Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 291-296

Conceptual Convergence: Disinformation, Fake News, and Information Influence as a Triad of Security Threats in the Context of Society 5.0

Dimitrina Stefanova
Department "Public Relations"
South-West University "Neofit Rilski"
Blagoevgrad; Bulgaria
d.stefanova.swu@gmail.com

Kristiana Bacheva
Department of Library Science
University of Library Studies and Information Technologies, Sofia, Bulgaria
christiana.stefanova05@gmail.com

Valentin Vasilev
Head of "Center for Leadership and Public Policies"
Higher School of Security and economics
Plovdiv, Bulgaria
valentin.vasilev@vusi.bg

***Abstract*— The rapid advancement of technologies and the widespread application of communication tools significantly transform how individuals perceive and interact with information. Concurrently, the increasing volume of data and the sophistication of information technologies necessitate robust conceptual frameworks to ensure information security. This shift underscores the evolution of information into a critical and valuable resource, making it a prime target for influence in both business and societal contexts. Disinformation, fake news, and information influence have emerged as tools of interference, posing severe threats to modern societies. These phenomena can undermine democratic institutions and processes by obstructing individuals' ability to make informed decisions regarding their professional, social, and public lives. In recent decades, their role as threats has become integral to the evolving paradigm of security. In the dynamic context of the contemporary world, the traditional understanding of "security" has gradually expanded to encompass a broader, interdisciplinary approach. This new perspective incorporates economic, informational, environmental, social, and technological dimensions, redefining security as a complex phenomenon requiring adaptive and comprehensive solutions. The scientific and applied research into disinformation, fake news, and information influence, as subversive processes, is multifaceted and spans various disciplines. In the security domain, these phenomena are defined and analyzed within strategic and normative frameworks. This paper aims to conduct a documentary review and analysis of the conceptual apparatus employed in national strategic and normative documents through the method of content analysis. Focusing on their application to countering information threats, the study will interpret and evaluate these concepts. The proposed approach seeks to establish conceptual convergence and develop a sustainable framework to address these challenges effectively.**

Keywords –Disinformation, Fake News, Information Influence, Security.

I. INTRODUCTION

In the context of security, it can be observed that the current digital era is bringing about profound transformations across all areas of society.

The Fifth Industrial Revolution presents both challenges and opportunities, driven by the collaboration between humans and artificial intelligence, which is reshaping work, innovation, and daily life. However, without a global consensus on technology governance and best practices, risks such as data breaches, misinformation, mass surveillance, and personal data threats will persist. Additionally, unregulated advancements in automated and immersive technologies may introduce unforeseen risks.

Technological innovations, alongside political and social changes, create not only new opportunities but also significant risks. In addition to traditional threats, emerging hazards such as cyberterrorism, communication-based violence, disinformation, fake news, disruptions to critical infrastructure, manipulations via genetic engineering, and the effects of climate change are increasingly interwoven with conventional risks, evolving into hybrid crises. These processes stimulate debates within the public and business sectors, as well as among the media and civil society, because despite the many positive aspects, the information age introduces unique

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8470

threats that substantially impact the security of organizations and society as a whole.

The balance between innovation and regulation is crucial for ensuring information security and promoting progress. Establishing expert capacity to detect fake news, disinformation, and provocative content is an important task that requires an interdisciplinary approach. It is essential to develop policies for effective counteraction, considering that digital processes must be examined within two interconnected dimensions—technological and social. The way in which new technologies intertwine with social relations fundamentally transforms the models of interaction among actors and influences both systems and their defenses. This necessitates a cautious perspective on the exponential increase in the volume, speed, and quality of information, as well as the new requirements for securing the informational environment and its participants. Consequently, there is a pressing need to establish a national management system that protects not only the information and the informational environment but also the human factor within it.

II.MATERIALS AND METHODS

The methods employed in this study include theoretical analysis, deductive reasoning, and content analysis of literary sources and national-level strategic documents. In a comparative perspective, European policies and practices for combating deliberately manipulated information and its impact have also been examined.

III. RESULTS AND DISCUSSION

Information is now the most significant and contested geopolitical resource in the world. The most profitable businesses have long claimed that data is “the new oil.” Data and innovation not only transform economies and societies but also reshape international relations. The pursuit of informational power compels states to reconsider their interactions with markets and citizens by rewriting their national interests and strategic priorities. This fundamental transformation in the role and behavior of the state can have serious, even seismic, consequences. In particular, authoritarian regimes, recognizing the strategic importance of information, have, over the past five years, implemented powerful domestic and international informational strategies—isolating their information environments from global flows and using information as a tool for attacking and destabilizing democracies [1].

Defining the key concepts and principles is of paramount importance for the development of any scientific discipline and practice. The vision for converging the concepts of “disinformation,” “fake news,” and “information influence” involves extracting their common characteristics, as well as considering them in the context of ensuring security from the perspective of the state as a primary priority and obligation to protect its interests. This vision comprises three core components - security, influence, and information - with security playing a regulatory role over the latter two. Hundreds, if not more, of the current studies dedicated to “disinformation,” “fake news,” and “information influence” attest to the fact that these topics belong to a multidisciplinary field that combines scientific research and professional practice in developing and implementing countermeasures. The goal is to strike a balance between these elements in order to guarantee the planet's and humanity's long-term prosperity [2].

Among the unifying definitions, for instance, Wardle (2017) defines disinformation as “the deliberate creation and dissemination of false or misleading information with the intent to deceive or manipulate public opinion” The topics of mis-, mal- and disinformation are too important to start legislating and regulating around until we have a shared understanding of what we mean by these terms [3]. Disinformation refers to information that is deliberately false and is disseminated with the purpose of deceiving its audience, manipulating beliefs, and harming its target.

False and misleading information in its varying forms may lead to increasing misperceptions and knowledge resistance, which in turn pose significant threats to the health and well-being of individuals as well as organizations, countries, democratic deliberation and democracy per se [4]. Gelfert (2018) discusses disinformation in a similar context:” The term ‘disinformation’, more so than the relatively recent expression ‘fake news’, has by now received considerable attention from epistemologists and has been subjected to extensive conceptual analysis [5]. Fake news is best defined as the deliberate presentation of (typically) false or misleading claims as news, where the claims are misleading by design. The phrase “by design” is then explicated in terms of systemic features of the process of news production and dissemination.

All these definitions emphasize that disinformation constitutes deliberately crafted and disseminated false or misleading information, aimed at deceiving or manipulating the audience. The common elements are:

Intent: The information is produced with a pre-determined objective in mind.

Falsehood/Misleading Nature: The information is defined as false, untrue, or distorted in a manner that misleads the recipient.

Manipulation: The primary aim is to manipulate the beliefs, opinions, or actions of the audience, which may be pursued for political or financial purposes.

In related research, Tandoc Jr. et al. (2018) define fake news as “news content that mimics the format and style of legitimate journalism but is deliberately fabricated or manipulated, containing false information intended to mislead its audience” [6].

Petko Dimov and Elislav Ivanov argue that "fake news is a neologism, often used to refer to unwanted pseudo-news or propaganda aimed at deliberate disinformation or the generation of revenue through online advertising. The dissemination of fake news constitutes 'informational pollution,' which significantly intensifies during elections" [7].

These definitions underscore the intentional nature of both disinformation and fake news, highlighting their roles in purposefully deceiving and manipulating audiences, with fake news being viewed as one of the forms through which disinformation manifests in the media sphere.

Drawing on longstanding practices, the European Union, through its institutions, proactively develops policies, methodologies, analyses, and responses related to disinformation instruments aimed at the tactical and strategic manipulation of phenomena and processes associated with informational and national security. The European Parliament defines "fake news" and disinformation as information that is deliberately manipulated with the intent to deceive people, and which is emerging as an increasingly prominent global phenomenon [8].

At its level, The European External Action Service (EEAS), which is the EU's diplomatic service, defines a process of Foreign Information Manipulation and Interference (FIMI) - also often labeled as "disinformation" - is a growing political and security challenge for the European Union.

„Defining FIMI: The EEAS defines FIMI as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.

This first edition of the EEAS report on Foreign Information Manipulation and Interference (FIMI) threats is informed by the work of the European External Action Service's (EEAS) Stratcom division in 2022. Based on a first sample of specific FIMI cases, it outlines how building on shared taxonomies and standards can fuel our collective understanding of the threat and help inform appropriate countermeasures in the short to the long term" [9].

Definition of FIMI: The European External Action Service (EEAS) defines FIMI as a behavioral model that threatens or has the potential to negatively affect values, procedures, and political processes. Such activities are characterized by their manipulative nature and are carried out deliberately and in a coordinated manner. Participants in these activities may be state or non-state actors, including their proxies both within and outside their own territory.

Context and Need for a Comprehensive Counteraction Framework: In the context of informational attacks and the deliberate, coordinated activities of "manipulation and interference of foreign information" (FIMI) aimed at exerting a negative influence on political and social processes and values, a comprehensive counteraction framework is required. This framework should encompass rules, theories, methods, and practical implementation approaches. Within this semantic framework, disinformation, fake news, and information influence are not only seen as communication phenomena but also as serious threats to national and global security. Implementing such an approach necessitates integrated efforts at technological, legal, and social levels to ensure stability and protection in the digital age.

European Commission Report on Online Disinformation: The European Commission's first report, titled Tackling online disinformation: a European Approach (published in 2018), underscores the Commission's strong resolve to combat all forms of disinformation, which underpin various types of fake news. The report "Disinformation is understood as verifiably false or misleading information that is created, presented, and disseminated for the purpose of economic gain or deliberately to mislead the public, and that may cause public harm. Public harm includes threats to democratic political processes and policy-making, as well as to public goods such as the protection of the health of EU citizens, the environment, or security."

At the same time, large-scale online disinformation campaigns are widely employed by a range of local and foreign actors to sow distrust and generate social tension, with serious potential consequences for security. Furthermore, disinformation campaigns orchestrated by third countries can be part of hybrid threats to internal security, including during electoral processes, especially when combined with cyberattacks. Measures to protect citizens from the destructive effects of misinformation at the European level highlight the necessity for coordinated actions across multiple domains [10].

Overall, these definitions emphasize the deliberate dissemination of false information with the aim of manipulating and undermining democratic processes, by strategically using information as a tool of influence. It is also a key instrument in human capital management within organizations [11].

Disinformation is intentionally manipulated information that misleads the audience, often referred to as "fake news." It is considered a form of "informational pollution," which becomes particularly pronounced during elections. The European Union is actively developing policies and methodologies to address these phenomena, which pose challenges to societal security by manipulating information and interfering with political processes.

From a security perspective, the reviewed publications highlight several key aspects:

Deliberate Deception: Disinformation is characterized as deliberately created, manipulated, and disseminated information intended to deceive or manipulate public opinion, an occurrence often labeled as "fake news" or informational pollution, especially noticeable during elections.

Strategic and Tactical Information Influence: Information influence manifests through strategic and tactical processes that manipulate informational flows to alter political, social, and economic processes.

Threat to National and International Security: Both the European Parliament and the European External Action Service (EEAS) define these phenomena as tools for manipulating values, procedures, and political processes, posing a serious threat to both national and international security.

Objective of Manipulation: Disinformation and information influence are aimed at deliberately deceiving the audience by altering perceptions and behaviors in favor of specific political, economic, or ideological objectives.

Undermining Public Trust: Disinformation can erode trust in state institutions, the media, and the judicial system, leading to destabilization and vulnerability in national security, thus creating an environment conducive to both internal and external manipulations.

Role of Digital Platforms: European documents stress the significance of digital platforms and algorithms in disseminating disinformation. This highlights the necessity for enhanced cybersecurity measures, increased algorithmic transparency, and improved monitoring of online content to prevent the rapid spread of fake news.

Hybrid Warfare Instrument: Disinformation is regarded as an instrument in hybrid warfare, utilized to manipulate public opinion and destabilize political and social structures. Such multifaceted attacks present significant challenges to national security, as they are complex and difficult to localize.

It should be noted that "disinformation," in all its forms and modes of dissemination, is a transnational problem that necessitates a coordinated approach among states. Common strategies and the exchange of information are key to effectively protecting democratic institutions against manipulation.

In this context, a pertinent yet critical question arises: can individuals, groups, organizations, and/or societies fall into an "information catastrophe" due to informational pollution? Just like that, many global experts have reached the conclusion that if pollution continues at the same rate, in 30 years the oceans may contain more waste than living matter, an outcome tantamount to an ecological catastrophe [12].

As an EU member, Bulgaria has undertaken commitments related to international conventions and EU legislation, which form the foundation for the development of national security law. The present study examines the necessity of establishing expert capacity to ensure security against manipulative informational influence, with such capacity needing to be institutionalized within the country's strategic and regulatory documents. According to the Law on Strategic Planning of the Republic of Bulgaria, the National Strategic Framework represents an integrated system of strategic documents (e.g., the National Development Program, National Strategy, Roadmap, and Action Plan) that defines national priorities and the means to achieve them [13].

Within the scope of this study, a content analysis was conducted on two key strategic documents selected based on expert criteria. The defined units of analysis are the key concepts: disinformation, fake news, and information influence, including an in-depth qualitative analysis of their meanings and interrelationships in the context of hybrid actions.

The Updated National Security Strategy of the Republic of Bulgaria (2018) emphasizes the growing threats associated with hybrid actions, which include targeted manipulations by state and non-state actors, organized criminal groups, and terrorist organizations. Particular attention is given to the exploitation of cyberspace to propagate radical ideas, manipulate public opinion, and disseminate disinformation [14].

In the Updated National Cybersecurity Strategy "Cyber Resilient Bulgaria 2023," different levels of threat awareness are defined (ranging from "known-knowns" to "known-unknowns"), emphasizing the complexity of modern cyber threats, including disinformation campaigns [15]. The document outlines factual tools within a hybrid warfare model, which integrates both conventional and unconventional actions, including cyberattacks, psychological and economic influence, and disinformation campaigns, aimed at achieving political and strategic objectives. It recognizes the uniqueness of each hybrid strategy, highlighting the necessity for responses to be tailored to its specific characteristics. The strategy underscores the importance of engaging all relevant stakeholders—government, the private sector, education, NGOs, media, and civil society—to enhance cyber culture and effectively manage cyber risks. The forms and methods of human growth and self-expression are important. "Culture, unlike the unifying effect of globalization, differentiates different communities" [16].

The integration of expert capacity for countering manipulative informational influence into strategic documents is crucial for national security. The results of the content analysis of current national security and cybersecurity strategies indicate that information manipulation tools are incorporated rather peripherally and primarily in the context of hybrid threats.

CONCLUSIONS

With a growing awareness of sustainable The systematic definition of seemingly homogeneous concepts—disinformation, fake news, and informational influence as subversive processes—within strategic security documents would offer several key benefits for ensuring institutional, organizational, societal, and national security. „Disinformation, or fake news, consists of false or misleading information that is created, presented, and disseminated for political or economic gain or to deliberately deceive the public, causing social harm. Today, this phenomenon has a greater impact than ever, as it has become easier for anyone to publish and share news or information online. Social media and online platforms play a crucial role in accelerating the spread of such news, enabling a global reach with minimal effort from the author" [17].

Successfully addressing the challenges of technical and social interactions requires the establishment of clear procedures for early detection and counteraction against hybrid threats, including disinformation and cyberattacks. An integrated strategy necessitates multidimensional solutions, combining effective governance and social policies with technical measures, striking a balance between technological advancement and the stability of national communication and cybersecurity systems.

Ensuring security in Society 5.0 requires robust institutional mechanisms. Moreover, fostering multi-stakeholder cooperation, involving the public sector, private sector, and civil society, is crucial. Expanding the scope and developing the expertise of human resources is a strong aspect of combating these threats. This is particularly significant in terms of effective human resource management in a broader context [18]. Such a focus on human resource management would likely attract more potential employees to these organizations and be crucial for balanced career and personal development [19].

The fundamental transformations associated with manipulative informational influence necessitate unified efforts to protect interconnected technological and social systems. From a technological and cybersecurity perspective, these challenges appear more structured; however, in the context of social systems and communities, vulnerabilities in protection seem more pronounced. Information, humans, and technology form the cornerstone in the pursuit of communication security, understood as a complex system of interconnected elements aimed at reducing societal vulnerabilities [20].

The "human-centric" paradigm is oriented toward Society 5.0, a society that integrates digital, physical, and social spheres [21]. The sustainable development of Society 5.0 requires a holistic approach, combining innovative technological solutions, a strong strategic and regulatory framework, and robust cross-sector partnerships. In the sustainability journey that started with the 2030 SDGs, sustainability impacts have begun to emerge in every sector and in most social and economic areas of human life. [22].

Only through a balanced integration of the constituent constructs of information-communication interaction can we effectively protect the information space, minimize risks from negative informational influence, and maintain the stability of social and cyber systems.

REFERENCES

[1] E. Rosenbach and K. Mansted, The Geopolitics of Information, Defending Digital Democracy Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2019. [Online]. Available: https://www.belfercenter.org/publication/geopolitics-information. [Accessed: Feb. 14, 2025].

[2] R. Marinov, S. Stoykov, and P. Marinov, "Urbanized Territories Non-Existing Part of Crisis Response Operations," 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, Bulgaria, 2019, pp. 1-4, doi: 10.1109/CREBUS.2019.

[3] C. Wardle and H. Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking, Council of Europe, 2017. [Online]. Available: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c. [Accessed: Feb. 14, 2025].

[4] A. Krishna and T. L. Thompson, "Misinformation about Health: A Review of Health Communication and Misinformation Scholarship,"2021, American Behavioral Scientist, vol. 65, no. 2, pp. 316–332, 2021. doi: 10.1177/0002764219878223.

[5] A. Gelfert, "Fake News: A Definition," Informal Logic, vol. 38, no. 1, pp. 84–117, 2018. [Online]. Available: https://philpapers.org/rec/GELFNA. [Accessed: Feb. 1, 2025]. p. 15

[6] E. C. Tandoc Jr., Z. W. Lim, and R. Ling, "Defining 'Fake News': A Typology of Scholarly Definitions," Digital Journalism, vol. 6, pp. 137–153, 2017. doi: 10.1080/21670811.2017.1360143. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/21670811.2017.1360143. [Accessed: Feb. 9, 2025].

[7] P. Dimov and E. Ivanov, Fake News: Recognizing Fake News and Disinformation in the Modern Hybrid Security Environment, Sofia, 2020, p. 21. [Online]. Available: https://rndc.bg/wp-content/uploads/2020/05/FakeNews-21-05-2020-pechat.pdf. [Accessed: Feb. 1, 2025].

[8] European Parliament, "Tackling Disinformation," 2017. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_BG.pdf. [Accessed: Feb. 1, 2025].

[9] The European External Action Service, "Tackling Disinformation and Foreign Information Manipulation," 2024. [Online]. Available: https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en. [Accessed: Feb. 14, 2025].

[10] European Commission, Tackling Online Disinformation: A European Approach, 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236. [Accessed: Aug. 28, 2024].

[11] V. Vasilev, D. Stefanova, and C. Popescu, "Human Capital Management and Digitalization - From Good Practices and Traditions to Sustainable Development," in Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, 2023, pp. 41–65. doi: 10.1108/978-1-83753-190-520231004.

[12] N. Dolchinkov, "Construction of a System for Monitoring the Pollution of Water Bodies with Waste," ETR, vol. 1, pp. 136–141, Jun. 2024, doi: 10.17770/etr2024vol1.7989.

[13] Law on Strategic Planning of the Republic of Bulgaria. [Online]. Available: https://www.strategy.bg/FileHandler.ashx?fileId=16428. [Accessed: Aug. 28, 2024].

[14] The Updated National Security Strategy of the Republic of Bulgaria, 2018, pp. 7-8 [Online]. Available: https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf. [Accessed: Feb. 11, 2025].

[15] Updated National Cybersecurity Strategy "Cyber Resilient Bulgaria 2023." pp. 10, 13, 49, and 58 [Online]. Available: https://egov.government.bg/wps/portal/ministry-meu/strategies-policies/cybersecurity/cyber-legislation. [Accessed: Feb. 11, 2025].

[16] M. Modeva, The Non-Verbal Communication of the Political Leader, Sofia, 2022.

[17] K. Kazakov, "Fake News as a Tool for Manipulating Public Opinion," in Knowledge Society and 21st Century Humanism: The 19th International Scientific Conference, Sofia, Bulgaria,

Nov. 1, 2021, pp. 438–444. Sofia: Za Bukvite – O Pismeneh, 2021. ISSN 2683-0094.

[18] V. Vasilev, D. Stefanova, and M. Icheva, "Green Human Resource Management as a Component of Sustainable Organizational Development in Environmental and Natural Economics," ETR, vol. 1, pp. 402–407, Jun. 2024, doi: 10.17770/etr2024vol1.7966.

[19] R. Marinov, "Contemporary Challenges to the Protection of the Country's Sovereignty," ETR, vol. 4, pp. 168–172, Jun. 2024, doi: 10.17770/etr2024vol4.8187.

[20] D. Stefanova, "Security in Public Communications - Myth or Reality?," in Proceedings of the XXV Summer School in Public Relations, 2023, pp. 160–171. Sofia: NBU, 2023. ISBN 978-619-233-278-5.

[21] D. P. Stefanova, V. P. Vasilev, and I. P. Efremovski, "Re-Innovative Organizational Design: Sustainable Branding and Effective Communication - Applied Models in a World With New Borders/Without Borders," in Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, pp. 112–127, 2023. doi: 10.4018/978-1-6684-8681-8.ch006. Available: https://www.igi-global.com/gateway/chapter/325452#pnlRecommendationForm. [Accessed: Feb. 11, 2025].

[22] S. Yıldırım and V. Vasilev, "The Future of Green Collar Workers: Green Transition in Employment," in Green Transition Impacts on the Economy, Society, and Environment, S. Yıldırım, D. Yıldırım, I. Demirtaş, and V. Kandpal, Eds. IGI Global Scientific Publishing, 2024, pp. 1-16. doi: 10.4018/979-8-3693-3985-5.ch001.