Disinformation Campaigns: Battling Misinformation for Resilience in Hybrid Threats Model

William Steingartner, Darko Galinec, Dávid Vaľko, Norbert Ádám

Technical University of Košice, Faculty of Electrical Engineering and Informatics
Letná 9, 042 00 Košice, Slovakia
william.steingartner@tuke.sk, david.valko@tuke.sk, norbert.adam@tuke.sk

Department of Informatics and Computing, Zagreb University of Applied Sciences; Vrbik 8, 10000 Zagreb, Croatia; darko.galinec@tvz.hr

Abstract: Recognizing truth from lies has become a critical and challenging task in our current environment, which is flooded with abundant information from various sources and platforms. The existence of false information and manipulative content in the public sphere is not an entirely novel phenomenon. On the other hand, the modern-day circumstance is one of a kind because of the rapid dissemination of a big quantity of false information, particularly via social media and smartphone applications. This presents an unprecedented challenge. The prevalence of contamination in the realm of information, along with the complex network of individuals, methods, and reasons behind this false information, now represent a key aspect of hybrid threats. An outstanding aspect is the speed at which false information disseminates through interconnected networks, platforms, and applications. This paper effectively achieved two objectives. The primary objective was to introduce a novel non-hierarchical conceptual framework for hybrid threats, with the aim of enhancing awareness and reinforcing the resilience of the system. The second objective was to investigate the feasibility of integrating AI technology to enhance the efficiency and speed of detecting and identifying growing misinformation.

Keywords: conceptual model of hybrid threats; internet resilience; information security; disinformation campaign; GPT-4

1 Introduction

In the modern age, characterized by the prevalence of digital information, we are constantly flooded with an endless stream of data. “One of the effects of living with electric information is that we live habitually in a state of information overload. There’s always more than you can cope with” [1]. By participating in

political processes that are completely free of discrimination and restrictions, citizens are able to voice their views and participate in public conversations. Generally speaking, these actions are secured by security protocols that have been thoughtfully developed and evaluated. These protocols make an effort to build communication between users that is both trustworthy and safe [2] [3] [4] [5] [6]. Social media and other online platforms have made it possible for almost everybody to share their thoughts, ideas, and perspectives with potentially large audiences, as well as making variety of educational resources available. [7] [8] [9] [10]. They enabled individuals who were unable to access traditional media to establish themselves as influencers, sharing their personal knowledge and experiences with their followers.

Considering the inherent inability of humans to manually discern and eliminate disinformation on the web, the implementation of an effective automated tool in the form of artificial intelligence would be highly beneficial. We intend to use the capabilities of generative AI, the latest cutting-edge technology, to combat the spread of disinformation.

All users are allowed to participate in an open hearing on any topic, regardless of their level of knowledge on the subjects being discussed. Various actors are involved in distinct phases of the production and dissemination of disinformation, each driven by different motivations and varying levels of awareness. The impact of correcting disinformation is often less potent than the misinformation being countered. Moreover, the act of repeating inaccurate and manipulative assertions in the corrections can unintentionally reinforce the disinformation further, as our attention is selective and limited. The corrections may be marginalized or ignored by audiences already primed by the prevalence of disinformation in their social circles. Furthermore, the corrections are generally less appealing and possess a diminished emotional impact compared to the disinformation.

The paper is structured as follows: Section 2 provides a comprehensive review of previously published studies. Section 3 explores the conceptual model of hybrid threats and its contribution to the modeling of hybrid threats. The subject of the Demaskuok study is introduced in Section 4. Section 5 dived into the capacity of the GPT-4 model to combat misinformation on the worldwide web. We will address the subsequent stages of our future research in Section 6. In conclusion, Section 7 marks the end of our paper.

2 Review of Past Research

When it comes to cybersecurity, member states include security features into their national policies that preserve particular values, such as human rights. The significance of this cannot be overstated, especially when considering the

dissemination of false information via traditional media channels or social networking sites. At the same time, cybersecurity has emerged as one of the most significant issues regarding elections. During the period leading up to elections that are of critical importance, various nations have, without a shadow of a doubt, been witnesses to the occurrence of actions such as the propagation of false information or negative propaganda. This security concern has the potential to do damage to the democratic process that is being carried out inside the European Union [11].

In regards to AI, many researches are currently being conducted in the field of generative AI. The GPT-4 model has been proven to work well in the field of situational awareness. One of the research studies suggests that GPT-4 can generate personas based on feedback data provided by users [12]. There have also been studies comparing the performance of ChatGPT models in terms of news and fact verification [13].

2.1 The Strategy of Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) was created by the U.S. Department of Defense (DoD) in partnership with Carnegie Mellon University and the Johns Hopkins University Applied Physics Laboratory. The primary goal of the Department of Defense (DoD) in developing this model is to secure information from the Defense Industrial Base sector (DIB). The CMMC focuses on two types of classified information: "Federal Contract Information," which refers to information provided to or generated for the government under a contract that is not meant for public release, and "Controlled Unclassified Information," which refers to information that requires particular security measures and dissemination controls in accordance with laws, regulations, and government-wide regulations. The Cybersecurity Maturity Model Certification (CMMC) examines the level of cybersecurity maturity and includes both recommended practices and a certification component to ensure the adoption of practices corresponding to each maturity level. The most recent iteration of the Cybersecurity Maturity Model Certification (CMMC) was revealed in 2020. Characteristics and measurements that CMMC includes are seventeen domains that represent groupings of cybersecurity techniques and capabilities. Each domain is subsequently divided into numerous processes that exhibit similarities across domains and possess a range of capabilities that extend across five stages of maturity. The capabilities are further elaborated into specific practices [11] for each corresponding level of maturity, as illustrated in Figure 1.

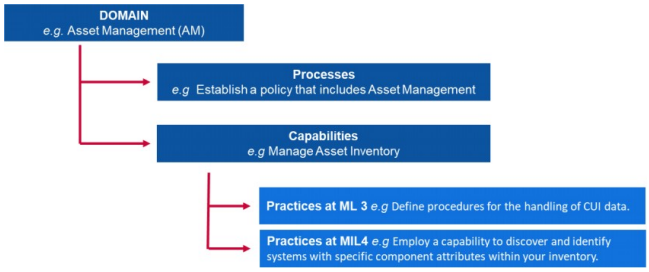

Figure 1
An example of CMMC Indicators

2.2 The Strategic Plan Against Disinformation and Cyber Threats

The Commission has formulated an Action Plan at the European level [14] to enhance efforts in combating disinformation in Europe. This plan concentrates on four main areas: detection, cooperation, collaboration with online platforms, and awareness. Its purpose is to enhance the European Union's abilities and foster cooperation among Member States. Four out of the nineteen countries that were interviewed have explicitly stated their intention to address the problem of disinformation and propaganda in their National Cybersecurity Strategy (NCSS). After interviews carried out by the European Union Agency for Cybersecurity (ENISA), it was revealed that several Member States do not consider the issue as a cybersecurity threat in their National Cybersecurity Strategies (NCSS). Instead, they address the issue at a wider societal level, such as through legislative efforts. [15]

2.3 Emerging State-of-the-Art Technologies

With the ongoing expansion of the cyber threat environment, the introduction of new technologies such as 5G, AI, and quantum computing is likely to lead to a rise in both the frequency and severity of cyber-attacks. Additionally, malicious individuals will likely employ a wider range of methods, means, and targets. During the desk research phase conducted on the National Cyber Security Strategies (NCSS) of Member States, the following advanced technologies were identified as being of interest: 5G, artificial intelligence (AI), quantum computing, cryptography, edge computing, connected and autonomous vehicles, big data and smart data, blockchain, robotics, and the Internet of Things (IoT). In early 2020, the European Commission issued a communication urging Member States to adopt the measures outlined in the 5G toolbox findings [16]. The 5G toolbox was developed following the adoption of Recommendation (EU) 2019/534 by the

Commission in 2019. This recommendation emphasized the need for a united European approach to ensure the cybersecurity of 5G networks [17]. The quick data transfer capabilities of current networks, notably the emerging 5G technology, could contribute to the growth of disinformation. The 5G networks, which are known for their fast speed and minimal delay, enable faster spread and possibly a broader impact of spreading disinformation. The advancement in technology also brings up significant cybersecurity vulnerabilities, as the growing number of interconnected devices and innovative network topologies provide multiple opportunities for cyberattacks. To effectively handle these threats in the future, it is necessary to implement strong cybersecurity measures, such as improved encryption and more stringent security regulations. ENISA's interviews emphasized that this subject is considered more of an intersecting issue, addressed throughout the National Cyber Security Strategies (NCSS), rather than being a specific objective *per se* [14].

3 Conceptual Hybrid Threats Model

The Conceptual Hybrid Threats Model, as outlined in Section 3.1, examines the term cyber as a domain and as part of the framework of hybrid attacks. Hybrid threats are characterized by the use of various tools, such as disinformation campaigns and cyber operations, by a threat actor to target different domains, such as society, cyberspace, and the economy. These threats exploit weaknesses or flaws and maintain plausible deniability while achieving specific goals. Hybrid threats are often challenging to recognize, assign responsibility to, and fight back effectively. A hybrid threat is usually the result of multiple attack vectors. The cyber dimension holds significant importance, although not all attacks are hybrid in origin.

3.1 Exploring the Field of Hybrid Threat Modelling

The model designing phase starts with the collection and analysis of the business specifications necessary for the modeling, simulation, and optimization of business processes. The essential skills necessary for modeling are process design and handling changes [18]. Disinformation predates the rise of social networks, however, these platforms have significantly amplified its reach and speed of dissemination. Humans are inherently social creatures, frequently motivated by their emotions and the desire for acceptance and affection. The architecture of social media combines multiple dimensions. Many scientists assert that each instance of user engagement, such as liking, commenting, or other forms of interaction on social networks, triggers the brain's reward center, leading to a sense of satisfaction. All of this promotes greater sharing of content and

interaction. Business social network models rely on various functions, such as the ability to like posts and the element of surprise, to encourage maximum user engagement and maintain their attention. This attention is then monetized by selling it to advertisers. This business model prioritizes content that generates higher levels of engagement, a characteristic that misinformation often possesses. Recently, social networks have emerged as a primary platform for crisis communication during emergency situations [19]. The recent event of an earthquake in Slovakia confirmed this theory. The earthquake took place on 9th October 2023 and was felt throughout the entire eastern part of Slovakia [20]. The first source of information on this situation were social networks, primarily Facebook. In a matter of minutes, there were hundreds of posts and comments in various groups speculating on what caused the shaking. Nowadays, social media will be ahead of every other source of information. Social media platforms enable the rapid dissemination of information from authoritative sources as well as individuals directly impacted by an event. However, these benefits can quickly turn into drawbacks when they start to grow uncontrolled, disseminating misinformation and false data. The dissemination of information during crises and emergencies is accelerated and amplified due to the greater emotional intensity of the situation and the demand for accurate data. Although social media has allowed the sharing and rapid dissemination of misinformation, it is traditional media that primarily contribute to this issue. If individuals fail to perform their duties in a professional manner, which includes fact-checking and providing explanatory context, their actions equate to nothing more than sharing posts, often from politicians, on social media platforms.

Disinformation typically originates from small organizations who initially disseminate it within their exclusive circles or among groups of conspiracy-minded individuals. The initial significant achievement of disinformation and its creators occurs when they begin disseminating it on social media, particularly if they are able to seamlessly transition from one platform to another. If a group is acquired and featured by traditional media, it grants them exposure, credibility and introduces them to a wider audience, increasing their chances of achieving their objective. Challenging falsehoods and manipulations propagated by traditional media outlets can be a difficult challenge. The digital world is recognized as the fifth operational domain, in addition to land, sea, air, and space. The effectiveness of EU missions and operations now heavily relies on continuous access to a secure cyberspace. Therefore, it is essential to have powerful and durable cyber-operational capabilities [21]. The Conceptual Hybrid Threats Model (Figure 2) integrates both military and nonmilitary activities, adopting both conventional and unconventional methods and tactics. It is important to keep in mind that the new conceptual model, which is not organized in a hierarchy, includes the Disinformation Campaigns domain (highlighted in bold). This domain is connected to the Media Protection domain in the hierarchical model of the CMMC.

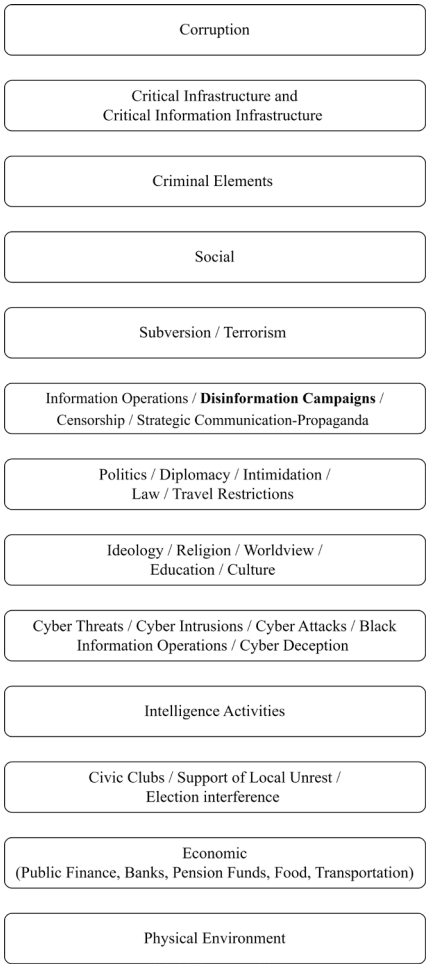

Figure 2
Conceptual Hybrid Threats Model

3.2 The Partnership between the European Union and NATO

According to Gartner in publication [22] stated that by 2023, 30% of chief information security officers' effectiveness will be evaluated through roˆle's capacity to generate value for the business. Also, Gartner identifies identity-first security as one of the top three priorities for CISOs (chief information security officers) in 2021. They also forecast that by 2023, 75% of security failures will be caused by insufficient management of identities as well as availability and rights. Recognizing the significance of the European Union's strategic duty to take action and its capacity to protect itself, it is crucial to acknowledge that in the current

highly unpredictable and unstable geopolitical environment, partnership between the EU and NATO is indispensable [23]. The security of the European Union (EU) and the North Atlantic Treaty Organization (NATO) is closely linked due to the fact that most EU Member States are also allies of NATO. Crucially, both international cooperation structures may combine a wide array of capabilities and resources to better address emerging challenges and provide mutual assistance. Therefore, the encouragement and support for open and organized collaboration between the two organizations, involving the exchange of information, synchronized planning and collaboration in the domains of hybrid threats, cyber security, defense, industry and research [23]. Member States of the EU may capitalize on EU-NATO cooperation to address cybersecurity supply chain risks. This cooperation involves ongoing collaboration on situational awareness and vulnerability disclosure, with the goal of enhancing the partnership between civilian and military activities. The aim is to maintain a strong cyber deterrence by continuously developing cyber defense capabilities and readiness for connected response in the event of a cybersecurity crisis. Additionally, this cooperation promotes responsible state behavior in the international context. Examining the EU's ability to withstand and recover from cyber security threats through the Strategic Compass also allows for an assessment of the effectiveness of existing strategic partnerships and their potential for future growth [23]. The EU has concentrated on the requirement for increasing its collective strength in the domain of cybersecurity. The primary focus is on the EU's capacity to promptly share information and maintain situational awareness in order to effectively address major cyber incidents and crises. This includes mitigating negative impacts across different sectors and incorporating a Mutual Assistance element. Additionally, it considers the EU's cyber resilience beyond its own boundaries. Furthermore, resilience primarily focuses on prevention and emphasizes various measures, including supply chain risk management, the cybersecurity diplomacy toolbox, civilian/military collaboration and the EU-NATO partnership.

4 Analysis of Demaskuok

This section focuses on the industrial solution for combatting disinformation in cyberspace, which is crucial for enhancing cyber resilience against hybrid attacks. Demaskuok, a Lithuanian term meaning "debunk," is an autonomous technology analysis center and non-governmental organization (NGO). Its primary objective is to investigate and counter misinformation in the public sphere while conducting educational programs to promote knowledge about the media.

As stated in [24], misinformation has emerged as a significant obstacle globally, affecting even the most influential nations and institutions, such as the United States, EU, and NATO. Misinformation additionally presents a challenge to our

strategic partners by presenting a deceptive alternative to truthful information across conventional and alternative media. The hesitant response to misinformation has already had a significant influence on the election outcomes of several nations, including the USA and the UK. It has resulted in substantial financial losses amounting to billions of euros and may have contributed to the creation of circumstances that generate a more widespread awareness of social chaos. In order to avoid the problem from becoming irreparable, the European Union has joined the battle against misinformation.

In the past, Lithuania has addressed these issues in a naive way, despite the fact that our nation is often targeted by misinformation using cyber methods and a constant stream of false information. These attacks include tens of thousands of deliberate assaults against the nation and its citizens throughout the course of the year. Disinformation generates ambiguity, fosters skepticism towards democratic institutions and the nation itself, and leads to adverse social, emotional, and economic outcomes. Therefore, in order to establish a proficient national and individual security system, it is essential to enhance coordination among the relevant competitors. Additionally, it is essential to establish a series of expeditious and effective activities and procedures. The prevalence of deception as a growing worldwide problem is generally recognized. Based on the 2018 statistics, a poll revealed that 85% of EU residents saw misinformation as a danger to democracy [24]. The magnitude of the problem becomes evident when considering the frequency of efforts to disseminate incorrect information. Disinformation encompasses any kind of incorrect or deceptive information that is deliberately created, produced, and disseminated with the goal of causing damage to the public or for personal advantage. These might range from inaccurate information to really destructive propaganda. Misinformation has the power to influence and mold public sentiment on certain matters via the use of written, visual, and auditory mediums that may be disseminated across several platforms. Disinformation tactics include several strategies, such as the dissemination of conspiracy theories, the creation of false information, the manipulation of public opinion, the use of sensationalized headlines to attract attention and other similar methods. Hostile actors use these strategies to influence and manipulate the facts.

As stated in the source [25], "Debunk EU" applies artificial intelligence to conduct extensive investigations on misinformation in the Baltic nations. Additionally, they collaborate on collaborative initiatives with their counterparts in the United Nations and North Macedonia.

Demaskuok [25] is a software program designed to identify the original sources of false information, often known as "patient zeros" of fake news. This software plays a crucial role in combating the spread of misinformation, as seen in Figure 3 [24]. The project was collaboratively produced by Delfi, a Lithuanian media company based in Vilnius, alongside with Google. Demaskuok identifies the suspects by analyzing their use of language that is reminiscent of themes widely exploited by propagandists. These themes include but are not limited to poverty,

destruction of the environment, war games, and societal divisions. Demaskuok does this analysis in Lithuanian, Russian, and English. The program also prioritizes the capacity of the provided language to elicit emotions, since it is evident that successful deception relies on this aspect. The program also distinguishes the thematic emphasis of the text. It is evident that news on weather or sports outcomes doesn't provoke the same emotional response in society as scandals or gossip. The crucial aspect is that the misinformation generated in this manner is designed to rapidly propagate and is anticipated to be widely disseminated, particularly via platforms such as social media.

Figure 3
Combating the dissemination of fake news

5 AI Implementation for Battling Misinformation

One of the nowadays trending AI technology can potentially improve battling misinformation campaigns. Some experiments in this field were already done. In 2023, Caramancion used ChatGPT 3.5 version to detect misinformation and fake news [26]. Since then, newer models have been released to the public like GPT-4. The GPT-4 model has also a potential for combating misinformation in various domains. Its uses natural language processing capabilities to process vast amounts of data, deciding between reliable and unreliable sources. In contrast to GPT-3.5 version, this model can also work with visuals or audio. The GPT-4 model can analyze context, detect inconsistencies, and cross-reference information to verify the accuracy of content [27]. In our experiment, we have used Fake News Prediction Dataset from author Rajat Kumar [28]. The datasets consists of 6335 records of fake and real news. Each record consists of 4 columns – ID, Title, Text, Label. In our experiment, we chose 863 random records from the given database. We have created a python script to append another column called "GPT4-output". This column as well as with "Label" can have only these two binary options: "FAKE" or "REAL". To fill our newly created column with a binary classification label we have used OpenAI API and GPT-4 model. In our API request, we have predefined a role for GPT-4 on how to behave and what to output. The prompt was: "I am going to give you a title and an abstract of an article. I want you to read it and output one of the two options: REAL if the article is real news or FAKE if the article is fake news." This prompt along with the specific title and text were packed into one command and send over to OpenAI.

The returned results were as expected. The model outputted “FAKE” or “REAL” according to its best judgment. The output value was stored in the newly prepared column “GPT4-output”. The parameters of the API command were set to values shown in Table 1.

Table 1
Command values

Parameter	Value
temperature	1
max_tokens	10
top_p	1
frequency_penalty	0
presence_penalty	0

After each successful execution of the command a timer of 30 seconds was set to wait before another command was sent. This was done due to “Rate limits” set by OpenAI. In this stage, we have compared values in rows “Label” and “GPT4-output”. We have used python library “sklearn.metrics” to calculate accuracy, precision, recall, F1-score and confusion matrix. The confusion matrix is presented in Figure 4.

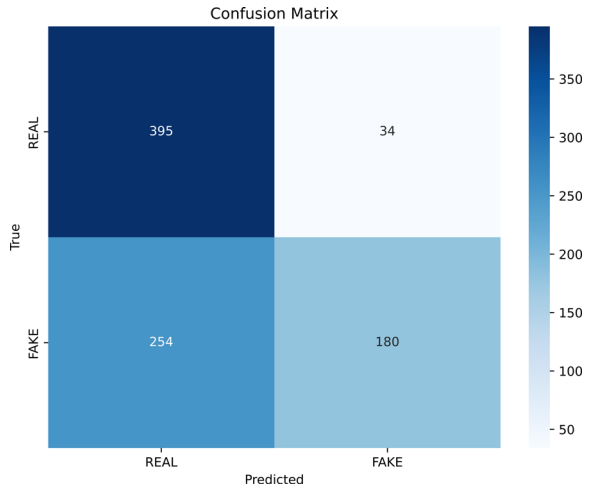

Figure 4
Confusion Matrix

The specific values of classification metrics are presented in Table 2.

In conclusion, the classification metrics achieved from our experiment reveal a surprising performance of the model. While achieving a moderate overall accuracy of 0.575, the precision score of 0.725 suggests a commendable ability to correctly identify positive instances. In the context of misinformation, minimizing

false positives is crucial to prevent the unnecessary labeling of legitimate information as fake news, which can have significant implications for freedom of speech. Therefore, a higher precision might ensure a more reliable identification of fake news.

Table 2
Achieved results

Accuracy	0.575
Precision	0.725
Recall	0.575
F1 Score	0.595

6 Future Research

The Croatian National Cybersecurity Strategy Action Plan was successfully implemented in 2020, leading to an enhanced level of security awareness at the national level [29]. Additionally, measures that were previously delayed in the implementation of the Action Plan from previous years were finally put into action. The significance of cybersecurity as an essential foundation for the digital revolution of society is now widely acknowledged, both in the public sector and among businesses and individuals. In the realm of cyber dangers, the perception is shifted from seeing them as uncommon occurrences to recognizing them as inevitable events that society must be ready for. The institutions that have a vested interest in the Strategy and are responsible for carrying out the measures included in the Action Plan are progressively engaging in collaboration and harmonizing their efforts. The plan, despite the many legal, budgetary, organizational, and personnel limitations and challenges, has been effective from its implementation till now. The implementation of new technology and the associated hazards, as well as the need to meet international alliances and obligations, make it crucial to have realistic and essential new requirements.

The current focus is on developing a new National Cyber Security Strategy to address future national demands. The first Strategy aimed to tackle priorities, but the new Strategy aims to establish additional organizational, legal, financial, and human prerequisites for a safe digital society in the future. On top of that, it is anticipated that there will be advancements in generative AI, resulting in the development of fresh models and approaches. Consequently, it is important to assess these advancements via new comparative studies. In addition, we are interested in doing research on combating not just textual disinformation, but also misinformation given via audio or visual means. We can expect a big increase in research in this field in the near future.

Conclusions

Misinformation has been around for a considerable period of time. They have existed from the dawn of humanity. The novelty is in the digital dissemination and rapid spread, the wide range of individuals involved in their creation and distribution, and the advanced tools used to produce and circulate misinformation to specific target audiences. Disinformation contaminates the information sphere, affects communication between people and democratic processes in society, and poses a risk to both health and human life, as has been especially apparent during the COVID-19 epidemic. From a social perspective, it is important to acknowledge that the pandemic not only influenced the digital realm and modern technology, but also had impacts on a person's health [30]. During high-intensity events like pandemics or earthquakes, if reliable information and guidelines are not provided promptly by relevant institutions through various platforms, it creates a fertile environment for the spread of false and intentionally modified publications. Disinformation expands most rapidly in the realm of political news and events, such as elections, as well as during exceptional situations, such as the COVID-19 pandemic or natural calamities like earthquakes. Failure of competent institutions to immediately respond and fully educate individuals in such circumstances creates opportunities for the unintended or deliberate propagation of speculation and fear, particularly via various communication channels, media, and social networks. Modern disinformation operations have the power to pose a threat to and disrupt social-technical systems. This study presents a conceptual model of hybrid threats in hybrid warfare, which involves the integration of many conventional and unconventional methods of fighting. Authors analyze the processes and methods used in misinformation campaigns, as well as strategies for identifying and recognizing the threats. Disinformation operations operate based on three fundamental principles: confidentiality, adaptability, and patience. Misinformation and fraud may be used to accomplish political objectives by disseminating offensive misinformation via local media, the Internet, and social networks with the involvement of government entities. Before engaging in open conflict, one might use covert tactics and exploit the weaknesses of the target system. Disinformation campaigns are used as a strategic approach to undermine the autonomy and autonomy of a system, without openly challenging its integrity. These efforts aim to weaken the target system by fostering internal conflicts and reducing its independence. Instead of making a quick and hasty endeavor to fully understand and control the system, it is better to take a calm and deliberate approach. In order to establish and sustain a safe society, it is important to consistently enhance public knowledge of cyber security and associated hazards via frequent and focused media efforts. It is important to focus on raising awareness among individuals responsible for handling personal data, such as controllers and executors, as well as implementing organizational and technical measures to prevent any harm or misuse of this data. This includes citizens of all ages, including young people and kids. Continuing to build and update systems for consistently notifying consumers and service providers in cyberspace about the

secure methods of use is essential. It is advisable to carry out customized advertisements using public media platforms for the broader population. Service providers must comply to the directions of regulators in their respective sectors and continue to do extra operations to ensure the sufficient protection toward both providers and their consumers. This study demonstrates the alignment of misinformation operations with the intentionally non-hierarchical Conceptual Hybrid Threats Model. Additionally, it highlights the tool Demaskuok as an effective means to combat disinformation. Furthermore, we have shown the successful use of generative AI in combating disinformation. Based on the provided trend, it can be concluded that AI models will exhibit even greater efficiency in the next few years.

Acknowledgement

This work was supported by KEGA project 030TUKE-4/2023 “Application of new principles in the education of IT specialists in the field of formal languages and compilers”, granted by the Cultural and Education Grant Agency of the Slovak Ministry of Education.

References

[1] M. McLuhan. The best of ideas. CBC Radio, Canada, 1967

[2] Noor, Noor Athirah Syazana Mat, and Salwa Abdul Patah. "The Evolution of Digital Era Did Impact the Intergenerational Communication in The Workplace." *Chapter in Book Compilation of Research Papers on Ssh (Social Sciences & Humanities)-October 2023*

[3] Matiaško, Karol, and Michal Kvet. "Medical data management." 2017 IEEE 14th International Scientific Conference on Informatics. IEEE, 2017

[4] Enli, Gunn, and Karin Fast. "Political solutions or user responsibilization? How politicians understand problems connected to digital overload." Convergence 29.3 (2023): 675-689

[5] Tayyab, Umm-e-Hani, et al. "A survey of the recent trends in deep learning based malware detection." Journal of Cybersecurity and Privacy 2.4 (2022): 800-829

[6] Szymoniak, Sabina. "Security protocols analysis including various time parameters." Mathematical Biosciences and Engineering 18.2 (2021): 1136-1153

[7] Djordje, Herceg, et al. "Possible improvements of modern dynamic geometry software." Компьютерные инструменты в образовании 2 (2019): 72-86

[8] Radaković, Davorka; and Steingartner, William "Common Errors in High School Novice Programming ", IPSI Transactions on Internet Research, Vol. 20(1), pp. 47-59, 2024, https://doi.org/10.58245/ipsi.tir.2401.05

[9] Ray, Partha Pratim. "ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope." Internet of Things and Cyber-Physical Systems (2023)

[10] R. Vasanth and S. Swamy. Social media's impact on teenagers. In P. L. P. Rau, editor, Cross-Cultural Design. Methods, Practice, and Case Studies. CCD 2013, Volume 8023 of Lecture Notes in Computer Science, Berlin, Heidelberg, 2013, Springer

[11] The European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework. https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework, 2020 [Online]

[12] Xishuo Zhang, Lin Liu, Yi Wang, Xiao Liu, Hailong Wang, Anqi Ren, and Chetan Arora. Personagen: A tool for generating personas from user feedback. In 2023 IEEE 31st International Requirements Engineering Conference (RE), pp. 353-354, 2023

[13] Kevin Matthe Caramancion. News verifiers showdown: A comparative performance evaluation of chatgpt 3.5, chatgpt 4.0, bing ai, and bard in news fact-checking, 2023

[14] R. S. Dewar et al. In R. S. Dewar, editor, National Cybersecurity and Cyberdefense Policy Snapshots: Collection 2, Series CSS Risk and Resilience Reports

[15] Kouroutakis, Antonios. "EU Action Plan Against Disinformation." The International Lawyer 53.2 (2020): 277-290

[16] European Commission. Policy and Legislation. Secure 5G deployment in the EU: Implementing the EU toolbox – Communication from the Commission. https://digital-strategy.ec.europa.eu/en/library/secure-5g-deployment-eu-implementing-eu-toolbox-communication- commission, 2020 [Online]

[17] da Ponte, Aureliano, Gonzalo Leon, and Isabel Alvarez. "Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach." Telecommunications Policy 47.1 (2023): 102459

[18] D. Galinec. Procurement Business Service Modeling in Service-Based Process Architecture of Equipping System. International Journal of Information Systems in the Service Sector (IJISSS), 1(4):50-60, 2009

[19] Abboodi, B.; Pileggi, S. F.; Bharathy, G. Social Networks in Crisis Management: A Literature Review to Address the Criticality of the Challenge. Encyclopedia 2023, 3, 1157-1177, https://doi.org/10.3390/encyclopedia3030084

[20] Staff, C. B. S. (2023, October 10) Earthquake shakes eastern Slovakia. spectator.sme.sk. https://spectator.sme.sk/c/23229570/earthquake-shakes-slovakia.html

[21] Council of the European Union. Eu cyber defense policy framework. https://www.consilium.europa.eu/media/37024/st14413-en18.pdf, 2018, [Online]

[22] C. Howard. Top Priorities for IT: Leadership Vision for 2021. Gartner, Inc., 2020

[23] The European External Action Service (EEAS) EU-NATO cooperation – Factsheets, https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheet_en, 2020 [Online]

[24] Debunk.eu. Debunking disinformation together. Power of Debunk. https://debunk.eu/about-debunk/ [Online]

[25] No author given. Lithuanians are using software to fight back against fake news. The Economist, https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news [Online]

[26] Caramancion, Kevin Matthe. "Harnessing the power of ChatGPT to decimate mis/disinformation: Using ChatGPT for fake news detection." 2023 IEEE World AI IoT Congress (AIIoT) IEEE, 2023

[27] Peng, Baolin, et al. "Instruction tuning with gpt-4." arXiv preprint arXiv:2304.03277 (2023)

[28] Rajat Kumar. Fake news dataset, 2023, https://www.kaggle.com/datasets/rajatkumar30/fake-news [Online]

[29] The Office of the National Security Council (UVNS), Republic of Croatia. Report on the implementation of the Action Plan for the Implementation of the National Cybersecurity Strategy 2020, 2020

[30] Long, Emily, et al. "COVID-19 pandemic and its impact on social relationships and health." J Epidemiol Community Health 76.2 (2022): 128-132