DOI: https://doi.org/10.34069/AI/2023.69.09.22

How to Cite:
Bidzilya , Y., Snitsarchuk, L., Solomin, Y., Hetsko, H., & Rusynko-Bombyk, L. (2023). Ensuring media security in the era of information globalization. *Amazonia Investiga*, *12*(69), 249-259. https://doi.org/10.34069/AI/2023.69.09.22

Ensuring media security in the era of information globalization

Забезпечення медіа-безпеки в епоху інформаційної глобалізації

Received: August 1, 2023 Accepted: September 29, 2023

Written by:
Yuriy Bidzilya[1]
https://orcid.org/0000-0001-5134-3239
Lidiya Snitsarchuk[2]
https://orcid.org/0000-0002-7272-9357
Yevhen Solomin[3]
https://orcid.org/0000-0001-6770-5505
Hanna Hetsko[4]
https://orcid.org/0000-0002-7684-4790
Liubov Rusynko-Bombyk[5]
https://orcid.org/0000-0002-0634-9217

Abstract

The aim of the study is to identify key threats to media security and ways of their minimization. The methods of statistical analysis, case studies, content analysis, and rating analysis were used in the article. The study established that the biggest threat to media security is the spread of misinformation. This threat is complex because of the ability to spread in multiple ways and channels using a number of tools hybridized by misinformation, including propaganda, fake news, information leakage, manipulation, falsification of media content, etc. The spread of disinformation from Russia and China is of particular concern. Case study proved that disinformation is spread in many ways, and new media only deepen this problem. The consequences of the use of disinformation are public unrest, riots, mistrust of the media, and a threat to democratic values. The main areas of ensuring media security are defined as: application of technological measures, improvement of the legislative framework at the national and international levels, improvement of media literacy of the population through

Анотація

Метою дослідження є визначення ключових загроз та напрямів їх мінімізації у сфері медіа-безпеки. У статті використано методи статистичного аналізу, кейс-стаді, контент-аналіз, рейтинговий аналіз. В результаті дослідження встановлено, що найбільшою загрозою для медіа-безпеки є розповсюдження дезінформації. Ця загроза носить комплексний характер через можливість розповсюдження численними способами та каналами з використанням ряду інструментів, які гібридизує дезінформація, у тому числі пропаганда, фейкові новини, витік інформації, маніпуляції, підробка медіа-контенту тощо. Особливу стурбованість викликає поширення дезінформації з боку Росії та Китаю. Проведений аналіз кейс-стаді дозволив довести, що розповсюдження дезінформації здійснюється багатьма способами, а нові медіа лише поглиблюють дану проблему. Наслідками застосування дезінформації є хвилювання населення, заворушення, недовіра до медіа, загроза демократичним цінностям.

[1] Doctor of Sciences in Social Communications, Professor, Professor of the Department of Journalism, Dean of the Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine.

[2] Doctor of Science in Social Communications, Professor, Deputy Director-General for Research, Director of Research Institute for Press Studies, Vasyl Stefanyk National Scientific Library of Ukraine, Lviv, Ukraine.

[3] Candidate of Sciences in Social Communications, Associate Professor, Head of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine.

[4] PhD in Philology, Associate Professor of Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine.

[5] PhD in Philology, Associate Professor of Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine.

appropriate educational programmes and specialized campaigns. The results of the study can be used by government officials and media content providers to improve media security.

Keywords: media security, traditional media, new media, misinformation, fake content, media literacy.

Основними напрямами забезпечення медіа безпеки визначено: застосування технологічних заходів, удосконалення законодавчої бази на національному та на міжнародному рівнях, підвищення медіа-грамотності населення через відповідні освітні програми та спеціалізовані кампанії. Результати дослідження можуть бути використані урядовцями та провайдерами медіа-контенту для покращення системи забезпечення медіа-безпеки.

Ключові слова: медіа-безпека, традиційні медіа, нові медіа, дезінформація, підроблений контент, медіа-грамотність.

Introduction

Ensuring media security in view of aggravating conflicts of various origins is the priority for the governments and media content providers. This is explained by the decisive impact of information resources on all processes in modern society, as well as the rapid development of new information technologies (Bahrini & Qaffas, 2019), which has a double impact. On the one hand, innovation facilitates quick access to information for users in real time, thereby enabling timely response to events and planning for the future (Ortiz-Ospina & Roser, 2019). On the other hand, many new ways of information misuse related to information theft, its use by criminals, data distortion, creation of fake content, etc. are emerging (Liu et al., 2021; Pennycook & Rand, 2021). Such actions may have serious implications both at the individual level and at the state level (Vraga & Tully, 2021; Colomina et al., 2021). In the field of media, dishonest use of information can be aimed at influencing the election process, spreading propaganda, provoking public unrest, and intimidating the population (Tandoc, 2019; Brody, 2019).

The main focus of the study is the problem of misinformation, as it is complex because of a large number of ways of distribution and serious implications for society and the state. In addition to the traditional ways of spreading disinformation (in person, in television news), new digital media create additional space for the spread of unreliable data. Disinformation hybridizes such threats as propaganda, fake news, information leakage, manipulation (Treverton et al., 2018). The large volumes of digital information and the uncertainty of the human factor make it almost impossible to develop a single practical approach to combating disinformation and ensuring media security in real time (Zhang et al., 2022).

Concrete examples can help to understand the harmful effect of misinformation. Thus, Colomina et al. (2021), examining the impact of disinformation on democratic processes and human rights around the world, reveal the role this phenomenon played during the spread of the COVID-19 pandemic. In 2020, between January 20 and February 10, 2 million messages were distributed on Twitter, which made up about 7% of the total number of messages on the social network, and spread conspiracy theories about the coronavirus. This contributed to growing anxiety among the population, who did not know where to look for truthful information, and even more, it contributed to the public's disregard for safety rules, which put many lives at risk. Gunther et al. (2018) performed calculations regarding the impact of misinformation on the 2016 US presidential election. As the scientists note, a large number of messages demonizing the candidates and containing distorted facts were spread through all the main means of information dissemination (television, radio, social networks). The researchers note that if their estimates are even remotely accurate, the effect of spreading such messages was enough to influence the results of the vote, which was very close.

The researchers study various technological means of combating the abuse of media content (Lian, 2009; Bindu et al., 2018), as well as legislative aspects in this area (Marsden et al., 2020) and ways to improve public awareness (Shen et al., 2019) At the same time, the researchers most often study individual aspects of the problem or, on the contrary, studies cover information security as a whole. This study contains a comprehensive analysis of threats to media security and determines directions for its provision.

The aim of the article is to identify key threats and directions for their minimization in the field of media security. The aim of the article involved the fulfilment of the following research objectives:

- Analyse media security threats, in particular, disinformation as the main threat and its components (propaganda, fake news, information leakage, manipulation, forgery of media content);
- Conduct a case study of individual cases of media security violations;
- Determine key areas of media security.

Accordingly, the research structure consists of the following subdivisions:

1) Analysis of threats - the subsection provides for the analysis of key threats to media security, the main of which is disinformation, which includes, among other things, their main characteristics, goals, ways of distribution.
2) Case studies of disinformation cases - at this stage, the countries that are the main actors in conducting global disinformation campaigns are identified, as well as individual examples of the use of technologies to spread disinformation, for example, deepfake, collection of user data, phishing attacks.
3) Regulatory measures to combat disinformation - the last section reveals the essence, advantages, disadvantages and directions for optimization of the latest EU legislation related to the fight against disinformation, and also contains statistical data on the values of Media Freedom Score and Media Literacy Index in 2022 and Most used media to access news in Europe.

Literature Review

Media security is a relevant issue, especially because of the new risks associated with digital technologies. This entailed the emergence of the concept of “new media”. Dhiman (2023) reveals the essence of new media as a digital form of communication and dissemination of information through the Internet and social networks. Temmermans et al. (2022) note that deepfake techniques enable creating near-realistic media content. Derner and Batistič (2023) report that the new platform ChatGPT, which has gained high popularity among consumers, is capable of generating malicious text and code, creating unethical content, disclosing confidential information, facilitating fraudulent schemes, and collecting information.

Most often, researchers are concerned about the spread of fake news, misinformation, propaganda, and the leakage of confidential information. These malicious actions are often associated with cyber-attacks aimed at violating the integrity of the information system. ALsaed and Jazzar (2021) identify the most common types of cyberattacks: phishing, malware, malicious domains, and fake news. The researchers propose micro-level countermeasures, while Nagasako (2020) examines the impact of cyberattacks at the interstate level, global cyberattacks committed by individual countries. The devastating consequences of such cyber-attacks can manifest themselves through their influence on election results and the threat to democracy, which is why such operations are defined in the article as “misinformation”. Caramancion et al. (2022) also wrote on the approach to disinformation as one of the main cyber threats, noting that the lack of inclusion of disinformation in the glossary of cyber threats is a shortcoming of modern standards in the field of cyber security. Petratos (2021) concludes that misleading information is not a cyber threat in itself, but poses cyber threats to business, healthcare, mass media, financial markets, electoral process, and geopolitical space.

Along with misinformation, fake news are often considered in the academic literature. Rodríguez-Ferrándiz (2023) defines this concept and analyse the perception of fake news by the public. Sousa-Silva (2022) recognize the dangers of fake news related to two factors: the threat to democracy and the difficulty of detecting such news.

So, the realized media security threats can have a global effect. Researchers often touch on the topic of the impact of media threats on the election process and their role in the development of information warfare. Pyrhönen and Bauvois (2020) note an increase in threats to media security during elections, when the community expects the expose of certain misdeeds of political elites, which creates a fertile ground for various smear campaigns. Tan (2020) offers his own election management digital readiness index. Kumar (2022) discusses the concept of information war, examining the adequacy of international law to counter it.

Methodology

Research design

In accordance with the tasks set in the study, the content of the study is divided into subsections that contain an analysis of threats to media security, a statistical review and case studies of cases of media security violations, and directions for ensuring media security. In the first stage of research using content analysis, key threats to media security were identified. This made it possible to establish a list of such threats, to briefly describe their essence, to outline the motivation of attackers to implement threats and to determine the most complex threat (disinformation), which combines a number of other tools (propaganda, fake news, information leakage, manipulation, forgery of media content, etc.).

At the second stage, using statistical analysis, the number of disinformation campaigns conducted during 2016-2020 was determined by the main actors who carried out such campaigns. It has been established which countries most often carried out disinformation campaigns, as well as in which territories they were implemented. With the use of a case study, several examples of the use of disinformation for the purpose of transforming public opinion were revealed. The types of disinformation that were considered in the case study are deepfake technologies and the use of personal data for the purpose of conducting phishing attacks.

The third stage, during which the method of content analysis was used, reveals the key regulatory measures to combat disinformation. At this stage, the main attention is paid to the analysis of the legal framework of the European Union, in particular, to such documents as the General Data Protection Regulation (GDPR), the Proposed Law of the European Union on Artificial Intelligence (EU Law on Artificial Intelligence), the Law on Digital Services (Digital Services Act, DSA). The analysis made it possible to identify the main tasks of the documents, their advantages and disadvantages, as well as to suggest directions for improvement. In addition, at this stage, the need to increase media literacy and public awareness of disinformation, especially in countries where socio-political processes have been significantly affected by disinformation and information warfare, is noted. In this context, the results of using the ranking method to determine the Media Freedom Score and the Media Literacy Index are presented. Media Literacy Index 2022 includes the following groups of indicators (which, in turn, contain several subindexes): Media Freedom indicators (40%), Education indicators (45%), Trust (10%), New forms of participation (5%). The weight of each group of indicators in determining the integral value of the media literacy index is indicated in parentheses. Also, with the use of statistical analysis, the shares of the European population using one or another channel for receiving news, namely television news, online news platforms, radio, social media and print publications, are given.

Sampling

The sample consists of European countries because the European Union was the most active in the field of legislative support of media security. During the analysis of the indicators Media Freedom Score and Media Literacy Index and Most used media to access news in Europe in 2022, data from 41 European countries were used, the full list of which is presented in Figure 2. During the analysis of the legislative framework, documents in force in the countries were used in the EU.

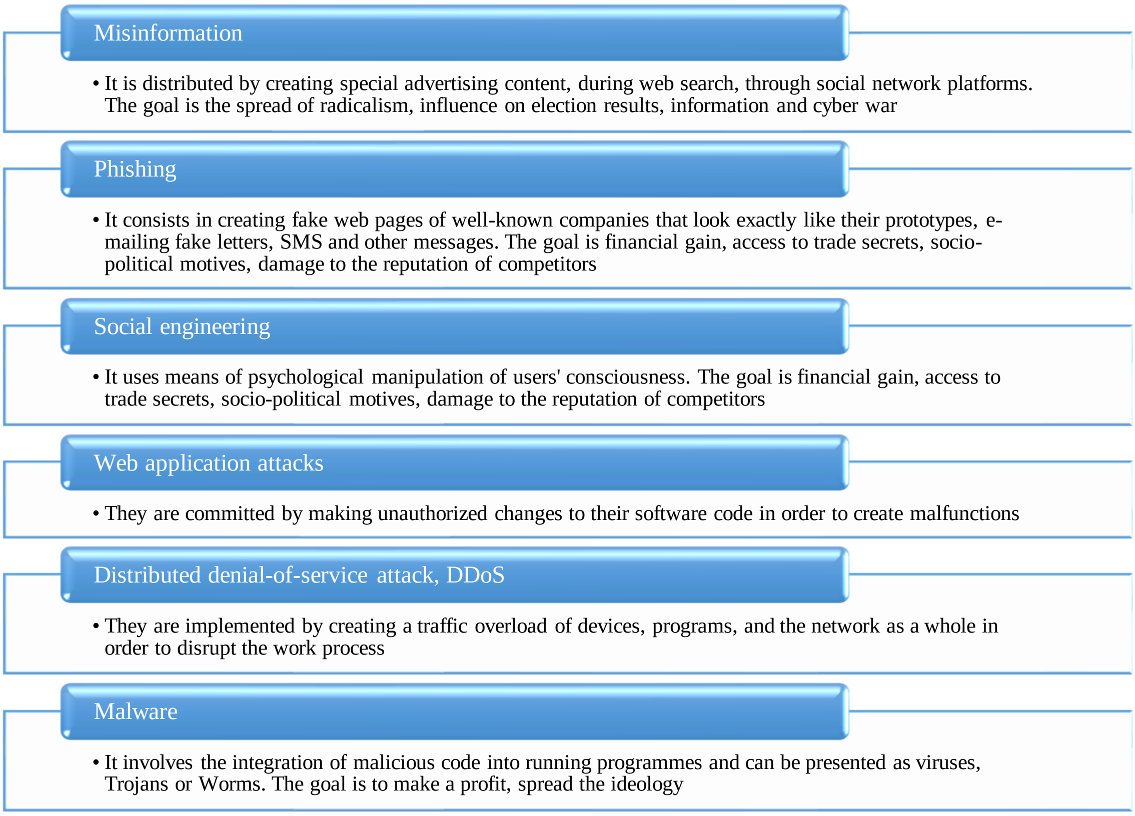
Information background of the research

Academic periodicals of different countries, the legislative framework of the European Union, and data from the report The 2022 Media Literacy Index Main Findings and Possible Implications were used as the background information for the research (Lessenski, 2022).

Results

Analysis of threats

Ensuring media security involves awareness of the entire range of threats that can disrupt it. However, the rapid development of technologies in the modern world causes an increasing number of new challenges. Therefore, recognizing the need for permanent monitoring of the information sphere regarding the emergence of new threats, it is advisable to focus on those threats that can cause the most significant negative geopolitical, social, and economic consequences. The main threats are presented in Figure 1.



Misinformation

- It is distributed by creating special advertising content, during web search, through social network platforms. The goal is the spread of radicalism, influence on election results, information and cyber war

Phishing

- It consists in creating fake web pages of well-known companies that look exactly like their prototypes, e-mailing fake letters, SMS and other messages. The goal is financial gain, access to trade secrets, socio-political motives, damage to the reputation of competitors

Social engineering

- It uses means of psychological manipulation of users' consciousness. The goal is financial gain, access to trade secrets, socio-political motives, damage to the reputation of competitors

Web application attacks

- They are committed by making unauthorized changes to their software code in order to create malfunctions

Distributed denial-of-service attack, DDoS

- They are implemented by creating a traffic overload of devices, programs, and the network as a whole in order to disrupt the work process

Malware

- It involves the integration of malicious code into running programmes and can be presented as viruses, Trojans or Worms. The goal is to make a profit, spread the ideology

Figure 1. The main threats to media security
(built by the author according to Caramancion et al. (2022))

Disinformation occupies an exclusive place among the threats presented in Figure 1. In the author's opinion, the mentioned threats (with the exception of disinformation and social engineering) relate mostly to the need to strengthen cyber security in the media sphere. In other words, the countermeasure against these threats should be aimed at improving the security and stability of technological solutions in the field of media against unauthorized interference. Many countries have a regulatory framework for countering such interference, but it is quite possible to detect them. At this time, disinformation is a complex phenomenon: it can spread through various channels even without the use of the latest technological means, although it acquires more forms with their use. Disinformation is difficult to detect, especially if it is not an outright deception and presented as the views of individuals or parties. Besides, the international and national legislation of countries have insufficiently defined or missing important aspects regarding countering misinformation.

So, disinformation should be considered as a key threat to media security. It combines a number of such tools as:

- propaganda;
- fake news;
- information leakage;
- manipulations;
- fake media content.

The complexity of the phenomenon of disinformation is expressed through the possibility of its realization through the information leakage by using cyber-attacks, the role of disinformation in information war, as well as significant influence on political processes through the transformation of public views. Disinformation can cause such serious consequences as the loss of public trust in the media, social unrest, and influence on democratic processes.

Case studies of cases of disinformation

The destructive impact of disinformation can be demonstrated by analysing cases in which disinformation campaigns played a significant role. Studies (Nagasako, 2020), analytical reports (Lublin Triangle Perspective, 2022) and statistics (OECD, 2022) testify that Russia is most often the main actor in conducting global disinformation companies, followed by China. The impact of Russian disinformation campaigns has particularly grave implications in the context of Russia's large-scale invasion of the sovereign territory of Ukraine on February 24, 2022. The use of deepfake technology to influence social sentiments in Ukraine can be an illustrative case of the use of disinformation tools. Although the origin of the video has not been established, it is believed to have been part of an information war waged by Russia. In the video, Ukrainian President Volodymyr Zelenskyi allegedly tells Ukrainian soldiers to give up the struggle and surrender the war. The record had clear signs of a fake, because the video was of low quality and it was easy to recognize a fake (Kumar, 2022; Papanis et al., 2014). The purpose of its distribution was to sow panic, create public unrest in the country, and it was also intended to sow doubts about the credibility of future addresses of the President.

In addition to deepfake technology, hackers also widely use the collection of user data (for example, collected by advertisers) that they obtain through data leaks. Information can be used to increase tension in society, because the data obtained is directed to the development of tools that deepen human prejudices. Moreover, hackers use personal information to commit phishing attacks, as happened before the 2016 US presidential election, when Russian cybercriminals hacked into the email of a US government official to obtain and release information (Kumar, 2022). The use of bots to spread disinformation in social networks is gaining popularity.

Key areas of ensuring media security

The main measures to ensure and strengthen media security can be divided into the following areas:

- technical measures;
- improvement of the national and international legal framework;
- improvement of user media literacy and awareness.

Technological measures include various methods of media content encryption during its reception, storage and transfer, watermarking and fingerprinting methods, digital signatures, certificates, secure communication protocols, etc. The effectiveness of using these tools depends on the involvement of qualified cyber security specialists, as well as the readiness to make appropriate investment.

The strengthening of threats of various origins, including hybrid ones, necessitated the development of legislation on countering misinformation. The EU activity, which conducts an effective policy to combat misinformation, deserves special attention. In this regard, it is appropriate to analyse the latest EU legislative acts in this area (Table 1).

Table 1.
Recent EU legislative acts on combating misinformation

Legislative act	Purpose	Advantages	Disadvantages	Areas for improvement
General Data Protection Regulation (GDPR)	Protection of privacy and regulation of campaigns for personal data processing and protection	Obliges companies to integrate privacy into the operation and creation of new systems. Possible positive impact on reducing the sale of personal data to brokers. Large fines for breaking the rules encourage compliance. Regulations governing the use of deepfake technology	Difficulties in implementing the requirements of the regulation, unregulated issues related to information attacks	To increase efficiency, companies should implement effective internal policies, implement reliable technological security measures, train personnel and cooperate with experts
The EU Artificial Intelligence Act (EU AI Law)	Regulation of the use of artificial intelligence technologies for consumer protection	Distribution of risks by levels and application of different measures for each level	Insufficient requirements for transparency, lack of their combination with a clear sanction for non-compliance	Strengthening requirements for transparency, introduction of sanctions for abuse of artificial intelligence

Digital Services Act, DSA	Combating misinformation	Demand that technology companies shall be held liable for content created by users and enhanced through the application of algorithms on their platforms. Demand to remove inappropriate content. for Transparency requirements	Determining the balance between responsibility for content and freedom of expression. Balancing transparency and privacy requirements. Difficulties during realization and implementation.	Creation of conditions for productive cooperation between regulators and companies, improvement of crisis protocols

Source: created by the author based on Kumar (2022)

The EU has taken a number of decisive actions in the field of combating misinformation, but the current legislation needs constant revision and improvement because of the rapid development of technologies and the increased number and scale of threats. Besides, international norms should be supplemented by the development of legislation in the field of media security at the national level, because the media sphere of different countries has its own peculiarities that must be taken into account. The need to conduct recurrent campaigns for Internet users and employees of companies in the field aimed at increasing their awareness and media literacy is worth noting in this context. Figure 2 shows the values of two important indices in this area for European countries, namely Media Freedom Score and Media Literacy Index.

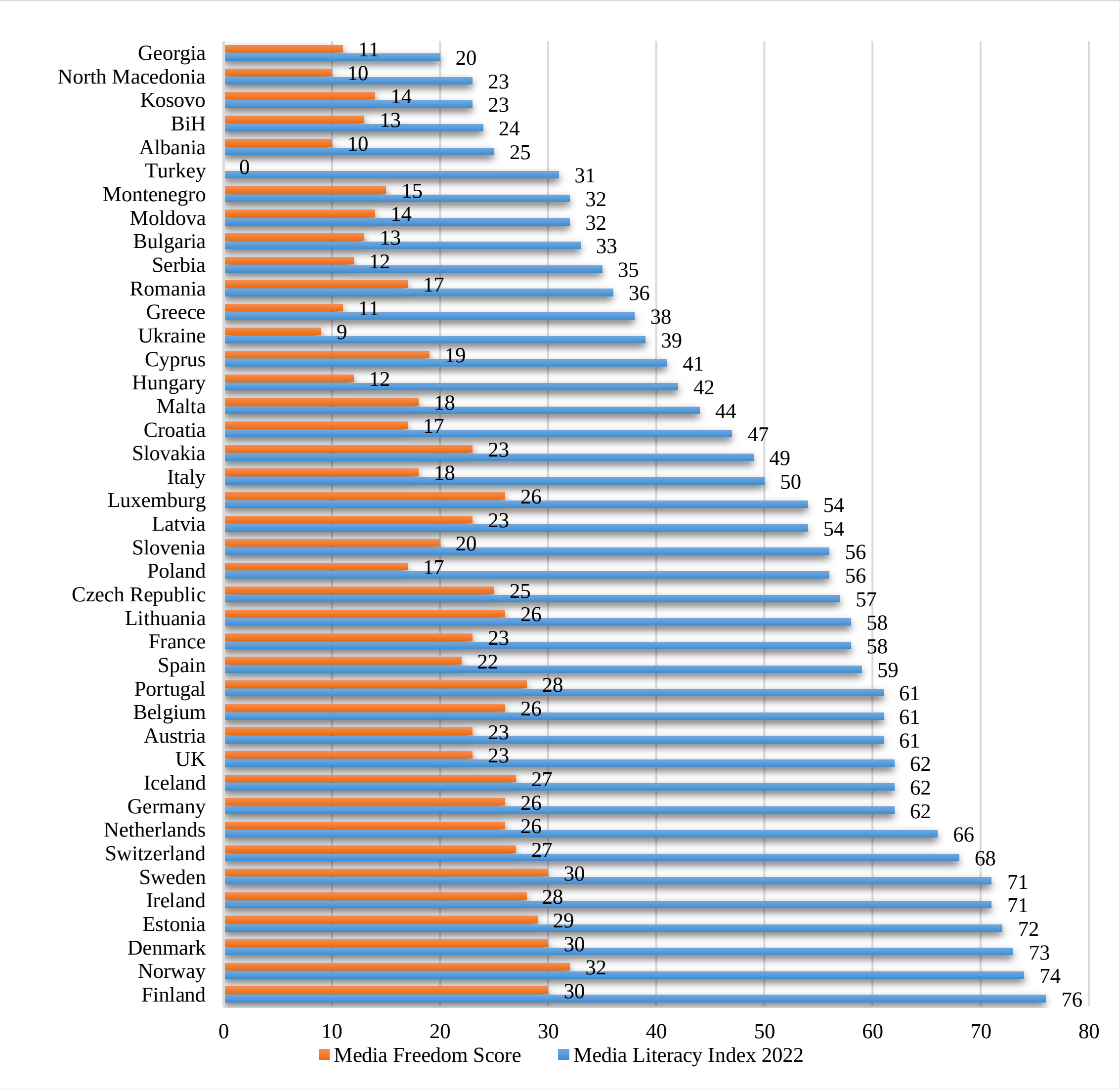


Figure 2. Media Freedom Score and Media Literacy Index 2022
(built by the author based on Lessenski (2022))

The greater the value of the indicators shown in Figure 2, the higher the country's position in terms of media literacy and media freedom. The list is headed by the Scandinavian countries - Finland, Norway and Denmark. At this time, countries such as Ukraine, which is a vivid example of a state that has been significantly affected by information war, is very low on the list for both indices. Therefore, it is critically important for the state to promote the development of responsible journalism and improve media literacy of the population, encourage it to critically evaluate the proposed content from various sources, especially in view of the full-scale invasion of Russia into Ukraine. Sources through which Europeans get news and their percentage of popularity are shown in Figure 3.

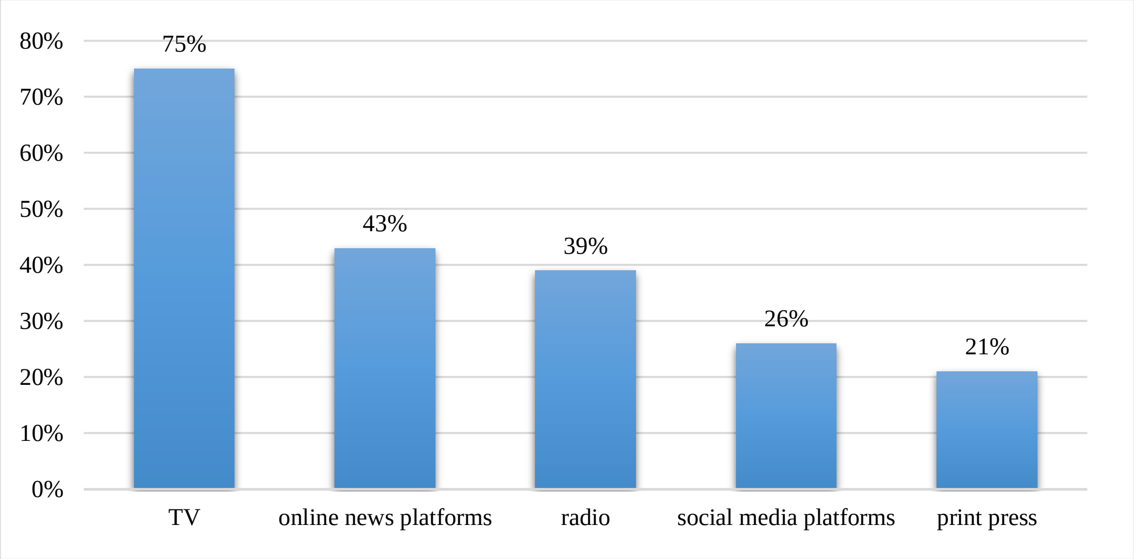


Figure 3. Most used media to access news in Europe
(built by the author based on Lessenski (2022))

The majority of users prefer television, although a significant share of the population increasingly uses new media, which necessitates close attention to aspects of their regulation. Television is heavily censored, and new media can be virtually unmanageable. This once again emphasizes the development of relevant legislation, means of technological countermeasures against disinformation and other threats, as well as promoting the improvement of media literacy. Improving media literacy will be most effective if special educational programmes are introduced in schools and universities. This will contribute to the regular assimilation of the necessary skills, which should be updated and reinforced through regular media awareness campaigns.

Discussion

The results obtained during the study of the legislative aspects of ensuring media security are consistent with those of Nagasako (2020), who focuses on the need for the development of international norms and rules of countering misinformation. A problematic aspect in the development of legislation in this area is combating disinformation while preserving freedom of speech. An emphasis on the need to develop national legal standards along with international ones is common in the studies.

The findings on improving media security through improved media literacy and the development of responsible journalism are consistent with those of Dhiman (2023). The researcher notes the need to develop critical thinking, conduct fact-checking, educational campaigns, develop responsible journalism, ensure ethical standards in the media, etc. The author of this article reveals these and other activities are elements of media literacy.

Temmermans et al. (2022) described an approach to overcome the challenges of deep fakes and non-fungible tokens. The essence of the method is to develop a modular scalable structure containing various protected media applications. Derner and Batistič (2023) provide strategies for mitigating the negative effects of using ChatGPT, including tagging data, advanced content filtering, scanning raw data, or using artificial intelligence to filter it. ALsaed and Jazzar (2021) propose solutions to mitigate cyber-attacks: developing general guidelines for teleworkers; rapid risk management mechanisms; fight against infodemic campaigns; international cooperation; use of software tools; application of safe and updated systems. Unlike these studies, the author's work does not dive deep into the technological aspects of media security, it focuses on legislative issues, problems of insufficient user awareness and media freedom.

Caramancion et al. (2022) conclude that cyber threats, where disinformation is identified as one of those threats, play on human weaknesses. In order to counter these threats, the cybersecurity content of manuals must be regularly updated, and disinformation must be viewed through the prism of the harm it causes to individuals, organizations, and governments. In general, agreeing with the reseachers' conclusions, the author of this article is inclined to separate disinformation from cyber threats. First, disinformation is not only spread in cyberspace, and second, it rather uses cyber means for its spread, but is not one of them.

Petratos (2021) provides recommendations for countering the cyber risks of misleading information: creating digital transformation strategies; recognition, identification and assessment of cyber risks; establishment and adoption of standards and norms; use of various tools to combat misinformation; partnership development; a sufficient amount of investment in measures to combat misinformation. Researchers consider disinformation as a factor that can create cyber risks for various actors in cyberspace. In the author's opinion, disinformation does not create cyber risks, but uses their potential to spread its harmful influence. Therefore, disinformation is the primary source of problems, and countermeasures should include not only countering cyber threats and strengthening technological characteristics, but also legislative, social, educational, and psychological aspects.

Rodríguez-Ferrándiz (2023) identified a trend in the spread of rumours as "virality" and "memeticity" that prevail over the credibility of the source and even the credibility of the reported event. The motivation that drives users to spread the news depends not so much on its accuracy, but on the tastes, moods of the community, as well as party support. These findings support the findings of this study regarding the need to improve media literacy.

Sousa-Silva (2022) note the availability of technological means to detect fake news, but find a lack of a proper mechanism in this area. The researchers believe that forensic linguistic analysis is an effective way to detect fake news. In the author's opinion, given the high speed of information dissemination, media literacy skills can be more useful, and forensic linguistic analysis should be used in some difficult cases.

A number of studies focus on the problems of spreading disinformation during elections. Pyrhönen and Bauvois (2020) analyse the nature of the spread of disinformation during elections, while Tan (2020) offers his own electoral management digital readiness index. The index provides an assessment of the legal framework, strengths and weaknesses of election management bodies, and includes criteria such as the type of election management model, the rules regulating online campaigns and disinformation, the degree of confidence in the rule of law, and technological aspects of digital economy readiness. In the author's opinion, the index proposed by the researcher can provide an approximate estimate of the readiness of the election process management, but it has limitations, because this process is influenced by too many factors. The author also believes that the assessment of the readiness of the election management should include the readiness not only of the governing bodies, but also of the citizens, which involves, among other things, in their ability to recognize disinformation.

Studying the problems of spreading disinformation during the information war, Kumar (2022) notes the Ukrainian case of the large-scale invasion of Russia on the territory of Ukraine. The researcher identifies the inadequacy of the current regime of international law in the field of combating disinformation as the main problematic aspect, and therefore the main way of combating it is to improve the legal system at the international level. This point is worth agreeing, because the development of legislative aspects regarding the introduction of certain rules and responsibility for their non-fulfilment is the most effective way of ensuring media security, and should be accompanied by the improvement of the technological resources and awareness.

Conclusions

The conducted analysis emphasizes the need to create a comprehensive approach to ensuring media security in the era of information globalization. the main threats to media security were determined as a result of the study, the most significant of which is disinformation. Disinformation is a complex phenomenon and can spread through numerous channels even without the use of the latest technological means. The latter contribute to acquiring an increasing number of forms of realization. Disinformation combines propaganda, fake news, information leakage, manipulation, fake media content. The complexity of the phenomenon of disinformation is manifested by the possibility of implementing it through the information leakage using cyber-attacks, the role of disinformation in information war, and a serious impact on socio-political processes.

Russia and China cause greatest concern regarding the volume of disinformation and propaganda being spread, especially in the context of Russia's invasion of Ukraine. Case studies of cases of disinformation gave grounds to note the variety of ways of its implementation, including through the latest deepfake technologies and phishing attacks.

The conducted analysis determined the main areas of ensuring media security, which include: technical measures, improvement of the national and international legal framework, improve media literacy and user awareness. The measures proposed in each of the areas will increase the level of media security in the countries, in particular by making the fight against disinformation more effective. The prospects for further research may be developing a comprehensive programme for improving the media literacy of the population in terms of different age groups and subjects of the implementation of the programme.

Bibliographic references

ALsaed, Z., & Jazzar, M. (2021). Covid-19 age: Challenges in cybersecurity and possible solution domains. *Journal of Theoretical and Applied Information Technology*, 99(11), 2648-2658. http://www.jatit.org/volumes/Vol99No11/12Vol99No11.pdf

Bahrini, R., & Qaffas, A. A. (2019). Impact of information and communication technology on economic growth: Evidence from developing countries. *Economies*, 7(1), 21. https://doi.org/10.3390/economies7010021

Bindu, G. H., Anuradha, C., & Chandra Murthy, P. S. R. (2018). A survey on multimedia content protection mechanisms. *International Journal of Electrical and Computer Engineering (IJECE)*, 8(6), 4204. https://doi.org/10.11591/ijece.v8i6.pp4204-4211

Brody, D. C. (2019). Modelling election dynamics and the impact of disinformation. *Information Geometry*, 2(2), 209-230. https://doi.org/10.1007/s41884-019-00021-2

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data*, 7(4), 49. https://doi.org/10.3390/data7040049

Colomina, C., Margalef, H. S., Youngs, R., & Jones, K. (2021). *The impact of disinformation on democratic processes and human rights in the world. Brussels*: European Parliament. https://acortar.link/vQgjU9

Derner, E., & Batistič, K. (2023). *Beyond the Safeguards: Exploring the Security Risks of ChatGPT*. arXiv:2305.08005. Cornell University. https://doi.org/10.48550/arXiv.2305.08005

Dhiman, D. B. (2023). Key Issues and New Challenges in New Media Technology in 2023: A Critical Review. *Journal of Media & Management*, 5(1), 1-4. https://ssrn.com/abstract=4387353

Gunther, R., Beck, P. A., & Nisbet, E. C. (2018). Fake news did have a significant impact on the vote in the 2016 election: Original full-length version with methodological appendix. *Unpublished manuscript, Ohio State University, Columbus, OH.* https://acortar.link/IiWzTx

Kumar, S. (2022). *Information Warfare in The Digital Era: An Analysis of The Existing Legal Framework*. The New York University School of Law. http://dx.doi.org/10.2139/ssrn.4344520

Lessenski, M. (2022). *Media Literacy Index 2022. Main Findings and Possible Implications*. OSI-Sofia. https://www.osce.org/files/f/documents/0/4/534146.pdf

Lian, S. (2009). Multimedia Content Protection Technology. In: Pagani M. (ed.), *Encyclopedia of Multimedia Technology and Networking*, Second Edition (pp. 957-964). Hershey, New York: IGI Global. https://acortar.link/t0PBYS

Liu, L., Zhang, W., & Han, C. (2021). A survey for the application of blockchain technology in the media. *Peer-to-Peer Networking and Applications*, 14(5), 3143-3165.

Lublin Triangle Perspective. (2022). Resilience to disinformation. *[File PDF]* https://acortar.link/ZhvWVF

Marsden, C., Meyer, T., & Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation?. *Computer law & security review*, 36, 105373. https://doi.org/10.1016/j.clsr.2019.105373

Nagasako, T. (2020). Global disinformation campaigns and legal challenges. *International Cybersecurity Law Review*, 1(1-2), 125-136. https://doi.org/10.1365/s43439-020-00010-7

OECD. (2022). *Disinformation and Russia's war of aggression against Ukraine*. https://acortar.link/IfqLXz

Ortiz-Ospina, E., & Roser, M. (2019). *The rise of social media*. Our world in data. https://ourworldindata.org/rise-of-social-media?ref=tms

Papanis, J. P., Papapanagiotou, S. I., Mousas, A. S., Lioudakis, G. V., Kaklamani, D. I., & Venieris, I. S. (2014). On the use of Attribute-Based Encryption for multimedia content protection over Information-Centric Networks. *Transactions on Emerging Telecommunications Technologies*, 25(4), 422-435. https://doi.org/10.1002/ett.2722

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in cognitive sciences*, *25*(5), 388-402. https://doi.org/10.1016/j.tics.2021.02.007

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, 64(6), 763-774. https://doi.org/10.1016/j.bushor.2021.07.012

Pyrhönen, N., & Bauvois, G. (2020). Conspiracies beyond fake news. Produsing reinformation on presidential elections in the transnational hybrid media system. *Sociological Inquiry*, 90(4), 705-731. https://doi.org/10.1111/soin.12339

Rodríguez-Ferrándiz, R. (2023). An Overview of the Fake News Phenomenon: From Untruth-Driven to Post-Truth-Driven Approaches. *Media and Communication*, 1*1*(2), 15-29. https://doi.org/10.17645/mac.v11i2.6315

Shen, C., Kasra, M., Pan, W., Bassett, G. A., Malloch, Y., & O'Brien, J. F. (2019). Fake images: The effects of source, intermediary, and digital media literacy on contextual assessment of image credibility online. *New media & society*, 21(2), 438-463. https://doi.org/10.1177/1461444818799526

Sousa-Silva, R. (2022). Fighting the fake: A forensic linguistic analysis to fake news detection. *International Journal for the Semiotics of Law-Revue*, 35(6), 2409-2433. https://doi.org/10.1007/s11196-022-09901-w

Tan, N. (2020). Electoral management of digital campaigns and disinformation in East and Southeast Asia. *Election Law Journal: Rules, Politics, and Policy*, 19(2), 214-239. https://doi.org/10.1089/elj.2019.0599

Tandoc Jr, E. C. (2019). The facts of fake news: A research review. *Sociology Compass*, 13(9), e12724. https://doi.org/10.1111/soc4.12724

Temmermans, F., Bhowmik, D., Pereira, F., & Ebrahimi, T. (2022, May). Media security framework inspired by emerging challenges in fake media and NFT. In *Optics, Photonics and Digital Technologies for Imaging Applications VII* (Vol. 12138, pp. 185-191). SPIE. https://doi.org/10.1117/12.2622223

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Addressing hybrid threats*. Architectural copy AB, Bromma. https://www.diva-portal.org/smash/get/diva2:1219292/FULLTEXT01.pdf

Vraga, E. K., & Tully, M. (2021). News literacy, social media behaviors, and skepticism toward information on social media. *Information, Communication & Society*, 24(2), 150-166. https://doi.org/10.1080/1369118X.2019.1637445

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, 19(3-4), 402-442. https://doi.org/10.1504/IJICS.2022.127169