Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 972 – 984
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4065

Analysis of Financial and Digital Literacy Aspects in Modern Economy: Combating Internet Disinformation and Hybrid Threats in OECD

Antonin Koraus[1], Jozef Lukac[2], Bohuslava Mihalcova[3], Patrik Javorcik[4], Zuzana Kudlova[5]

Abstract

In the current political and economic context, the world is actively addressing the issue of combating disinformation and influencing public opinion. Within the OECD, various initiatives and projects focus on strengthening citizens' critical thinking, promoting media literacy and increasing information transparency. The organization also addresses digital influence and disinformation, considering ways to enhance society's resilience to these issues. Research examines the ability of individuals to combat internet traps, hoaxes, and disinformation in OECD countries, analyzing how individuals identify and detect disinformation and false information online. The research employs various statistical methods, primarily clustering analysis, as well as the analysis of statistical relationships between variables and country comparison analysis. The research indicators are based on OECD data from 2022. The study's results provide useful information for cyber security experts, policymakers, and the general public who are working to combat the spread of disinformation, hybrid threats and hoaxes on the internet.

Keywords: *Oecd, Disinformation, Work with The Internet, Hoax, Hybrid Threats.*

Introduction

Hoaxes, hybrid threats and disinformation are part of our daily lives today. They are encountered across different social platforms and in alternative media publications, and are represented by political groups and various other interest groups. The company's task is to be able to avoid these disinformation and hoaxes and to offer true and safe content on social networks. By sharing various hoaxes and disinformation, users contribute to the spread of polarity in our society, which causes not only its cognitive but also moral decline. Social networks are online platforms that people use to build social relationships with other people who share similar personal or career content, interests, activities, backgrounds, or real-life connections. They differ in format and number of functions. They can include a whole range of new information and communication tools working on classic computers and laptops, on mobile devices such as tablets and smartphones. Social networks may contain digital photos and videos that are shared with other users. Broadly defined as websites, their sites facilitate the building of a network of contacts to exchange different types of content online, providing a space for interaction that can continue beyond face-to-face interactions. These interactions connect members of different social networks and help create, maintain and develop new social and professional relationships regardless of gender or age. Their success is evident in their prevalent role in today's society, as seen through their daily use (Schrape 2017). However, euphoria alternates with skepticism due to the use of social networks, which, as mentioned at the beginning, not only offers benefits but also presents numerous negatives and becomes a tool for hybrid threats. Therefore, it is extremely important to pay enough attention to this issue and continue research that reveals not only demographic trends in the use of social networks, but also the abilities of individuals in digital literacy. The paper focuses on clustering countries to identify groups with similar characteristics, based on analyzing selected indicators that assess individuals' capabilities to use the Internet. Future developments are planned for this research. According to Smith (2022), the ability of individuals to distinguish between truthful and

[1] Academy of the Police Force in Bratislava, Slovak Republic, Email: antonin.koraus@akademiapz.sk, (Corresponding Author).
[2] Faculty of Business Economy with seat in Košice, Department of Corporate Financial Management, University of Economics in Bratislava, Slovak Republic; Email's: jozef.lukac@euba.sk
[3] Faculty of Business Economy with seat in Košice, Department of Corporate Financial Management, University of Economics in Bratislava, Slovak Republic; Email's: bohuslava.mihalcova@euba.sk
[4] Faculty of Management, Economics and Business, Prešov University in Prešov, Slovak Republic, Email: patrik.javorcik@gmail.com.
[5] Faculty of Business Economy with seat in Košice, Department of Corporate Financial Management, University of Economics in Bratislava, Slovak Republic, Email: zuzana.kudlova@euba.sk

misleading information on the internet is an integral part of modern society. These skills are crucial not only for personal financial decisions but also for protection against hybrid threats that use disinformation to destabilize society.

Literature Review

The world has never been as interconnected as it is today. Asia, Europe, America, Africa are at our fingertips. It is possible to contact them directly from home or office. This convenience is due to social networks, which on the one hand provide people with comfort at work and in connection with family and friends, but on the other hand are a source of disinformation and hoaxes. Social networks are websites and applications through which people communicate and connect over the Internet. They thus share the same interests, impressions, and needs, both in family life and in the workplace.

The first social networks began in the form of general online communities such as Theglobe.com (1995), Geocities (1994) and Tripod.com (1995). Many of these early communities focused on bringing people together to interact through chat rooms and encouraged users to share personal information and ideas through personal websites by providing easy-to-use publishing tools and free or low-cost web space. In the late 1990s, user profiles became a central feature of social networks, allowing users to compile "friends" lists and search for other users with similar interests. In the late 1990s, new methods of social networking were developed and many sites began to develop more advanced features for users to find and manage friends. This newer generation of social networks began to "bloom" with the creation of Six Degrees in 1997, Open Diary in 1998, Mixi in 1999, Makeoutclub in 2000, Cyworld in 2001, Hub Culture in 2002, and Friendster and Nexopia in 2003. Cyworld also became one of the first companies to profit from the sale of virtual goods. MySpace and LinkedIn were launched in 2003 and Bebo in 2005. The rapid rise in popularity occurred in 2005 when MySpace had more page views than Google. Many of these services were replaced by Facebook, which was implemented in 2004 and became the largest social network in the world in 2009 (Lugmayr, 2013). According to DataReportal, a January 2022 Kepios analysis showed that there are more than 4.74 billion social network users worldwide (Wright and Yasar 2022).

There are different types of social networks, through which they also fulfill their main functions, such as sharing, teaching, marketing, or mutual interaction. Understanding these functions provided the basis for the creation of network types.

To summarize, social networks are no longer an achievement used only by young people, but are necessary for all age groups. Burdick (2001) stated that the use of information technology is a means of bridging the generation gap, although many, especially younger people, are skeptical about this issue. Rather, they lean towards the fact that older people are less prepared and use the Internet. They argue that many seniors do not own a computer, or that they are not mentally prepared for it.

Analyses show that OECD countries are investing in raising the literacy levels of their citizens, which is essential for strengthening their resilience to digital threats (Johnson, 2023). Studies emphasize the need for an interdisciplinary approach that combines economic, social, and technological perspectives in combating the spread of disinformation and ensuring the sustainable development of digital literacy (Davis, 2023).

Some studies (e.g. Marcelino, I .et. al. 2015, Saracchini, R. et.al. 2015) indeed point out that older people have problems accessing social networks due to lack of skills and problems using modern mobile phones , making them feel isolated in society. Due to demographic trends and the aging of the population on a global level, the need for a digital society is becoming more and more urgent. The fact that the silver generation is becoming increasingly digital is also evidenced by Klímová et.al. (2021), who state that "in relation to the respondents surveyed, the hypothesis that older adults' interest in using the Internet decreases with age was not confirmed. In addition, the results indicated that future research should focus on comparing the use of the Internet by older adults from different countries and therefore from different cultural areas or areas implementing different social policies". Fratiglioni et. Al. (2000) report that there is even a positive relationship of social network use to protection against dementia.

Another detailed analysis by Kepios showed that in July 2023, there were 4.88 billion active social network users worldwide, regardless of age. This corresponds to 60.6% of the total world population. This is 3.7% year-on-year growth at an average rate of 5.5 new users every second. The most used social platform is Facebook with 2.989 billion active users. It is followed by YouTube, WhatsApp, Instagram and WeChat in that order. Menšík, M. (2023)

However, it is important to recognize that despite their undeniable benefits and necessity, social networks also possess several disadvantages, and a misunderstanding of their use can lead to the exploitation of their users.

Users often encounter hoaxes and disinformation, cyberbullying and the like on social networks. It is sometimes difficult for users of social networks to distinguish whether a given piece of information is a hoax or not and whether it is dangerous for society at all. As an easy space for the spread of disinformation and hoaxes, the sensationalism in the headline of the message or in its brief summary affects the users. So the user of the social network is immediately interested in the sensation in the headline, but does not even have to read the entire article. The unverified information that social media creates and offers then have a snowball effect. Other users create so-called a false identity that helps them build illusions and self-delusions. They focus on the number of likes on their photos or blogs, while in reality they do not communicate with the people around them at all. Depression and addictions then result. Related to the previous one is also the danger of social networks when it is necessary to gain friends in order to create the impression of popular, popular and successful people in front of themselves, but also in front of others. Such dependence is more easily formed by mentally unstable people, with a tendency to low self-esteem and dependence on relationships. There are many more dangers in the uncritical and incorrect use of social networks, which is why many users are calling for control of disinformation networks by state authorities or for them to be controlled directly by social network administrators. Some even speak out for the direct blocking of social networks with dangerous content. It is therefore necessary to continue research that reveals not only demographic trends in the use of social networks, but also reveals the abilities of individuals in digital literacy. (Jian, 2021; Teichman, 2023; Posseti, 2021)

Digital literacy and the ability to verify information on social networks are key to the healthy functioning of the information society. Studies have shown that a lack of digital literacy among Ghanaian journalists has contributed to the spread of disinformation through social media during the COVID-19 pandemic. This example emphasizes the need to increase digital literacy, which enables better recognition and verification of the truth of information on social networks (Alhassan et al., 2024).

On the other hand, W. Reyes and NE Gurubel-Tec, in a study on the digital competence of teachers in the Mayan region of Mexico, revealed that although there are national programs to improve digital literacy, adequate tests to verify the level of this literacy among teachers are often lacking. This lack can lead to the ineffective use of digital tools in education and the insufficient ability of teachers to teach students how to properly verify information obtained through social networks (Reyes and Gurubel-Tec, 2024)

Digital literacy has a direct impact on the ability of Internet and computer users to identify and protect themselves from the threats they may encounter online. Increased digital literacy provides users with the necessary skills to recognize and adequately respond to various types of online threats such as phishing, malware and fraud. (Valenza, 2022) A study by E. Sina shows that children and adolescents who grow up in a digital environment are often exposed to risks that can have a negative impact on their health and behavior. Increasing digital literacy in this group can significantly contribute to their ability to protect themselves from harmful online content and interactions (Sina, 2023).

Research has explored the impact of digital literacy on students' critical thinking and their capacity to analyze and evaluate online information. Findings indicate that strong digital literacy skills greatly lower the likelihood of accepting false or misleading information as true. (Karipbayeva et al., 2023). Another study emphasizes that digital literacy can have negative effects if it is not properly managed, especially if users do not have the ability to recognize content that may be harmful or incorrect. This fact highlights the need for comprehensive educational programs that teach users how to protect themselves online (Gunadi & Lubis, 2023).

Digital literacy influences student satisfaction with online learning during the COVID-19 pandemic. They found that students with higher levels of digital literacy had better educational outcomes because they could effectively navigate digital content and recognize potential threats (Schwartz & Aharoni, 2023). Another study examines how smartphones are used by primary care physicians to seek information. This study highlights how digital literacy can improve the ability of healthcare professionals to effectively and safely search for information, which is essential for providing quality patient care (Lee, 2023). Increasing digital literacy is necessary so that residents can fully use these technologies and protect themselves from possible online threats that these technologies bring (Kuzior et al., 2023).

These examples clearly show that digital literacy is an essential tool for ensuring safety and efficiency in the use of Internet and computer technologies. It is essential that education programs at all levels include digital literacy instruction so that users are able to effectively counter online threats and use digital technologies safely and responsibly. (Steingartner, 2021)

In the digital age, individuals inevitably encounter a lot of disinformation on the Internet. The role of the individual in combating this disinformation is crucial and includes multiple aspects, from increasing digital literacy to actively participating in information verification. (Spálova, 2023)

One of the first steps in the fight against disinformation is to increase digital literacy, which enables individuals to better recognize incorrect or misleading information. Grabowska (2023) points to the importance of the digital media observatory in the European Union, which strengthens the capacity of individuals to identify fake news. Supporting psychological health is also an important aspect, as disinformation can cause significant emotional and mental burdens. Chimbwete-Phiri (2024) discusses the impact of COVID-19 disinformation on mental health in Malawi and emphasizes the need for psychological resilience to disinformation. At the same time, individual responsibility also includes the selection and evaluation of resources. Wilmot, Asare, and Opoku (2023) state that it is critical for individuals to distinguish between verified and unverified information when making health care decisions. Active participation in social networks and online platforms also means that individuals should make efforts to correct disinformation whenever possible. Otieno (2024) highlights the challenges of disinformation about female politicians in Kenya and calls on individuals to actively counter gendered disinformation. These resources emphasize the importance of an individual approach to combating disinformation, which includes education, psychological resilience, critical thinking and active participation on digital platforms. Every individual has the potential to contribute to a healthier information environment, thereby protecting themselves and their communities. (Ronchi, 2023; Tkáčová, 2023)

Research Methodology

The aim of the research is to analyze selected indicators of individuals' ability to work with the Internet and, importantly, to identify the current pitfalls observed on the Internet and social networks. The aim within the methods used is to focus on analyzing relationships between variables, employing the principal components method, and the clustering method. For the aim of analyzing the relationships between variables, the Pearson correlation coefficient will be utilized. By performing correlations of the input variables, the aim is to observe the dependence between the variables. The research will concentrate on several sub-areas, attempting to answer the established hypotheses:

Hypothesis 1: Indicators of an individual's skills and abilities to work with the Internet, social networks, and the online environment are interdependent.

Hypothesis 2: V4 countries that are regionally close achieve similar results and their placement in the cluster is the same.

Hypothesis 3: Developed OECD countries differ significantly from less developed OECD countries in terms of their results in key research indicators.

Research Instrument

The analysis will cover data from the year 2022, representing 35 OECD countries that have reported on selected aspects of combating disinformation, Internet pitfalls, and the use of information from social networks. The variables utilized in the survey were indicators of people's skills and ability to work with information and data on the Internet and social networks. These indicators are listed in the following composition, and for future reference, they are labeled V1 to V14:

False information and social media content

Verifying the veracity of information on social media

Control of sources of information on social media

Verification of information on social networks through discussion

Verification of information on social media through discussion with third parties outside the Internet

Verification of information using the I_TICCSFOI, I_TICIDIS or I_TICNIDIS methods

Information verification - suspicion of hoax and disinformation

Non-verification of information due to lack of digital literacy

Non-verification of information for other reasons

Online identity theft

Getting redirected to fake websites asking for personal information

Social network or e-mail account being hacked and content being posted or sent without individuals' knowledge

Loss of documents, pictures or other data due to a virus or other computer infection

experienced any of the following security related incidents: I_SECFRD2, I_SECVIR1, I_SECMPI, I_SECSNH, I_SECOIT, I_SECPHI or I_SECPHA

Clustering Method.

However, a high degree of dependence between variables can be a problem, which can affect clustering results. Elimination of the problem can be achieved through the method of principal components, in which the input indicators are transformed into new variables. These new variables, called principal components, are already mutually independent, allowing us to perform clustering analysis. Statistical clustering of countries is a process used to identify groupings of countries based on the similarity of their statistical characteristics. This procedure is usually carried out in order to analyze and compare data between countries, and also to identify patterns and trends between them. Clustering countries can be useful for policy making, development planning or international comparisons.

Research and Discussion

As mentioned, the primary objective is to analyze selected indicators related to Internet use and its associated pitfalls. This research is conducted within the context of OECD countries. The following table displays the descriptive statistics for the selected variables. Using the Shapiro–Wilk test, the distribution of the data values is compared to a normally distributed dataset with the same mean and standard deviation. A non-significant result of the test for indicators V1, V6, V7 ($p > 0.05$) suggests that their data distribution does not significantly deviate from a normal distribution. Conversely, significant test results for indicators V4, V8, V9, V12 ($p < 0.01$) indicate that the distribution of these data significantly differs from the normal distribution.

Table 1. Descriptive Statistic

	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14
Valid	35	35	35	35	35	35	35	35	35	35	35	35	35	35
Median	48.180	22.850	19.790	5.990	10.330	22.330	16.580	3.370	5.300	1.460	14.840	0.920	2.050	20.990
Mean	47.613	23.414	20.502	7.988	11.649	22.904	16.297	4.154	6.455	2.147	20.111	1.149	2.231	26.529
Std. Deviation	13.102	9.873	9.617	5.993	7.372	9.603	5.281	2.765	4.980	1.938	15.080	0.860	1.310	16.317
Variance	171.675	97.483	92.489	35.918	54.352	92.216	27.887	7.644	24.803	3.756	227.405	0.740	1.716	266.243
Shapiro-Wilk	0.975	0.967	0.961	0.760	0.928	0.973	0.983	0.846	0.853	0.873	0.917	0.855	0.932	0.946
P-value of Shapiro-Wilk	0.592	0.368	0.246	< .001	0.024	0.523	0.851	< .001	< .001	< .001	0.012	< .001	0.033	0.084
Minimum	19.530	5.230	4.170	1.420	2.090	5.050	5.630	0.720	0.330	0.040	1.170	0.180	0.470	3.070
Maximum	69.770	45.270	42.440	32.230	32.230	44.600	26.740	13.860	25.030	7.310	58.750	3.960	5.590	65.920

Source: the result of statistical testing

Based on descriptive statistics, it is evident that not all indicators originate from a normal distribution, which could significantly impact the results of the analysis. To address this issue, the method of principal components is employed. Additionally, the mutual relationships between variables are analyzed using the Pearson correlation coefficient. Successful clustering depends on analyzing the dependencies between individual variables. The starting point was the correlation matrix, which contains Pearson correlation

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4065

coefficients.

Table 2. Pearson´s Correlations

Variable		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V
1. V1	Pearson's r	—													
	p-value	—													
2. V2	Pearson's r	0.836	—												
	p-value	< .001	—												
3. V3	Pearson's r	0.847	0.990	—											
	p-value	< .001	< .001	—											
4. V4	Pearson's r	0.481	0.550	0.549	—										
	p-value	0.003	< .001	< .001	—										
5. V5	Pearson's r	0.745	0.858	0.873	0.736	—									
	p-value	< .001	< .001	< .001	< .001	—									
6. V6	Pearson's r	0.843	0.998	0.989	0.525	0.844	—								
	p-value	< .001	< .001	< .001	0.001	< .001	—								
7. V7	Pearson's r	0.558	0.149	0.209	0.203	0.296	0.159	—							
	p-value	< .001	0.394	0.227	0.241	0.085	0.363	—							
8. V8	Pearson's r	0.397	0.342	0.380	0.373	0.440	0.350	0.340	—						
	p-value	0.018	0.044	0.024	0.027	0.008	0.040	0.045	—						
9. V9	Pearson's r	0.488	0.076	0.098	0.023	0.089	0.094	0.366	0.183	—					
	p-value	0.003	0.664	0.575	0.897	0.609	0.592	0.031	0.294	—					
10. V10	Pearson's r	-0.058	-0.152	-0.099	-0.294	-0.214	-0.138	0.183	-0.086	-0.116	—				
	p-value	0.740	0.383	0.571	0.086	0.217	0.431	0.292	0.624	0.509	—				
11. V11	Pearson's r	-0.207	-0.280	-0.258	-0.259	-0.297	-0.261	5.7×10^{-4}	-0.019	-0.090	0.724	—			
	p-value	0.232	0.103	0.135	0.133	0.084	0.130	0.997	0.912	0.606	< .001	—			
12. V12	Pearson's r	-0.040	-0.013	0.024	-0.112	-0.052	2.6×10^{-5}	-0.048	-0.028	-0.188	0.724	0.584	—		
	p-value	0.819	0.941	0.890	0.520	0.766	1.000	0.785	0.875	0.280	< .001	< .001	—		
13. V13	Pearson's r	-0.115	-0.148	-0.104	-0.210	-0.090	-0.123	0.014	0.147	-0.041	0.554	0.619	0.616	—	
	p-value	0.509	0.395	0.551	0.227	0.608	0.483	0.937	0.399	0.815	< .001	< .001	< .001	—	
14. V14	Pearson's r	-0.150	-0.213	-0.181	-0.285	-0.252	-0.191	0.031	0.021	-0.091	0.798	0.982	0.664	0.651	
	p-value	0.388	0.219	0.299	0.097	0.145	0.272	0.860	0.905	0.603	< .001	< .001	< .001	< .00	

Table 3. Component Characteristics

	Unrotated solution			Rotated solution		
	Eigenvalue	Proportion var.	Cumulative	SumSq. Loadings	Proportion var.	Cumulative
Component 1	5.707	0.408	0.408	5.030	0.359	0.359
Component 2	3.482	0.249	0.656	3.851	0.275	0.634
Component 3	1.529	0.109	0.766	1.836	0.131	0.766

Source: the result of statistical testing

The previous table indicates that the first component accounts for the greatest variability, while the last component accounts for the least. It is also observed that to account for 76.6% of the variability of the original dataset, only 3 principal components (RC) are required. This satisfies the rule stipulating that the number of principal components (RC) should explain at least 70% of the total variance of the data. The subsequent diagram illustrates the individual relationships during the creation of components and characterizes how the original data, represented by indicators V1 to V14, are depicted on the new RCs.

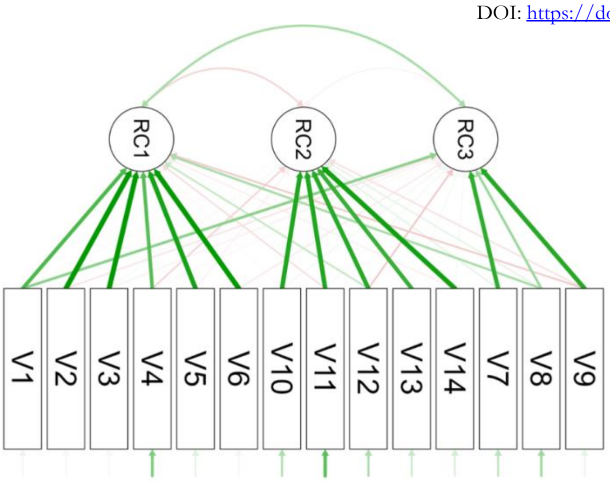


Figure 1 Links Between Indicators and Principal Components

Source: the result of statistical testing

Using a heuristic approach, the analyzed set of countries was divided into 3 clusters. The key criterion for this classification was the minimization of the intra-cluster sum of squares, which serves as the optimal condition, and the choice of 3 clusters was found to be statistically significant. Choosing more clusters would have resulted in too few enterprises within each cluster due to the reduction in the intra-cluster sum of squares. On the other hand, opting for fewer clusters would lead to excessively high values of the within-cluster sum of squares. It can be confirmed that the countries within each cluster share similar characteristics regarding the indicators of proficiency in using the Internet, social networks, and navigating Internet pitfalls, while exhibiting distinct characteristics from countries in other clusters.

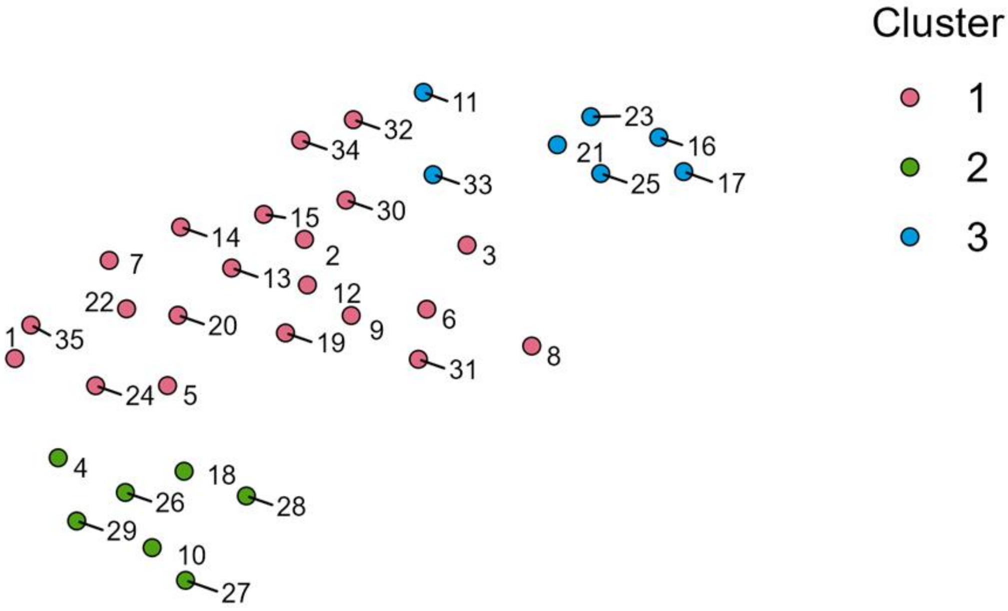


Figure 2 Position of Countries with Respect to The Analyzed Indicators

Source: The result of statistical testing

Based on the analysis conducted, the results obtained in the investigated area are as follows:

Cluster: Spain, Switzerland, Slovakia, Belgium, Czechia, Croatia, Hungary, Austria, France, Denmark, Slovenia, Germany, Greece, Latvia, Cyprus, Lithuania, Montenegro, Albania, Turkye, North Macedonia, Bulgaria.

Cluster: Bosnia and Herzegovina, Poland, Serbia, Estonia, Italy, Romania, Portugal.

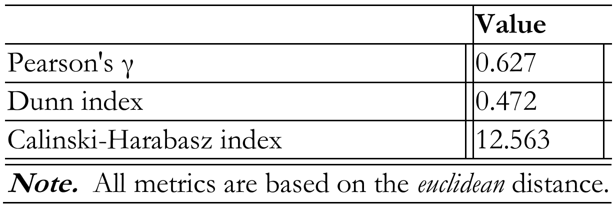
Cluster: Finland, Sweden, Luxembursko, Netherlands, Norway, Iceland, Ireland

Using hierarchical agglomerative cluster analysis, clusters were identified for selected OECD countries based on selected indicators of Internet use and associated pitfalls. The Euclidean distance measure was utilized, and the Ward method was selected as the clustering method. Through the principal components method, clusters of countries were formed and illustrated in a graph that categorized the countries according to selected indicators. Consequently, the countries were grouped into clusters sharing similar characteristics, distinct from those in other clusters. Prior to clustering, the relationships between individual variables were analyzed.

The result of our research is the identification of 3 clusters among OECD countries, depending on the level of abilities of the citizens of the countries to identify the threat, pitfalls of social networks and the Internet. Criteria for internal validity and performance of the results were also implemented.

The cluster quality index is used to estimate the number of clusters in a set of datasets partitioned by several algorithms. R2, Dunn index, Calinski-Harabasz index these indices are based on internal cluster validity indices. Of course, these indicators are not enough to determine the quality of the cluster. Performing good statistical clustering is a relative term, based on the analyst's perspective and knowledge.

Table 4 Evaluation Metrics



	Value
Pearson's γ	0.627
Dunn index	0.472
Calinski-Harabasz index	12.563

Note. All metrics are based on the *euclidean* distance.

Note. All metrics are based on the euclidean distance.

The Calinski-Harabasz index is the ratio of the sum of the within-cluster variance to the within-cluster variance for all clusters; the higher the score, the better the performance. It can also be stated that, from our point of view, the clustering result is statistically correct. Dunn's index is an indicator where cohesion is estimated by the nearest neighbor distance and separation is estimated by the maximum cluster diameter. Algorithms creating clusters with a high Dunn index are more suitable - in our conditions it is 0.4, which are deemed sufficient.

Part of the discussion also involves seeking answers to the established hypotheses, relying on statistical testing, analysis, and substantiated information.

Hypothesis 1: Indicators of an individual's skills and abilities to work with the Internet, social networks, and the online environment are interdependent.

In the first part of the scientific research, the focus was on analyzing the relationships between individual input variables. Pearson's correlation coefficient, a statistical method, is used to gauge the strength and direction of the relationship between two continuous variables. Examining the dependency between the variables related to working with the Internet and hybrid threats suggests a potential relationship. It was observed that for most variables, there is a high positive Pearson correlation coefficient, such as between indicator V3 and V6. This reflects a strong positive relationship between controlling information sources on social media and verifying information using methods like I_TICCSFOI, I_TICIDIS, or I_TICNIDIS.

Conversely, a high negative Pearson correlation coefficient would signify a strong negative relationship between the variables. However, it is crucial to remember that correlation does not establish causation between variables and should be approached with caution. The correlation could be coincidental or influenced by other factors. Thus, Pearson's correlation coefficient merely provides information about the strength and direction of the relationship between variables, but not the underlying causes. For more comprehensive analyses, other statistical methods and procedures, especially agglomerative cluster analysis, were employed. It has been demonstrated through statistical testing that certain indicators of an individual's ability to navigate the Internet, social networks, and online environments are interdependent.

Hypothesis 2: V4 countries that are regionally close achieve similar results and their placement in the cluster is the same.

The analysis of the V4 countries—Czech Republic, Hungary, Poland, and Slovakia—reveals that they are increasingly vulnerable to hybrid threats and disinformation, which include propaganda campaigns aimed at destabilization. These threats utilize a mix of tactics such as cyber attacks, influence operations, and financial manipulations to spread false information and undermine political stability. Despite some exceptions, similar trends in these threats were observed across all four countries.

The Czech Republic significantly differentiates its results in the area of the indicator of non-verification of information on the Internet (except for non-verification in the context of digital literacy). Poland deviates from the average of V4 countries on the indicator of redirection to fake websites requesting personal information and the indicator that characterizes security-related incidents: I_SECFRD2. In connection with the comparison of countries, Hungary and Slovakia have developed indicators at a similar level. The development can be illustrated in more detail using the graph below.

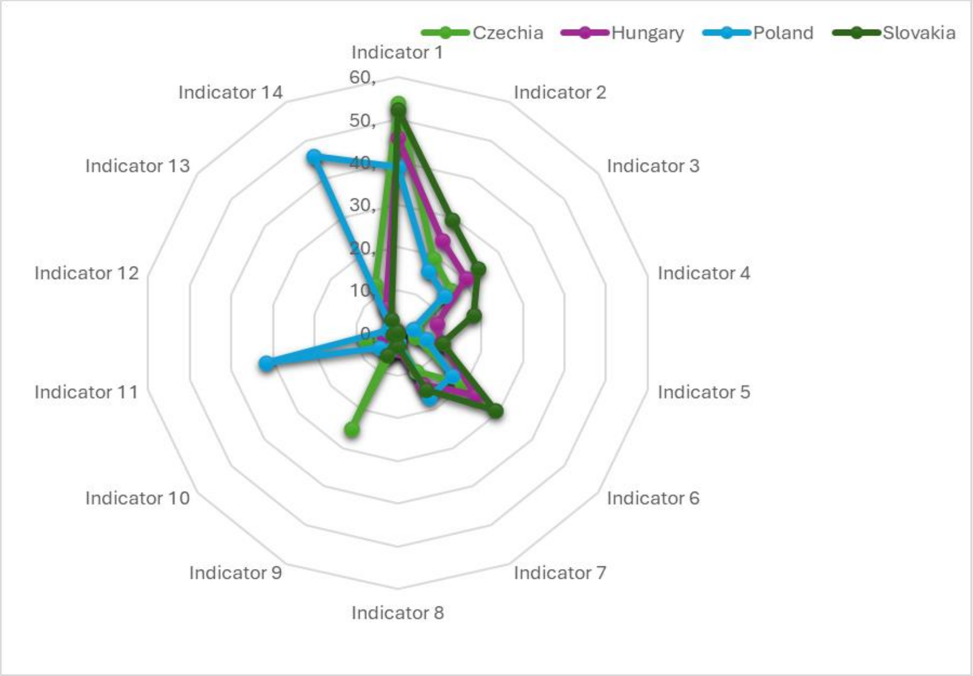


Figure 3 Comparison of Indicators in V4 Countries

Source: the result of statistical testing

The V4 countries are working to combat these threats by increasing cooperation within the group, strengthening cyber security, increasing citizens' media literacy, and better monitoring and detecting disinformation. These countries are also working with international partners such as NATO and the EU to deal with these threats effectively and in a coordinated manner. Currently, the fight against disinformation and hoaxes is very important even at the level of a joint struggle of several countries, since the Internet and social media enable the rapid spread of unverified information even across countries.

Raising awareness of how to recognize and detect fake news is key to protecting the public from the manipulation of public opinion. Overall, combating disinformation and hoaxes is an ongoing process that requires the cooperation of everyone—individuals, media, governments, and technology companies. As part of the statement regarding the established hypothesis 2. It can be asserted that the countries are similar in terms of results, grouping them together in one cluster. However, these results are not achieved by Poland, which found itself in a cluster with other countries, namely: Bosnia and Herzegovina, Poland, Serbia, Estonia, Italy, Romania, Portugal.

Hypothesis 3: Developed OECD countries significantly differ from less developed OECD countries in terms of their results in key research indicators.

OECD countries, including the United States, Germany, and Japan, maintain high economic development and living standards, characterized by strong GDP per capita, quality healthcare, and robust infrastructure. However, some OECD countries in Central and Eastern Europe, as well as certain Central African and South American countries, face lower living standards and issues like political instability and corruption. All OECD members aim to support each other to foster sustainable growth and tackle shared challenges such as disinformation and security threats through enhanced media literacy and international cooperation.

The OECD has several common solutions for hybrid threats, combating disinformation and working with the Internet. It is clearly cooperation between member countries and international organizations to improve cyber security and protection against hybrid threats (exchange of information and joint discussions to improve capacities to respond to these threats). Next, it is necessary to discuss the legal and regulatory frameworks that protect against disinformation and the manipulation of information on the Internet. This may include the introduction of new laws and measures to strengthen the transparency and accountability of media and online platforms. These goals cannot be achieved without the support of the media and civil society in combating disinformation and propaganda through public education and support for independent journalists and media. An integral part of the OECD countries is the support of innovation and technological solutions to improve cyber security and protection against hybrid threats, including the development of tools for detecting and filtering disinformation and manipulation on the Internet. These are the tools that the countries placed in cluster no. 1 they certainly comply with and are united in this area. These joint OECD solutions are important for protecting democracy, freedom of expression and human rights in the digital world, and their implementation requires cooperation and coordination between governments, international organizations, industry and civil society.

Hypothesis 3 can be concluded as follows: Developed OECD countries do not significantly differ from less developed OECD countries in terms of their results in key research indicators, therefore, this hypothesis is rejected.

Conclusion

Slovakia actively combats disinformation through various measures, including improving media literacy, engaging in international cooperation, and promoting transparency in information dissemination. Educational initiatives aim to enhance the critical thinking skills of residents, while collaborations with international organizations facilitate the exchange of best practices and information. These efforts are designed to reduce the spread of disinformation and strengthen information security within the country.

Regarding internet proficiency, Slovakia's population demonstrates average levels compared to other OECD countries. According to OECD statistics from 2020, about 85% of Slovaks have internet access, slightly below the OECD average of 90%. Regular internet usage in Slovakia stands at approximately 80%, also trailing the OECD average of 85%. Various factors such as access to infrastructure, economic conditions, and education influence these figures. Slovakia is committed to improving its digital infrastructure and promoting digital literacy through numerous programs and initiatives.

Cyber security is another critical focus area for Slovakia. The country has enacted laws and regulations to safeguard against cyber threats and has launched initiatives to raise awareness about cyber security. Education and training programs for citizens and organizations are in place, alongside international cooperation for information exchange and collective defense against cyber threats. Slovakia emphasizes protecting critical infrastructure sectors like energy, telecommunications, and finance from cyber-attacks. Citizens and organizations are encouraged to adopt robust cyber security practices, such as using strong passwords, updating software, avoiding suspicious links, and utilizing secure internet connections.

Efforts to combat disinformation are also evident within the broader OECD framework. While there is no specific list of fake websites, the OECD collaborates with member countries to enhance cyber security and ensure the reliability of online information. The organization supports legal and regulatory frameworks aimed at protecting personal data and fighting cybercrime. Raising awareness about cyber security among citizens and businesses through campaigns and education is a priority. International cooperation is vital for maintaining a safe and trustworthy online environment in OECD countries. Nonetheless, individuals are encouraged to critically evaluate the information they encounter online and take personal measures to safeguard their data and privacy.

Overall, Slovakia, in line with OECD practices, is committed to improving digital literacy, cyber security, and the integrity of information, thereby fostering a safer and more informed online community.

Acknowledgements

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 ITMS2014+: 314011CDW7 and of the Project of Young Researchers and PhD Students, number: I-24-102-00, 2024.

References

Alhassan, R., Tsekpo, K., Sikanku, E., et al. (2024). Ghanaian journalists and the spread of rumors during the Covid19 pandemic: Views from five regions. Retrieved from https://www.opastpublishers.com/open-access-articles/ghanaian-journalists-and-the-spread-of-rumors-during-the-covid19-pandemic-views-from-five-regions.pdf.

Burdick, D. (2001). Digital divide or tool for understanding and collaboration: Computers and intergenerational relationships. Paper presented at the 54th Annual Scientific Meeting of the Gerontological Society of America, Chicago.

Davis, M. (2023). Interdisciplinary approaches to digital literacy. Ecohumanism Review, 14.2, 345-367.

Fratiglioni, L., Wang, H. X., Ericsson, K., Maytan, M., & Winblad, B. (2000). Influence of social network on occurrence of dementia: A community-based longitudinal study. Lancet, 355(9212), 1315-1319.

Grabowska, M. (2023). The role of the European Digital Media Observatory (EDMO) in countering disinformation in the European Union. Poland's Experience in Combating Disinformation. Retrieved from https://eprints.uklo.edu.mk/9663/1/disinformation-book.pdf#page=72.

Gunadi, R. A. A., & Lubis, M. (2023). The effect of digital literacy on children violence. In 1st UMSurabaya Multidisciplinary International Conference Proceedings. Atlantis Press. Retrieved from https://www.atlantis-press.com/article/125986622.pdf.

Chimbwete-Phiri, R. (2024). Online COVID-19 discourse and mental health impacts in Malawi. In COVID-19 and Psychological Distress in Africa. Retrieved from https://library.oapen.org/bitstream/handle/20.500.12657/86272/9781003849872.pdf?sequence=1#page=227.

Jian, M.-S., & Wu, J. M.-T. (2021). Hybrid Internet of Things (IoT) data transmission security corresponding to device verification. Journal of Ambient Intelligence and Humanized Computing, 1-10.

Johnson, L. (2023). Combating internet disinformation and hybrid threats. Ecohumanism Journal, 15.4, 234-256.

Karipbayeva, R. K., Haas, M., & Bakirova, K. (2023). Development of critical thinking skills in the context of digitalization of education. Retrieved from https://elibrary.ru/item.asp?id=60234871.

Kuzior, A., Postrzednik-Lotko, K., & Rodzeń, K. (2023). Social challenges resulting from the implementation of technical solutions in smart cities. IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/10401824/.

Lee, M. M. (2023). The role of smartphones in information-seeking behaviour among primary care clinicians: Evaluating evidence to support high-quality patient care. Retrieved from https://dr.ntu.edu.sg/handle/10356/173461.

Marcelino, I., Laza, R., Fdez-Riverola, F., & Pereira, A. (2015). Removing barriers to promote social computing among senior population. Int. J. Distrib. Sens. Netw., 2, 1-13.

Menšík, M. (2023). Sociálne siete vládnu svetu: Používa ich viac ako polovica populácie. Retrieved from https://www.mojandroid.sk/socialne-siete-vladnu-svetu-pouziva-ich-viac-ako-polovica-populacie/.

Otieno, M. A. (2024). Gendered disinformation of female politicians on social media in Kenya: A case of Migori Republican Council Facebook page. Retrieved from http://41.89.203.227/handle/123456789/2551.

Posetti, J., & Bontcheva, K. (2021). Infodemic: Disinformation and media literacy in the context of COVID-19. Internet Sectoral Overview, 3.13, 1-21.

Reyes, W., & Gurubel-Tec, N. E. (2024). Digital competence of teachers in the Mayan region of Mexico: Results of a preliminary research in secondary education. International Journal of Instruction. Retrieved from https://e-iji.net/ats/index.php/pub/article/view/579/685.

Ronchi, A., et al. (2023). Human factor, resilience & cyber/hybrid influence. Communications in Computer and Information Science, 1-25.

Saracchini, R., Catalina, C., & Bordoni, L. (2015). Augmented reality assistive technology for the elderly. Comunicar, 45, 65-73.

Schrape, J.-F. (2017). Reciprocal irritations: Social media, mass media and the public sphere. In Society, Regulation and Governance: New Modes of Shaping Social Change? (pp. 138–150). doi:10.4337/9781786438386.00016.

Schwartz, T., & Aharoni, N. (2023).. Meidaat: Journal for Information Studies. Retrieved from

Sina, E. (2023). Growing up in a digital environment: The role of digital media use in European children's and adolescents' health and health behaviours. Retrieved from https://media.suub.uni-bremen.de/handle/elib/7428.

Smith, J. (2022). Analysis of financial and digital literacy in modern economy. Ecohumanism Studies, 12.3, 123-145.

Spálová, L., & Mikuláš, P. (2023). Digital resilience in the area of hybrid threats: Perception of concepts associated with the Ukrainian military conflict by Generation Z in Slovakia. Communication Today, 14.2.

Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18.3, 25-45.

Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). International management amid fake news and corruption. Journal of Financial Crime, 30.6, 1674-1691.

Tkáčová, H., et al. (2023). Individual (non) resilience of university students to digital media manipulation after COVID-19 (case study of Slovak initiatives). International Journal of Environmental Research and Public Health, 20.2, 1605.

Valenza, F., et al. (2022). A hybrid threat model for smart systems. IEEE Transactions on Dependable and Secure Computing.

Wilmot, D., Asare, K. K., & Opoku, Y. K. (2023). Antimalarial health seekers' preferences and perceptions: Insights from Ghana. J Infect Dis Epidemiol. Retrieved from https://www.researchgate.net/profile/Kwame-Asare/publication/376191990_Antimalarial_Health_Seekers'_Preferences_and_Perceptions_Insights_from_Ghana/links/65721623ea5f7f02054ce481/Antimalarial-Health-Seekers-Preferences-and-Perceptions-Insights-from-Ghana.pdf.

Wright, G., & Yasar, K. (2022). Retrieved from https://www.techtarget.com/whatis/definition/social-networking..