ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

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

THE RISKS OF MISUSING SOCIAL NETWORKS IN THE CONTEXT OF HYBRID THREAT*

Bohuslava Mihalčová [1], Antonín Korauš [2], Stanislav Šišulák [3], Peter Gallo [4], Jozef Lukáč [5]

[1,5] Faculty of Business Economy of the University of Economics in Bratislava with seat in Košice, Tajovského 13, 04001 Košice, Slovak Republic
[2,3] Academy of the Police force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovak Republic
[4] University of Presov, Faculty of Art, St. 17, Novembra č.15 080 01 Prešov, Slovak Republic

E-mails:[1] bohuslava.mihalcova@euba.sk; [2]antonin.koraus@minv.sk; [2]stanislav.sisulak@akademiapz.sk; [2]peter.gallo1@unipo.sk; [5]jozef.lukac@euba.sk

Received 11 February 2023; accepted 14 June 2023; published 30 June 2023

Abstract. The world today is ceaselessly under the influence of changing conditions and threats. The contemporary digital age enables the provision of information that serves not only as common information but also as disinformation and hoaxes. This risk is high, specifically on social networks, dramatically impacting society. The paper's main objective is to point out the danger of misusing social networks to spread disinformation as a hybrid threat to influence people's thinking and behaviour, thus endangering democratic processes in developed democratic countries. The study, which focused on the risks of misusing social networks, was conducted using the questionnaire method and was subsequently assessed using statistical tests. The results indicate no link between age and the ability to distinguish desinformation, and that age does not influence the effects of disinformation. However, we did find the opposite result in terms of education, where people with lower education share hoaxes and disinformation more. Alternative media, whose posts are shared by more than 20% of social network users, have a relatively strong presence in our environment. The possibilities of spreading disinformation are also evident in the social impacts on users, who, according to our study, fear lowering their economic well-being. The study focuses on the effects of social networks on individuals' thinking and behaviour. Because we consider this issue insufficiently studied thus far, attention must also be paid to it in the future.

Keywords: disinformation; hoaxes; social impacts; social networks; economic well-being.

Reference to this paper should be made as follows: Mihalčová, B., Korauš, A., Šišulák, S., Gallo, P., Lukáč, J. 2023. The risks of misusing social networks in the context of hybrid threat. *Entrepreneurship and Sustainability Issues*, 10(4), 357-371. http://doi.org/10.9770/jesi.2023.10.4(22)

JEL Classifications: H55, O35, Z13

* *The contribution was created as a result of the project: Research of educational concepts in the field of hybrid threats within selected EU countries with the subsequent elaboration of the education concept for SR conditions project code in ITMS 2014+: 314011CDW7*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

1. Introduction

Misusing social media as an instrument for hybrid threats and modern hybrid warfare is unsurprising (Tvaronavičienė et al., 2020; Milbradt et al., 2023). And it is specifically Internet technology that has been developed to meet the needs of information age warfare. Around 2006, Web 2.0 began allowing Internet users to create "news" content instead of just consuming it online. An individual can thus decide what is essential for them to know. Users not only choose news and media but also create these things themselves, declaring their own views, often without considering their truth and their effect on individuals and society. The social nature of people ultimately led also to the creation of virtual networks in the past.

On the one hand, social networks are necessary in today's digital age; on the other hand, they have become a node for information operations and cyber warfare. Social networks enable people who share interests and activities across political, economic and geographic spectra to connect. An ever-increasing number of individuals are searching the Internet and social media to fulfil cognitive, affective, personal, integrational, and social integrational needs in a stress-free way. Aside from fulfilling such requirements, social networks impact everyday life, including relationships, school, religion, entertainment and family. People use social networks to obtain information about the personalities and behaviours of potential employees, and a presence on social networks also contributes to a new form of abusive communication. Academic research has pointed out many socio-technological explanations for this behaviour, including the anonymity provided through interpersonal communication, factors related to boredom or attention-seeking, or the result of more polarised online discussions. The impact of this abuse has been manifested in the rise in online cyberbullying and so-called trolling, and there has also been a significant increase in political violence through the misuse of social media platforms (Hawi & Samaha, 2017). To understand the given issue, the authors decided to examine the impact that the modern trend of using social media is having on people. The authors' primary objective is to point out the danger of misuse of social networks for spreading disinformation as a hybrid threat aimed at influencing people's thinking and behaviour, thus endangering democratic processes in developed democratic countries.

2. The current state of domestic and foreign knowledge

Hybrid threats and disinformation are not new concepts; they are not even an achievement of the 21st century or the current information age. The famed Chinese general Sun Tzu refers to the strategy of indirect combat using lies and fraudulent messages as early as in the 6th century BCE in his work The Art of War, where he states that the best war is the one that has not even started. In his view, military art is a struggle for advantage or gain without the clatter of weapons. Sun Tzu is considered the most significant military strategist of all time. His strategic art rested in the proposition, "Never declare battle tactics in advance. Herein lies the mastery of the victors of wars". In his work, Sun Tzu focuses much more on alternatives to war than on armed battle, considering such alternatives as robbery, delay, spies, lies and false, deceptive information or forming and maintaining alliances. Palau-Sampio et al. (2022) point out that we can also find textbook examples of the use of disinformation in ancient Greece from the period of the Greco-Persian wars, when the Athenian duke Themistocles, for example, defeated the Persian king Xerxes in some battles with the help of false messages sent through supposedly escaped enslaved people.

Another excellent strategist was Philip II of Macedonia, who implemented significant military reforms during his reign and initiated the most glorious period of old Macedonia. He succeeded in stabilizing the situation domestically and abroad and gradually launched Macedonia's expansionist policy using military force, especially diplomacy. A significant strategist of the 18th century was Napoleon Bonaparte, a renowned French duke and later emperor who conquered much of Europe in the early 19th century and changed the world. Napoleon was born on the island of Corsica and rose quickly by serving in the army during the French Revolution. After gaining political power in France, he was crowned emperor in 1804. His strategic strength consisted not only in the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

military might of his army but also in four fundamental strategic innovations, one of which was a circumvention strategy based on information about the enemy, deceiving him with fake news and diplomacy. We can also observe hybrid threats or elements of them in the practices of Germany during the Second World War. The Germans used not only political means but also propaganda, information and resources of an economic nature (Lukáčová, 2019). The modern history of the 21st century relating to this concept began in 2008 when Russia and separatists declared the independence of two regions of Georgia (Abkhazia and South Ossetia). The Russians began using hybrid threats on a larger scale in 2014, when they annexed Crimea. This involved deploying unmarked soldiers (green men), mobilizing domestic paramilitary groups supported by the intelligence services and the cyber and information operations that have become typical tactics used in eastern Ukraine. At present, the importance of such a hybrid threat in Russia's military conflict in Ukraine is deepening, while the dimension of direct military conflict between the armed forces of these two countries is also increasing. The significance of the hybrid threat is multiplied by aerial missile and artillery attacks on schools, hospitals, residential buildings and essential infrastructure. These methods cast a shadow over the free-thinking of the citizens of the war-stricken regions, limit the resolution of the resistance and disrupt the completeness of Ukraine's offensive activities. The crucial goal of Russian hybrid threats is to disrupt the spontaneous will of the Ukrainian people to defend themselves against the aggressor.

The development and ever-increasing use of digital technologies have revolutionized how we acquire information and make a wide range of decisions. Spreading news via the Internet or updating statuses on social networks can be done by almost anyone through social networks. A prerequisite for effective research in this area is a thorough analysis of the environment, the region, the European Union or a global comment (Linkov, 2019). Hybrid threats of the 21st century are a challenge for all countries, and we are generally seeing a growing sense of insecurity and friction in communities. The reach and impact of hybrid threats are asymmetric, complex and ambiguous (Treverton, 2018). The users of social networks, and not only in Un-recognized countries, enter personal and private information (e.g. family status, date of birth, name of work/school, e-mail address, telephone numbers and even residential address) onto these networks, and this information can fall into the wrong hands and be used to harm users in both the virtual and real worlds (Fire et al., 2014). Privacy threats can be generally categorized as threats to the privacy of information, physical privacy, and state privacy (O'Brolcháin et al., 2016). The misuse of social media is causing increased levels of harm for larger populations and groups of users compared to previous decades, as we registered a record amount of social media use during the COVID-19 pandemic (Luo et al. 2022).

To reduce security risks on social networks, combinations of five solutions, the simultaneous use of which will help the user, have been proposed. This is mainly in restricting the sharing of certain information, setting the personal data of the social network user, securing access to applications, or thinking twice about how you use the social network approach (Sadeghian et al., 2013). The result of Atkinson and Chiozza (2021) research is that women (rather than men) and internationalists (rather than nationalists) are the people who make a more critical distinction between targeted surveillance, which is acceptable to them, and blanket surveillance, which they are unwilling to respect. In their research, Kirichenko et al. (2018) focus on the basic methods of graph theory and data mining, which he uses to analyze social networks. He examines the security risks of social networks, concentrating on detecting network communities, community leaders, network detection experts and text information clustering, among others.

Popularizing social networks among users also influences public administration, intending to create a system of open administration, thus changing the relationship between a government and its citizens. The consequences of using social networks and security in e-government should become a subject of research. The security threats a citizen can find on social networks are methodically assessed and classified according to selected criteria. The essential criteria are the gathering of confidential information, a loss of reputation in government-to-citizen (G2C) relations and the organizing of socio-political conflicts (Alguliyev et al., 2018). For example, based on a study by

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Pathe Duarte (2020), cyber-attacks in Portugal by foreign groups aiming to collect information and data have increased in recent years, which causes governmental and private critical infrastructure to become vulnerable.

Dragos et al. (2020) report on studies that used different approaches to identify hidden patterns in social media texts, where the text is highly unstructured, arrives with a mixture of modalities and potentially has incorrect spatiotemporal errors. The study states that the uncoupled use of machine-learning models and semantically driven approaches in social media data mining has several areas for improvement. Tagarev and Sharkov (2016) address the proactive identification of advanced hybrid threats in modern social networks. Since these threats are invisible and require the long-term comprehensive monitoring of technologies and users, a mixed methodological framework is proposed for them. Mareš and Mlejnková (2023) state that pan-Slavism and Slavophilia are being used to mobilize specific actors within Czech politics who undermine the official, pro-Western orientation of the Czech Republic.

Hybrid threats are one of the new security challenges in Europe and can shape the continent's future in terms of current geopolitical developments. The policy of the EU is that the primary responsibility for combatting them lies with member states and that NATO's mandate for the security of Europe makes it an essential partner for the military and conventional aspects of deterrence when handling hybrid threats (Lonardo, 2021). Hybrid threats are also monitored from the viewpoint of media, which starts with recognizing the extent of such threats. The target here is society, not armies, and they examine how the cyber dimension and social media offer new, low-cost methods of attack (Treverton et al., 2018). Research by Tagarev and Sharkov (2016) outlines a general model of the hybrid nature of terrorism, accenting the role of modern cyberspace and reminding institutions to look deeper into the issue from both the technological and human sides to contribute to a more secure future for the world. In the view of Bodnar-Pidhurska et al. (2022), the battle against hybrid challenges should focus on developing and implementing new innovative technologies intended to reduce the release of harmful information into the environment while also updating the issue of the still forming ecological awareness of employees and the ecological code of businesses, which affect the environment of their social networks. Industry 4.0 and intelligent manufacturing are associated with cybernetic systems housing and controlled by collective intelligence. Research in this area has found a particular analogy between the (cognitive) resistance of human and artificial intelligence towards mental hacks (particular hybrid adversary activity) and proposed approaches to teaching resistance using special training techniques (Kaiková et al., 2022).

3. Selected social network platforms and ways of spreading disinformation there

Among the most crucial social network platforms are Facebook, Instagram and Twitter. Facebook, founded in 2004 by Mark Zuckerberg, is currently the largest social network in the world, with roughly 3 billion active users. It allows users to connect with people, companies, and organizations. It can be used to post updates, react to the posts of others, share photos and links to online content, chat live and record and share videos. Users can communicate directly with each other via Facebook's Messenger app. They can, join groups with similar interests and stay informed about the activities of friends and the pages they choose to follow. Facebook was designed to be open and social.

Instagram, founded in 2010 by Kevin Systrom and Mike Krieger, is a similar social network and can even be called a direct relative. It is focused on the sharing of visual media. It allows users to upload media that can be edited with filters and organized employing hashtags and geotags. Posts can also be shared publicly. Instagram today has about 1.5 billion active users.

In 2006, Jack Dorsey, Noah Glass, Biz Stone and Evan Williams founded Twitter, a social network that allows people to communicate using short message posts called "tweets". Tweeting is also sometimes referred to as microblogging. Twitter allows users to scan and distribute content quickly, conveniently and easily, which may be

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

why it is popular among those who want to get a lot of news out into the world and those who wish to follow such users quickly. According to Paradowski et al. (2021), Twitter had about 430 million users in 2021, expected to grow to nearly 500 million users and followers by 2025.

Disregarding the positive sides of using social media, it can also become a tool for disinformation. Selected employees of Twitter and Facebook are responsible for the algorithms that analyze words, phrases and the most discussed topics in order of importance. Thus, Social media algorithms can create echo chambers in which polarised discussions occur and share polarised information. Political "bots" (software agents used to generate simple messages and "conversations" on social networks) pretending to be fundamental movements serve to manipulate public opinion. By using existing online networks combined with an automated "bot", foreign agents can also "insert" disinformation into social media, thus creating a platform and a trend to spread the message as quickly and cheaply as possible, and they can do it at a lower cost than through any other medium. "Bots" are computer algorithms that operate on social networking sites and perform tasks autonomously and repeatedly. They simulate people's behaviour on the social network, interacting with other users and sharing information and posts. On Twitter, for example, "bots" can mimic social interactions, making them appear "regular" people. They seek out Twitter influencers (Twitter users with a lot of followers), and users contact them by sending questions to be noticed and gain their trust and the trust of other users. They react to posts or questions from others based on pre-programmed scripts and also spark debates by posting news on trending topics (Sheoran & Yadav, 2021).

Disinformation algorithms contain three essential components: technical, social and financial. The technical component is computational disinformation, which represents an autonomous grouping of social media platforms whose task is to manipulate public opinion. The social element is focused on the way people think. This type of propaganda has existed in our political systems for millennia. It represents a way of communication that deliberately presents misleading information and disinformation intending to appeal to our base emotions and prejudices and bypass rational thinking to achieve the specific goals of its distributors. Financial disinformation also plays a significant role, manipulating people's thinking about finances and often can even trick them out of their savings.

The spreading of disinformation on social networks is also made possible with the help of so-called trolling and cyberstalking. Trolling is an IT term that represents harassing activity, whether in discussions, chats or posts. A troll intends to spark conflict and controversy, for example, by initiating provocative debates, using insults and sending offensive messages. Trolls operate on forums, social networks and in any other online format, and in general, they adopt false identities that make them feel comfortable on social media. They do not know their victims directly, but as with cyberbullying, they can act at any time. Given their increasing number and danger, many discussion forums are ongoing in governments in the US and the old continent. An organization was even founded in the USA to deal with this issue.

Rainie and Wellman (2012) note that trolls are people with severe sociological, mental and deeply rooted psychological problems that arise from regulatory transgression, mental illnesses and issues with their sexual identity. Garton et al. (2006) state that we also study the idea of cyberstalking – the use of social networks to follow or harass a private person or company – concerning trolling. A cyberstalker is a person who posts deceptive or scurrilous statements about their target on social media to incite the victim to respond. Like trolls, they often create profiles and social network pages in the name of the victim with scandalous or pornographic content (Dino, & Gustilo, 2018; Aral, 2020; Winkler et al., 2021).

4. Methodology of the paper

The main objective of our survey was to point out the danger of spreading hoaxes and disinformation and to analyze selected aspects of such application on social networks. The stated aim of the study was defined in

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

connection with the determined hypotheses, which we subsequently verified through statistical methods. We decided on a questionnaire as the primary method of obtaining data for our study, as this is suitable for this type of research. The questionnaire comprised predetermined questions and answers associated with the issue of spreading hoaxes and disinformation on social networks, and we also used the possibility of combining open and closed questions. The questions on the questionnaire were also presented in the form of the Likert scale. Our research subjects were respondents of different demographic characteristics from public administration. For research purposes, we divided the questionnaire into two parts. The first was demographic, and the second was empirical, which was made up of questions and responses related to the issue of spreading disinformation and hoaxes on social networks. The demographic questions addressed the gender of the respondents, their age, the highest level of education, place of residence and work and social status, while the empirical part focused on questions specifically addressing hoaxes and disinformation on social networks. In the questionnaire, we asked about what type of social networks the respondents use for obtaining information, expressing their views on individual statements, with a focus on hoaxes and disinformation on social networks, on the trustworthiness of personal social networks, the monitoring of a person's information on social networks in terms of mainstream and alternative media and the possibilities which, in their view, prevent the spread of disinformation and hoaxes on social networks. Along with open and closed questions, we also used to queries in the form of a five-point Likert scale, with options ranging from agree to disagree completely. We presented this method of expressing opinions mainly when the respondents stated that they agreed or did not agree with individual statements aimed at the possibilities of combatting disinformation and hoaxes on social networks.

The questionnaire survey was conducted from October 2022 to February 2023. We approached 643 total respondents this way; however, only some were willing to participate in our survey. Only 171 completed questionnaires were returned to us, representing a 27% response rate. However, we consider this a standard return for this type of survey. For the needs of our study, we processed the data from the respondents using research methods such as descriptive statistics, contingency tables, and others, as well as analysis, comparison, synthesis, selection, induction and deduction. We verified the determined hypotheses using Pearson's Chi-square test of independence. We then compared the Chi-square calculation with the critical tabular value for our selected probability of error and the detected degree of freedom. We processed the hypothesis verification using the Chi-square test in Statistica statistical program from StatSoft version 12.0.

H1: We assume that there is a statistically significant relationship between age and the ability to distinguish disinformation.
H2: We assume a statistically significant relationship between education achieved and the sharing of verified information.
H3: We assume that more than 20% of respondents share the information reported by alternative media.
H4: We assume a statistically significant relationship between education achieved and people's behaviour under the influence of disinformation and hoaxes.
H5: We assume a statistically significant relationship exists between the spreading of information on social networks and users' concerns about social impacts on economic well-being.

5. Survey results

In the study, we dealt with the issue of hoaxes and disinformation on social networks, focusing on the ability to distinguish disinformation depending on the age of the user of social networks. In this context, we set a hypothesis in which we verified the dependence between the respondents' age and their ability to distinguish disinformation and hoaxes. Based on the data obtained, we assessed the presented hypothesis using the Chi-square test of independence. The test results are shown in Tab. 1.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Table 1. The results of testing the hypothesis

Pearson's Chi-square Test of Independence			
Calculated value	Error profitability	Degree of freedom	Critical value
p = 0.5936	α = 5% (0.05)	DF = 1.00	x^2 = 0.01

Source: own processing

The value calculated using the Chi-square test of independence was p = 0.5936, which, because it is more significant than 0.05, means that there is no statistically significant relationship between the respondent's age and the ability to distinguish disinformation and hoaxes. The presented data show that the respondent's age plays a minor role in the knowledge of social network users to determine whether the information is a hoax. We do not accept this hypothesis.

Figure 1 shows the hypothesis aimed at exploring the relationship between a respondent's age and the ability to distinguish disinformation and hoaxes.

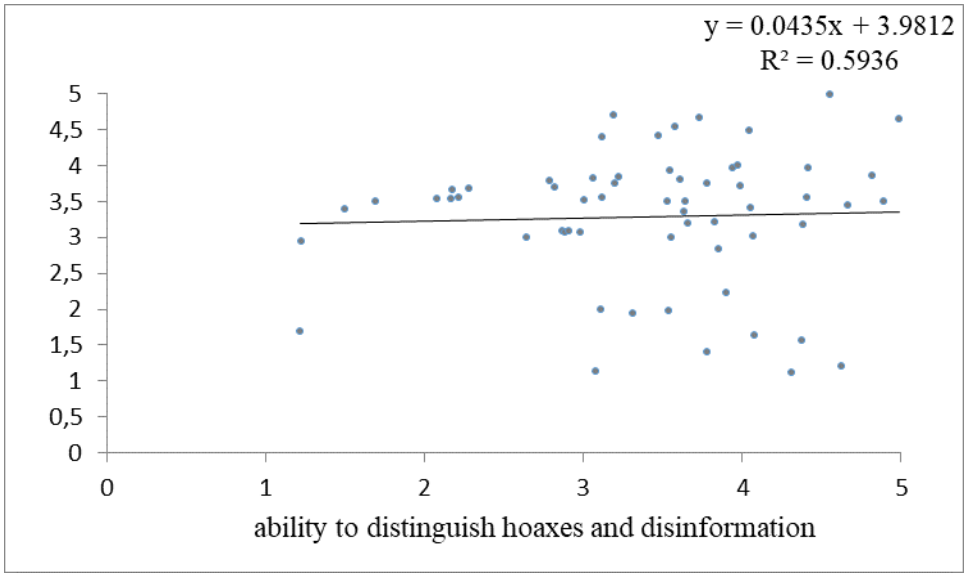

Figure 1. Dependencies between age and the ability to distinguish disinformation
Source: own processing

The education achieved by social network users also dramatically influences the spreading of disinformation and hoaxes. The subject of our research was also obtaining data that examines the respondents' education in terms of their dissemination of information on social networks. In this context, for our study, we determined a hypothesis to explore the dependence between respondents' education and the sharing of verified information on social networks. To verify the given hypothesis, we used the Chi-square test of independence method. The test results are shown in Tab. 2.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Table 2. The results of testing the hypothesis

Pearson's Chi-square Test of Independence			
Calculated value	Error profitability	Degree of freedom	Critical value
p = 0.0299	α = 5% (0.05)	DF = 1.00	x^2 = 0.01

Source: own processing

Based on data obtained from respondents, in verifying this hypothesis, our assumption was confirmed, as the test gave a calculated value of p=0.0299. This value is lower than 0.05, indicating a statistically significant relationship between education achieved and sharing verified information on social networks. When examining the responses from respondents in more detail, education plays an important role, which means that the higher the level of education, the more users share verified information. In this case, we accept the presented hypothesis. Figure 2 shows the relationship between education achieved and the sharing of verified information.

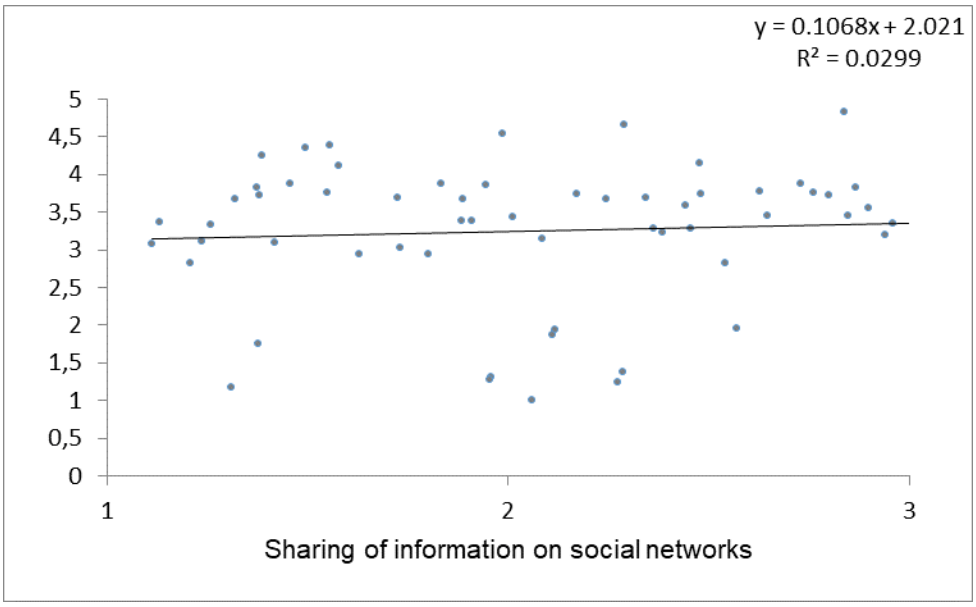

Figure 2. Dependencies between achieved education and the sharing of verified information
Source: own processing

In connection with various negative factors, such as the pandemic and the war in Ukraine, more alternative media are getting into the online space on social networks. In this regard, our study was interested in how information from this media type is shared on social networks. Therefore, we specified a hypothesis in which we assumed that information from alternative media on social networks is shared by more than 20% of the research respondents. The test results are shown in Tab. 3.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Table 3. Method of the proportion of the given phenomenon in the population

Indicator	Formula	Explanatory note
Method of proportion of a given phenomenon in population	$\hat{p} = 0.26923$ $\hat{q} = 0.67033$	$p = 0.2692? \pm 1.96 * \sqrt{\frac{0.2692 * 0.67033}{182}}$ $p = 0.26923? \text{“} 0.03149$ $0.2075? \%_{00} \text{¤} p? \%_{00} \text{¤} 0.3309$

Source: own processing

When verifying the hypothesis focused on the sharing of alternative media information on social networks, we used the method of the proportion of the given phenomenon in the population, which is suitable for use in the mentioned type of study, as we do not have data from all respondents. In this case, we set the probability coefficient value at 1.96, meaning validity at 96%. This calculation shows that sharing information from alternative media on social networks ranges from 20.75% to 33.09%. Fig. 3 shows the range of users who share alternative media content on social networks.

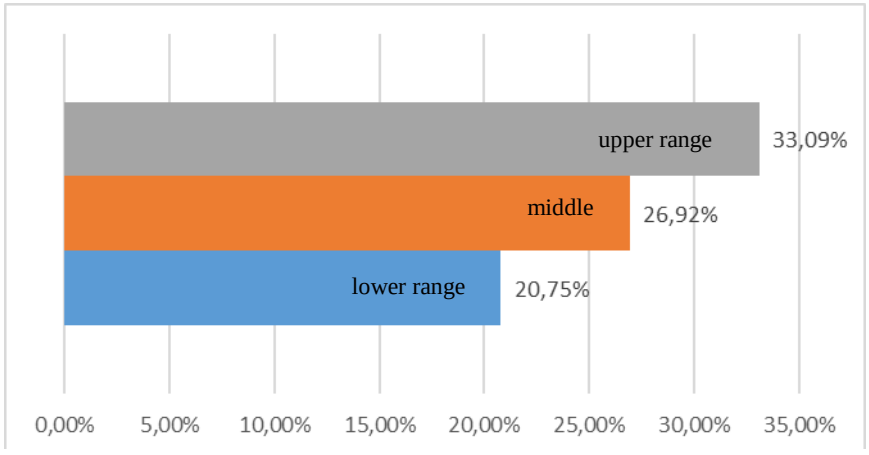

Figure 3. Range of users sharing alternative media content
Source: own processing

The hypothesis was confirmed because the stated values are above the set value of 20%. More than 20% of the study respondents shared information from alternative media. Thus, we accept the stated premise. The spread of disinformation and hoaxes also significantly impacts people's actions. Hoaxes influence many people to such an extent that changes occur in their actions that affect their society and family relationships.

The more educated a society is, the more resistant it is to disinformation and hoaxes. In this context, we examined the relationships between education and people's behaviour. We determined a hypothesis for the study looking at the assumption that there is a statistically significant relationship between education achieved and the way people act under the influence of disinformation and hoaxes. The results from the statistical verification of this hypothesis are shown in Tab. 4

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Table 4. The results of testing the hypothesis

Pearson's Chi-square Test of Independence			
Calculated value	Error profitability	Degree of freedom	Critical value
p = 0.0163	α = 5% (0.05)	DF = 1.00	x^2 = 0.01

Source: own processing

From the presented results, in verifying this hypothesis, our assumption was confirmed, as the test determined a calculated value of p=0.00163. The stated value is lower than 0.05, meaning there is a statistically significant relationship between education achieved and how people act under the influence of disinformation and hoaxes. A more detailed examination of the data from the respondents confirms that the lower the respondents' education, the more significant the effects of disinformation and hoaxes on their behaviour. In this case, we accept the stated hypothesis.

Figure 4 shows the relationship between education achieved and people's behaviour under the influence of disinformation and hoaxes.

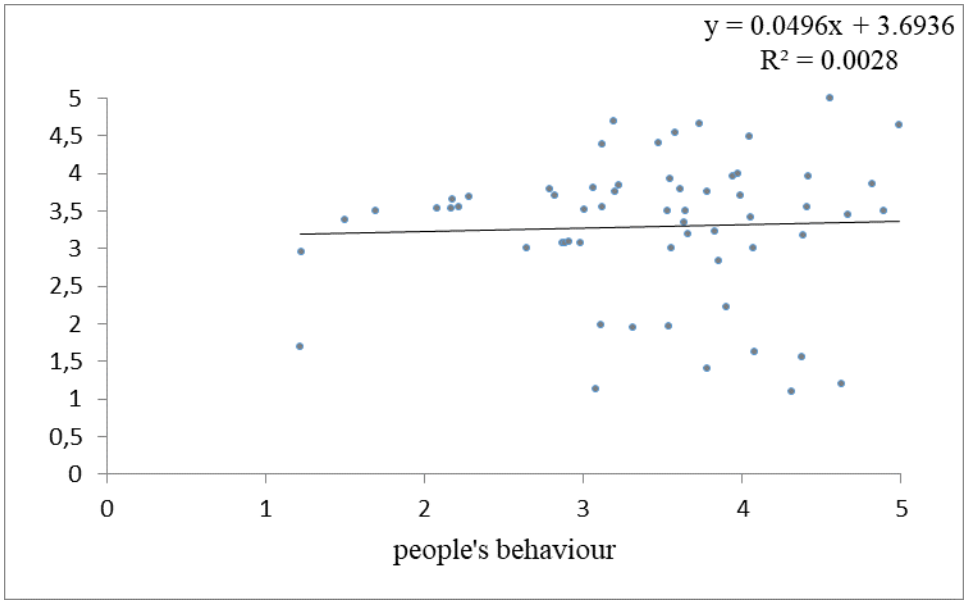

Figure 4. Dependencies between achieved education and people's behaviour
Source: own processing

Disinformation and hoaxes aim to cause people to panic, fear and worry about the future. One of these fear factors is the social impact that affects users of social networks. Many users need clarification on whether sufficient energy will be provided for the comfortable functioning of households in winter and whether there will be enough oil for motor vehicles and various energy machines and devices. Based on this, we specified a hypothesis, the main idea of which is the assumption that there is a statistically significant relationship between the dissemination of information on social networks and users' concerns about social impacts on economic well-being. The results from the statistical verification of the hypothesis are shown in Tab. 5

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

Table 5. The results of testing the hypothesis

Pearson's Chi-square Test of Independence			
Calculated value	Error profitability	Degree of freedom	Critical value
p = 0.0487	α = 5% (0.05)	DF = 1.00	x^2 = 0.01

Source: own processing

In the statistical evaluation of the data obtained from the respondents, this assumption was also confirmed, though very narrowly. The calculated value of p=0.0487 is lower than 0.05, meaning there is a statistically significant relationship between the dissemination of information on social networks and users' fears about social impacts on economic well-being. Therefore, in this case, we accept the stated hypothesis.

Figure 5 shows the relationship between information spread on social networks and users' concerns about social impacts on economic well-being.

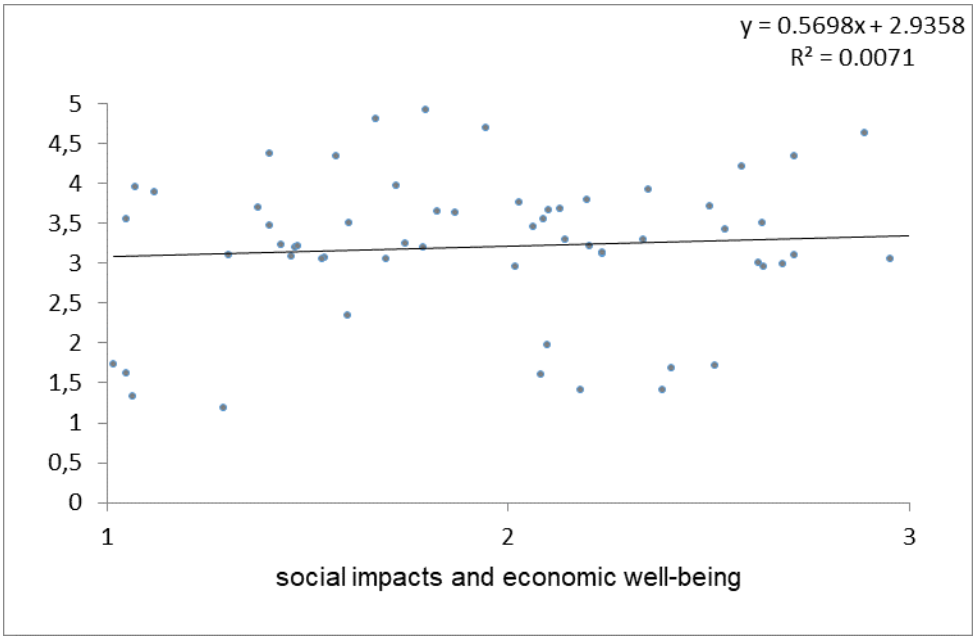

Figure 5. The dependencies between the dissemination of information on social networks and users' concerns about social impacts on economic well-being
Source: own processing

6. Discussion and conclusion

When combatting hybrid threats on social networks, it becomes essential to take note of their nature, which is diverse. These threats are versatile, variable and highly adaptable to individuals concerning their digital footprint. The problem is that it is impossible to significantly check them because government authorities still need to adopt a framework for identifying, deterring or restricting the negative impacts of threats, for example, on juveniles.

Naturally, it is also necessary to educate people so that they can thoroughly understand such threats and how to reduce their effects or prepare users of social networks to resist them. It is also necessary to create a trustworthy

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

relationship between the users of a social network and the authority that will monitor, control and receive information and suggestions from the users in case of suspicion of possible threats spreading in this environment.

In our study, we focused on testing hypotheses and came to some interesting results. The first part was the assumption that a statistically significant relationship exists between age and the ability to distinguish disinformation. This hypothesis was rejected, concluding that age plays no role in a hybrid threat or hoax on a social network.

Suppose we consider the user's age a damaging social network threat. In that case, young students are exposed to such hazards more often, as they primarily use social networks to strengthen their social ties within their residence, school or university. From this point of view, Facebook is a social network that provides a low level of self-disclosure, and the risk of creating fictitious accounts designed not only to track users but also to spread disinformation to influence other young people, is growing. Despite the advantages that social networks bring, we have to say that the frequent use of social networks by young people results in a deficit of social skills, which can lead users to information overload from these sources, the absence of real-world communication skills and helping them to avoid school and family obligations. With adult users of social platforms, the aim of their activity on a social network is mainly social contact with their surroundings and family and sharing and accepting their interests or attitudes.

We can further state that there is a statistically significant relationship between achieved education and the sharing of verified information. The assumption is that, depending on the education achieved, we perceive a lower number of spreading hoaxes, disinformation and links with the character of propaganda. Based on our sample, we can confirm this trend among all age groups. The decline of the digital divide between individuals and the development of social networks links young and older users with different communities and can significantly affect their behaviour.

There are known facts that reflect the behaviour of individuals gathered into social platform groups, where individual members brag about publishing videos of fights, insults or threats, and the identification factor is the education achieved by the social network user. This is linked to the growth of so-called Internet bashing, and the implications for preventing violence and criminal investigation caused by challenges on various social platforms are being discussed.

We perceive the use of social networks and the threats they bring with them, specifically at this time, when we are now at the end of the COVID-19 pandemic and war is just over our borders, as essential factors that influence the development of young people, shape their thinking and no doubt are capable of controlling their decision-making, opinions and attitudes. We confirm through statistical testing the hypothesis that more than 20% of respondents share information reported by alternative media. In the present time, when military operations are taking place in various parts of the world, much has been done in recent years during the course of these conflicts to strengthen the issue of spreading false information on the Internet, particularly on social networks.

The credit for this goes to the European Union and NATO. These two organizations perceive the field of hybrid threats as being very serious. Still, with the current development of information and communication technologies, hybrid threats are constantly changing their character, pace and intensity of spread and influence. The goal for the future would be to create a strategic approach to combat hybrid threats and to implement national legislation aimed not only at eliminating disinformation, threats and hoaxes from social networks but also at educating individuals in this area.

Young people today need measures in this area that will help them prevent mental and physical health problems related not only to the long-lasting pandemic or current wars but because, in the last years of their adolescence,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 4 (June)
http://doi.org/10.9770/jesi.2023.10.4(22)

the content offered by social networks, among other things, which is full of disinformation, hoaxes and politically or otherwise motivated opinions, has affected them. For both young people and the rest of the population, it is necessary to analyze the causes and reasons why they feel it is essential to share information whose content shows signs of hoax or disinformation.

With the fourth hypothesis, we tested whether there is a statistically significant relationship between education achieved and people's behaviour under the influence of disinformation and hoaxes, and we can state that social networks substantially influence people's ability to detect fake news. The ability to recognize disinformation depends on the education of the individual. Furthermore, other studies have shown that the most critical factors in detecting hoaxes and disinformation that influence a person's behaviour are education, income, interest in politics, time spent on social networks and confirmation bias, while age, as stated above, has no influence on the behaviour of an individual under the influence of hoaxes. Someone spreads disinformation as a text, image or video concerning digital literacy. We assume that, as with education, the higher the literacy, the less disinformation and hoaxes can influence an individual.

We likewise state that there is a statistically significant relationship between spreading information on social networks and users' concerns about social impacts on economic well-being. Among the effects of hoaxes, individuals perceive harmful content distributed through social networks as affecting their social and economic well-being. This is primarily the case with the young generation, who most often use social networks. Another group, for example, comprises mothers on maternity leave and pensioners, who, due to limited contacts, spend more time on social platforms and thus take information related to the development of the economy or political issues as accurate, causing them to fear their social or economic future.

The use of social networks leads to many opinions on the effects of social networks on individuals. The influence of social networks on the thinking and behaviour of individuals has yet to be sufficiently explored; therefore, it is necessary to pay attention to this issue in the future. In any case, there is a significant lack of regulation and control in social networks concerning the spreading of hoaxes, disinformation and propaganda.

References

Alguliyev, R., Aliguliyev, R., & Yusifov, F. (2018). Role of social networks in E-government: Risks and security threats. *Online Journal of Communication and Media Technologies*, 8(4), 363-376. https://doi.org/10.12973/ojcmt/3957

Atkinson, C., & Chiozza, G. (2021). Hybrid threats and the erosion of democracy from within: US surveillance and European security. *Chinese Political Science Review*, 6(1), 119-142. https://doi.org/10.1007/s41111-020-00161-2

Aral, S. (2020). The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt. Currency. ISBN 978-0-525-57451-4.

Bondar-Pidhurska, O.V., Karangwa, Ch., & Ammar, A.O.A. (2022). Management of competitiveness of enterprises in conditions of hybrid threats of sustainable development: innovative technologies and ecosconsciousness. 2022. http://dspace.puet.edu.ua/handle/123456789/11588

Dino, C., & Gustilo, L. (2018). FB Digitalking: Standard, Non-Standard, or Hybrid? 3rd International Conference on Education (ICOED). Melaka, Malaysia, 24(11), 8328-8331. https://doi.org/10.1166/asl.2018.12554

Dragos, V., Forrester, B., & Rein, K. (2020). Is hybrid AI suited for hybrid threats? Insights from social media analysis. 2020 IEEE 23rd International Conference on Information Fusion (FUSION). IEEE, 2020. p. 1-7. https://doi.org/10.23919/FUSION45008.2020.9190465

Fire, M., Goldschmidt, R. & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4), 2019-2036. https://doi.org/10.1109/COMST.2014.2321628

Garton, L., Haythornthwaite, C., & Wellman, B. 2006). Studying Online Social Networks. *Journal of Computer-Mediated Communication*, 3(1) https://doi.org/10.1111/j.1083-6101.1997.tb00062.x

Hawi, N. S., & Samaha, M. (2017). The Relations among Social Media Addiction, Self-Esteem, and Life Satisfaction in University Students. *Social Science Computer Review*, *35*(5), 576–586. https://doi.org/10.1177/0894439316660340

Palau-Sampio, D., Carratala, A., Tarullo, R., & Crisostomo, P. (2022) Quality recognition as a prescriber against disinformation. *Comunicar*, 30(72). https://doi.org/10.3916/C72-2022-05

Luo, T., Chen, W., & Liao, Y.H. (2021). Social media use in China before and during COVID-19: Preliminary results from an online retrospective survey. *Journal of Psychiatric Research*, 140, 35-38. https://doi.org/10.1016/j.jpsychires.2021.05.057

Kaiková, O., et al. (2022). Hybrid threats against Industry 4.0: adversarial training of resilience. In: E3S Web of Conferences. EDP Sciences, 2022. https://doi.org/10.1051/e3sconf/202235303004

Kirichenko, L., Radivilova, T. & Carlsson, A. (2018). Detecting cyber threats through social network analysis: short survey. arXiv preprint arXiv:1805.06680, 2018. https://doi.org/10.48550/arXiv.1805.06680

Linkov, I., et al. (2019). Applying resilience to hybrid threats. *IEEE Security & Privacy*, 17(5), 78-83. https://doi.org/10.1109/MSEC.2019.2922866

Lonardo, L., (2021). EU law against hybrid threats: A first assessment. *European Papers-A Journal on Law and Integration*, 6(2), 1075-1096. https://doi.org/10.15166/2499-8249/514

Lukáčová. J., (2019). Hybridné hrozby a ich vplyv na bezpečnostné prostredie - teória, vývoj, prax. Vojenské reflexie. Liptovský Mikuláš: Akadémia ozbrojených síl M.R. Štefánika. 2020, XV, no. 1/2020. ISSN: 1336-9202.

Mareš, M., & Mlejnková, P. (2023). Pan-Slavism and Slavophilia in the Czech Republic within the Context of Hybrid Threats. In: Pan-Slavism and Slavophilia in Contemporary Central and Eastern Europe: Origins, Manifestations and Functions. Cham: Springer International Publishing, p. 309-327. https://doi.org/10.1007/978-3-031-17875-7_15

Milbradt, D., et al. (2023). A Hybrid Robust Adaptive Sliding Mode Controller for partially modelled systems: Discrete-time Lyapunov stability analysis and application. *Nonlinear Analysis: Hybrid Systems*, 48, 101333. https://doi.org/10.1016/j.nahs.2023.101333

O'Brolcháin, F., Jacquemard, T., Monaghan, D. et al. (2016). The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. *Science and Engineering Ethics*, 22, 1-29. https://doi.org/10.1007/s11948-014-9621-1

Paradowski, M., Andrzej Jarynowski, A., Jelińska, M& Czopek, K (2021). Out-of-class peer interactions matter for second language acquisition during short-term overseas sojourns: The contributions of Social Network Analysis. *Language Teaching*, 54(1), 12-24. https://doi.org/10.1017/S0261444820000580

Pathe Duarte, F., (2020). Non-kinetic hybrid threats in Europe–the Portuguese case study (2017-18). *Transforming Government: People, Process and Policy*, 14(3), 433-451. https://doi.org/10.1108/TG-01-2020-0011

Rainie, L., & Wellman, B. (2012). Networked: The New Social Operating System. Cambridge, Mass.: MIT Press. ISBN 978-0262017190. https://doi.org/10.7551/mitpress/8358.001.0001

Sadeghian, A., Zamani, M., & Shanmugam, B (2013). Security threats in online social networks. In: 2013 International Conference on Informatics and Creative Multimedia. IEEE, p. 254-258. https://doi.org/10.1109/ICICM.2013.50

Sheoran, S., K., & Yadav, P. (2021). An Extended Work Architecture for Online Threat Prediction in Tweeter Dataset. International *Journal of Computer Science and Network Security*, 21(1), 97-106, https://doi.org/10.22937/IJCSNS.2021.21.1.14

Tagarev, T, & Sharkov, G. (2016). Multi-stakeholder Approach to Cybersecurity and Resilience. *Information & Security: An International Journal*, 34(1), 59-68. https://doi.org/10.11610/isij.3404

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, 2(4), 802-.813. http://doi.org/10.9770/IRD.2020.2.4(6)

Treverton, G.F. et al. (2018). Addressing hybrid threats. ISBN 978-91-86137-73-1

Treverton, G.F. (2018). The intelligence challenges of hybrid threats: Focus on cyber and virtual realm. 2018. ISBN 978-91-86137-75-5

Winkler, S., Körner, A., & Breitenecker, F. (2021). Modelling framework for artificial hybrid dynamical systems. *Nonlinear Analysis: Hybrid Systems*, 42, 101072. https://doi.org/10.1016/j.nahs.2021.101072

Funding: The contribution was created as a result of the project: Research of educational concepts in the field of hybrid threats within selected EU countries with the subsequent elaboration of the education concept for SR conditions project code in ITMS 2014+: 314011CDW7

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

prof. Ing. Bohuslava MIHALČOVÁ, PhD. & PhD. EUR ING, Department of Management, Faculty of Business Economy, University of Economics in Bratislava, 852 35 Košice, Slovakia.
ORCID ID: https://orcid.org/0000-0001-7958-3429

prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA**,** Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia.
ORCID ID: https://orcid.org/0000-0003-2384-9106

assoc. prof. Ing. Stanislav ŠIŠULÁK, PhD., MBA, Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia;
ORCID ID: https://orcid.org/0000-0003-4727-9582

Ing. Peter GALLO, PhD, Faculty of Arts, Institute of Educology and Social Work, University of Prešov in Prešov, 080 01 Prešov, Slovakia.
ORCID ID: https://orcid.org/0000-0001-5193-1997

Ing. Lukáč JOZEF, PhD. Department of Management, Faculty of Business Economy, University of Economics in Bratislava, 852 35 Košice, Slovakia
ORCID ID: https://orcid.org/0000-0003-2513-4390