DOI: https://doi.org/10.52651/vr.a.2025.3.57-69

VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 57-69

# EMERGING AND DISRUPTIVE TECHNOLOGIES AND DISINFORMATION IN UN PEACEKEEPING MISSIONS

**Elisabeta-Emilia HALMAGHI, Alin CÎRDEI, Ileana-Gentilia METEA, Daniela CĂRUȚAȘU**

ARTICLE HISTORY

Submitted: *05.11.2025*
Accepted: *27.11.2025*
Published: *31.12.2025*

**ABSTRACT**

*Emerging and disruptive technologies are increasingly present in our lives, determining the increase in people's living standards and the progress of society. The influence of this type of technologies is present in both the civilian and military environments. In the military environment, by transforming into capabilities, the impact will be significant on defense institutions, but also on classic security strategies, military doctrines, operational concepts, wars. In this paper, using the bibliographical and analytical method, it will be highlighted how emerging and disruptive technologies can be used by hostile forces to increase disinformation and uncertainty in conflict areas where peacekeeping missions are carried out under the auspices of the UN. Personnel participating in UN missions must identify the signs of a disinformation campaign as early as possible and have the necessary knowledge to combat it.*

**KEYWORDS**

*disinformation; disruptive technologies; emerging technologies; false information; peacekeeping missions; UN.*



## INTRODUCTION

In an era where information circulates extremely quickly thanks to the online environment, a new major challenge has emerged: disinformation. This challenge manifests itself at all levels, in all areas, and contributes to the manipulation of people. Disinformation spreads rapidly online, but also offline and in the media.

Emerging and disruptive technologies are changing the way the world works. In their use, emerging and disruptive technologies present both advantages and disadvantages and "will have a major impact, with specific effects and risks related to the new products and services that could emerge and disrupt markets, as well as how businesses will be adapted, transformed and run in accordance with the new business model" (Coman et al., 2024).

The paper aims to present the role that emerging and disruptive technologies play in the propagation of disinformation in UN peacekeeping missions.

To achieve the objective, we presented and analyzed, based on the study of the bibliography and our own observations, the importance of emerging and disruptive technologies in military activities and their role in the propagation of disinformation during the conduct of UN peacekeeping missions.

## 1 EMERGING AND DISRUPTIVE TECHNOLOGIES – TECHNOLOGIES THAT INCREASE THE RESILIENCE OF PEACEKEEPING OPERATIONS

Among the first researchers to note the disruptive nature of technological change was Joseph Schumpeter. He noted in 1939 that this disruptive nature of technological change could lead to waves of "creative destruction" (Chandra Shekar, Anjali, Pavithra, 2017). Many of the technologies that define the modern era (computers, nuclear power, space-based ICT systems and GPS, etc.) emerged as a direct result of public investment driven by geopolitical competition and the dynamics of the arms race between the US and its allies, and the Soviet Union, during the Cold War. The most striking difference in the nature of research and development in science and technology was represented by the increased volume of private investment in so-called "dual-use technologies", usually reserved for civilian purposes but with notable military applications (Vincić, 2021).

Currently, emerging and disruptive technologies (EDT) are increasingly part of our lives, changing the way the world works and "driving societal progress and increasing the standard of living of the individual" (Popescu, 2021, p. 221). These technologies, which come with both opportunities and challenges, are expected to reach maturity in the next 20 years (Popescu, 2021, p. 2019). and have an increasing impact on security and the armed forces. They allow the armed forces to "become more effective, resilient, cost-efficient and sustainable as well as address immediate capability shortfalls and deliver on their capability targets" (NATO, 2025) changing the nature of war (Mills, 2023, p. 4). Beyond the positive impact, EDT present "a huge threat to society, both civil and military, from their misuse" (The Geostrata, 2024).

Emerging technologies are considered to be those technologies that require longer time horizons (between 10 and 20 years) to mature and whose development trajectories are currently less certain (Vincić, 2021).

Disruptive military technology represents "an improved or completely new technology capable of producing fundamental changes to traditional models of security and defense" (Iancu, 2019) and is in a more advanced state of technological maturity already having/expected to have significant and potentially revolutionary impacts on the nature of warfare and collective defense and security in the period 2020-2040 (Vincić, 2021).

These technologies, by transforming into military capabilities, will have an impact on classic security strategies, military doctrines, operational concepts, wars, but also on the organization of defense institutions.

Like any product, disruptive technologies have four life phases (Figure 1).

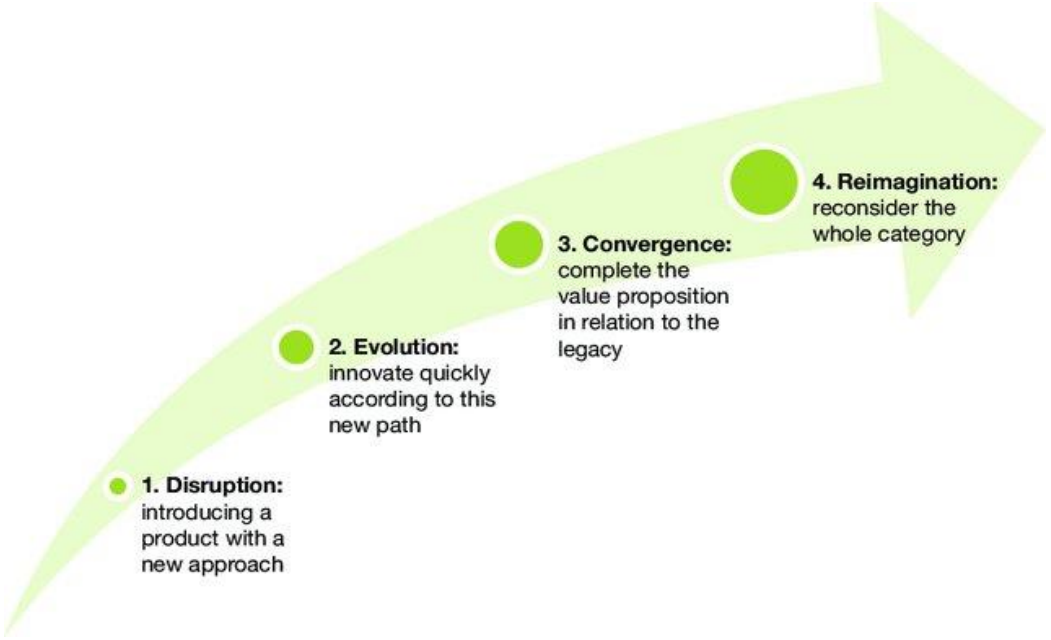


Figure 1 Phases of disruptive technologies
*Source: Veuger, 2018*

The phases of disruptive technologies are presented in Tab. 1, where column 2 lists the characteristics of the disruptor evolving from a niche solution to an asset used in both civilian and military environments, and column 3 lists the prototype result.

Table 1 Phases of disruptive technologies

| Phase | Disruptor | Incumbent / Prototype |
|---|---|---|
| Disruption of the established order | Introduce a new product with a well-defined approach, recognizing that it may not meet all the needs of the entire existing market, but it improves on state-of-the-art technology. | The new product/service is not relevant to existing customers or the market (also known as "denial") |
| Rapid linear evolution | Adds features and capabilities, increasing value based on feedback from a group of early adopters. | Compares the complete product with its own new product and identifies defects (also known as "validating") |
| Convergence. Completely reinvented product | Sees an opportunity to broaden the customer base by attracting new companies. Recognizes the limitations of its | Disruptive core features are added to the existing product line to demonstrate attention to future trends while minimizing disruption |

| Phase | Disruptor | Incumbent / Prototype |
|---|---|---|
| | new product and learns from previous practices, but applies them in a new way.<br>Potential risks are continuously addressed with new technologies and business models, and the focus shifts to the "installed base" of the already existing order. | to existing customers (also known as "competition").<br>A potential risk is that disruptive products are not recognized as truly valuable or do not offer opportunities relative to the limitations of existing products. |
| Completely reinvented product | Approaching a decision point because new entrants to the market can benefit from everything the new product has demonstrated, without considering existing customers.<br>Focusing more on market legacy or continuing the path already taken. | It is too late to react.<br>Begins defining the new product as part of a new market and the existing product as part of a larger, existing market (also known as "retraction"). |

*Source: Processing after Veuger, 2018*

Emerging and disruptive military technologies are: artificial intelligence (AI), hypersonic systems, autonomous systems, biotechnologies and human enhancement technologies, quantum technologies, space, next-generation communication networks, energy and propulsion, new materials and their production (NATO, 2025).

Artificial intelligence is a catalyst for the development of emerging and disruptive technologies and a basic element in the implementation of other technologies in the military field, because systems equipped with artificial intelligence will be able to perform analyses, identify threats, solutions and courses of action, assist decision-making or even make decisions independently, thus optimizing other systems and acting as an amplifier of human strength and intelligence (Cîrdei, 2025).

Technologies are developing at a dizzying pace, and their impact on all areas is unimaginable. Artificial intelligence is an engine of development of all other areas and is driving the development of new emerging and disruptive technologies. Moreover, artificial intelligence will allow for the achievement of quantum supremacy, thus creating the conditions for tasks and activities that normally take a long time to be completed in a few seconds. The fundamental question that arises here is if and when this technology will become widely accessible, because then every terrorist, insurgent or other entity or organization will have access to almost unlimited computing power.

When quantum power is widely available, its impact on military operations will be immense. Taking advantage of this emerging technology, the speed, scale, and quality of disinformation campaigns will be so great that it will be almost impossible to identify and very difficult to combat, because it will be a significant challenge to distinguish between real and simulated actions, between those specific to current activities and legitimate military operations and those that support disinformation actions.

These technologies are fundamentally changing the missions of the United Nations (UN) to maintain peace. In general, UN peacekeeping missions aim to assist states in the transition from conflict to peace. In carrying out peacekeeping missions, the UN has "unique strengths, including legitimacy, burden-sharing, and the ability to deploy troops and police from around the world, integrating them with civilian peacekeeping forces to fulfill a range of mandates set by the UN Security Council and the General Assembly" (United Nations Peacekeeping, 2025c).

If the Action for Peacekeeping Initiative aimed to strengthen, secure and make UN missions more effective, A4P+ aims to accelerate its implementation (Figure 2). To this end, "concrete measures have been adopted across all areas of A4P+, from improving the safety, security and well-being of our personnel to increasing the participation and expanding the role of women in our missions" (United Nations Peacekeeping, 2025a).

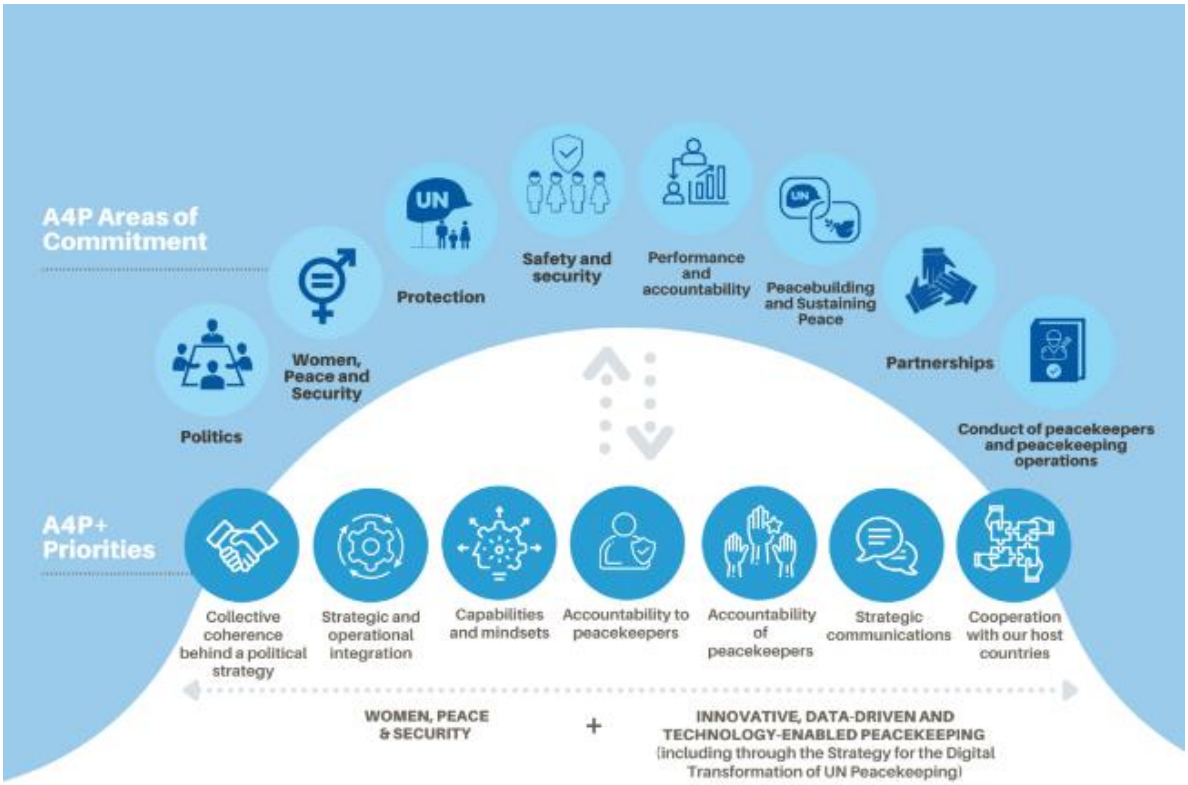


Figure 2 Action for Peacekeeping and Action for Peacekeeping+
*Source: United Nations Peacekeeping, 2025c*

It should also be borne in mind that threats to peacekeeping personnel do not only come from the physical environment and do not only endanger the physical safety of the personnel. In the age of technology and the Internet, military and civilian personnel participating in peacekeeping operations are faced with risks arising from the cyber environment that can have faster and more intense effects than actions carried out in the physical environment, even using military means.

Cyber threats and those specific to information warfare are, most of the time, invisible and therefore difficult to counter, especially due to the fact that the target would be aware that it is subject to an attack only after the attack is underway or even after it has been completed. Thus, the attention of decision-makers and peacekeeping personnel will not be focused on preventing attacks, but on countering them and limiting their effects and damage.

That is why personnel participating in peacekeeping missions must have training in cyber and information operations in order to be aware of the danger they represent, the damage they can cause and the indications of such hostile actions in order to be able to counter them. While cyber threats and information operations are not new in the military field, we can observe that new confrontations are taking on a hybrid character, because the environments of confrontation, the methods of conducting military actions and their targets are increasingly diverse, and their countering is increasingly difficult.

Hybrid threats are becoming a constant of current activities and especially of the actions of the armed forces that must get used to operating in such conditions, marked by uncertainty, volatility, unpredictability and multidimensional and multidomain risk. Hybrid threats are a significant concern today due to their ability to exploit vulnerabilities in interconnected, open societies, using a combination of conventional and unconventional tactics. These threats are increasingly visible in all domains and are predominantly manifested in parallel with classical military or peacekeeping actions, with the aim of creating insecurity, distrust and suspicion.

Technology and connectivity have significantly amplified the scope and impact of hybrid threats on armed forces and their ability to conduct military actions. The ability to disseminate disinformation on a large scale, to conduct sophisticated cyber-attacks, to exploit global interdependencies and to coordinate operations in real time are key factors that make hybrid threats particularly challenging in the modern era.

The UN is currently involved in 11 peacekeeping operations led by the Department of Peacekeeping Operations. These are mainly conducted on the African continent in Western Sahara, Congo, Central African Republic, Abyei, and South Sudan. Other areas where peacekeeping operations are conducted include: Kosovo, Cyprus, Lebanon, Golan, Middle East, on the border between India and Pakistan. As of 31 July 2025, 68,255 personnel were involved in the 11 peacekeeping operations (United Nations Peacekeeping, 2025b).

The nature of contemporary conflicts has evolved, requiring continuous adaptation of peacekeeping operations. Despite the fact that this adaptation is in continuous dynamics, UN peacekeeping missions are affected by disinformation.

UN-led missions, regardless of the geographical area in which they are deployed, are exposed to hybrid threats and disinformation actions that are directly directed against the mission and participating personnel, but which also indirectly affect the efficiency and legitimacy of UN forces by targeting the local population, political decision-makers and international public opinion, through coordinated and well-planned actions, which aim to achieve short- and medium-term effects. The initiators of disinformation actions use the advantages offered by modern technologies, especially artificial intelligence, to prepare and carry out real disinformation campaigns, with minimal effort and maximum potential benefits.

## 2 DISINFORMATION IN UN PEACEKEEPING MISSIONS

Disinformation is not a new phenomenon, but given the dynamics in the communications area and the continuous development of digital platforms, the large-scale use of AI (voice and facial recognition systems, image analysis software, virtual assistants, etc.), the scale of the problem is amplified, which makes it even more difficult to trust information and to present real facts in conflict situations.

What is new is that digital technology has allowed the creation, dissemination and amplification of false or manipulated information by various actors, for ideological, political and/or commercial reasons, at a scale, speed and coverage never seen before. Interacting with real-world political, social and economic grievances, disinformation can have serious consequences for democracy because it distorts public debate, polarises society and prevents people from making informed choices, free from interference and manipulation (European Parliament, 2025), incites hatred, discrimination and violence, prevents people from meaningfully exercising their rights and destroys their trust in governments and institutions (United Nations 2021).

Disinformation (false information that is deliberately created to cause harm to an individual, social group, organization, or country), misinformation (false information that appears in the public domain without the intention of causing harm by the people spreading it), and malinformation (fact-based information used to cause harm to an individual, social group, organization, or country) (United Nations 2023) have become a serious threat, both to members of society and to institutions. The boundary between the three is volatile (Figure 3), and what began as disinformation tends to turn into misinformation as it spreads, since most people do not share false information with malicious intent.

There is an important difference between fake news and disinformation (Tătaru et al., 2024), as false information can blur into disinformation when seemingly true information is lacking nuance or context (Trithart, 2022).

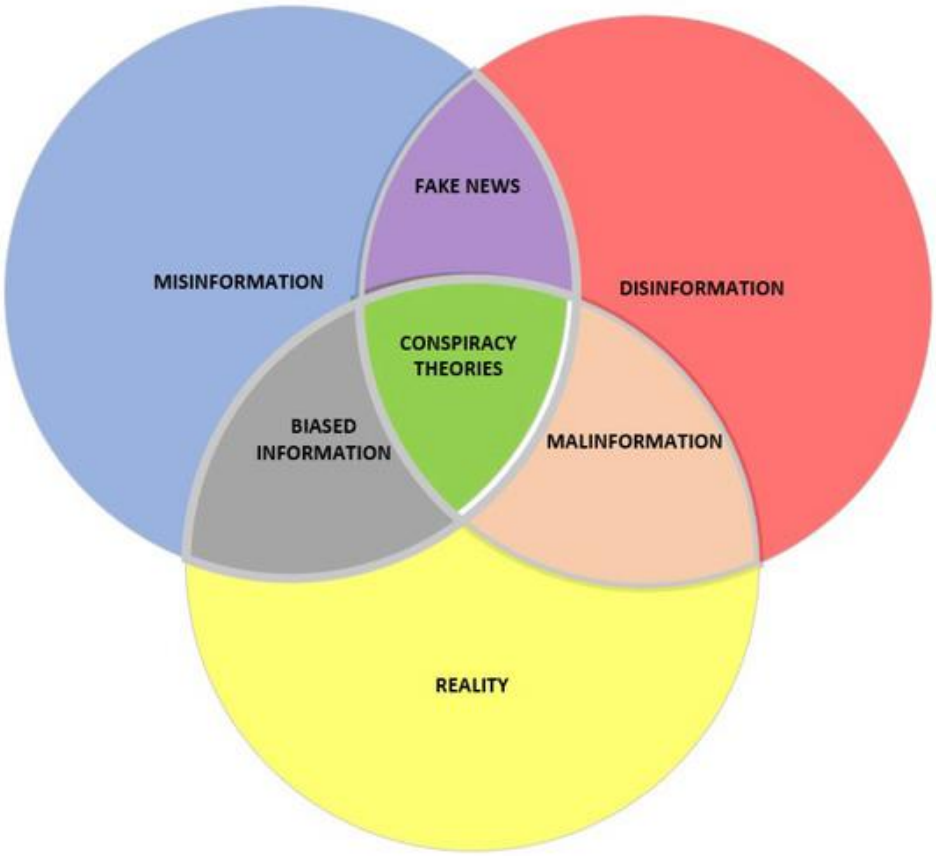


Figure 3 The Disinformation – Misinformation - Malinformation Connection
*Source: Tătaru et al., 2024*

In the case of UN peacekeeping operations, the increase in disinformation can undermine trust in peacekeeping missions, exacerbate conflicts and encourage violence against UN personnel, limit the mobility and expansion of peacekeeping missions, compromising the protection of civilians. The number of disinformation has increased in recent years and includes (also false) accusations that UN peacekeepers support terrorist groups, traffic in arms and/or human beings, or exploit natural resources. Disinformation about the work of UN peacekeepers is not new, but in recent years, thanks to social media, it has spread at an accelerated pace. Based on public frustration, but also on real cases of mistakes or misconduct by UN peacekeepers, anti-UN disinformation makes it difficult to implement the mandates of peacekeeping operations and endangers the safety of peacekeepers (Trithart, 2022).

For example, in early 2025, M23, with the support of Rwandan armed forces, launched large-scale offensive operations in eastern Democratic Republic of Congo. During the offensive, women peacekeepers were threatened with rape and other acts of sexual violence, following an online disinformation campaign, which affected their safety and freedom of movement. This made it difficult to restore security to Congolese communities.

Disinformation is a consequence of the use of advanced technologies aimed at resisting, hindering, slowing down and annihilating UN missions considered beneficial in their areas of operation, but which contradict opposing interests. Mobile phones used as explosive devices, unmanned combat aircraft or cyber-attacks are realistic attack scenarios that are becoming increasingly relevant with digitalization. The figures and challenges show that the UN must not only promote peace and security, but also protect its personnel from threats (Parlamentul European, 2022).

However, there are also logistical issues, as access to modern technology is limited in some conflict zones. Furthermore, overuse of technologies can lead to dependency, which can jeopardize mission success if systems fail.

UN personnel engaged in peacekeeping missions can mitigate the effects of disinformation in the following ways (Stockholm International Peace Research Institute, 2023):

a) Understand and address the roles of different actors when it comes to the spread of mis- and disinformation. There are situations where government officials or civil society representatives challenge the legitimacy and implementation of the mandate of UN operations. In this case, it is necessary for the UN Security Council to provide more guidance and political support to the peacekeeping mission.
b) Recognize that multiple narratives may exist within a country and analyse who owns them. Understanding local culture and history, the causes of conflicts, provides a holistic perspective on the conflict. To better understand the context, it must be borne in mind that in any society there are multiple voices that influence a country politically, economically and socially: the host government, local communities, diaspora. Therefore, it is necessary for UN members to be aware of the sources of information and their potential biases.
c) Analysis of the root causes of a shifting media landscape. Modern conflicts are characterized by a dynamic media environment. Therefore, for propaganda purposes and the dissemination of contradictory information, governments, local communities, and the diaspora fund media institutions.
d) Keep investing in mission-wide communication strategies. Providing information in the media about the mission's role and purpose can help counter fake news and disinformation campaigns. Strategic communication is also essential, and therefore training senior mission leaders in communication and media is an asset.

e) Whole of mission approach. A proactive approach is needed, where the risk of disinformation is considered for the "whole mission". Therefore, for the safety of personnel and to support the implementation of the peacekeeping operation, disinformation should be part of the planning and decision-making process.
f) UN peace operations are complex and large, involving actors with different social, language and cultural settings. The cultural, social and linguistic gap between peacekeeping personnel and members of local communities leads to increased distrust among the indigenous population, undermines the legitimacy of the mission and increases disinformation. By improving linguistic, cultural and social understanding, better conditions for dialogue arise, which leads to transparency, reduces disinformation and increases the trust of local community members in the role of the peacekeeping mission.
g) Keep in mind that criticism of the UN is not always mis- or disinformation. Engaging in dialogue with local community members is essential for the successful implementation of peacekeeping missions. This requires that the information transmitted by UN personnel is accurate, impartial and accessible to communities. That is why it is important to support the rule of law in host countries, train journalists, support independent media and civil society organizations.

Disinformation and propaganda actions take place over time and target both the forces participating in peacekeeping operations, the population and decision-makers. The first step is to create a favorable climate for these actions to be carried out successfully. After the framework is created and a core of supporters and sympathizers is formed, from among the population or even influential people from different fields and political decision-makers, the actual action begins, exploiting the weaknesses of the system and attacking the essential points of the peacekeeping forces.

Once the action is launched, by using means of influence, propaganda and disinformation, misleading, etc., the attackers focus their efforts on achieving the objectives and achieving the desired end state, affecting the ability of the peacekeeping forces to fulfill their mission and affecting the image and respect they enjoy locally and among the international community.

## CONCLUSION

The weaponization of digital communications and social media poses new challenges in identifying and countering hostile influences that negatively impact UN peacekeeping operations. Today's peacekeepers not only face disinformation in their operational contexts, but are increasingly becoming targets of disinformation campaigns. Such campaigns are often designed to erode trust in peacekeeping operations, delegitimize international interventions, and deepen divisions in conflict regions.

By jeopardizing the safety and security of UN peacekeepers, disinformation, along with hate speech, limits the mobility and reach of peacekeeping operations, thereby reducing the operations' ability to protect civilians in the host country.

In the case of conflicts in fragile democracies through disinformation, social media can decisively influence how, when and if a conflict manifests. The spread of false information online and in the media with the intention of misleading the public poses increased risks to the well-being of people and society in general. Disinformation polarizes society, jeopardizes the implementation of economic and social policies, and undermines trust in state institutions and democracy.

To combat disinformation, it is necessary for people to develop critical thinking skills and be digitally literate. Through the two components, they will be able to identify and combat the spread of false and/or misleading information. However, the use of social media and AI as a weapon remains a challenge for future work in the field of peace and security.

**REFERENCES**

CÎRDEI, A. 2025. Folosirea inteligenței artificiale în operațiile militare. In: CÎRDEI, A., BOJOR, L. *Impactul tehnologiilor emergente asupra securității naționale*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2025.

COMAN, M.-M. - KIFOR, C.V. - PIELE, C. 2024. Exploring the Impact of Emerging and Disruptive Technologies Development on Evolution of Industry 5.0. In: *International conference KNOWLEDGE-BASED ORGANIZATION. Nicolae Balcescu Land Forces Academy*, 2024, Vol. 30, No. 3. 49-57. Available at: https://doi.org/10.2478/kbo-2024-0084

European Parliament. 2025. Disinformation: 10 steps to protect yourself and others, Published: 05-06-2025. Available at: https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others

CHANDRA SHEKAR, N. - ANJALI, K. - PAVITHRA, A. 2017. Disruptive Technologies. In: *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, 2017, Vol. 4, No. 3. 81-83. ISSN (Online) 2394-2320. Available at: https://www.technoarete.org/common_abstract/pdf/IJERCSE/v4/i3/Ext_23047.pdf

IANCU, N. 2019. Noul dicţionar al apărării: tehnologiile disruptive, 29 iulie 2019. In: Monitorul Apărării și al Securității. Available at: https://monitorulapararii.ro/noul-dictionar-al-apararii-tehnologiile-disruptive-1-21024

MILLS, C. 2023. Emerging and disruptive defence technologies. Commons Library Research Briefing, 13 November, 2023, House of Commons Library. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9184/

NATO, 2025. Emerging and disruptive technologies. Last updated: 25 Jun. 2025. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm

Parlamentul European. 2022. Securitate cibernetică, principalele amenințări. 2022. Available at: https://www.europarl.europa.eu/topics/ro/article/20220120STO21428/securitate-cibernetica-principalele-amenintari

POPESCU, S. 2021. Impactul tehnologiilor emergente și disruptive asupra domeniului militar. In: Conferința Științifică Internațională Gândirea Militară Românească, Ediția a III-a, 2021. Available at: https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2021%20gmr/2021/4%20proceedings%202021/POPESCU.pdf. https://doi.org/10.55535/GMR.2021.4.12

Stockholm International Peace Research Institute. 2023. Tackling mis- and disinformation: Seven insights for UN peace operations. 2023. Available at: https://www.sipri.org/commentary/blog/2023/tackling-mis-and-disinformation-seven-insights-un-peace-operations

TĂTARU, G.-C. - DOMENTEANU, A. - DELCEA, C. - FLORESCU, M. S. - ORZAN, M. - COTFAS, L.-A. 2024. Navigating the Disinformation Maze: A Bibliometric Analysis of Scholarly Efforts. In: *Information*, 2024, Vol. *15*, No. 12. 742. Available at: https://doi.org/10.3390/info15120742

The Geostrata, 2024. Emerging and Disruptive Technologies in Defence, Feb 27, 2024. Available at: https://www.thegeostrata.com/post/emerging-and-disruptive-technologies-in-defence

TRITHART, A. 2022. Disinformation against UN Peacekeeping Operations. International Peace Institute, November 2022. Available at: https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf

United Nations Peacekeeping. 2025a. Actions for Peacekeeping+. Available at: https://peacekeeping.un.org/en/action-peacekeeping

United Nations Peacekeeping. 2025b. Data. Available at: https://peacekeeping.un.org/en/data].

United Nations Peacekeeping. 2025c. What Peacekeeping Does. Available at: https://peacekeeping.un.org/en

United Nations. General Assembly. 2021. *Disinformation and freedom of opinion and expression* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan. 2021. Available at: https://docs.un.org/en/A/HRC/47/25

United Nations. General Assembly. 2023. *Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training.* 2023. Available at: https://webarchive.unesco.org/web/20230926213448/https://en.unesco.org/fightfakenews

VEUGER, J. 2018. Trust in a viable real estate economy with disruption and blockchain. In: *Facilities*, 2018, Vol. 36, No. 1-2. 103-120. Available at: https://doi.org/10.1108/F-11-2017-0106

VINCIĆ, N. 2021. *The Future of Warfare: Security Implications of Emerging and Disruptive Technologies (EDTs),* 2021. Available at: https://natoassociation.ca/the-future-of-warfare-security-implications-of-emerging-and-disruptive-technologies-edts/

Assist.prof. Elisabeta-Emilia HALMAGHI, PhD
Faculty of Military Management, "Nicolae Bălcescu" Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
emmahalmaghi@gmail.com

LTC Assoc.prof. Alin CÎRDEI, PhD
Faculty of Military Sciences, "Nicolae Bălcescu" Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
cirdei_alin@yahoo.com

Assist.prof. Ileana-Gentilia METEA, PhD
Faculty of Military Sciences, "Nicolae Bălcescu" Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
meteaileana@yahoo.de

COL.eng. Daniela CĂRUȚAȘU, PhD
"Nicolae Bălcescu" Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
d.carutasu@yahoo.com