# *FAKE NEWS* AS A FORM OF HYBRID AGGRESSION IN THE MILITARY ENVIRONMENT

*Colonel Professor Adrian LESENCIUC, PhD*
*"Henri Coandă" Air Force Academy, Brașov*

*The concept of **fake news**, which has been recently included in the literature – although it had an important history before being acknowledged as such, the term designating the rumours and gossip associated with media personalities in **late night shows** –, has already enjoyed constant attention, its meaning being associated with terms such as disinformation, propaganda or even deception (military deception). In relation to the latter concept, which is perceived as an umbrella term covering both denial and deception, well-known authors in the field of information operations consider denial and deception as military actions/ operations per se: "denial hides the real and deception shows the fake", while propaganda and disinformation are products (Johnson & Meyeraan, 2003, p. 4).*

*Therefore, it is natural to start placing the concept in the doctrinal apparatus in relation to the projection of information operations in the category of operations dubbed Military Deception (MILDEC), Cyber Network Operations (CNO) and Psychological Operations (PSYOPS), as long as they operate with fake technology & weapons, fake retreats or other actions, fake information. Therefore, **fake news** should be understood as neither fully **fake** nor fully **news**, but insertions with an intentional informative role, which "incorporate, melt halves, if not quarters of truth and false, plausible and invented etc.":*

> *Under the umbrella of the phenomenon of "digital disinformation" or "disinformation 2.0" comes the mixture, in different doses, between true information (which can be verified) and false one.*

*The finer the dosage is, the less noticeable the false dose could be, thus being more difficult to realise the fact that we are dealing with disinformation (Bârgăoanu, 2018, p. 138).*

*In the new **National Defence Strategy of the Country for the period 2020-2024**, the concept of fake news is included in the category of "subtle and subversive" hostile actions defined as hybrid threats, to which the strategy attaches great importance in relation to a number of indicators of the concept of regional security evolution, including the aggressive behaviour of the Russian Federation[1], the possibility of adapting hybrid actions to technological developments and the increase in the complexity of risks, considering the new technologies for civil use employed in asymmetric and hybrid actions, the development of a series of measures and actions meant to contribute to enhancing societal resilience, including the launch of extensive security education programmes, the increase in internal capabilities to prevent and combat asymmetric and hybrid threats, the enhancement of the capacity to identify possible adaptations of hybrid offensive actions to new, as yet undeveloped technologies, by facilitating the implementation of the NATO-EU cooperation agenda in areas such as combating hybrid threats and strategic communication (to remain in our area of interest).*

*On the other hand, the **White Paper on Defence** (2020, p. 12) highlights the existence and manifestation of "hostile information actions, conducted both to influence social perception and affect public confidence in state institutions and to obtain necessary information to influence the decision-making process" as a threat to national security, entailing a consistent risk factor, which is why, in the set of modern defence capabilities to be developed, it is necessary to "create and develop specialised capabilities, at the level of the Armed Forces, to counter information aggression, destabilising propaganda and hybrid campaigns" (CAAp, 2020, p. 15), which can lead, over time, to increased levels of resilience to asymmetric and hybrid risks and threats.*

*The perspectives of the **National Defence Strategy** (2020) and of the **White Paper on Defence** (2020) are justified by the extensive studies conducted in the already narrow field of **fake news** in the military environment. For a clear theoretical approach, we should start from the communication/information architecture of the military organisation and, by extension, of the contemporary battlefield, with emphasis on the purposes of communication: information, keeping open communication channels, and influence. In relation to the mass media, classic and new, it is talked, first of all, about influence and only then about information, which is why the military action communication architecture entails two different types of infrastructure.*

*Specifically, we have in mind an information communication infrastructure, which is built on the fundamental principle of public relations – "Tell the Truth!" and whose main purpose is to increase the degree of trust between the military*

[1] Among the Russian hybrid tools used in contemporary confrontations, James Rogers (2018, pp. 263-264) explicitly includes *fake news,* more precisely *"Spread of disinformation and fake news to sow confusion and prevent an opponent from establishing an understanding of Russia's policy or intentions"*.

*organisation and its audiences, internally and externally (in this case, we are talking about the structures of public relations and media operations, MEDIA OPS, depending on how they are defined in different doctrinal apparatuses).*

*A second communication infrastructure would be that of influence, which aims to create the desired effects on the "will, understanding and capabilities of opponents, potential opponents and approved audiences" (AJP-3.10, 2015, p. I-3; DOI, 2017, p. 52), which is achieved explicitly through information operations (INFO OPS) and through the entire range of subsumed operations/ fields: psychological operations; presence, posture, profile/PPP; operation security; information security; deception/masking; electronic warfare; physical destruction; key leader engagement; computer network operations and civil-military cooperation (DOI, 2017, pp. 21-22).*

*The two communication infrastructures should not be concurrent, because under such conditions, the second, the influence infrastructure, would corrupt and reduce the level of the only guarantor of the functionality of the first infrastructure, the information infrastructure: trust. The information infrastructure presupposes the correct, complete and timely information of the target audiences and aims "to promote understanding and to obtain domestic and international public support for the military operations conducted by the Romanian Armed Forces, while ensuring the operations in preparation or in progress" (DOI, 2017: 52), while influence infrastructure, corrupting trust, contributes decisively to blocking any means of promoting trust and obtaining public support. Apparently, aiming for the information infrastructure, **fake news**, in the military environment, has as main target the information infrastructure itself, by creating mistrust, by cultivating subjective truth (**post-truth**), by focusing on personal emotions and beliefs at the expense of substantiation in relation to evidence.*

*This generalised hybrid framework therefore allows the use of coordinated information influence (through complex information operations, themselves hybrid in relation to the types of subsumed operations), implicitly through **fake news**, with the ultimate goal of weakening societal resilience and lowering trust in institutions. In relation to **disinformation**, the use of **fake news** as **disinformation** is not limited to the actions of disseminating information that is obviously false or altered, in relation to the truth, specific to new media (social networks), but represents the complex form of disinformation in which the truth is qualitatively altered, preserving certain features, in which the media complex can be understood as a **hybrid media system**. In such a weakened environment, through concerted information actions aimed at diminishing the trust and, implicitly, the information infrastructure of the organisation (alliance, state, military institution), it is created the predisposition to align with subjective, group, highly polarised and ideological truths, while evidence-based rational discourse is continually undermined, and objective truth is subordinated to contextual and consensual truths, in a disturbing flow of data that contributes to affiliation and communication in order to keep communication channels open, thus strengthening the affiliation with digital tribes.*

*The new soldier is the agent of influence (according to Kearns, 2019, p. 99[2]) or the **influencer**, who, on the one hand, generates disturbance in relation to the **establishment**, traditional institutions, values and principles, using an "anti-system, anti-**establishment**, anti-policy, anti-expertise" rhetoric (Bârgăoanu, 2018, p. 153), and, on the other hand, regroups around the values of the new "digital tribe", polarising and engaging strong ideological discourses that diverge from those of other groups. This soldier in the hybrid confrontation, who uses communication in order to influence, generates multiple effects by using a single weapon: **information influence**, which is illegitimate (and, implicitly, produces morally asymmetrical effects), considering that "Information influence **breaks the rules** […]; Information influence **exploits vulnerabilities** […]; Information influence deceives people […]" (Nothhaft et al., 2019, p. 42). In the projection of the **influencer** actions in the information warfare virtual, hybrid, battlespace, this deception weapon covers a spectrum of interpretations that are difficult to prefigure.*

*The palpable problem of **fake news** is that, for a complex and efficient response, it requires a solid, consistent construct, which is atypical to these times of weakness, and the prevalence of networks in relation to hierarchies. Therefore, it is necessary, on the one hand, a consistent security culture, through a national project meant to develop and consolidate it, and, on the other hand, a training of the military to respond to the new type of soldier: the **influencer**, capable of using communication in order to achieve effects on those unprepared to respond appropriately. From this point of view, the reactive response – which is usually the product of strategic communication – is insufficient, as new avenues of influence diversify and benefit from the surprising opportunities provided by new technologies.*

*A form of hybrid confrontation thus occurs when the military can use the **hard** tools and, to a lesser extent, the **soft** tools, on the level on which they are attacked by **information influence**. Moreover, this **fake news** action produces effects on the information infrastructure of the military organisation and the state structure, discrediting the institutions and lowering the level of trust in them. The response can only come through the influence infrastructure, through a set of countermeasures that, coupled with a high level of security culture and the democratisation of hybrid confrontation, can lead to strong and lasting effects, relative to the contextual truths of "digital tribes". In essence, the high level of security culture, obtained by democratising hybrid confrontation, allows the transformation of all, military or ordinary citizens, into agents of positive change: "(…) the democratisation of hybrid warfare gives us all opportunity to be agents of positive change" (Kearns, 2019, p. 120).*

---

[2] *"Governments and military organisations globally are grappling with the changing nature of influence: the democratisation of information and truth as the next stage in the development in the hybrid warfare and violent extremism. […] The difference in the Digital Age is the soldiers. For the actors in the battle are no longer solely states, the media, or well-financed terror or organised crime groups, it is all of use: because we are all now agents of influence".*