In addition, telephone numbers can be rented temporarily. Apart from that, even third-party online services can be used for authorization (Bard and Soderqvist 2004).

It should be noted that bots are actively used not only for destructive effects by spreading fakes. They have both neutral and even quite useful business functions. Generally, there are 4 types of bots in the sphere of social bots’ owner (Shalama 2021). The first type is social bots in e-commerce, that is, bots sales managers. Identifying features: styling under the service of its owner. As a rule, no one hides them. The second type is SEO-bots, likers and re-posters. Identifying features are a huge number of groups, subscriptions, reposts and a complete lack of personal information. The third type is multi-day bots. Identifying features: an active link to a third-party service in the profile or on the user wall with the note: “I rarely visit here, look for me by the link”. The fourth type is political bots.
Countering fake information as a guarantee of state information

Trolls and thoughts leaders. Identifying features: not clearly expressed, maximum correspondence to the real account. Typically, such bots are connected to communication systems and can respond to messages in one sentence.

Quite a significant spread of bots and bot farms is due to their effectiveness, because it is difficult for one person to resist the collective opinion, while the “collective” opinion is formed by bots. The outstanding psychologist S. Asch proved this in his studies back in the middle of the last century. In 1951, he conducted a series of experiments aimed at investigating the influence of the group on the behaviour of an individual. During the experiment, 8 participants had to compare the lengths of the segments of different lengths depicted on the cards. At the same time, only one out of eight was subject, the other seven were “false”, deliberately giving the wrong answer. As a result, three quarters of the subjects, despite what they saw with their own eyes, at least once gave a deliberately incorrect answer, if it was chosen by the whole group. A quarter of the subjects consistently agreed with a false answer. Consequently, the individual is more likely to agree with the opinion of the group (especially if the opinion is unanimous), even if the wrong of this opinion is obvious (Asch 1951).

Bots work in a similar way. By massively commenting on a certain post on social networks and putting “likes” under these comments, bots create the impression of total dissatisfaction with the published information. Conversely, when one bot publishes fake news, other bots with their comments and “likes” try to convince the reader of the correctness and truthfulness of the information. In addition to anonymous bots, fake news can be spread by real people such as journalists, public activists or even officials. In some cases, this is the deliberate distribution of fakes, in others, it is the retransmission of unverified information, without the intention of deliberately spreading fakes. Using a real person to spread a fake has both advantages and disadvantages. On the one hand, such a person is usually quite famous or even popular (the so-called “thought leader”). So, her opinion will be listened to. Additionally, communication is more effective, which, unlike bots on social networks, can also include video calls and even live feedback.

Therefore, the efficiency of such a fake information delivery channel will usually be higher than the efficiency of bots. Nevertheless, the systematic promotion of outright fakes can quickly reduce a person’s authority to the level of a regular bot. All this determines certain features of the use of real people to spread fakes, which can be conditionally represented in two ways. The first is that the speaker is obviously in opposition to the pro-government group. He or she does not hide it, but on the contrary, regularly demonstrates, having a steady circle of listeners who also adhere to opposition views and who are its target audience. These listeners are the second link in the spread of fakes, spreading them among their acquaintances, including pro-government ones. In the second case, the speaker pretends to be objective of opinions and views, or even tries to pass himself off as “his own” among the pro-government circle of persons. In general, it follows the general paradigm of the pro-government group. Fake information is voiced infrequently and carefully so as not to lose confidence. Such speakers are most valuable because they are perceived as their own, have authority and their opinions are listened to. However, such speakers are used with caution so as not to harm their authority.
Fake information is often spread unintentionally. Desiring to raise the rating of popularity, some mass media or individuals (politicians, public figures, etc.) without resorting to verification of the received information try to publish it as soon as possible. And the more “sensational” the fake news will look, the more likely it is that they will want to publish it quickly, thus attracting attention. One of the most effective sources of fake information dissemination is the mass media. In some cases, certain media are generally used to disseminate false information (of course, false information is presented among the truth, otherwise the trust of readers will fall sharply). In others, false information is published by some unscrupulous journalists whose publication has not been verified. In this case, the country of origin of the media may be important. For example, the average reader is usually more trusted by the media of their own country or one of the leading democracies, as it seems that democracy and freedom of speech ensure the objectivity of the publication (although, as we see, this is not always the case). That is why the intelligence agencies of some authoritarian countries have recently been trying to use some Mass Medias of democratic countries to disseminate fake information beneficial to them (Novikovas et al. 2017).

The next fake element under consideration is the fake message itself. The message can also be divided into two components, which are informational and emotional. It is not enough to simply publish a false text. This text should impress the target audience quite emotionally. It is the significant emotional load that ensures the spread of fakes and a significant social reaction to them. The more intense a person’s emotions, the less his ability to adequately analyse the news and understand its falsity; instead, the desire to share the news with relatives increases significantly, and thus, the probability that a person will spread fake news among acquaintances increases (Pocheptsov 2015). Other people, having received this fake news not just from the news, but from an acquaintance, will usually trust this false information more. And again they will spread the fake further, already among their acquaintances. There is a kind of chain reaction. Of course, some people will immediately understand that this is fake news. But you need to consider the percentage of trust and the target audience. The vast majority of fakes are designed for people who will not be able to detect their falsity (due to ignorance, poor understanding of the issue, etc.).

They usually try to make the informational component believable, because this strengthens the credibility of the news. Fake news can be based on real events, but conclusions about the causes and/or consequences of them are obviously wrong. For example, the following technique can be applied (Schiller 1980). A pseudo-journalist, describing a certain event, brings his own (false) conclusions, after which he invites the audience to watch the video of the event and draw their own conclusions. At the same time, even having watched the video on their own, not every person is able to draw adequate conclusions. First, a person may be incompetent in the issue. Secondly, she will be pressured by the authority of the journalist, because schematically the emotional load of the message looks like this: “I am a journalist. I’m smart. I know the subject. I explained everything to you on my fingers. Now see for yourself and draw conclusions. If your conclusions coincide with mine, you are as smart a person as I am. If they don’t match, you’re a fool who doesn’t understand basic
things”. Thus, a significant number of audiences may agree with the pseudo-journalist’s false conclusions.

Often fakes are supported by various special operations of support which are called to create an occasion for fakes and/or to confirm them as if truthfulness. One of the most famous examples is the so-called “picture of Yarosh” during the 2014 presidential election in Ukraine. During the cyberattack, criminals broke into some of the servers of the Central Election Commission and posted images of the results of the vote count, where Dmytro Yarosh allegedly received the largest number of votes (over 37%). Then, this picture was shown on the Russian TV channel “ORT”.

However, not only cyberattacks can be accompanied by throwing fakes. Unfortunately, the shelling of civilians in the Donetsk and Luhansk regions of Ukraine by Russian troops and pro-Russian separatists has already become commonplace, followed by accusations of these shelling on the Ukrainian military. Also, often to create fakes, not special operations of the support are used, but real facts, which are significantly distorted at the same time. For example, on April 2, 2021, in the village of Oleksandrivske in the temporarily occupied territory, a child born in 2016 found a mine in the garage. The mine exploded, the child died on the spot. Russian media immediately brought charges against the Ukrainian Armed Forces, which allegedly dropped a bomb from a UAV on purpose (Stop Fake 2021; Strizhova 2021).

The stages of countering fakes and capabilities of forensic expertise in fakes prevention

An important point is the purpose of the fake. As mentioned, the purpose of fakes is almost always destructive (Holovkin et al. 2021). However, the directions of destructive impact can be different. For example, it can be an inducement of public opinion in a certain direction. Or simply the build-up of the situation in the country, provoking conflicts between different groups of the population on a political, religious, national basis, etc. Besides, the final consumer of fakes in general can be a third party, for example, in order to form a negative impression of a certain country among the world community. Taking into account the complex nature of fakes, it is quite natural that countering them is also a complex process. The following stages of countering fakes can be distinguished:

– fake search—usually involves viewing (monitoring) of social networks and mass media;
– detection of fakes—identification of knowingly false information directed against the security of the state, society or individual person;
– analysis of fake information—research of information on the subject of its origin, drawing up a portrait of the author, identification of the author, definition of the target audience, delineation of harmful influence (vector of information attack), etc.
– analysis of the source of the fake—the study of the profile of a social network, mass “disinformation”, etc. for their attitude to the aggressor country or other
entities hostile to Ukraine, the establishment of the constituent data of the person who manages the profile on the social network, etc.

– response—refutation of fake information, the introduction of a ban on the entry of certain foreigners into Ukraine, the introduction of sanctions against the media, etc.

In some cases, it is possible to prevent fakes. If intelligence or analytical information indicates a high probability of throwing fakes on a certain topic, it is possible to wonder about the possibility of such fakes in advance and inform the target audience about the real situation. It is clear that all the described actions must take place within the framework of international and national legislation in the field of information. As it can be observed, countering fakes is a complicated, complex process. Each stage has its own characteristics and different entities have different degrees of effectiveness at these stages. For example, finding and detecting fakes will be much more difficult without public involvement. At the same time, the establishment of the constituent data of the present person, who manages the profile in the social network and the termination of the “bot farm” activity, is the prerogative of the intelligence agencies and law enforcement agencies (Novikovas et al. 2017).

Let us consider the capabilities of forensic expertise in the framework of countering the adversary’s IPs0. Thus, the most effective can be the expert’s special knowledge in the analysis of fake information and its source. Consequently, the first considered element of fakes is their source. In this case, the bot or bot farm is usually assigned a computer and telecommunications expertise. The telecommunication equipment of the bot farm as well as computer equipment (desktop PCs, laptops, tablets and smartphones) is examined. Setting the mark/model of equipment allows you to prove the possibility of using equipment for controlling bots.

Research of information carriers can reveal information on bot management, as well as information on correspondence with the customer about specific actions of the bot farm (for example, the scenario of a fake and its distribution tactics), prove the connection between the customer and the executor. The second element of fakes, as already mentioned, is the message itself. By linguistic analysis of its content, it is possible to determine whether the message contains calls for illegal actions, to make an approximate portrait of the author or to identify the author. Psychological and psychological-linguistic analysis of the text can determine what actions the message motivates (if it does not contain direct appeals) or what attitude and to whom/what it forms in the reader. You can also set the target audience to fake, and so on. If the fake information contains an edited sound recording or a photo image edited in a graphic editor, the expertise may reveal signs of editing (Parfylo 2021).

Depending on what security operations are performed to reinforce the fakes, various expert studies may be appropriate. In the case of a cyberattack, it is, first of all, a telecommunication expertise, because its subject includes detecting the signs of a cyberattack, determining the source of this attack, establishing the facts of access to computer systems, etc. (Holovkin et al. 2021). In the event of a shelling, it is necessary to establish the direction and approximate location from which the shooting took place. It should be noted that the possibilities of forensic expertise can be useful not only at the stage but also within the framework of pre-trial investigation.
Forensic experts and specialists in this area can provide significant assistance in the course of technical and forensic support of pre-trial investigation of crimes in the field of information security. For example, a solid argumentation of the untruthfulness of a fake message and its origin from an aggressor country can be used both in the investigation itself and in countering fakes by informing the population about their nature and origin.

**Conclusion**

Summing up the above, it is possible to state that countering fakes is a complex process that is impossible without the involvement of both state institutions (including intelligence services) and the public. Forensic experts also do not stand aside and are ready to help both with special knowledge and special expert equipment. It is increasingly difficult to distinguish true information from fake information, even for professionals, so it is necessary to use all means of identification, and study foreign experience in countering fakes, combining efforts at both international and national levels. Undoubtedly, the use of artificial intelligence greatly simplifies the detection and blocking of fake information, but the development and implementation of new and better legislation to regulate the media is also important. The first positive steps have already been taken to disseminate and conduct activities to teach media literacy and critical thinking of the population of Ukraine, such as online distance learning courses, educational projects, educational games to test knowledge and skills, specialized publications and online manuals. Only educated citizens with critical thinking skills are able to resist the spread and influence of fake information.

In some cases, the spread of fakes is part of the tactics when conducting hybrid wars, because the spread of rumours, disinformation and manipulation have long been one of the ways to covertly influence the enemy. The formation of favourable narratives among the population of a "hostile" country, demoralization of the population, an increase in the number of radical citizens, including extremists and terrorists, is one of the most effective ways to win in geopolitical, civilizational or interstate confrontations, especially in the era of the information society. As the study showed, the strategy of countering fakes, first of all, should contain proactive behaviour, that is, preventing the possibility of the formation of disinformation and fake messages.

Countering disinformation and manipulative information is aimed primarily at preventing, effectively identifying information threats, responding to them, and preventing such threats to the state and society. As already mentioned, the linguistic expertise of the text is important in identifying fake information, as establishing the fake nature of the statements of the author of the disputed text allows assessing his or her argument and submitting to the court material that determines the need to verify the facts. The detection of fakes on the basis of certain features (markers) of the text is only one of the stages of fact-checking as a procedure of checking the text for the accuracy of information.

One of the means of counteracting the spread of fakes can be a kind of "quarantine" for the most doubtful information messages. For instance, a delay in
publication. At the same time, it is necessary to maintain a balance between information security of the state and freedom of speech, the right of citizens to information, in particular, to access it quickly. The creation of a system for countering fake information is a huge complex work of both the state, society and each individual citizen, consisting of developing critical thinking, the ability to correctly search and analyse information, introducing new forms and methods for identifying fake information and developing ways to minimize its impact. It is this ability to resist information and psychological operations, including those related to the spread of fakes, that society (its technical, intellectual, moral and ethical, political development) should achieve. In this case, external information influences will not be crucial in making decisions aimed at ensuring the interests of human and society, while protection from them will be one of the most important guarantees of state information security.

Author contributions Authors’ contributions are equal.

Funding The authors did not receive support from any organization for the submitted work. No funding was received to assist with the preparation of this manuscript. No funding was received for conducting this study. No funds, grants, or other support were received.

Data availability Data will be available on request.

Declarations

Conflict of interest The authors declare they have no financial and competing interests.

Ethical approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Consent to participate Informed consent was obtained from all individual participants included in the study.

Consent for publication All individual participants agreed to be included in the study.

References

Allcott, H., and M. Gentzkow. 2017. Social media and fake news in the 2016 election. Journal of Economic Perspectives 31 (2): 211–236.
Asch, S.E. 1951. Effects of group pressure upon the modification and distortion of judgments. In Groups, Leadership and Men; Research in Human Relations, 177–190. Pittsburgh: Carnegie Press.
Bard, A., and J. Soderqvist. 2004. Netocracy: The new power elite and life after capitalism. St. Petersburg: Stockholm School of Economics in St. Petersburg.
Biloš, A. 2019. Emerging focus on fake news issues in scientific research: a preliminary meta-analysis approach. In Interdisciplinary Management Research XV, 1139–1150. Osijek: Faculty of Economics in Osijek, Hochschule Pforzheim University.
Blakely, R. 2018. Russian accounts fuel French outrage online. The Times. https://www.thetimes.co.uk/article/russian-accounts-fuel-protesters-outrage-online-xx2f2g8th Accessed 18 Feb 2022.
Countering fake information as a guarantee of state information...

Conroy, N.K., V.L. Rubin, and Y. Chen. 2015. Automatic deception detection: Methods for finding fake news. *Proceedings of the Association for Information Science and Technology* 52 (1): 1–4. https://doi.org/10.1002/pra2.145052010082.

Corera, G. 2021. Pro-Kremlin trolls target news website comments, researchers say. *BBC News*. https://www.bbc.com/uk-news-58441662, Accessed 18 Feb 2022.

DELFI. 2021. Fake: the protest outside the Seimas was caused by Lithuania’s migration policy. https://www.delfi.lt/ru/detektor-lzhi/tozh/fejk-protest-u-sejma-vyzvala-migracionnaya-politika-lityvy.d?id=87943849, Accessed 18 Feb 2022.

Donik, R. 2021. Ukrainian troops used Bayraktar in Donbas for the first time. *BBC News Ukraine*. https://www.bbc.com/ukrainian/news-59055022, Accessed 18 Feb 2022.

Figueira, A., and L. Oliveira. 2017. The current state of fake news: Challenges and opportunities. *Procedia Computer Science* 121: 817–825. https://doi.org/10.1016/j.procs.2017.11.106.

Forbes. 2014. Sun Tzu’s 31 best pieces of leadership advice. https://www.forbes.com/sites/ericjackson/2014/05/23/sun-tzus-33-best-pieces-of-leadership-advice/?sh=16976a525e5e, Accessed 18 Feb 2022.

Frenkel, Sh. 2021. The storming of Capitol Hill was organized on social media. *The New York Times*. https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html, Accessed 18 Feb 2022.

Gelfert, A. 2018. Fake news: A definition. *Informal Logic* 38 (1): 84–117.

Holovkin, B.M., O.V. Tavolzhanskyi, and O.V. Lysodyed. 2021. Corruption as a cybersecurity threat in the new world order. *Connections: the Quarterly Journal* 20 (2): 75–87.

Information Resistance. 2021. Migration crisis on the Belarusian border: a blogger clarified the current situation. https://sprottyv.info/analitica/migracionnyj-krizis-na-granice-belarusi-blogger-poyasnil-tekushuju-situaciju, Accessed 18 Feb 2022.

Irkha, Yu. 2021. The influence of fakes on the emergence and spread of extremism. In *Anti-fake measures as an integral part of the information security of the state: Interdepartmental round table*, 47–51. Kyiv: Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine.

Matlack, C., and R. Williams. 2018. France to probe possible Russian influence on yellow vest riots. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage, Accessed 18 Feb 2022.

Munn, L. 2021. More than a mob: Parler as preparatory media for the U.S. Capitol storming. First Monday 26 (3). https://journals.uic.edu/ojs/index.php/fm/article/view/11574, Accessed 18 Feb 2022.

Nizovtsev, Y. 2021. The capabilities of forensic expertise in the context of anti-fake measures in Ukraine. In *Anti-fake measures in Ukraine as an integral part of the information security of the state: Interdepartmental round table*, 43–47. Kyiv: Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine.

Novikovas, A., L. Novikoviene, R. Shapoval, and K. Solntseva. 2017. The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues* 7 (2): 369–380.

Parfylo, N. 2021. The negative influence of fake information on the society and effective methods of counteraction. In *Anti-fake measures in Ukraine as an integral part of the information security of the state: Interdepartmental round table*, 87–91. Kyiv: Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine.

Pochepstov, H. 2015. *Modern information wars*. Kyiv: Kyiv Mohyla Academy Publishing House.

Reuters. 2020. Fact check: Joseph Goebbels misquote on “converting intellectuals” resurfaces. https://www.reuters.com/article/uk-factcheck-joseph-goebbels-misquote-co-idUSKBN2492TD, Accessed 18 Feb 2022.

Schiller, H.I. 1980. *The mind managers*. Moscow: Mysl.

Shalamai, A. 2021. Bots around us: Everything you wanted to know about bots and their habitat. https://www.umn.com.ua/uk/publication/1924205-boti-navkolo-nas-vse-scho-vi-khotili-znati-pro-botiv-tareal-yikhnoogo-poshirennnya, Accessed 18 Feb 2022.

Sheinov, V.P. 2006. *Disguised control over a person*. Minsk: Harvest.

Shestak, E. 2021. Lavrov incriminated Ukraine in the desire to show “coolness” in Donbas. *Look Business Newspaper*. https://vz.ru/news/2021/11/1/1127055.html, Accessed 18 Feb 2022.

Sopilko, I. 2021. Information security as an object of regulation in the law of Ukraine. *Journal of International Legal Communication* 1 (1): 11–22. https://doi.org/10.32612/uw.27201643.2021.1.pp.11-22.
Stop Fake. 2021. Fake: A child died in Donbas as a result of a Ukrainian drone attack. https://www.stopfake.org/en/fake-a-child-died-in-donbas-as-a-result-of-a-ukrainian-drone-attack/. Accessed 18 Feb 2022.

Strizhova, O. 2021. A child’s death in Donbas: Could this be a Ukrainian UAV? Radio Svoboda. https://www.radiosvoboda.org/a/death-child-donbas/31188059.html. Accessed 18 Feb 2022.

Tandoc, E.C., Jr., Zh.W. Lim, and R. Ling. 2018. Defining “fake news”: A typology of scholarly definitions. Digital Journalism 6 (2): 137–153. https://doi.org/10.1080/21670811.2017.1360143.

Timofeev, V.I. 2007. Napoleon I issued “victorious bulletins” and intentionally published false information. Military-Historic Journal 11: 27–32.

Vosoughi, S., D. Roy, and S. Aral. 2018. The spread of true and false news online. Science 359 (6380): 1146–1151. https://doi.org/10.1126/science.aap9559.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Andrii V. Svintsytskyi1 · Oleksandr H. Semeniuk2 · Olena S. Ufimtseva3 · Yurii B. Irkha4 · Serhii V. Suslin5

Oleksandr H. Semeniuk semeniuk8228@edu.cn.ua

Olena S. Ufimtseva ufimtseva8228@neu.com.de

Yurii B. Irkha irkha8228@sci-univ.com

Serhii V. Suslin suslin8228@edu-knu.com

1 Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, 3 Mykoly Vasylenka Str., Kyiv 03113, Ukraine

2 Interagency Scientific and Research Center on Problems of Combating Organized Crime Under the National Security and Defense Council of Ukraine, 1 Solomyanska Sq., Kyiv 03035, Ukraine

3 Scientific and Organizational Center, National Academy of the Security Service of Ukraine, 22 Mykhaila Maksymovycha Str., Kyiv 03066, Ukraine

4 Research Department, State Research Institute of the Ministry of Internal Affairs of Ukraine, 4A Yevhena Gutsala Lane, Kyiv 01011, Ukraine

5 Department of General Legal Disciplines, National Academy of the Security Service of Ukraine, 22 Mykhaila Maksymovycha Str., Kyiv 03066, Ukraine