

---

# Security and Credibility of Information about Wartime Conflicts on the Internet

Vesna Simović<sup>1</sup>, Žaklina Spalević<sup>2</sup> and Bojan Prlinčević<sup>3</sup>

<sup>1</sup>Academy of Applied Studies of Kosovo and Metohija, Department  
Leposavić, Serbia

<sup>2</sup>Singidunum University, Belgrade, Serbia  
Faculty of Tourism and Hotel Management

<sup>3</sup>Academy of Applied Studies of Kosovo and Metohija,  
Department Zvečan, Serbia

## Article Information\*

Review Article • UDC: 355.48:004.738.5

Volume: 21, Issue: 2, pages: 151–175

Received: May 17, 2024 • Accepted: June 20, 2024

<https://doi.org/10.51738/Kpolisa2024.21.2r.151ssp>

## Author Note

Vesna Simović  <https://orcid.org/0009-0001-1271-1841>

Žaklina Spalević  <https://orcid.org/0000-0001-8502-2038>

Bojan Prlinčević  <https://orcid.org/0000-0003-2951-2184>

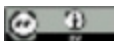
We have no known conflicts of interest to disclose

Corresponding author: Žaklina Spalević

E-mail: [zspalevic@singidunum.ac.rs](mailto:zspalevic@singidunum.ac.rs)

---

\* Cite (APA): Simović, V., Spalević, Ž., and Prlinčević, B. (2024). Security and Credibility of Information about Wartime Conflicts on the Internet. *Kultura polisa*, 21(2), 151–175, <https://doi.org/10.51738/Kpolisa2024.21.2r.151ssp>



© 2024 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

### **Abstract**

The complex dynamics of information that is constantly being marketed in the modern digital age lead to an excessive amount of information of questionable accuracy and credibility. Fake news, misleading information, rumors and satire take precedence over instinctive information, especially in the domain of information about war conflicts, which are rapidly losing their credibility. This social phenomenon is labeled as an information disorder. War conflicts in the modern era are taking on a new form, we are introduced to the term hybrid war, which, in addition to physical battles, is also realized through the struggle for control over information systems. Information warfare is aimed at achieving control over the consciousness of the people of a country, especially through the distribution of false and misleading news, and as a countermeasure, the services of "fact-checkers" organizations can be used. We look at information warfare and the distribution of fake news through the prism of the latest war conflicts between Israel and Hamas in the Gaza Strip.

*Keywords:* information, fake news, information disorder, hybrid war, Fact-Checker.

## **Security and credibility of information about war conflicts on the Internet**

For more than twenty years, many researchers have analyzed various aspects of the Internet's impact on human life and society. This may indicate that from its inception, the Internet was recognized as such a powerful phenomenon that it could become decisive for many spheres of life and work of the modern human. (Bjelajac & Filipović, 2020). We live in an era of digital transformation in which the Internet plays a key role in information and communication, both between individuals and between businesses and states. The ubiquitous use of the Internet, however, also brings us various challenges regarding the security and reliability of the information we receive in this way. It is especially important that we pay attention to the credibility of information coming from war-affected areas because war events, political tensions and military operations are reflected and transmitted through electronic media. In this way, the way is opened for manipulation, misinformation and the spread of false information.

The aim of this paper is to investigate the security and credibility of information about war conflicts on the Internet with special reference to the challenges in the modern information environment. When analyzing the wide spread of digital platforms in the transmission of information, we will pay special attention to the mechanisms that contribute to data security and the preservation of data integrity during wartime conflicts.

In this paper, we investigate how different parties in conflicts use the Internet as a tool for manipulating public opinion, spreading propaganda, and creating disinformation. At the same time, the role of new technologies such as artificial intelligence and deep learning in the creation of sophisticated forms of disinformation is considered.

We will also analyze the effectiveness of existing information protection mechanisms on the Internet, as well as technological innovations that can be applied in order to improve information security. This work aims to contribute to a better understanding and a more effective coping with the challenges brought by the digitization

of information about war conflicts in the context of security and credibility on the Internet.

### **The digital age and the challenges it brings**

The digital age is an era in which digital information technology is a key driver of social, economic and cultural change. This period is marked by the rapid development and use of digital technologies through the process of digital transformation, which deeply affects the way of life of people and organizations. Digital transformation represents a comprehensive process of applying digital technologies in various aspects of society, economy and everyday life. Digital transformation is terminologically used to explain or describe social changes that take place under the influence of new technologies, as well as how these changes as a whole have an impact on the operations of companies and the work of public services. (Celik, 2019)

Digital transformation has brought changes at all social levels and in all economic fields, so that it encouraged not only leaders and large companies, but also the whole world to think differently. Thanks to social media and the exchange of ideas made possible by their use, even the areas of political and social freedoms have gained a new dimension. The Internet and social networks are powerful weapons for shaping thoughts and ideas, but also for communication, so there is almost no person who does not have an account on one of the popular networks and does not use the Internet. (USAID)

In the digital age, information is readily available through the Internet, mobile devices, and other digital media. Technologies such as computers, smartphones, the Internet of Things (IoT), artificial intelligence (AI) and blockchain play a key role in shaping everyday life. Communication takes place through social networks, email and other digital channels, facilitating global connectivity.

Given the amount and flow of information, information has actually turned out to be the most important and sought-after resource in the modern business context. That's why we can conclude that the basic factor of digital transformation is the information itself that is marketed through the media.

Digitization of the media and their exponential growth has led to such a rapid flow of information that it is impossible to check how accurate and true they are and with what motive they were published. The Internet was originally conceived as a network that would allow the dissemination of information, ideas and opinions regardless of borders and without the influence of any government. However, over time the Internet changed its shape, when it became apparent that freedom of expression had turned into its own opposite. Individuals, as well as different groups, political, extremist, and all others, began to understand this freedom literally, in the sense of the impossibility of anyone preventing them from expressing their views and opinions in a way that can be offensive to other members of society. This led to the appearance of hate speech, the strengthening of extremist attitudes and insults on various grounds (national, religious, ethnic, etc.), which mean a violation of one's value system and strengthens intolerance. (Vučković, 2021)

However, in 2016, in the election campaign for the American president, journalists went a step further. They used the freedom of speech in order to spread fake news as a combination of untrue, inaccurate and incomplete information. This was not an isolated case, the results of the vote for "Brexit" in Great Britain as well as the canceled national election results in Kenya led to the conclusion that this phenomenon directly affects democracies in various countries of the world. The amount of fake news such as misleading information, fake reviews, fake advertisements, rumours, false political statements, satires and so on, which have been presented as authentic has increased dramatically, which has led to the need for very serious scientific analyzes of this phenomenon. (Sukhodolov & Bychkova, 2017). This phenomenon is defined in the Council of Europe Report from 2017 as an information disorder with the aim of introducing some kind of regulation of information that is marketed via the Internet and social networks as the most active and massive channels of communication today. (Wardle & Derakhshan, 2017)

Wardle and Derakhshan (2017) introduced a new division of false information to their report using as a measure the amount of

harm and lies they bring. So they divided the information that leads to information disorder into three groups (Figure 1):

- Mis-information – it is false information, but it does not cause harm, such as an unintentional mistake by a journalist,
- Dis-information – this is false information that is knowingly shared with the aim of harming someone (an individual, a social group or the state), and
- Mal-information – this is true information that is shared to cause harm to someone, usually by sharing private information publicly.

As society as a whole has come to a situation where fake news is now more popular and spreads faster through social media than mainstream media (Balmas, 2014), fake news has become the main concern of both the industry and the scientific community with the goal of building an effective system to detect fake news. In order to do this, we must first get to know the characteristics of fake news.

Zhang and Ghorbani (2020) say that every fake news has (Figure 2):

- The volume or spread of fake news because there are many websites that are deliberately set up to market fake news and stories, such as: denverguardian.com, wtoe5news.com, ABCnews.com.co, etc.
- Variety, fake news can be in the form of rumours, satirical news, fake reviews, misinformation, fake advertisements, conspiracy theories, false statements by politicians, etc.
- Speed, fake news tends to spread very quickly because most of such news is focused on current events and hot affairs to easily grab the attention of online users.

Detection and identification of fake news on networks is very difficult because it spreads very quickly, it is complicated to estimate how many online users are involved in a certain part of a current message, and it is also difficult to say when and how the far-reaching consequences of fake news stop.

## **War conflicts in the Internet environment**

Digitization as a process of transition from analog to digital technologies has brought changes in various spheres of society, so the military area is not left out of it either. It is manifested through the integration of high-tech digital systems, artificial intelligence and information technologies in military operations. These advanced technological elements enable faster exchange of information, more precise analyzes and more efficient conduct of war operations. Also, digitalization enables military forces to operate more effectively in the domain of cyber warfare, where the fight for control over information systems is being waged. Therefore, the way of warfare has gone through significant transformations, under the influence of technological progress, globalization and changes in the geopolitical environment.

"In the 21st century, war does not have to start with an armed attack, but with a series of hostile activities designed to weaken the state. Strategic futurists speculated that it could be a computer attack from an unidentified source, a projected economic crisis or even a pandemic" (Mandić, 2016).

Forms of conflict that have moved into the information space are becoming a key field of struggle. They include propaganda, disinformation, psychological warfare via social media as major parts of warfare strategies, and as such bring new concepts to war terminology. The concepts of special, hybrid, information warfare are concepts that arose at the end of the 20th and the beginning of the 21st century.

By trying to look at the diversity of emerging terms, researchers have offered different perspectives, thereby significantly enriching the discussion of the field. Although it is a relatively new term, its definition is often confusing, imprecise and leaves numerous dilemmas. (Subotic, 2018).

Rančić and Beriša (2018) determined that the term "hybrid war" contains different meanings, starting from cyber war, information war, various scenarios of asymmetric conflicts of low intensity, via global

terrorism, piracy, illegal immigration, corruption, ethnic and religious conflicts, transnational organized crime, up to the systematic economic collapse of states with the aim of creating demographic changes and the application of weapons of mass unification.

The use of a new name for today's wars and aggressions, by politicians and military officials, affects a better perception by public opinion, which is always important for approval and agreement with certain decisions of state authorities. The term hybrid war is useful from the point of view of state officials because, on the one hand, it elevates the issue in the eyes of the public, and on the other, it enables security structures to more comprehensively and responsibly plan and develop responses in crisis situations. (Cvetković et al., 2019)

The hybrid model of warfare is based on avoiding the declaration of war, which avoids both state responsibility and the influence of international law. It uses conventional capabilities, irregular tactics and formations, terrorist and criminal acts, which aim to achieve a common result of the physical and psychological dimensions of the conflict. (Slijepčević, 2023).

Hybrid warfare maintains a constant atmosphere of tension that is often neither in the domain of war nor in the domain of peace. The gray area between peace and war is renewed by periodic escalations in different dimensions of the conflict, with each new escalation gradually becoming more severe than the last. The strategic gradualism exhibited here serves as a means of testing the will and commitment of the opposing side to political goals in a hybrid conflict. (Pejić, 2019).

In their work, Cvetković et al. (2019) conclude that the most significant content of hybrid warfare can be taken as the following forms of action against the opponent in order to force the fulfillment of demands:

- Information-psychological-ideological action;
- Political action;
- Economic pressures;
- Intelligence-subversive activity;

- IT methods;
- Criminal activities;
- Terrorism and armed insurgencies, as well as
- Conventional military action.

In addition to the concept of hybrid war, space in the literature is also occupied by the concept of information war, which exists as a consequence of society's dependence on information and communication technologies, which creates numerous weak points.

From a military point of view, information warfare in the world is defined as activities undertaken to achieve information supremacy, attacking the opponent's information, i.e. data, information-based processes, information systems and computer-based networks, while at the same time protecting and defending one's own data, information processes and systems and computer networks. (Marinković, 2018).

However, Rančić and Beriša (2018) claim that the aspiration of information warfare is to gain complete control over the consciousness of the people of the state – the victims of aggression, and therefore to gain opportunities to influence their future.

Alispahić (2020) believes that propaganda as a "mind control" and demoralizing weapon, directed against the population of the target country, is one of the most effective instruments for achieving the occupation's goals. The occupation of the mind and soul – the abstract part of the human being, accomplishes and achieves much more than the military occupation of the territory.

Therefore, we conclude that it is very important to understand information warfare, because it exists independently of physical warfare, and has unfathomable dimensions on society as a whole because it is very difficult to control.

### **How to get accurate information?**

In today's information-inundated world, where the rapid availability of content on the Internet often makes it difficult to identify accurate information, fact-checking programs and organizations are becoming essential to the formation of an informed society. With the

spread of misinformation, fake news and information manipulation, there is a growing need for independent entities dedicated to verifying claims and assessing the accuracy of statements. Verifying the reliability of news and ensuring information security are key steps in the era of digital information availability.

Slijepčević (2023) states that fact-checking has become a new element of the media system that has its foundations in investigative journalism, and on the other hand, it is clearly separated from media that have lost the trust of the audience. Special fact-checking organizations have become a new, independent part of the modern information system.

Fact-checkers mainly deal with checking and establishing, putting in a certain context and explaining what journalists, and especially "anti-journalists" (those who produce fake news and engage in fake journalism) publish; on the other hand, when media companies need reliable, verified, credible information, they can certainly rely on fact-checking platforms. Fully verified information, obtained from all relevant sources and clarified from every aspect, is exactly what fact-checkers bring. It can also be a starting point, an important source or an important segment of a new story, a new research. Such, as fact-checkers call it "unproblematic fact", can become a sure foundation for any future good journalistic story. And there will be no mistakes. (Obrenović, 2022)

Fact-checker organizations were originally focused exclusively on investigating the claims of politicians, but there are also those that are focused almost exclusively on the media. Also, in addition to these, organizations have also developed to verify scientific and health information, as well as for information that is marketed in the entertainment industry. We will provide an overview of several well-known fact-checking programs and platforms:

- FactCheck.org: This independent organization focuses on fact-checking related to politics in the United States of America. FactCheck.org provides analyzes of the claims of political leaders and political campaigns.

- Snopes: Snopes is the leading platform for checking urban legends, myths and misinformation on the Internet. They investigate and evaluate claims from various fields.
- PolitiFact: This Poynter Institute project evaluates the accuracy of statements by political leaders and political campaigns. They use a "Truth-O-Meter" to assign grades.
- AFP Fact Check: Agence France-Presse (AFP) provides a global fact check in various languages. They evaluate politicians' claims, viral news and other information.
- BBC Reality Check: The BBC provides fact-checking through its Reality Check platform, focused on political claims and other significant events.
- The Washington Post Fact Checker: This publication provides fact-checking for politicians' statements and other relevant information. Use the "Pinocchio scale" to rate the accuracy of statements.
- Google Fact Check Tools: Google has developed fact-checking tools that allow users to check information directly from search results. This includes a browser extension that helps identify fake information.
- Istinomer: Istinomer is a media that since 2009 has been engaged in fact-checking by evaluating the statements of public officials and politicians, as well as through analyzes of important social and economic issues. Statements are evaluated according to the criteria of truthfulness, consistency and fulfillment of promises.

Since July 2020, Istinomer has been the official partner of Meta for Serbia in combating misinformation on social networks Facebook and Instagram. Istinomer daily checks the content and scans misinformation in the Serbian language that is published on these platforms. And he analyzes the manipulations that spread in the media and on social networks (istinomer.rs).

It's important to note that critical thinking and comparing multiple sources is still key in fact-checking. No program is completely

perfect, so it is advisable to use multiple resources to create a complete picture. Developers and the scientific community play a key role in finding solutions to effectively detect fake news, including various technological innovations, algorithms, data analysis and cooperation with news organizations.

One of the proposals is the development of a system that will provide credible automated indexing, or rating the credibility of different publishers and news contexts. A methodology is proposed to create a model that will detect whether an article is authentic or fake based on its words, phrases, sources, and titles, by applying supervised machine learning algorithms to an annotated dataset that has been manually classified and guaranteed. Then, feature selection methods are applied to experiment and select the best matching features to obtain the highest accuracy, according to the results of the confusion matrix. (Khanam, 2021). The use of machine learning for the purpose of detecting fake news is covered through the topic of smart systems and in the work of Jain et al (2019).

Fake news detection is also discussed from a data mining perspective, including feature extraction and model construction, as well as a discussion of datasets and evaluation metrics. (Shu et al. 2017). Also, the perspective of the use of artificial intelligence, which analyzes and evaluates information based on various parameters in order to detect fake news, was also discussed (Kozik et al. 2024).

The rapidly growing activity of automated fact-checking initiatives and research by both academic researchers and professional fact-checking organizations, and the consensus within both groups that fully automated fact-checking remains a distant goal. The most promising developments today are in automated fact-checking tools that help fact-checkers respond more quickly and effectively to political lies, online rumors, and other forms of misinformation. Automated fact-checking is an area of unusually close collaboration between researchers and practitioners. Further progress will depend mainly on two factors: continued financial support for basic research and real-world experiments, and progress by governments and civil society groups in establishing open data standards (Graves, 2018)..

## **Current conflicts and their projections on the world of information**

The state of war conflicts in the world changes over time, but we have witnessed that in the last few years the state of the world has worsened significantly with the outbreak of new conflicts and the escalation of wars.

The Palestinian extremist group Hamas carried out an attack on Israel on October 7, 2023, in which more than 1,400 people were killed and more than 220 were kidnapped. This attack was the biggest threat that Israel faced, and the Israeli army was taken aback, but soon launched a bombing of Gaza on an unprecedented scale - and declared the goal: the total destruction of Hamas and their structure. But a huge number of civilians were killed in the bombing. According to the Hamas-controlled Ministry of Health, 23,000 people, including many women and children, have died in 100 days of fighting. Thousands of dead are believed to be still under the rubble. Palestinian officials say 85 percent of Gaza's population has been displaced. (Davis, 2024).

Israel responded to the latest attacks by Hamas with military force, but for the first time also in cyberspace. Although Israeli cyber experts and various military and civilian groups have attacked Palestinian cyber-infrastructure before, the main goal now is to completely cut off the Gaza Strip from the Internet. The "digital war" in Gaza is different – Israel's goal is not only to disable communication, but also to prevent news, photos and videos from the front lines from going out into the world.

On the night between October 7 and 8, one of the biggest DDoS cyber attacks since the internet has existed was recorded. DDoS stands for "Distributed Denial of Service" and is one of the most common types of "massive" cyber-attacks. In this case, the DDoS attack on systems in Israel was with 1.25 billion requests to just a few IP addresses in Israel, belonging to the Ministry of Defense and the Government. By October 9, two entire state networks (operational subnets) were disabled. Although Israeli and American experts believed that such a large attack could not come only from the Gaza

Strip, since Hamas does not have such cyber resources, due to the general confusion it was not possible to determine the exact source of this much "fake" Internet traffic. A few days later, it was found to be a network of more than 14,000 "zombie" computers (computers of ordinary users infected with a computer virus), many of which were located throughout the Middle East, Turkey and European countries. This way of "working" is very characteristic of hackers from another country in the region - Iran.

On the other hand, the most famous and largest Indian hacking group, "Indian Cyber Force", supported Israel and took responsibility for taking down the websites of Palestinian Telecom, the Palestinian National Bank, as well as Hamas itself. Experts estimate that at least 80 hacker groups from all over the world are currently carrying out cyber attacks in Israel and Palestine.

A major online disinformation operation has been launched by both sides, and media around the world have great difficulty independently verifying claims from the ground, as well as videos and photos appearing on social media. (Trajković, 2023).

Censorship that is present on the Internet is systematic and refers to a large number of Palestinian and pro-Palestinian Internet accounts. Journalists are censored and their content is unjustifiably removed if they have anything to do with Palestine. At the same time, Hebrew content, especially hate speech, inflammatory content and open calls to violence, remain untouched on the Meta platform simply because it does not have 'classifiers', i.e. AI algorithms to detect and automatically remove such content in the Hebrew language, which violates standards. their online communities.

The Israeli government is also paying YouTube, which is owned by Google, to reduce anti-war content and promote pro-Israeli narratives. Thus, the Western public cannot see the footage of the massacre of children and civilians in Gaza. We are witnessing the same practice on Facebook and LinkedIn.

Here we can also introduce the term digital occupation of Palestine, because Israel controls the ICT infrastructure in the occupied territories. This allows them to shut down the Internet and cut off the

flow of information, which they have done at least 10 times in the Gaza Strip. Even before the war, its inhabitants only had access to a 2G mobile network, while the rest of the world switched to 5G mobile networks. (Mazlić, 2024)

And in these conflicts we can see the characteristics of information warfare regarding the distribution of fake news. The most common form of news manipulation is the manipulation of existing events, i.e. changing the context of the event, its location or time of occurrence, which happens in a large number of cases. These are real events that have been decontextualized. All of this points to the influence of various corrupt forms and activities (Bjelajac, 2015 & Bjelajac, 2008), which, supported by mass media, remain in the gray zone, inventive and invisible.

Such a video, which is claimed to show Israeli airstrikes on Gaza in the first days of the October conflict between Israel and Hamas, has spread among Telegram and Facebook users and in our language. However, we are talking about the shots of the bombing of Ariha, a Syrian city, which also happened at the beginning of October. (Kilibarda, 2023). (Figure 3)

In a similar way, the photo from 2018)

image showing the use of white phosphorus weapons in Syria is being shared on social networks along with information about the use of these weapons in Gaza, without mentioning that it is an old photo. (Murić, 2023), (Figure 4).

One of the frequently used characteristics of information warfare is blaming the opposite party and shifting responsibility, as well as the use of audiovisual materials that can be assumed to affect the emotions of media consumers. Most often, it is about generally accepted values of society.

Social media users have shared footage of children locked in cages claiming it depicts prisoners of war in the current conflict in the Middle East. While some claimed that the footage showed "kidnapped Israeli children", others claimed that it was "Palestinian". The disputed video is not related to the current conflict between Hamas and Israel and does not show victims of the war in the Middle East. The clip was

posted on TikTok days before the Palestinian militant group Hamas attacked Israel on October 7, 2023. (Tančić, 2023) (Figure 5).

Unfounded accusations against the Palestinians that they use "crisis actors" and manipulate the number of casualties in Gaza are spreading on social networks. This time, the recording, made in 2013 in Egypt, is being presented as current "proof" that Palestine is faking victims. In the 19 seconds of the video, the corpses of civilians killed in Gaza are allegedly shown. As most of the "dead" in the video are moving, conspiracy theorists insist that it is a planned action to stage the death and increase the number of dead in Gaza. The original video was published on October 28, 2013 by the Egyptian portal Elbadil. The title in Hindi reads "Performas with dead bodies inside Al-Azhar University". (Kilibarda, 2023) (Figure 6).

## **Conclusion**

This paper provides an insight into the complexity of problems related to the security and credibility of information about war conflicts in the context of fake news, fact-checking mechanisms and modern information warfare. Analysis of war-related fake news reveals deep-rooted challenges in interpreting events, which points to the need for additional efforts in media literacy education and awareness to equip the public to critically understand information.

Fact-checking platforms have shown significant potential in suppressing disinformation, but at the same time they face challenges in the speed of response to dynamic changes in the information space. Their efficiency can be improved by continuous development of technological solutions and cooperation with the media, scientific and educational institutions and social networks.

In terms of modern information warfare, the need for a strategic approach in defense against digital threats was emphasized. Institutions and states must continuously adapt their policies and strategies to adequately respond to changes in tactics and technologies used in information warfare.

Through a comprehensive review, we conclude that it is necessary to establish a holistic approach that includes cooperation

between governments, technology companies, media organizations and civil society. Only through joint efforts can we build resistance to disinformation, improve the credibility of information and strengthen security in the digital age, thereby contributing to stability and peace in the global context.

## References

- Alispahić, B. (2020). Propaganda kao oblik specijalnog rata, [Propaganda as a form of special war], *Društvena i tehnička istraživanja*, 6(2), 71-90.
- Balmas, M. (2014). When fake news becomes real: Combined exposure to multiple news sources and political attitudes of inefficacy, alienation, and cynicism. *Communication Research*, 41(3), 430-454.
- Bjelajac, Ž. (2008). Korupcija kao vid organizovanog kriminala [Corruption as a form of organized crime]. *Pravo – teorija i praksa*, 25(3-4): 47-54.
- Bjelajac, Ž. (2015). Korupcija kao izazov savremenog demokratskog društva [Corruption as a challenge of modern democratic society]. *Kultura polisa* 12(26): 43-57.
- Bjelajac, Ž., Filipović, A. (2020). Internet addiction disorder (IAD) as a paradigm of lack of security culture. *Kultura polisa*, 17(43): 239-258.
- BBC, (2024, januar, 25). [https://www.bbc.com/news/reality\\_check](https://www.bbc.com/news/reality_check)
- Cvetković, N., Kovač, M. & Joksimović, B. (2019). Pojam hibridnog rata, [The concept of hybrid war]. *Vojno delo*, 71(7), 323-343.
- Čelik, P. (2019). Bezbednosne implikacije digitalnog poslovanja [Security implications of digital business]. *Ekonomija teorija i praksa*, 12(4), 61-81.
- Dejvis, V. (2024, januar 14). Izrael i Palestinci: 100 dana od napada Hamasa na Izrael koji je pokrenuo rat u Gazi [Israel and the

- Palestinians: 100 days since the Hamas attack on Israel that triggered the Gaza war], *BBC NEWS na srpskom*. <https://www.bbc.com/serbian/lat/svet-67973999>
- Digitalna transformacija – ko, gde, šta, kako i zašto?, [Digital transformation – who, where, what, how and why?], Project “ICT Hub Belgrade – Playground of Innovations”, United States Agency for International Development (USAID). [https://pdf.usaid.gov/pdf\\_docs/PA00W7DG.pdf](https://pdf.usaid.gov/pdf_docs/PA00W7DG.pdf)
- FactCheck.org, (2024, januar, 25). <https://factcheck.afp.com/about-afp>
- FactCheck.org, (2024, januar, 25). <https://www.factcheck.org/-about/our-mission/>
- Google Fact Check Tools, (2024, januar, 25). <https://toolbox.google.com/factcheck/explorer>
- Graves, L. (2018). *Understanding the Promise and Limits of Automated Fact-Checking Author*. Digital News Publications, Reuters Institute for the study of journalism & University of Oxford. <https://www.10.60625/risj-nqnx-bg89>
- Istinomer, (2024, januar, 25). <https://www.istinomer.rs/o-istinomeru/>
- Jain, A., Shakya, A., Khatter, H. & Gupta, A. (2019). *A smart System for Fake News Detection Using Machine Learning*. In X.Sh. Yang. S, Sherratt & N. Dey (Eds.), *Issues and Challenges in Intelligent Computing Techniques:ICICT* (pp. 1-6). IEEE:Ghaziabad, India.
- Khanam, Z., Alwasel, B., Sirafi, H. & Rashid, M. (2020). *Fake News Detection Using Machine Learning Approaches*. *IOP Conference Series: Materials Science and Engineering*, 1099, 012040. <https://www.10.1088/1757-899X/1099/1/012040>
- Kilibarda, N. (2023, novembar 11). Video sa demonstracija 2013. u Kairu deli se kao „dokaz” da Palestinci lažiraju žrtve u Gazi [Video of 2013 Cairo demonstrations shared as 'proof' Palestinians are faking Gaza casualties], *Istinomer*. <https://www.istinomer.rs/facebook-provere/video-sa->

[demonstracija-2013-u-kairu-deli-se-kao-dokaz-da-palestinci-laziraju-zrtve-u-gazi/](#)

- Kozik, R., Ficco, M., Pawlicka, A., Pawlicki, M., Palmieri, F. & Chora's, M. (2024). When explainability turns into a threat - using xAI to fool a fake news detection method, *Computers & Security*, Elsevier, 137,103599.
- Mandić, I. (2016). Definiiranje rata za 21. stoljeće, [Defining War for the 21st Century], *Polemos*, 19(1), 77-87.
- Marinković, D. (2018, avgust 1). Informacioni rat – Zamke virtuelnog sveta, [Information War – Pitfalls of the Virtual World], *Odbrana*, 62-65.  
<http://www.voa.mod.gov.rs/sr/publikacije/zamke-virtuelnog-sveta>
- Mazlić, L. (2024. Januar 27). Marwa Fatafta: Gaza i globalne rasprave o njoj su pod digitalnom opsadom Izraela [Marwa Fatafta: Gaza and global discussions about it are under digital siege by Israel], *Al Jazeera*.  
<https://balkans.aljazeera.net teme/2024/1/27/marwa-fatafta-gaza-i-globalne-rasprave-o-njoj-su-pod-digitalnom-opsadom-izraela>
- Murić, E. (2023, novembar 14). Fotografija napada oružjem s bijelim fosforom nije nastala u Gazi, već u Siriji [The photo of the attack with white phosphorus weapons was not taken in Gaza, but in Syria], *Raskrinkavanje*.  
<https://raskrinkavanje.ba/analiza/fotografija-napada-oruzjem-s-bijelim-fosforom-nije-nastala-u-gazi-vec-u-siriji>
- Obrenović, M. (2022). Fact-checking platforme kao izvori za novinare: Kako doći do 'neproblematične' činjenice [Fact-checking platforms as sources for journalists: How to get 'unproblematic' facts] <https://journalift.org/bhsc/fact-checking-platforme-cao-izvori-za-novinare-kako-doci-do-neproblematične-cinjenice/>
- Pejić, I. (2019), Ruske vojne hibridne operacije u Ukrajini: prilagođavanje strategije i taktike savremenoj strukturi rata,

- [Russian Military Hybrid Operations in Ukraine: Adapting Strategy and Tactics to the Contemporary Structure of War]. *Medjunarodni problemi*, 71(4), 423–446.
- Politifact, (2024, januar, 25). <https://www.politifact.com/article/-/2018/feb/12/principles-truth-o-meter-politifacts-methodology-i/>
- Rančić, I. & Beriša H. (2018). Hibridni rat – mit ili stvarnost (Rekonceptualizacija hibridnog rata), [Hybrid War – Myth or Reality (Reconceptualization of Hybrid War)]. *Vojno delo*, 70(5), 255–271.
- Sukhodolov, A. & Bychkova, A. (2017). Fake news as a modern media phenomenon: definition, types, role of fake news and ways of counteracting it. *Theoretical and Practical Issues of Journalism*, 6(2), 143–169.
- Slijepčević, M. (2023). Analiza obrazaca informacijskog ratovanja i dekonstrukcije lažnih vijesti na primjeru Ukrajinske krize, [Analysis of patterns of information warfare and deconstruction of fake news on the example of the Ukrainian crisis]. [Doktorska disertacija, Sveučilište Josipa Jurja Strossmayera u Osijeku]. <https://urn.nsk.hr/urn:nbn:hr:236:822399>
- Shu, K., Sliva, A., Wang, S., Tang, J. & Liu, H. (2017). Fake News Detection on Social Media: A Data Mining Perspective. *ACM SIGKDD Explorations Newsletter*, 19(1). <https://www.10.1145/3137597.3137600>
- Snopes, (2024, januar, 25). <https://www.snopes.com/latest/>
- Subotić, M. (2018). *Hibridni rat – novost ili istorija koja se ponavlja novim sredstvima* [Hybrid war – innovation or history repeating itself with new means]. U N. Nikolić (Ured.) Zbornik radova Hibridno ratovanje – dilemma koncepta savremenih sukoba (str. 28-45). Beograd: Institut za strategijska istraživanja.
- Tančić, T. (2023, oktobar 19). Snimak dece u kavezima nastao pre početka aktuelnog sukoba Hamasa i Izraela [The footage of children in cages was taken before the start of the current conflict between Hamas and Israel], *Istinomer*.

<https://www.istinomer.rs/facebook-provere/snimak-dece-u-kavezima-nastao-pre-pocetka-aktuelnog-sukoba-hamasa-i-izraela/>

The Washington post, (2024, januar, 25).

<https://www.washingtonpost.com/politics/fact-checker/>

Trajković, I. (2023, oktobar 19). Uz malu pomoć prijatelja: Izrael i Hamas ratuju i u virtuelnom svijetu [With a little help from friends: Israel and Hamas are also at war in the virtual world], *Al Jazeera*. <https://balkans.aljazeera.net teme/2023/10/19/uz-malu-pomoc-prijatelja-izrael-i-hamas-ratuju-i-u-virtuelnom-svijetu>

Vučković, J. (2021). Verodostojnost medijskih sadržaja – usluga na internetu [Credibility of media content – service on the Internet]. U D. Vujsić (Ured.) *Zbornik radova „XXI vek – vek usluga i Uslužnog prava“ (str. 137-150)*. Kragujevac: Pravni fakultet Univerziteta u Kragujevcu, Institut za pravne i društvene nauke.

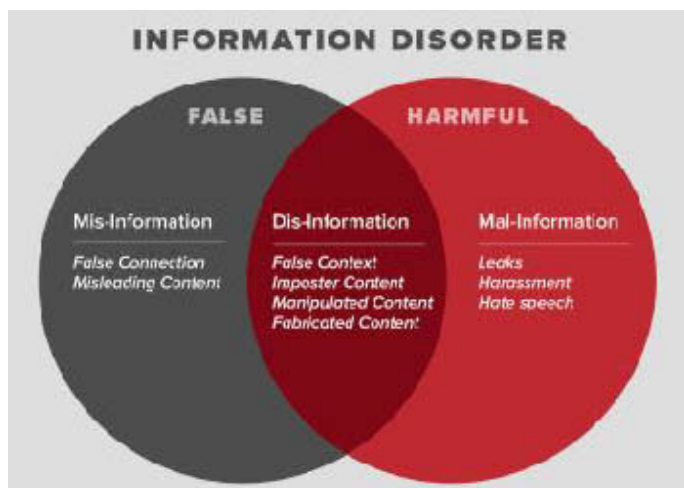
Wardle, C. & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe report DGI .

Zhang, X. & Ghorbani, A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing and Management*, 57(2), 102025.

## Appendix

**Figure 1**

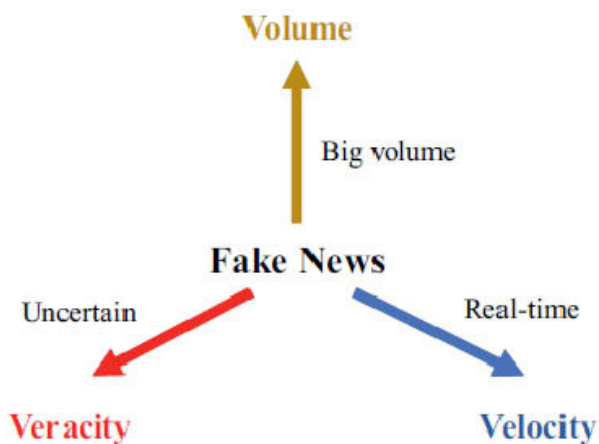
Types of information in information disorder



(Wardle & Derakhshan, 2017, p. 5)

**Figure 2**

The volume, variety and speed of fake news



(Zhang & Ghorbani, 2020, p. 2)

### **Figure 3**

Bombardment of the Syrian city of Ariha



(Kilibarda, 2023)

### **Figure 4**

Attack with white phosphorus



(Murić, 2023)

**Figure 5**

A picture of children in cages



(Tančić, 2023)

**Figure 6**

Demonstrations in 2013 in Cairo



(Kilibarda, 2023)

## **Bezbednost i verodostojnost informacija o ratnim sukobima na Internetu**

Vesna Simović<sup>1</sup>, Žaklina Spalević<sup>2</sup> and Bojan Prlinčević<sup>3</sup>

<sup>1</sup>Akademija strukovnih studija kosovsko metohijska, Odsek  
Zvečan, Leposavić, Srbija

<sup>2</sup>Fakultet za turistički i hotelijerski menadžment, Beograd, Srbija

<sup>3</sup>Akademija strukovnih studija kosovsko metohijska, Odsek  
Zvečan, Leposavić, Srbija

### **Sažetak**

Kompleksna dinamika informacija o koje se u savremenom digitalnom dobu neprestalno plasiraju dovode do prevelike količine informacija upitne tačnosti i kredibiliteta. Lažne vesti, obmanjujuće informacije, glasine i satire preuzimaju primat nad instinitim informacijama, posebno u domenu informacija o ratnim sukobima, koje rapidno gube svoju verodostojnost. Ovaj društveni fenomen ozmačen je kao informacijski poremećaj. Ratni sukobi u savremenom dobu dobijaju novi oblik, upoznajemo se sa pojmom hibridni rat, koji se pored fizičkih borbi ostvaruje i kroz borbu za kontrolu nad informacionim sistemima. Informacijsko ratovanje usmereno je na postizanje kontrole nad svešću naroda jedne države naročito putem plasiranja lažnih i obmanjujućih vesti, a kao kontra mera mogu se koristiti usluge organizacija za proveru informacija "fact-checkeri". Informacijsko ratovanje i plasiranje lažnih vesti posmatramo kroz prizmu najnovijih ratnih sukoba između Izraela i Hamasa u pojasu Gaze.

*Ključne reči:* informacija, lažne vesti, informacijski poremećaj, hibridni rat, Fact-Checker.