EDUCATION AGAINST DISINFORMATION

Krunoslav Antoliš*

University of Applied Sciences in Criminal Investigation and Public Security
Zagreb, Croatia

DOI: 10.7906/indecs.22.1.4
Regular article

Received: 19 October 2023.
Accepted: 1 February 2024.

ABSTRACT

In the contemporary world, disinformation has serious consequences, including undermining democracy, the economy and public health. They influence electoral processes, undermine trust in companies, encourage divisions and divert attention from key issues. Social networks play a key role in spreading disinformation and lack of transparency. Prevention of disinformation requires the cooperation of different sectors and the application of effective detection, removal and education strategies. Artificial intelligence is playing an increasingly important role in spreading and combating disinformation.

Psychological factors such as confirmation bias, cognitive dissonance, and social influence contribute to the spread of disinformation. Education, media literacy and critical thinking are key to overcoming these factors. Software tools such as InVID & WeVerify, Google Fact-Check Explorer and others help debunk disinformation by verifying sources and analysing content.

Exploratory research conducted at the University of Applied Sciences in Criminal Investigation and Public Security in Zagreb studied attitudes and behaviours related to disinformation. Participants recognized the importance of checking sources and content analysis, but fewer of them felt that they were sufficiently informed about ways to recognize disinformation. Critical thinking and media literacy play a key role in understanding and combating disinformation.

KEY WORDS

prevention of disinformation, social media, debunking disinformation, media literacy, education

CLASSIFICATION

JEL: D84, I21

*Corresponding author, η: kantolis@fkz.hr; -; -

INTRODUCTION

In today's world, information and communication technologies play a key role, but they also form the basis for various hybrid threats such as hacktivism, cyber terrorism, espionage, warfare and disinformation campaigns. These activities use technology to achieve goals that can seriously threaten the security of individuals, organizations, and entire nations. Cooperation between governments, companies and individuals is necessary to develop effective strategies to counter these threats.

Hacktivism uses hacking and computer activities to advance social or political goals, including disrupting government operations and leaking information. Terrorism in cyberspace relies on digital tools to spread propaganda, recruit and plan attacks. Espionage involves unauthorized access to sensitive data, while cyber warfare uses technology to attack and defend military targets. Disinformation campaigns manipulate public opinion by spreading false or distorted information, often via social media, clickbait headlines and deepfakes. Disinformation can originate from rumours, but also from fiction, governments and politicians, and vested interests. Moreover, changes in the media environment, including the advent of the Internet, have significantly affected the ways in which information is communicated and disinformation spread [1]. Stakeholders in crime prevention face major challenges due to the volume, speed and increasing sophistication of disinformation on the Internet [2]. In Europe, units have been created that are dedicated to identifying, collecting and reviewing disinformation and fake news, warning the media and the public about them (e.g. EU East StratCom Task Force) [3]. At the UN level, the problem of disinformation is also recognized and, for example, in the UNHCR guide on protection on social media, "types of misinformation and disinformation" are presented [4]. Disinformation and fake news spread on social media platforms and mainstream and non-mainstream media. Automated bot accounts assist in this effort by disseminating information at a faster and more frequent pace than individual users can. Disinformation and bot supporters also amplify disinformation and fake news on the Internet [5]. Disinformation can take many forms, including fake news, propaganda and conspiracy theories.

Disinformation campaigns manipulate public opinion by spreading false or distorted information. Declining levels of trust in government have contributed to the rapid spread and consumption of fake news by the public [6]. Disinformation spread through social media, clickbait headlines, deepfakes and other techniques. Perception of disinformation and its effects requires education about the differences between disinformation (inaccurate information without the intent to mislead) and disinformation (deliberately false information for manipulation).

Disinformation has serious consequences, including undermining democracy, the economy and public health. They influence electoral processes, undermine trust in companies, encourage divisions and divert attention from key issues. Social networks play a key role in spreading disinformation, encouraging sensationalism and lack of transparency. Disinformation also serves to recruit extremists through Twitter, which requires efforts to detect and remove extremist content and education to build resilience to extremist tactics. ISIL recruiters used a variety of tactics on Twitter to attract potential recruits. ISIL developed an application *The Dawn of Glad Tidings* that members and supporters would download to their mobile devices; the application is among other things, designed to access the user's Twitter account and tweet on behalf of the user [7].

Prevention of disinformation requires cooperation between different sectors and the application of effective detection, removal and education strategies.

PSYCHOLOGICAL TRIGGERS

There are several psychological triggers that lead individuals to accept and spread disinformation and resist correcting these misconceptions even when presented with evidence [8].

Confirmation bias is the tendency to look for information that confirms existing beliefs, ignore contradictory information, and thus cause biased judgments. Cognitive dissonance is an uncomfortable state when we are faced with information that contradicts our beliefs, prompting us to reject the new information and remain consistent.

Overconfidence and the illusion of knowledge make people less open to new information and able to overestimate their knowledge.

Social influence plays a role in the spread of disinformation because people often accept information that is consistent with the social groups they belong to.

Emotional thinking is based on emotion instead of evidence and often leads to accepting false information.

Fact-fighting occurs when conflicting information is rejected due to identity threats or embarrassment.

More generally, the two strategies are preventive intervention (prebunking) and reactive intervention (debunking). Prebunking aims to help people recognize and resist disinformation they later encounter, even if it is new. Debunking emphasizes responding to certain disinformation after exposure to show why it is false [8]. The common fallacies are divided into three categories: Fallacies of Relevance, Fallacies of Unacceptable Premises, and Formal Fallacies [9].

To overcome these psychological triggers, strategies such as encouraging critical thinking, promoting media literacy, exposing people to different perspectives, and educating people about the mechanisms of disinformation are useful. Governments, technology companies and individuals have a role to play in combating disinformation through regulation, education and promoting accountability. Media literacy is key to identifying and countering disinformation, while critical thinking encourages questioning and impartial evaluation of information. Similar to digital citizenship, a key premise for defining media literacy is that literacy includes the ability to interact intelligently with media and information sources [10]. In line with the growing amount of fake news and disinformation on the Internet, there are numerous platforms on the web for authenticating, analysing and/or fact-checking news [11]. Exposure to different perspectives develops tolerance and broadens understanding. Hearing about someone else’s experience can shed light on a life different from your own and give you a new perspective.

We need new ideas, views, and practices to encourage and inspire us, to show us how others eat, celebrate and love! Therefore, it is important to recognize that diversity is critical to our survival, but it is also critical to our progress. Bringing together people from different backgrounds with different life experiences can generate ideas or perspectives that others may have never considered or been aware of, which can directly affect productivity [12]. Overall, education and awareness play a key role in combating disinformation.

DEBUNKING OF DISINFORMATION

Debunking false information is a key method that can contribute to better informing and educating the public. It is important to thoroughly check information sources, analyse content and circumstances, and apply critical thinking and software tools. It is also important to educate people on how to recognize and challenge false claims, especially in professional policing where professionalism and integrity are crucial. There are variety of software tools for debunking disinformation, depending on the type of information being verified. Some of these tools are:

- InVID & WeVerify Chrome Extension – this technology enables reverse image and video searches to find the original source and authenticity. It also enables keyframe extraction from videos and metadata analysis,

- Google Fact-Check Explorer – this database allows you to search for claims and sources based on keywords, languages, and countries,
- Google Earth – this tool provides a 3D view of parts of the planet and provides additional information about different places,
- SunCalc – this technology makes it possible to determine the position of the sun at a certain time and place.

It is important to invest time, research and critical thinking in debunking false information. It is necessary to check sources, seek confirmation from independent sources, analyse content, recognize illogicalities and manipulative techniques, and share only verified information. Education on debunking of disinformation should be available in order to perform quality police work and become a responsible consumer of information.

CHECKING THE SOURCE OF INFORMATION

The first step is to carefully examine the source of the information. It is necessary to determine whether the source is known, reliable and has a good reputation for providing accurate information. It is also important to ensure that other reliable sources confirm the same information. Regardless of your role (journalist, researcher, and professional), identifying accurate information and using it correctly are key challenges in the 21st century [13]. The contribution to contemporary scientific discussions on journalism therefore lies in the definition of different journalistic strategies related to the exposure, that is, the public exposure of false information that is marketed in order to influence or rather manipulate the whole society or at least its larger parts [14].

There are several criteria you can apply to assess the credibility of a source:

- check who is the author of the information.
- research his credentials, professional experience and reputation in the relevant field.
- compare the information with other reliable sources to confirm accuracy.
- check the relevance of the information to your topic and needs.
- make sure the information is up-to-date, especially with rapid changes.
- look for independent sources that confirm or dispute the information.
- analyse content to identify illogicalities and manipulative techniques.
- using guidelines like the “5 W” questions (Who, What, Where, Why, How), smart checks, and the CRAAP test, you can better assess the reliability of sources [15].
- additional sources.

Finding independent sources is key to verifying information. Use search engines, news browsers and fact-checking platforms as additional sources of information. Fact-checking organizations and journalistic teams often check claims and evaluate their veracity.

ARTIFICAL INTELLIGENCE AND DISINFORMATION

Artificial Intelligence (AI) can be used to create and spread disinformation, and at the same time to detect and suppress it. Here are a few ways artificial intelligence is influencing disinformation: generation of disinformation, disinformation detection, social network analysis, information verification, content personalization, automating fact-checking.

Generative models like GPT-3 have the capability to produce highly realistic and coherent text that can mimic human writing. Advances in generative models such as GPT-3 make it possible to create convincing false information. The ability of these models to generate authentic-sounding text can be abused to create disinformation.

While these models have numerous positive applications, they can also be exploited to generate disinformation, misleading content, and fake news. The generation of disinformation using AI models can have serious consequences, as it becomes increasingly difficult for people to distinguish between authentic information and fabricated content. This can further erode trust in media, institutions, and even online interactions. Addressing this challenge involves a combination of technological, social, and educational measures. Some of these strategies include: algorithmic accountability, content verification tools, media literacy, transparency in AI-generated content, human review, collaboration with AI, public awareness campaigns, regulation and policy. It is a complex issue that requires a multi-pronged approach involving technology, education, policy, and public awareness to effectively address the challenges posed by AI-generated disinformation.

It is important to note that although artificial intelligence has a significant role to play in the fight against disinformation, it is not perfect. Detection algorithms can have false positives or false negatives, and the technology itself can be misused to create sophisticated disinformation. Therefore, it is important to use diverse approaches, including human verification and collaboration, to effectively counter disinformation.

A SYSTEMATIC APPROACH TO DISINFORMATION RESEARCH

There are numerous reasons that point to the need for a coordinated strategy to combat all forms of disinformation, because it is not possible to expect all social groups to take a critical approach on their own initiative, recognize the intention and verify the veracity of the content. However, considering that disinformation represents a great threat to democracy, it is necessary to create adequate educational content. This claim can be supported by numerous previous studies that have confirmed the seriousness of threats, especially in relation to young people. For example, authors in [16] point out that disinformation spread by human action, bots and paid organized groups, so-called troll factories operate maliciously to gain political influence and financial gain, approval of ideas and popularity. Special attention should be paid to social networks and platforms with the role of spreading disinformation, and the issue of regulating these platforms is raised. Self-regulation and encouraging greater accountability of the platforms on which disinformation is spread are becoming increasingly important.

In view of the aforementioned, in this article a research question was asked about the perception, attitudes and habits of the younger population with greater digital and media literacy, related to disinformation on the Internet, with the basic aim of determining the level of recognition and information about disinformation, as well as habits that contribute to less the possibility of manipulating disinformation and determining differences with regard to the level of education in order to coordinate the most appropriate education program with the necessary learning outcomes in international institutional cooperation. This specifically emphasizes the importance and ways of dealing with the problem of disinformation in the digital age.

The specific research questions are: is there a connection between the perception of the frequency of disinformation and checking the truth of information, is there a connection between the frequency of using social networks and checking the truth of information, and are there differences in the perception of two different groups of respondents (university students and high school students, including students course) with regard to experiences with cyber threats and with regard to the perception of the strength of the influence of disinformation. In doing so, survey, comparative and descriptive methods and correlation analysis were used.

The methods used are: survey method, comparative method, descriptive method and correlation analysis, and the data were processed with the statistical package SPSS ver. 25.0.

It was hypothesized that there is a statistically significant connection between the perception of the frequency of disinformation and the verification of the truth of information, and a statistically significant difference between the high school and high school groups of respondents with regard to the experiences of cyber threats and the perception of the impact of disinformation.

METHODOLOGY

PROCEDURE

The research was conducted at the University of Applied Sciences in Criminal Investigation and Public Security in Zagreb during March and April 2023. The research was part of the Erasmus+ project entitled "Collaboration on the development of a common curriculum on combating hybrid threats – HYBRIDC". The Ethics Committee of the University of Applied Sciences in Criminal Investigation and Public Security previously gave a positive opinion on the implementation of the research. The participants were informed about the purpose of the study and gave their consent before participating.

Data were collected through an online survey, and statistical analysis was performed using the SPSS program. General statistical data are presented using means (M) and standard deviations (SD).

PARTICIPANTS

The research participants included 278 persons (63,3 % men and 36,7 % women) with an average age of 29,29 years (standard deviation 6,36 years). All participants are students of the University of Applied Sciences in Criminal Investigation and Public Security, of which 71,9% are studying professional studies in criminology, and 28,1% are specialized graduate studies. Among the participants, 74,8% are employees of the Ministry of the Interior. The average length of service of the police officers in the sample was 6,23 years (standard deviation 5,37 years). The participants performed various jobs within the police, where 23,4% worked in basic police work, 18% in criminal work, 15,1% at the border, 8,6% in traffic and smaller percentages in other specialized units.

RESEARCH INSTRUMENTS

The research used three survey questionnaires: Questionnaire of sociodemographic data, Questionnaire of attitudes and beliefs about disinformation, Questionnaire of behaviour on the Internet.

The sociodemographic data questionnaire contained 11 questions that explored various aspects of the participant's characteristics such as age, gender, occupation, work experience, level of education, grade point average, place of residence, and level of English proficiency.

The questionnaire of attitudes and beliefs about disinformation consisted of 42 items divided into 4 subscales: the impact of disinformation, the purpose of creating and disseminating disinformation, the recognition of disinformation and the frequency of disinformation in the media. Participants responded to these items using a 5-point scale. The reliability of these subscales is acceptable, and the Cronbach α coefficients for each subscale are 0,854 for the influence of disinformation, 0,723 for the purpose of creating and spreading disinformation, 0,660 for recognizing disinformation and 0,938 for the frequency of disinformation in the media.

The Internet behaviour questionnaire consisted of 38 items that were divided into 4 subscales: security protection, protection from disinformation, negative experiences on the Internet, use of social networks and Internet portals. Participants responded to these items using a 5-point scale.

On the security protection and disinformation protection scales, participants answered questions using a 5-point scale (1 – never, …, 5 – almost always), and the particles consisted of recommended behaviours/methods for security protection (e.g. “I regularly change passwords and passwords”) and protection against disinformation on the Internet (e.g. “When I come across some information, news, content on the Internet: I check the credibility of the author of the content”). The scale of negative experiences on the Internet consisted of a list of items corresponding to different methods of cyberattacks (e.g. “Have you been the target (victim) of a cyberattack via: virus, identity theft, card fraud”, etc.) to which participants answered using a scale of 4 degrees (1 – never, …, 4 – often). The use of social networks and Internet portals scale consisted of multiple-choice questions that examine the use of different social networks and Internet portals, the frequency of using them using a 5-point scale (1 – I do not use every day, …, 5 – more than 10 times a day) and the time spent on them daily using a scale of 5 degrees (1 – up to 15 minutes, …, 5 – more than 2 hours). The calculated reliability of all subscales is acceptable and for the scale protection of security is Cronbach α = 0,825, for the scale protection from disinformation Cronbach α = 0,861, for the scale negative experiences on the Internet Cronbach α = 0,865, for the scale use of social networks and Internet portals Cronbach α = 0,735.

FINDINGS

The participants recognized that disinformation has the greatest influence on people’s political attitudes, social events and the perception of events. As the purposes of creating and disseminating disinformation, the participants rated the distraction from social problems and the manipulation of people’s opinion and behaviour the most.

Regarding the impact of disinformation and the purpose of creating and spreading disinformation, the participants believe that disinformation has the greatest impact on people’s political attitudes (M = 4,26), then on social events (M = 4,15) and social perception of an event, person or group (M = 4,14) while they have the least influence on the perception of the population’s health condition (M = 3,89) and the course of the war in Ukraine (M = 3,53).

Regarding the purpose of creating and disseminating disinformation, the participants gave the highest rating to divert attention from important social problems (M = 4,25) and the manipulation of people’s opinions and behaviour (M = 3,24), while the lowest rating rated entertainment (M = 3,06) as the purpose of disinformation.

In the part of the questionnaire on recognizing disinformation and being informed about disinformation, the first three questions refer to the respondent himself, while the other three questions refer to the respondent’s perception of other people. The majority of respondents (66,9%) believe that they are sufficiently informed about the dangers of disinformation, and that they can easily distinguish disinformation from the truth (55,4%), while less than half of them (48,9%) believe that they are sufficiently informed about ways to distinguish disinformation. On the other hand, only 9% of respondents believe that people easily recognize disinformation from true information, 6,9% of them believe that people easily recognize disinformation from disinformation, while 67,7% of them disagree with the thesis that people on the Internet/social networks do not share the news for which they know is disinformation.

Regarding the frequency of disinformation in the media, the participants believe that the highest percentage of disinformation is present on social networks (70,79%) and internet portals (66,87%), while printed newspapers (46,55%) and radio (41,01%) are rated with a lower percentage of disinformation.

Regarding media areas, the participants believe that the highest percentage of disinformation is found in the area of the topic of COVID 19 (67,45%) and politics and marketing (63,02%), while the least amount of disinformation is found in the area of sports (33,85%).

The Internet behaviour the results show that the majority of participants use all of the listed security and privacy protection methods. Using private profile settings on the Internet is the most frequently used method of privacy protection, which is often or always used by 81,7% of participants, while 64,7% of them declare that they are often or always careful about the way they publish text and image content. Strict privacy settings on the Internet are often or always used by 64,8% of participants, while only 1,8% of participants declare that they never use such settings. Creating complex passwords is often or always used by 53,6% of participants, while only 25,9% of them change their passwords regularly.

On the scale of behaviour on the Internet related to disinformation, which represents the central interest of this research, of the seven offered activities (I think before sharing content, I check the veracity of the content, I check the date of the event, I check the credibility of the author of the content, I check the credibility of images and videos, I check the source of the URL address, I ask the experts for their opinion), most participants state that they simply think before sharing content on the Internet, which is often or always 68,4% of them, while 12,6% of participants state that they never or rarely think before sharing some content they come across on the Internet. Only 42,4% of participants often or always check the veracity of the content (the central part of this scale) with 15,8% of them doing it rarely or never. Checking the date of the event, the credibility of the author and content, image and video, and the source of the URL address is done even less often by the participants, while the smallest number of participants ask for an opinion from an expert – 35,6% of them never do this.

A comparison of the different groups from which the research sample was composed, using the t-test for independent samples, shows that there is a statistically significant difference in checking the truth of information with regard to gender (M, F), in such a way that men use methods to check the truth and credibility of information more often than women (MM = 3,13, SdM = 0,759; MF = 2,87, SdF = 0,817; *t* = 2,674, *p* = 0,008) with a small to medium effect size (Cohen *d* equals 0,329). The participants did not differ in the frequency of checking the veracity of information with regard to employment or level of study.

The use of methods for verifying the truth of information (protection against disinformation) is most closely related to security protection (*r* = 0,736) and to being informed about disinformation (*r* = 0,354). People who think they are more informed about ways to recognize disinformation and people who more often use methods to protect security and privacy on the Internet also more often use methods to verify the truth and credibility of information. Low but significant positive correlations were also obtained between protection against disinformation and the perceived amount of disinformation on the Internet (*r* = 0,253) and the perceived impact of disinformation (*r* = 0,206), which indicates that those who believe that there is more disinformation on the Internet and those who believe that disinformation has a more significant impact on individuals and social changes also more often use methods to verify the truth and credibility of information. The frequency of using social networks is not related to protection against disinformation (*r* = 0,074), nor is it the year of study (*r* = 0,01), the grade point average (*r* = 0,049) or age (–0,055).

In order to examine the predictors of protection against disinformation, a regression analysis was performed and out of a total of 4 predictors used in the regression model, 2 predictors were found to be significant in relation to protection against disinformation as a criterion - security protection and recognition of disinformation. According to the beta standardized coefficients, it is evident that security protection is the best predictor of protection against disinformation (β = 0,696), which means that with the increase in the use of methods for security protection on the Internet, the use of methods for verifying the truth of information also increases. Another significant predictor, with a much lower beta coefficient (β = 0,109), is the recognition of disinformation – with the increase in information about the dangers of disinformation and ways to recognize it, the probability of using methods to verify the truth of information also increases. The regression model significantly explains 54,5% of the total variance of protection against disinformation.

DISCUSSION OF FINDINGS

This article presents the results of an exploratory study aimed at collecting preliminary data on the attitudes, beliefs and behaviour habits related to disinformation on the Internet among students of the University of Applied Sciences in Criminal Investigation and Public Security and examining potential predictors of these behaviours.

The results show that the majority of respondents (66,9%) believe that they are sufficiently informed about the dangers of disinformation, and that they easily distinguish disinformation from the truth (55,4%), while less than half of them (48,9%) believe that they are sufficiently informed about the ways to distinguish disinformation.

Furthermore, men use methods to verify the truth of information significantly more often than women (t = 2,674, df = 276, p = 0,008), while the regression model resulted in the two most significant predictors: individuals who are more likely to use methods to protect their privacy and security on the Internet (β = 0,696, p < 0,01) and individuals who believe that they are better informed about the dangers and ways to recognize disinformation (β =0,109, p < 0,05) more often use methods to verify the truth of information (R^2 = 0,545, F = 84,021, p < 0,01).

Further analysis of the correlations suggests that those individuals who believe that disinformation has a more significant impact on society and that disinformation is more frequent in the media also use methods to verify the veracity of information more often.

EDUCATIONAL POTENTIAL

These results provide valuable insight into participants’ attitudes, beliefs and behaviours regarding disinformation. They can serve as a basis for the development of educational content and interventions aimed at raising awareness and promoting proper behaviour in relation to disinformation on the Internet.

Different aspects of disinformation and hybrid threats in the digital world, as well as psychological factors that support their spread are clearly recognized and investigated in the paper. The key points highlighted are as follows.

Information and communication technologies and the threats that are realized through them represent a major security challenge today. For example, the effectiveness of countering hybrid threats really requires cooperation between different sectors, including governments, technology companies and ordinary users. These threats, such as hacktivism, cyber terrorism, espionage and disinformation, all rely on technology to achieve their goals.

Analysis of the relationship between disinformation and social networks shows that the role of social networks in the spread of disinformation is crucial. These platforms enable the rapid spread of information, but also disinformation. It is important to make people aware of the differences between true and false information and to encourage media literacy so that users are better equipped to recognize manipulation.

Analysis of psychological factors that support the spread of disinformation indicates that: confirmation bias, cognitive dissonance, overconfidence and social influence are factors that can contribute to the spread of disinformation and make it difficult for people to accept corrections even when they are presented with the facts.

An integral part of the strategy to combat disinformation must be education and the promotion of media literacy play a key role in this fight. It is also important that governments and tech companies take responsibility in regulating and curbing the spread of disinformation on their platforms.

In accordance with the introductory considerations of this paper and the results of research related to the debunking of disinformation, we could divide the educational approach to this issue into three types of learning outcomes, namely: those that check information sources, content analysis and context checking.

LEARNING OUTCOMES: CHECKING INFORMATION SOURCES

After studying this part, the student will be able to:

- recognize the importance of checking information sources in order to determine their credibility,
- identify key steps for verifying sources, including analysis of authorship, author expertise, comparison with other sources, and relevance and timeliness of information,
- understand the role of fact-finding organizations and reviews of other reliable sources in verifying information,
- develop a critical approach when checking sources, recognizing possible biases, (manipulations or deficiencies in information.

Content analysis is a key step in verifying information and identifying manipulative techniques, so it is important to know how to analyse content. There are numerous definitions of content analysis, such as:

- Definition 1 – "Any technique for drawing conclusions by systematically and objectively identifying particular characteristics of messages" [17].
- Definition 2 – "Interpretive and naturalistic approach. It is both observational and narrative in nature and relies less on experimental elements that are normally associated with scientific research (reliability, validity, and generalizability)" [18].
- Definition 3 – "A research technique for the objective, systematic and quantitative description of the apparent content of communication" [19].

In general, there are two types of content analysis: conceptual analysis and relational analysis. Conceptual analysis determines the existence and frequency of terms in the text, while relational analysis further develops conceptual analysis by examining the relationships between terms in the text [20].

LEARNING OUTCOMES: CONTENT ANALYSIS

After studying this part, the student will be able to:

- recognize the importance of content analysis in evaluating information and recognizing manipulative techniques,
- identify key steps in content analysis, including careful reading, identifying sensationalism, looking for inconsistencies and manipulations, and checking sources and evidence,
- understand the different definitions of content analysis and how they apply to information evaluation,
- develop critical thinking skills when analysing content, recognizing author's motives, verifying factual claims, and recognizing and understanding manipulative techniques.

LEARNING OUTCOMES: CHECK THE CONTEXT

After studying this part, the student will be able to:

- recognize the importance of understanding context when interpreting information,
- identify the steps in properly interpreting the context, including carefully reading the entire content, looking for additional sources for the bigger picture, and identifying hidden motives or interests,
- understand how different sources of information provide different perspectives and contextual information.

Develop the ability to think critically when interpreting the context, recognizing potential biases, ambiguities or incompleteness of information.

These learning outcomes provide guidance for understanding and applying key steps in the processes of information verification, content analysis, and context interpretation. Through their application, students will develop critical thinking skills and better prepare for understanding, interpretation and evaluation of various information.

By implementing these types of learning outcomes in teaching courses at the University of Applied Sciences in Criminal Investigation and Public Security, a significant step forward will be achieved in the field of prevention of misuse of information and communication technologies from the point of view of the creation and spread of disinformation.

The analysis carried out in the paper clearly shows that countering disinformation and hybrid threats is a complex process that requires comprehensive strategies, cooperation of various actors, and education and awareness in order to train people to recognize and face these challenges.

These studies are exploratory in nature, so further research could deepen these results and analyse other variables that could influence participants' attitudes and behavior regarding disinformation.

CONCLUSION

Countering disinformation requires comprehensive and collaborative strategies that include education, regulation, cooperation between sectors, and the application of technological tools to verify and analyse information. It is important to note that although artificial intelligence has a significant role to play in the fight against disinformation.

This research provides a valuable insight into the perception and behaviour of the participants regarding disinformation on the Internet and points to the importance of education and information in order to fight against the spread of disinformation.

The hypothesis that there is a statistically significant connection between the perception of the frequency of disinformation and the verification of the truth of information and a statistically significant difference between the high school and high school groups of respondents with regard to the experiences of cyber threats and the perception of the impact of disinformation was confirmed by this research.

Namely, checking the truth of information is positively and significantly related to the perception of the frequency of disinformation in the media (r = 0,181, p < 0,01) and on social networks (r = 0,253, p < 0,01), and it was also shown that students, who believe that in the media and there is more disinformation on social networks, they use more methods of verifying the truth of information. It was also shown that the perception of the frequency of disinformation in the media and on social networks is positively significantly related (r = 0,547, p < 0,01).

A statistically significant difference was also confirmed in the sample groups regarding the experiences of cyberattacks on the Internet (t = –3,470, p = 0,001), and the group of students experienced more cyberattacks compared to the group of high school and course participants. In the context of the previously presented research results, it can be concluded that it is a moderating effect of the participant's age. There is also a statistically significant difference between the sample groups with regard to the perception of the strength of the influence of disinformation (t = –3,947, p = 0,000), which shows that the group of students attributes to disinformation a more significant impact on the individual and social events than the group of high school and course participants.

In today's digital age, the ability to recognize false information is important for making informed decisions. In professional policing, this becomes crucial to ensure safety and public confidence. Critical thinking, using fact-checking tools and being educated about various disinformation techniques will help maintain the integrity and effectiveness of police work.

The digital landscape is constantly evolving, and addressing these challenges requires a multi-pronged approach involving governments, tech companies, civil society, and individuals. Balancing the regulation of ICT and addressing disinformation with the principles of free speech, privacy, and open communication is a complex endeavour. Effective regulation and response strategies need to be carefully crafted to address the challenges posed by the rapid evolution of technology and the dissemination of information. Striking the right balance between regulating ICT, safeguarding privacy, and addressing disinformation is essential for creating a safe, inclusive, and informed digital environment.

In conclusion, the work emphasizes the importance of dealing with the problem of disinformation in the modern digital age, and through different teaching methods for different age groups opens up space for further research regarding the selection of the most appropriate approaches and teaching methods. It is certainly a research challenge to investigate the breadth and depth of content related to disinformation and the fight against it in the educational space in accordance with the level of education and the expected learning outcomes when creating the curriculum.

REFERENCES

[1] Lewandowsky, S., et al.: *Misinformation and Its Correction: Continued Influence and Successful Debiasing*.
Psychological Science in the Public Interest **13**(3), 106-131, 2012,
http://dx.doi.org/10.1177/1529100612451018,

[2] Hook, K. and Verdeja, E.: *Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities, Atrocity prevention stakeholders face profound challenges from the quantity, speed, and increasing sophistication of online misinformation*.
https://www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities,

[3] Morrelli, V.L. and Archick, K.: *European Union Efforts to Counter Disinformation*.
CRS Insight, 2016,

[4] UNHCR: *Using Social Media in Community-Based Protection A Guide. Factsheet 4: Types of Misinformation and Disinformation*.
https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf,

[5] Jarred, P.: *Commanding the Trend Social Media as Information Warfare*.
Strategic Studies Quarterly **11**(4), 50-85, 2017,

[6] Morgan, S.: *Fake news, disinformation, manipulation and online tactics to undermine democracy*.
Journal of Cyber Policy **3**(1), 39-43, 2018,
http://dx.doi.org/10.1080/23738871.2018.1462395,

[7] Berger, J.M.: *How ISIS Games Twitter*.
https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856,

[8] Ecker, U.K.H., et al.: *The psychological drivers of misinformation belief and its resistance to correction*,
Nature Reviews Psychology **1**, 13-29, 2022,
http://dx.doi.org/10.1038/s44159-021-00006-y,

[9] Dare, T.: *How to Argue Against Common Fallacies*.
https://www.futurelearn.com/info/courses/logical-and-critical-thinking/0/steps/9131,

[10] KnowledgeHut: *Media and Information Literacy: Need, Importance, Example*.
https://www.knowledgehut.com/blog/learning/media-and-information-literacy,

[11] Center for Information Technology and Society at UC Santa Barbara: *Protecting Ourselves from Fake News: Fact-Checkers and their Limitations*.
https://cits.ucsb.edu/fake-news/protecting-ourselves-fact,

[12] O’Boyle, T.: *5 Reasons Why Diversity is Important in the 21st Century*.
https://www.ampglobalyouth.org/2020/06/20/5-reasons-diversity-important-21st-century,

[13] Krahenbuhl, L.E.: *How to Identify Reliable Information*.
https://www.stevenson.edu/online/about-us/news/how-to-identify-reliable-information,

[14] Kvetanová, Z.; Kačincová Predmerská, A. and Švecová, M.: *Disinformation and Fake News.*
https://www.intechopen.com/chapters/73323,

[15] University Libraries University of Washington: *FAQ: How do I know if my sources are credible/reliable*?
https://guides.lib.uw.edu/research/faq/reliable,

[16] Howard, P.N.; Neudert, L.M.; Prakash, N. and Vosloo, S.: *Digital misinformation/disinformation and children*.
UNICEF. Retrieved on February, 20, 2021,

[17] Holsti, O.R.: *Content Analysis*.
In: Gardner, L. and Aronson, E., eds.: *Handbook of Social Psychology*. Vol. 2. Addison-Wesley, Reading, 1968,

[18] WAC Clearinghouse: *Ethnography, Observational Research, and Narrative Inquiry, 1994-2012*.
https://wac.colostate.edu/repository/writing/guides/ethnography,

[19] Berelson, B.: *Content analysis in communication research*.
The Free Press, Glencoe, p.220, 1952,

[20] The Columbia University Mailman School of Public Health: *Content Analysis*.
https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis.