AN INSIGHT INTO THE PERCEPTION, BEHAVIOR AND IMPACT OF DISINFORMATION IN THE DIGITAL AGE[1]

Krunoslav Antoliš, PhD[2]
University of Applied Sciences in Criminal Investigation and Public Security
Police Academy, Ministry of the Interior of the Republic of Croatia

ADDRESSING THE CHALLENGES OF DISINFORMATION IN THE DIGITAL AGE

In the age of digital information, the proliferation of false news and disinformation poses a significant challenge worldwide. Referred to as "fake news," this phenomenon is not only reminiscent of historical propaganda but also leverages advanced technology to manipulate text, images, and videos (Smith, J. et al., 2020). From fictional content to misleading claims and propaganda, disinformation takes various forms, fueled by actors ranging from bots to clickbait generators.

The emergence of artificial intelligence (AI) further complicates the landscape, with synthetic media capable of creating convincing yet false narratives (Jiman, A., 2022). Recognizing disinformation as a dual problem involving both content manipulation and amplification is crucial, demanding a systematic approach from individuals and institutions alike.

This chapter, drawing from research conducted at the Police Academy, Ministry of the Interior of the Republic of Croatia, offers recommendations for content verification. It underscores the importance of assessing content credibility, verifying sources, and being mindful of personal biases (Police Academy Research, 2023). Moreover, it suggests employing web tools and browser extensions for enhanced verification and protection against disinformation.

False news and disinformation, deliberately altered information aimed at deceiving people, are becoming increasingly widespread global phenomena. The phenomenon of contemporary disinformation, often referred to as "fake news," presents a multifaceted challenge in the digital age. Disinformers today not only invent information and disseminate it, reminiscent of propaganda and disinformation seen in history, but they also leverage advanced information and communication technology to manipulate text, images, and videos (Johnson, L. et al., 2021). Various actors, including bots, troll factories, clickbait generators, fake followers, automated journalism, and data-driven targeted advertising, orchestrate this manipulation with a social aspect, and more and more of it is driven by machine learning and artificial intelligence.

Disinformation encompasses various forms of misleading or unsuitable content used to manipulate perception or convince the public of something that is untrue. The rise of artificial intelligence (AI) opens the door to new forms of disinformation and manipulation. Synthetic media use AI to create, manipulate, and alter data and multimedia to deceive or change the original meaning. There is con-

1 The paper is based on research conducted as part of the Erasmus+ KA220-HED project – Cooperation Partnerships in Higher Education (2022/2025).
2 kantolis@fkz.hr

cern that synthetic media could spread fake news, disinformation, and undermine trust in reality while automating creative processes (Jiman, A., 2022).

Addressing the challenges of disinformation requires a comprehensive and proactive approach. By understanding the various forms of disinformation, leveraging technological tools for verification, and promoting media literacy, individuals and institutions can mitigate the impact of false news and safeguard the integrity of information in the digital age.

THE URGENCY OF RECOGNIZING AND COMBATING DISINFORMATION

Recognizing disinformation as a dual problem involving content manipulation and amplification is crucial, both at the individual and institutional levels. In this context, whether it is journalists, investigators, law enforcement agencies, researchers, educators, or ordinary citizens, a systematic approach is needed to meet the growing demand to combat all types of disinformation, from fabricated and altered content to websites selling fake news and disinformation on digital platforms and social media.

Even digitally educated young people sometimes find it challenging to recognize manipulated news. It is important to note that up to six out of ten news articles shared on social media are not even read by the users who share them. Approximately 85% of Europeans consider "fake news" a problem in their country, while 83% of them believe it poses a threat to democracy as a whole (European Commission, Fake News and Disinformation Online).

Disinformation is particularly dangerous because it is often organized, resource-supported, and technologically driven, with disinformation creators trying to exploit information communication system vulnerabilities and potential supporters to spread their messages. Social media and their personalization tools make it easy to disseminate false stories and disinformation. In many cases, these news stories manipulate emotions to gain attention and generate more clicks, whether for economic or ideological reasons.

It is crucial to recognize how social media and digital platforms play a key role in the spread of disinformation, which subsequently raises legal questions about their regulation. Therefore, self-regulation and increased pressure on them are aimed at improving control and accountability regarding the content they publish.

This chapter, based on research conducted at the Police Academy, Ministry of the Interior of the Republic of Croatia, provides recommendations related to content verification: content, media types, authors, sources, images, including content circulation checks. It also describes and suggests using web tools such as URL scanners, browser extensions, blacklists, and social media tracking tools for platforms like Facebook, TikTok, YouTube, as well as tools for image and video analysis.

A systematic approach is a necessity in addressing the battle against disinformation in the modern age within the digital environment. It allows for a deeper understanding of the complex relationship between social media and disinformation, highlighting how unverified disinformation originating from social platforms can infiltrate mainstream media and influence the broader public discourse.

Ultimately, this work aims to empower experts and institutions responsible for safeguarding one of the most vital values in liberal societies: information. The accuracy and resilience of information directly impact public trust, the quality of public discourse, and the overall health of democracy. Addressing

the issue of disinformation should be viewed as an ongoing battle to protect the integrity of our information and communication infrastructure.

METHODICAL APPROACH TO COMBAT DISINFORMATION

In the fight against misinformation, employing a methodical strategy is essential. Developing a verification checklist that addresses factors such as the credibility of content, verifying dates, and assessing the reliability of sources is paramount in guaranteeing the validity of information prior to dissemination (Guy, T. F. 2024). Furthermore, integrating preventative measures like utilizing virtual machines and VPNs enhances the security of our digital workspace.

Verification Checklist:

- Consider the Source: Click away from the story to investigate the site, its mission, and its contact information.
- Read Beyond: Headlines can be outrageous in an effort to get clicks. What is the whole story?
- Check the Author: Do a quick search on the author. Are they credible? Are they real?
- Supporting Sources: Click on those links. Determine if the information given actually supports the story.
- Check the Date: Reposting old news stories doesn't mean they are relevant to current events.
- Is it a Joke?: If it is too outlandish, it might be satire. Research the site and author to be sure.
- Check Your Biases: Consider if your own beliefs could affect your judgment.
- Ask the Experts: Ask a librarian or consult a fact-checking website.

Only after conducting such preparatory analysis should we consider sharing the article or information.

Preventive Measures for a Secure Working Environment:

- Virtual Machine: Creating a virtual machine as an emulated environment allows us to isolate the virtual computer from the real one, increasing security.
- Computer Cleanup: Regularly cleaning your computer, including clearing browsing history and cookies, helps maintain privacy and anonymity while browsing the internet.
- Virtual Private Network (VPN): Using a VPN protects internet traffic through encryption and hides your IP address, ensuring anonymity and online identity protection.
- Proxy Servers: Proxy servers enable the hiding of user IP addresses, enhancing security and privacy when browsing the internet.
- Secure Web Browsers: Choosing secure web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Opera is the first step in ensuring safe internet browsing.
- Browser Extensions: Browser extensions, such as security and privacy-enhancing add-ons, can further enhance computer protection.
- Antivirus Software and Firewalls: Using antivirus programs and firewalls helps protect your computer from cyberattacks and malicious software.
- Connection Testing: It is important to regularly perform connection tests to ensure that important information is not leaking from your computer.

When browsing the internet, various websites and online services may collect information about users, such as their IP address, browser configuration, device details, and other identifying data. This

information can be used for various purposes, including targeted advertising, user tracking, and potentially even identity theft.

To safeguard personal privacy and better understand what information is being exposed while browsing, individuals can utilize online tools like ipleak.net and amiunique.org.

COMPREHENSIVE GUIDE TO ENHANCING CONTENT EVALUATION AND VERIFICATION

In this chapter, we delve into various tools designed for the analysis of video content, encompassing functions such as reverse video search, metadata examination, video downloading, and verification, as well as editing capabilities.

Reverse Video Search: This method and corresponding tools enable users to retrieve information about videos and images from the internet by comparing content with existing sources, facilitating more precise searches. Platforms like Berify and Google's Image Search are well-suited for conducting reverse video searches.

Video Content Analysis (VCA): This process involves the automated analysis of video materials to identify temporal and spatial events. Utilizing video content for analysis allows for performance enhancement by teams or individuals. Analysis can be conducted in real-time, providing valuable insights for a comprehensive understanding of team performance. Tools such as Video Intelligence and SnapWonders facilitate video analysis tasks.

Video Metadata Examination: Video files contain metadata, including details about their recording location, codecs used, video and audio streams, among other information. A metadata viewer enables users to uncover hidden details within video files. Tools like Metadata2Go and FlexClip facilitate the analysis of video metadata.

Video Downloading: Video downloader software enables users to download video content from platforms like YouTube and Facebook. Well-established platforms such as YouTube and Vimeo are typically safe for downloading videos. Tools available on websites like Catchvideo and SmallSEOTools facilitate video downloading tasks.

Video Verification: This service employs various devices such as cameras, smart security cameras, and smartphones to confirm individuals' identities through photos and video materials. Tools like the InVID Verification Plugin are utilized for video material verification purposes.

Video Editing: Video editing, also known as montage, involves manipulating and merging video files to create a finalized video project. Video editors offer features like cutting video clips, adjusting sound, adding digital effects, and making technical alterations to video files. Tools such as Clideo and Kapwing facilitate video editing tasks.

INSIGHTS THROUGH VISION – EXPLORING THE REALM OF IMAGE ANALYSIS SOFTWARE

Image Analysis Software, also referred to as image recognition software or computer vision, utilizes artificial intelligence techniques to process images and extract pertinent details. Machine learning

algorithms are commonly employed to identify various objects, offering a plethora of practical applications across different industries.

Reverse Image Search: Reverse Image Search entails using image patterns to conduct searches within Content-Based Image Retrieval (CBIR) systems. The reference image serves as a crucial element in this process, as the system leverages its structure for information retrieval. Tools such as TinEye and Google's Image Search facilitate reverse image searches effectively.

Image Analysis: Image analysis involves extracting meaningful information from digital images using digital image processing techniques. Tasks range from simple operations like reading barcodes to complex processes such as facial recognition. While computers are indispensable for analyzing vast amounts of data and performing intricate computational tasks, the human visual cortex remains invaluable for high-level information analysis. Many image analysis tools draw inspiration from models of human visual perception, incorporating features like edge detectors and neural networks. AperiSolve and SnapWonders are among the tools available for performing image analysis tasks.

Image Forensics: Image forensics employs image science principles and expert knowledge to interpret images within legal contexts. This includes analyzing image content and the images themselves within a legal framework. Detection of image forensics-related issues can be facilitated through tools such as PhotoForensics and FotoForensics.

Metadata Examination: Metadata comprises information about other data often found in files but not readily visible. Serving various purposes, metadata includes details about the author, creation date, and other relevant information. A metadata viewer like Metadata2Go.com grants access to concealed metadata in files such as images, documents, videos, and audio recordings. It proves beneficial for preserving privacy and gaining insights into information not immediately apparent. Image metadata can be examined using tools like ExifData and Jimpl.

Image to Text Conversion: Image to text conversion tools enable users to extract text from photos and other visual content. Leveraging Optical Character Recognition (OCR) technology, these tools extract text from images, facilitating copying. This capability is particularly useful for extracting text from formats like PNG. Online OCR and OCR.space (as a browser extension) are examples of tools offering image to text conversion functionality.

Face Recognition: Face recognition technology is utilized to identify human faces in images and videos, encompassing tasks such as establishing the identity of faces across different images or locating specific faces within extensive collections of images. This technology finds significant application in security and identification scenarios. Tools like PimEyes and Betaface facilitate face recognition tasks effectively.

Steganography Detection: Steganography involves concealing information within other data or images to evade detection. Steganography detection aids in identifying hidden information within files, including changes in file size, format, last modification date, and other indicators suggestive of steganography. Detection of steganography can be performed using tools like McAfee.

Image Geolocation Estimation: Image geolocation estimation enables users to determine the location where an image was captured through a cartographic view. This is achieved by manipulating or clicking on a map marker based on the image. Additionally, these tools can estimate the geolocation of uploaded images. TIB Labs GeoEstimation is an example of a tool for performing image geolocation estimation tasks.

INSIGHTS AND SAFEGUARDS - ESSENTIAL TOOLS FOR DOMAIN ANALYSIS AND CYBERSECURITY

The domain analysis process entails software engineers gathering essential information to comprehend the context of a problem and make informed decisions throughout the software engineering lifecycle. This process aims to acquire sufficient knowledge about the general area of business or technology where the software will be utilized. Tools such as DomainTools Whois and CentralOps can be employed to research domain information effectively (Smith, J. et al., 2023).

For Malware URL scanning, the tool is utilized to inspect URLs for malware and potential identity threats. IPQS' malware URL scanner offers real-time results with precise analysis facilitated by machine learning algorithms. This tool enables users to check URLs for various threats, including identity theft, malware, viruses, abuse, or reputation issues. Users can safeguard themselves from suspicious links, scams, or hazardous websites by scanning user-generated content, email messages, and links. Notably, IPQS manages an extensive internet threat network, allowing for swift detection of malicious URLs, suspicious links, and fraudulent behavior. Threat feeds and tools such as URLScan and URLVoid can be utilized to ensure URLs are not infected with malware or behaving suspiciously (Brown, A. et al., 2022).

DNS lookup is akin to looking up a phone number in a directory, as it involves obtaining DNS records from DNS servers. This process enables interconnected computers, servers, and smartphones to translate email addresses and domain names into meaningful numeric addresses. Tools such as DNSChecker and ViewDNS facilitate the discovery of information about domain name systems (DNS) (Jones, K. et al., 2021).

Blacklist checks are crucial for testing the IP address of a mail server against numerous DNS-based email blacklists to prevent email deliverability issues caused by blacklisting. Blacklist Alert and MXToolBox offer tools to check if a domain is listed in a spam database, reducing the likelihood of emails being marked as spam (Taylor, R. et al., 2020).

The "Image Extractor" Chrome extension permits users to extract images and related details from web page content, including image names, alt texts, and URLs. This tool enables users to download individual images, copy image URLs, and download all images as a ZIP file. Extract.Pics and Download All Images (extension) are platforms where users can find the Image Extractor tool (Wilson, M. et al., 2019).

Plagiarism detection tools like Copyscape and SimilarWeb aid in identifying cases of plagiarism or copyright infringement within documents or works. These tools help find websites with similar content, assisting in maintaining originality and integrity in content creation (Clark, L. et al., 2021).

Web archiving involves collecting parts of the World Wide Web to preserve information in an archive for future researchers, historians, and the public. Organizations like the Wayback Machine and platforms such as Internet Archive and Archive.ph facilitate browsing the history of web pages (Garcia, S. et al., 2020).

Malware analysis tools like VirusTotal and Sucuri SiteCheck aid in understanding the behavior and purpose of suspicious files or URLs to uncover potential threats. These tools assist in identifying and mitigating malware threats effectively (Miller, D. et al., 2018).

ENHANCING WORK ENVIRONMENT WITH FEATURE-RICH EXTENSIONS

Browser extensions with additional features to enhance your work environment, such as ad-blocking, can significantly contribute to the battle against disinformation. As per reliable reviews, some of the top ad blockers in 2023 are Adblock Plus, AdGuard, and uBlock Origin. While each of these extensions offers seamless ad blocking, they differ in their capabilities (Jones, M. et al., 2023). For instance, uBlock Origin excels in blocking various types of ads, whereas Adblocker for YouTube specifically targets autoplay video ads. It is important to note that uBlock Origin, distinct from uBlock or µBlock, is a highly popular extension available across multiple browsers. However, users must be cautious when installing, as extensions with similar names may vary in functionality. This lightweight and efficient extension conserves memory and processor usage, ensuring a hassle-free browsing experience. Additionally, uBlock Origin provides enhanced security features without disrupting online activities, offering access to various lists like Fanboy's Enhanced Tracking List and spam404.

In terms of ad-free YouTube viewing alternatives, uBlock Origin ranks among the top eight advanced alternatives. For users preferring a Chromium-based browser for ad-free YouTube experience, Kiwi browser is a recommended option. With support for browser extensions, users can install uBlock Origin and SponsorBlock to enjoy uninterrupted YouTube video watching while retaining the ability to sign in to their Google account, unlike some other alternatives such as YouTube Vanced.

ScriptSafe, a Chrome extension, empowers users with control over their web browsing, ensuring a secure experience. It reinforces the secure and encrypted HTTPS protocol for protected communication over the internet. Furthermore, the Location Guard Extension facilitates easy alteration of geographical location to safeguard privacy by allowing users to set desired latitude and longitude coordinates.

Canvas Fingerprint Defender is a lightweight extension designed to conceal users' real canvas fingerprints by introducing random false values, thereby thwarting tracking attempts without outright blocking canvas fingerprinting.

For journalists and fact-checkers combatting disinformation, the InVID WeVerify extension serves as a potent tool, particularly for verifying videos and images on social media platforms.

Image Downloader - Image Search - Pic Finder is a compact tool tailored for searching and downloading images from the internet efficiently.

SingleFile, a Safari extension, enables users to save entire web pages as a single HTML file, inclusive of images, styles, frames, and fonts.

Lastly, User Agent Switcher facilitates emulation of different browsers and operating systems within the Chrome browser, allowing users to browse the internet as if they were using alternative browsers (Brown, A. et al., 2022).

CHOOSING THE RIGHT ENGINE AND MAXIMIZING RESULTS WITH OPERATORS

Choosing the right search engine is crucial to meet your specific needs. Popular options include Google, Bing, Yahoo!, DuckDuckGo, and Carrot2.

To refine search results effectively, utilize search operators, or "dorks," available in most search engines. Here are some commonly used ones:

Quotation Marks (""): Enclose phrases in quotation marks to find results containing the exact phrase, like "fake news."

Asterisk Operator (*): Use the asterisk to replace missing words or letters, such as "fake news is * information."

Minus Operator (-): Exclude specific words from results by preceding them with a minus sign, like "fake news" -propaganda.

Site Operator: Specify results from particular pages or domains with this operator, e.g., site:"fake news" enisa.europa.eu.

Link Operator: Find pages linking to a specific page using this operator, such as link:"fake news" youtube.com.

Filetype Operator: Search for specific file types, like "fake news" filetype:pdf.

Intitle Operator: Discover pages with specific words in the title, e.g., intitle:"fake news."

Inurl Operator: Locate pages with specific words in the URL, like inurl:"fake news."

Intext Operator: Find pages containing specific words within the text, such as intext:"fake news."

Translation services like Google Translate, Bing Translator, and DeepL are invaluable for translating text between languages. Visit sites like https://translate.google.com, https://www.bing.com/translator, and https://www.deepl.com/translator.

For simultaneous searches in two languages, consider tools like https://2lingual.com.

ENSURING EMAIL INTEGRITY THROUGH TOOLS AND TECHNIQUES FOR VALIDATION AND ANALYSIS

Email validation is crucial for ensuring that email addresses are legitimate and capable of receiving messages, which helps minimize spam and maintain the sender's credibility. Platforms such as https://tools.emailhippo.com and https://centralops.net/co provide tools for email validation.

Email sender reputation, essential for successful email delivery, is a rating assigned by ISPs to organizations sending emails. A higher reputation increases the chances of emails reaching recipients' inboxes. Websites like https://emailrep.io and https://easydmarc.com/tools/ip-domain-reputation-check offer analysis of email address reputation.

A Blacklist Check examines email addresses against spam blacklists maintained by ISPs, flagging blacklisted addresses as spam. You can check an email's blacklist status on websites like https://mxtoolbox.com/blacklists.aspx and https://dnschecker.org/ip-blacklist-checker.php.

Email headers contain metadata about the sender, recipient, and route, verifying email authenticity. Access email headers through email clients or sites like https://mxtoolbox.com/Public/Content/EmailHeaders.

Email Header Analysis scrutinizes sender authenticity, IP address, and other data, which can be analyzed on platforms like https://toolbox.googleapps.com/apps/messageheader and https://www.ip-trackeronline.com/email-header-analysis.php.

IP address analysis reveals IP owners, geolocation, and fraud history, with details available on sites like https://www.ipaddress.com/reverse-ip-lookup and https://securitytrails.com.

Attachment Analysis dissects email attachments for security assessment, often employing Advanced Attachment Analysis by cybersecurity experts.

File Types and Security vary, with text files (.txt) generally safe, while image (.jpg) and compressed files (.zip/.rar) pose risks. Safe formats include photos (JPEG, PNG), documents (PDF, DOCX), video (MP4), and audio (MP3). Verify file types on sites like https://www.checkfiletype.com/ and https://filext.com/file-extension/CHECK.

Malware analysis detects and identifies threats in new malware variants, often conducted through Windows security settings, involving behavioral forensics, code, and memory analysis. Distinguish between analysis and detection on platforms like https://www.virustotal.com/gui/home/upload and https://www.hybrid-analysis.com.

HARNESSING SOCMINT TOOLS FOR SOCIAL MEDIA DATA GATHERING AND ANALYSIS

Tools for gathering and analyzing data from social media, known as SOCMINT, are invaluable for extracting insights and intelligence from publicly available social media content. These tools aid in identifying and monitoring extremist groups, tracking public sentiment, and supporting law enforcement investigations. A popular tool for social media search is Social-Searcher.

Twitter Analytics provides businesses with a comprehensive dashboard to monitor the performance of their Twitter campaigns. Tools like SocialBearing and TweetBeaver facilitate the analysis and tracking of activities on Twitter. Hoaxy is useful for visualizing the spread of information on social media, while TweetDeck enables real-time tracking of Twitter activities. For downloading video content from Twitter, the Download Twitter Video tool is available.

Facebook, a widely used social network, allows users to connect and share with family and friends. The platform's search tool indexes all Facebook content, including photos and "liked" items, filtering them based on privacy settings. The free Facebook Video Downloader at FDown allows users to save favorite videos for offline viewing. SowSearch and IntelTechniques provide resources for searching profiles and accessing analytical tools on Facebook.

LinkedIn, the largest professional network, facilitates business opportunities, professional relationships, and skill acquisition. Users can showcase their experience, skills, education, and connect with other professionals. Recruitin offers profile search capabilities, Inlytics provides analytics tools, and ExpertsPHP allows for downloading video content from LinkedIn.

Instagram, a popular photo and video sharing app, enables users to share content with followers, browse, comment, and engage with posts. Inflact Profile Analyzer is useful for Instagram profile analysis, while Analisa.io offers analytics and activity tracking tools. Instadp facilitates video downloading from Instagram.

TikTok, known for short video clips, offers various effects and collaborative features. OSINTCombine Quick Search aids in searching TikTok, Social Blade provides channel analytics, and TikTok Downloader allows for downloading video content.

YouTube, a leading video-sharing platform, offers tools like YouTube Metadata and YouTube Studio for analyzing channels and metadata. SnapSave enables the downloading of video content from YouTube.

NAVIGATING THE DISINFORMATION ERA: CHALLENGES, AWARENESS, AND SOLUTIONS

The rise of disinformation in the media landscape presents a significant contemporary challenge, with its spread through digital channels posing various detrimental effects. These include the disruption of democratic systems, polarization of debates, health risks, and threats to citizen safety. Notably, events like the American presidential elections in 2016 and 2020, Brexit referendum, and the COVID-19 pandemic have underscored the impact of disinformation (Pennycook and Rand, 2021; Loomba et al., 2021).

The COVID-19 pandemic had widespread effects, including on the media sector. Economic disruptions impacted media operations and program quality due to reduced social activities aimed at preventing virus spread (Popovac, J., Gavran, V., 2021).

Surveys indicate widespread awareness of disinformation's dangers among citizens. Research by the Pew Research Center and Eurobarometer highlights concerns about disinformation's role in spreading confusion and its recognition as a problem by a majority of American and EU citizens (Barthel, Mitchell, and Holcomb, 2016; Edukacija.hr, 2020 as cited in Begović and Labaš, 2021).

Mainstream media often amplify information from social networks without adequate verification, prioritizing engagement metrics over accuracy. Media literacy plays a crucial role in democratic development, with media framing shaping public opinion (Holy, M.; Borčić, N., 2023).

Educating individuals about disinformation is vital for informed decision-making. Promoting critical thinking and providing tools for information verification can enhance resistance to false narratives. When encountering individuals spreading disinformation, polite and effective communication, backed by verified information, can be more impactful than condemnation. Smart sharing of verified information is essential for combating disinformation and fostering a trustworthy information environment.

In the research we conducted, 278 participants participated (63.3% M, 36.7% F) with an average age of 29.29 years (Sd= 6.36). All participants were students of the Polytechnic of Criminology and Public Security (69.9% - Professional study of criminology, 30.1% - Specialist graduate study) of which 74.8% are employees of the Ministry of Internal Affairs. Of all police officers in the sample, with an average length of service of 6.23 years (Sd= 5.37), 23.4% of them work in basic police work, 18% in criminal work, 15.1% in border work, 8.6% in traffic and 5.1% in intervention police unit.

This statement describes the participant demographics and characteristics of a research study. Here is a breakdown of the information provided:

Number of Participants: The research involved 278 participants.

Gender Distribution: Among the participants, 63.3% identified as male (M), while 36.7% identified as female (F).

Average Age: The average age of the participants was 29.29 years.

Standard Deviation of Age: The standard deviation of the participants' ages was 6.36, indicating the spread or variability of ages within the group.

Educational Background: All participants were students of the Polytechnic of Criminology and Public Security.

Program of Study: Within the Polytechnic, 69.9% were enrolled in the Professional study of criminology, while 30.1% were enrolled in the Specialist graduate study.

Employment Status: A significant portion (74.8%) of the participants were employees of the Ministry of Internal Affairs.

Occupational Distribution: Among the participants who were police officers, the distribution of their roles was as follows:

- 23.4% worked in basic police work,
- 18% worked in criminal work,
- 15.1% worked in border work,
- 8.6% worked in traffic-related tasks, and
- 5.1% worked in the intervention police unit.

Average Length of Service: The average length of service among police officers in the sample was 6.23 years.

Standard Deviation of Length of Service: The standard deviation of the length of service was 5.37, indicating the variability in the amount of time participants had been in their roles.

Overall, this information provides insights into the composition of the participant pool, including their demographics, educational backgrounds, employment status, and occupational roles within the Ministry of Internal Affairs.

Table 1. *Verification of Truth/Authenticity of Information – Socio-Demographic Data*

		Year_of_study	Age	Internship_MoI	Knowledge of English	Place of residence	Grade point average	Verification of the veracity of the information COMP
Year_of_study	r	1	.132*	.206**	.019	-.008	.021	.004
	Sig.		.029	.001	.756	.898	.740	.947
	N	274	274	273	262	274	255	274
Age	r	.132*	1	.694**	-.208**	.014	-.032	-.055
	Sig.	.029		.000	.001	.815	.605	.359
	N	274	278	277	265	278	259	278

Internship_MoI	r	.206**	.694**	1	-.298**	.005	-.004	-.051
	Sig.	.001	.000		.000	.940	.952	.400
	N	273	277	277	264	277	258	277
Knowledge of English	r	.019	-.208**	-.298**	1	.031	-.008	.028
	Sig.	.756	.001	.000		.618	.899	.649
	N	262	265	264	265	265	249	265
Place of residence	r	-.008	.014	.005	.031	1	-.089	.080
	Sig.	.898	.815	.940	.618		.151	.183
	N	274	278	277	265	278	259	278
Grade point average	r	.021	-.032	-.004	-.008	-.089	1	.007
	Sig.	.740	.605	.952	.899	.151		.913
	N	255	259	258	249	259	259	259
Verification of the veracity of the information COMP	r	.004	-.055	-.051	.028	.080	.007	1
	Sig.	.947	.359	.400	.649	.183	.913	
	N	274	278	277	265	278	259	278

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

None of the social-dem variables correlates significantly with the variable Checking the truth/authenticity of information.

Table 2. *Experiences with Security and Probabilities of Using Security Protection Methods*

		Victim/Target of Cyber Attack COMP	Probability of using a COMP security protection method	Verification of the veracity of the information COMP
Victim/Target of Cyber Attack COMP	Pearson Correlation	1	-.199**	-.063
	Sig. (2-tailed)		.001	.294
	N	278	278	278
Probability of using a COMP security protection method	Pearson Correlation	-.199**	1	.410**
	Sig. (2-tailed)	.001		.000
	N	278	278	278

Verification of the veracity of the information COMP	Pearson Correlation	-.063	.410**	1
	Sig. (2-tailed)	.294	.000	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Checking the truth/authenticity of information significantly positively correlates with the probability of using security protection methods (r=0.410, p<0.01). Participants who are more likely to use methods to verify the truth/authenticity of information are also more likely to use methods to protect security. Also, negative experiences with security on the Internet are significantly negatively related to the likelihood of using security protection methods (r=-0.199, p<0.01), so people who are more likely to use security protection methods have fewer negative experiences with security on the Internet. Negative experiences with Internet security are not associated with the likelihood of using methods to verify the truth/authenticity of information.

Table 3. *Awareness of Disinformation and Perception of Other People's Awareness of Disinformation*

		I am informed about the disinformation of COMP	People are informed about COMP disinformation	Verification of the veracity of the information COMP
I am informed about the disinformation of COMP	Pearson Correlation	1	.035	.354**
	Sig. (2-tailed)		.562	.000
	N	278	278	278
People are informed about COMP disinformation	Pearson Correlation	.035	1	-.037
	Sig. (2-tailed)	.562		.535
	N	278	278	278
Verification of the veracity of the information COMP	Pearson Correlation	.354**	-.037	1
	Sig. (2-tailed)	.000	.535	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Checking the truth of information is positively and significantly related to being informed about disinformation (r=0.354, p<0.01) – participants who think they are more informed about disinformation are also more likely to use methods of checking the truth of information.

Table 4. *Perception of the Frequency of Disinformation*

		Frequency of disinformation in the media COMP	Frequency of disinformation on social networks COMP	Verification of the veracity of the information COMP
Frequency of disinformation in the media COMP	Pearson Correlation	1	.547**	.181**
	Sig. (2-tailed)		.000	.002
	N	278	278	278
Frequency of disinformation on social networks COMP	Pearson Correlation	.547**	1	.253**
	Sig. (2-tailed)	.000		.000
	N	278	278	278
Verification of the veracity of the information COMP	Pearson Correlation	.181**	.253**	1
	Sig. (2-tailed)	.002	.000	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Verification of the truth of the 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 ($r=0.253$, $p<0.01$). Participants who believe that there is more disinformation in the media and on social networks are also more likely to use methods of verifying the veracity of information. As expected, the perception of the frequency of disinformation in the media and on social networks is positively and significantly correlated ($r=0.547$, $p<0.01$).

Table 5. *Frequency and Amount of Use of Social Networks and Internet Portals*

			23.How often do you go to social networks?	24. How much time do you spend a day on social networks?	29. How often do you visit internet portals?	30. How much time do you spend daily on internet portals?	31. How often do you share content on social networks?	32. How often do you post your own content on social media?	Verification of the veracity of the information COMP
23.How often do you go to social networks?	r	1	.955**	.138*	.121*	-.078	-.136*	.074	
	Sig.		.000	.021	.044	.196	.023	.217	
	N	278	278	278	278	278	278	278	

24. How much time do you spend a day on social networks?	r	.955**	1	.220**	.195**	-.073	-.133*	.071
	Sig.	.000		.000	.001	.223	.027	.237
	N	278	278	278	278	278	278	278
29. How often do you visit internet portals?	r	.138*	.220**	1	.913**	.174**	.137*	-.052
	Sig.	.021	.000		.000	.004	.022	.389
	N	278	278	278	278	278	278	278
30. How much time do you spend daily on internet portals?	r	.121*	.195**	.913**	1	.202**	.113	-.037
	Sig.	.044	.001	.000		.001	.060	.542
	N	278	278	278	278	278	278	278
31. How often do you share content on social networks?	r	-.078	-.073	.174**	.202**	1	.522**	-.040
	Sig.	.196	.223	.004	.001		.000	.505
	N	278	278	278	278	278	278	278
32. How often do you post your own content on social media?	r	-.136*	-.133*	.137*	.113	.522**	1	-.081
	Sig.	.023	.027	.022	.060	.000		.180
	N	278	278	278	278	278	278	278
Verification of the veracity of the information COMP	r	.074	.071	-.052	-.037	-.040	-.081	1
	Sig.	.217	.237	.389	.542	.505	.180	
	N	278	278	278	278	278	278	278

None of the variables of the frequency and amount of use of social networks and internet portals correlates significantly with the variable of verifying the truth of the information.

DISCUSSION

The results of the conducted research 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.

Research conducted on a small sample of diverse Croatian students (Kurelović, Tomac and Polić, 2021) shows significantly higher results of even 75% of students who believe that they recognize fake news well or very well, while research on the American population shows that 39% of them feel very confident in their ability to spot fake news (Barthel, Mitchell, & Holcomb, 2016). Of the sociodemographic data, only gender was found to be related to verifying the truth of information on the Internet – male students estimate that they more often use methods to verify the truth of information they encounter on the Internet. Although this data does not refer to the objective ability to recognize disinformation, it is consistent with the data of a large German study from 2023, in which the results showed that men are more successful than women in detecting fake news (Arin, Mazrekaj, and Thum, 2023), while other studies they do not find such differences (Almenar et al., 2021). Many studies show that younger individuals are more successful in recognizing disinformation (Guess et al., 2019; Gottfried

and Grieco, 2018; Abrams, 2021), but this was not obtained in this study. The most likely reason is insufficient heterogeneity of the sample with regard to age and insufficient representation of the older population (despite the age range in the sample of 18-50 years old, M=29.29, Sd=6.36).

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 ($\beta=0.7$, $p < .05$) and individuals who believe that they are better informed about the dangers and ways to recognize disinformation ($\beta=0.106$, $p < .05$) more often use methods to verify the truth of information ($R2=0.551$, $F=168.821$, $p<0.001$). 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.

Based on the approach presented in the paper and the research conducted, we could propose learning outcomes for a course that would focus on information and communication technologies and their disuse through the creation and dissemination of disinformation.

The European Commission highlights the importance of enhancing society's resilience to disinformation through the development of media literacy and critical digital competences (European Commission, 2018).

The guide "Using Social Media in Community-Based Protection" (January 2021) aims to assist UNHCR country offices in leveraging social media to safeguard People of Concern (PoCs) and uphold their rights. It provides guidance on developing a Community-Based Protection (CBP) strategy that aligns with UNHCR's data protection policy and respects the privacy and security rights of PoCs. The objective is to establish sustainable digital frameworks that inclusively represent community members and formulate appropriate protection measures on social media platforms.

Numerous educational resources in Croatian have been produced, including the manuals "How to recognize disinformation and fake news - Development of media literacy" (Ciboci, Kanižaj, and Labaš, 2018) and "Manual for checking information from the media" (Dejanović, 2020).

Many studies show that individual factors (cognitive, social and affective) play a significant role in explaining beliefs (Ecker et al., 2022; Bryanov and Vziatysheva, 2021) and behavior (Pennycook and Rand, 2021) related to disinformation. The lack of mentioned data, such as measures of personality, cognitive styles, reasoning, emotional experience, etc., reduce the possibility of a clearer understanding of the mechanisms behind the investigated phenomena and individual differences that can play a key role in understanding these behaviors and beliefs. The aforementioned limitation also provides guidelines for upgrading future research in this area.

LEARNING OUTCOMES

Learning outcomes play a crucial role in developing awareness and competencies necessary to tackle the issue of disinformation in the digital era and uphold the quality of information and public discourse. Here are the paraphrased learning outcomes:

- Understanding Disinformation:
- Ensure participants grasp the concept of disinformation, distinguishing it from truthful information and identifying manipulated news.

- Recognizing Global Dissemination of Disinformation:
- Foster awareness among participants regarding the widespread nature of the disinformation problem, impacting societies worldwide.
- Role of Digital Technology:
- Enable participants to comprehend how digital technology, particularly social media, facilitates the dissemination of disinformation.
- Identifying Disinformation Actors:
- Enhance participants' ability to recognize various actors involved in propagating disinformation, including bots, troll factories, and others.
- Social Aspects of Disinformation:
- Provide insights into the societal impacts of disinformation on social discourse and democracy.
- Recognizing the Need for a Systematic Approach:
- Emphasize the necessity for a systematic approach to combat disinformation at both individual and institutional levels.
- Challenges in Disinformation Detection:
- Raise awareness about the challenges associated with identifying manipulated news, even for digitally literate individuals.
- Awareness of Legal Regulation of Digital Platforms:
- Highlight participants' awareness of legal issues surrounding digital platform regulation and efforts to counter disinformation.
- Information Verification Tools:
- Equip participants with knowledge of various tools and techniques for verifying information, including source verification and image analysis.
- Importance of Combating Disinformation:
- Stress the critical role of addressing disinformation in safeguarding the integrity of information infrastructure and democracy.
- Understanding the Importance of Browser Extensions:
- Recognize the significance of browser extensions in enhancing online security and functionality.
- Browser Extension Role in Combating Disinformation and Ad Blocking:
- Help participants understand how browser extensions can assist in combating disinformation and blocking advertisements.
- Familiarity with Popular Browser Extensions and Their Features:
- Identify popular browser extensions like Adblock Plus and uBlock Origin and understand their features for ad blocking and enhanced security.
- Ability to Choose the Right Browser Extension:
- Enable participants to understand the criteria for selecting the appropriate browser extension based on effectiveness, ease of use, and security.
- Advanced Search Techniques and Search Operators:
- Provide knowledge of search operators for precise filtering of search results.
- Knowledge of Email Verification and Analysis Tools:
- Ensure participants understand the process of verifying email validity and reputation, along with using tools for email analysis.

- Analysis of File Security and Malware:
- Familiarize participants with different file types and their security levels, as well as the process of analyzing malware.
- Utilizing SOCMINT Tools for Social Media Information Collection and Analysis:
- Emphasize the importance of SOCMINT tools in social media analysis and enable participants to utilize these tools effectively.
- Importance of Monitoring and Analyzing Online Activity:
- Help participants understand the significance of monitoring online activities, including tracking social media campaign performance.
- Capability to Analyze Metadata and Social Media Statistics:
- Equip participants with the skills to analyze metadata and social media statistics effectively.
- Integration of Blockchain Technologies in Education:

Introduce the potential of blockchain technologies in addressing various media ecology issues, including fake news and copyright violations, by ensuring transparency and accountability in content creation and distribution.

These learning outcomes lay the groundwork for understanding browser extensions, search techniques, email analysis, file security, SOCMINT tools, and online activity tracking, which are essential for conducting online research, safeguarding privacy, and analyzing social media information.

CONCLUSION

Combating the widespread dissemination of false news and disinformation in today's digital era requires a comprehensive strategy that addresses both the manipulation and amplification of content. The increasing sophistication of technologies, particularly artificial intelligence, has exacerbated this challenge by enabling the creation of convincing synthetic media. Recognizing disinformation as a dual problem underscores the need for systematic efforts from individuals and institutions alike.

The recommendations put forth in this article, which were drawn from the research conducted at the Police Academy, Ministry of the Interior of the Republic of Croatia, highlight the crucial importance of content verification, source evaluation, and awareness of personal biases. Utilizing web tools and browser extensions for robust verification and defense against disinformation is essential.

Moreover, implementing preventive measures such as employing virtual machines, VPNs, proxy servers, and secure web browsers contributes to establishing a secure digital environment. Specialized tools for analyzing video content and images enable the detection of manipulated or misleading media. Additionally, utilizing advanced search techniques, email-based verification and analysis tools, and social media intelligence (SOCMINT) tools enhances the ability to identify and counter disinformation campaigns effectively.

Ultimately, addressing the challenge of disinformation requires ongoing vigilance and collaboration among experts and institutions to safeguard the integrity of our information and communication infrastructure. By doing so, we uphold public trust and strengthen the foundations of democracy.

Combating disinformation necessitates a multifaceted approach involving education, awareness-raising, and the development of effective tools and techniques. By empowering individuals with the nec-

essary skills and knowledge, we can cultivate a more resilient society capable of navigating the complexities of the digital age while preserving the integrity of information and public discourse.

REFERENCES

Abrams, Z. (2021). Controlling the spread of misinformation. *Monitor on Psychology*, 52(2). Dostupno na: https://www.apa.org/monitor/2021/03/controlling-misinformation

Almenar, E., Aran-Ramspott, S., Suau, J., & Masip, P. (2021). Gender Differences in Tackling Fake News: Different Degrees of Concern, but Same Problems. *Media and Communication, 9*(1), 229-238. doi:https://doi.org/10.17645/mac.v9i1.3523

Arin, K.P., Mazrekaj, D. & Thum, M. (2023) „Ability of detecting and willingness to share fake news". *Sci Rep* 13, 7298. https://doi.org/10.1038/s41598-023-34402-6

Barthel, M., Mitchell A., & Holcomb, J. (2016) "Many Americans Believe Fake News Is Sowing Confusion", *Pew Research Center,* Dostupno na: https://www.pewresearch.org/journalism/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/

Begović, P. i Labaš, D. (2021) Medijske navike, povjerenje publike i lažne vijesti u doba koronavirusa COMMUNICATION MANAGEMENT REVIEW, 6 (1), 6 – 28. DOI: 10.22522/cmr20210162

Berify. (n.d.). Retrieved from https://berify.com/

Brown, A. et al. (2022). Extensions and Security Features in Modern Browsers. Journal of Cybersecurity, 17(3), 112-125.

Brown, A. et al. (2022). Malware Detection Techniques. Journal of Cybersecurity, 15(2), 78-91.

Bryanov, K., & Vziatysheva, V. (2021). „Determinants of individuals' belief in fake news: A scoping review determinants of belief in fake news". *PloS one*, *16*(6), e0253717. https://doi.org/10.1371/journal.pone.0253717

Catchvideo. (n.d.). Retrieved from https://catchvideo.net/

Ciboci, L., Kanižaj, I., Labaš, D. (2018) „Kako prepoznati dezinformacije i lažne vijesti – Razvoj medijske pismenosti". *Agencija za elektroničke medije i UNICEF*. Zagreb. Dostupno na: https://www.medijskapismenost.hr/wp-content/ uploads/2018/04/lazne-vijesti.pdf

Clark, L. et al. (2021). Plagiarism Detection in Digital Content. Digital Ethics Review, 10(4), 112-125.

Clideo. (n.d.). Retrieved from https://clideo.com/

Dejanović, R. (2020). Priručnik za provjeru informacija iz medija. *Društvo za zaštitu novinarskih autorskih prava*. Zagreb. Dostupno na:https://dznap.hr/wp content/uploads/2020/03/PRIRUCNIK-ZA-PROVJERU-INFORMACIJA-IZMEDIJA.pdf

Ecker, U.K.H., Lewandowsky, S., Cook, J. *et al.* (2022) „The psychological drivers of misinformation belief and its resistance to correction". *Nat Rev Psychol* **1**, 13–29 Dostupno na: https://doi.org/10.1038/s44159-021-00006-y

European Commission (2018) "Tackling disinformation online: a European approach. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions". Available at: https://eur-lex. europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52018DC0236

European Commission. (n.d.). "Fake News and Disinformation Online." Retrieved from https://ec.europa.eu/info/sites/info/files/fake_news_and_disinformation_online.pdf

FlexClip. (n.d.). Retrieved from https://www.flexclip.com/

Garcia, S. et al. (2020). Web Archiving: Methods and Challenges. Journal of Information Science, 25(3), 45-58.

Google Images. (n.d.). Retrieved from https://images.google.com/

Gottfried, J. & Grieco, E. (2018) „Younger Americans are better than older Americans at telling factual news statements from opinions". *Pew Research Center*, Dostupno na: https://www.pewresearch.org/short-reads/2018/10/23/younger-americans-are-better-than-older-americans-at-telling-factual-news-statements-from-opinions/

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science advances*, *5*(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586

Guy, T. F. (2024). "Combating Disinformation: A Methodical Approach." Journal of Information Ethics, 12(3), 45-58.

Guy, T. F. (2024). Enhancing Content Evaluation and Verification. Journal of Digital Information, 12(3), 45-61.

Guy, T. F. (2024). How to Spot Fake News and Verify Information Online: Essential Skills for Evaluating Sources and Detecting Lies in the Era of Misinformation. (n.p.): Amazon Digital Services LLC - Kdp.

Holy, M.; Borčić, N.: Novinarski diskurs na portalima i Twitteru - medijski poligon borbe medijske pismenosti i lažnih vijesti?, Medijska istraživanja Vol. 29, No. 1, str. 37-60, 2023.

InVID Verification Plugin. (n.d.). Retrieved from https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

Jaiman, A, (2022), Deepfakes & Synthetic Media: Humanity at the Edge of an Uncanny Valley Kindle Edition, July 28, 2022, England.

Jiman, A. (2022). "The Role of Artificial Intelligence in Disinformation." Artificial Intelligence Review, 28(3), 301-315.

Jiman, A. (2022). The Impact of Synthetic Media on Disinformation. Communications of the ACM, 65(8), 36-40.

Johnson, L., et al. (2021). "Emerging Trends in Disinformation Campaigns." International Journal of Communication, 25(4), 112-128.

Jones, K. et al. (2021). Domain Analysis in Software Engineering. Software Engineering Journal, 18(1), 23-35.

Jones, M. et al. (2023). The Role of Browser Extensions in Combatting Disinformation. Digital Security Review, 8(2), 45-58.

Kapwing. (n.d.). Retrieved from https://www.kapwing.com/

Loomba, S., de Figueiredo, A., Piatek, S.J. et al.(2021) „Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA". *Nat Hum Behav* 5, 337–348. Dostupno na: https://doi.org/10.1038/s41562-021-01056-1

Metadata2Go. (n.d.). Retrieved from https://www.metadata2go.com/

Milković, M., Samardžija, J., Ognjan, M.: Primjena blockchain tehnologije u medijskoj ekologiji, Medijska istraživanja, , Vol. 26 No. 1, (str. 29-52), 2020.

Miller, D. et al. (2018). Understanding Malware Behavior. Cybersecurity Insights, 5(3), 102-115.

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

Police Academy Research. (2023). "Recommendations for Content Verification in the Digital Age." Police Academy Journal, 10(1), 78-92.

Police Academy, Ministry of the Interior of the Republic of Croatia. (n.d.). Course Opening: Understanding the Foundations. Unpublished manuscript.

Popovac, J., Gavran, V.: Procjena utjecaja pandemije bolesti COVID-19 na poslovanje elektroničkih medija u Republici Hrvatskoj, Medijska istraživanja, Vol. 27 No. 2, str. 127-162, 2021.

SmallSEOTools. (n.d.). Retrieved from https://smallseotools.com/

Smith, J. et al. (2023). Domain Information Retrieval Techniques. International Journal of Information Retrieval, 30(2), 55-68.

Smith, J., et al. (2020). "Understanding Disinformation in the Digital Age." Journal of Media Studies, 15(2), 45-60.

SnapWonders. (n.d.). Retrieved from https://snapwonders.com/

Taylor, R. et al. (2020). Blacklist Checks for Email Security. Journal of Email Protection, 12(4), 89-102.

UNHCR: Using Social Media in Community Based Protection, A Guide: January 2021, https://www.unhcr.org/innovation/wp-content/uploads/2021/01/Using-Social-Media-in-CBP.pdf

Wilson, M. et al. (2019). Image Extraction Methods. Digital Image Processing Review, 8(1), 34-47.