

KEY ASPECTS OF STRATEGIC COMMUNICATION ANALYSIS AS A TOOL FOR ACHIEVING COGNITIVE SUPERIORITY 5.0

Mirela CĂPÎLNEAN, Diana RANF

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
capilnean.mirela@armyacademy.ro, ranf.diana@armyacademy.ro

Abstract: *The article aims, first and foremost, to present an analysis of how cognitive warfare is currently perceived, with a focus on NATO's approach to this field. Secondly, the article offers a perspective on the importance of strategic communication in achieving cognitive superiority, illustrated through a case study. At the same time, the article also addresses the field of Industry 5.0, which through its components (digitalization, collaboration between people and intelligent technologies, etc) represents, alongside strategic communication, a catalyst for cognitive superiority. The scientific approach is qualitative, based on an analysis of key words in the specialist literature. The results highlight the important role of strategic communication in cognitive superiority 5.0, with technology serving as the link between the two concepts.*

Keywords: strategic communication, cognitive domain, cognitive warfare, cognitive superiority, Industry 5.0

1. Introduction to the relevance of the concept of “cognitive superiority”

In a digital age characterised by the unprecedented speed of information dissemination, contemporary conflicts are increasingly characterised by actions carried out in the information environment, with simultaneous effects on the political, social and military domains. The rapid development of emerging technologies, particularly in the field of artificial intelligence, is redefining the traditional form of conflict, shifting the centre of gravity from territorial control to influencing human perception and the way reality is perceived. The writing of this article was based on the premise that the role of strategic communication is becoming increasingly important in achieving, consolidating and maintaining cognitive superiority. In the current security context, the exploitation of human actors' cognitive vulnerabilities marks the transition to a context in which the

relationship between reality and its representation is becoming increasingly fragile. Beyond strategic communication, another catalyst for cognitive superiority is the process of digitalisation and the technologies associated with Industry 5.0.

The central objective of this article is to answer the following research question: To what extent can strategic communication protect human decision-making processes against complex cognitive manipulation tactics? At the same time, how does this tool contribute to building a “collective mental defence” essential for achieving cognitive superiority in the 5.0 era? To answer this question, the analysis focuses on the intersection between the psychological dimension of cognitive warfare and the defensive capabilities offered by StratCom in the era of Industry 5.0.

The research method is based on a documentary and conceptual analysis of the specialist literature, complemented by an

interdisciplinary perspective that highlights the relationship between the concepts addressed: cognitive warfare, strategic communication and new technologies.

2. Cognitive warfare and cognitive superiority - operational complementarity

Despite numerous studies and debates surrounding the concept of cognitive warfare, a comprehensive understanding of it remains elusive. Cognitive warfare is often equated with hybrid warfare, but the latter involves the coordinated use of multiple instruments of power, with information being just one of them. Cognitive warfare differs from information, hybrid or psychological warfare in its primary objective, which is to target human cognition, shaping perceptions, beliefs and, implicitly, the behaviour of human actors.

Around 2020, the concept of cognitive warfare came to the fore in analyses conducted at NATO level, being defined as a set of actions aimed at affecting cognitive processes [1].

It has been interpreted in various ways in the specialist literature and within NATO studies, evolving from a manipulative technique into a distinct domain of conflict. Recent studies emphasise that *“cognitive warfare has become a sixth emerging domain of conflict, alongside land, air, sea, space and cyber”* [1].

Cognitive warfare has evolved recently, yet its fundamental principles were laid down 25 centuries ago by the Chinese philosopher Sun Tzu, who argued that *“...the whole secret lies in confusing the enemy, so that he cannot fathom our real intent”*. – Sun Tzu on the Art of War. In the modern era, cognitive warfare retains these strategies and extends them into the informational and cognitive dimensions, incorporating state-of-the-art technologies and exploiting human psychological vulnerabilities.

We face multiple forms of threats today. In the context of cognitive warfare, the rise of information as a supreme form of power can affect both the security of nations and that of

individuals, by undermining thought processes. Competition is shifting into the cognitive realm, where influence, persuasion and the manipulation of emotions can have cumulative long-term effects on individual and group behaviour. Contrary to the popular belief that decisions are purely rational, neuroscientific research demonstrates that emotions are an integral part of human cognition. As author Waltzman points out, *“to compromise an adversary’s decision-making capacity, one approach is the appropriate manipulation and compromise of the emotions essential to decision-making”* [2].

Whereas a few centuries ago war was viewed as an inter-state military confrontation, in today’s environment, the centre of gravity of conflict has shifted to a broader scale, down to the individual level. In their paper entitled Cognitive superiority, Dean S. Hartley III and Kenneth O. Jobson define combatants as being *“numerous, nuanced and adaptable, allowing a greater diversity of adversaries to participate in cognitive warfare”* [1].

As Hartley III and Jobson point out [1], the current spectrum of combatants includes:

- multiple national opponents who employ various modes of attack on all facets of national life;
- non-state opponents, both external and internal;
- individuals or small groups motivated by ideological or economic objectives;
- corporate entities seeking to achieve their own goals through influence operations;
- digital adversaries who exploit the fact that social media can become dissociative spaces that facilitate attacks.

This diversity of adversaries necessitates a reassessment of the defence strategy against cognitive threats.

According to NATO, cognitive warfare is defined as *“the struggle for cognitive superiority, ...consisting of deliberate and synchronised military and non-military activities, conducted across the entire spectrum of competition, with the aim of*

gaining, maintaining and protecting a cognitive advantage” [3]. In this context, “cognitive warfare focuses on attacking and degrading rationality, which can lead to the exploitation of vulnerabilities and systemic weakening” [3].

Since 2021, with the advent of NATO’s Warfighting Capstone Concept, the research activities of the NATO Science and Technology Organisation have placed greater emphasis on understanding human cognition.

According to the Report of the NATO Chief of Scientific Research, the conceptual framework *The House Model* (HFM-ST-356), developed within the NATO Science and Technology Organization, highlights seven areas of knowledge necessary for achieving cognitive superiority [4]:

- situational awareness: this area concerns the study of how we succeed (or are prevented) in making sense of information in unclear situations, forming the basis of any sound decision;
- cognitive effects: focuses on the techniques an attacker uses to distract us, mislead us or alter our perception of events;
- modus operandi (methods of attack): analyses the enemy’s plans and strategies to identify exactly how and when they act to manipulate us psychologically;
- technology and force multipliers: studies how artificial intelligence, big data and new digital technologies make cognitive attacks much faster, more widespread and harder to detect;
- cognitive neuroscience: investigates the physical and neurological mechanisms through which our brain processes information and makes decisions, in order to understand how it can be programmed or influenced;
- behavioural science: focuses on the central role of emotions, trust and human relationships in shaping behaviour and the way we communicate;

- social and cultural science: analyses how values, group identity and the political context determine how we act collectively.

The synergy between these areas of knowledge involves complex research and extensive studies to understand the neuroscientific mechanisms of human reasoning. The aim is, in particular, to understand the factors that influence the decision-making process at an operational level. According to [4], the application of these fields of knowledge supports the OODA loop (Observe, Orient, Decide, Act) by identifying and countering vulnerabilities that disrupt the decision-making process in the operational environment. The scientific findings of this conceptual framework have been applied in practice since 2025 by a specialised unit within HQ SACT (Supreme Allied Commander Transformation Headquarters).

To protect Alliance nations from this new form of conflict, NATO is recalibrating the traditional tools that interact with the cognitive dimension: Psychological Operations (PsyOps), Information Operations (InfoOps) and Strategic Communication (StratCom) [4]. Within this complex architecture, where cognitive warfare targets the hacking of the human mind, strategic communication has become a form of collective mental defence.

3. Strategic communication – the NATO perspective and reality in contemporary military operations

In the simplest sense, communication is the process by which people transmit and receive information, with the aim of fostering understanding and human interaction. Strategic communication, on the other hand, is a complex approach that seeks not only to deliver a message but also to produce effects in the cognitive dimension in order to gain a strategic advantage (Figure 1).

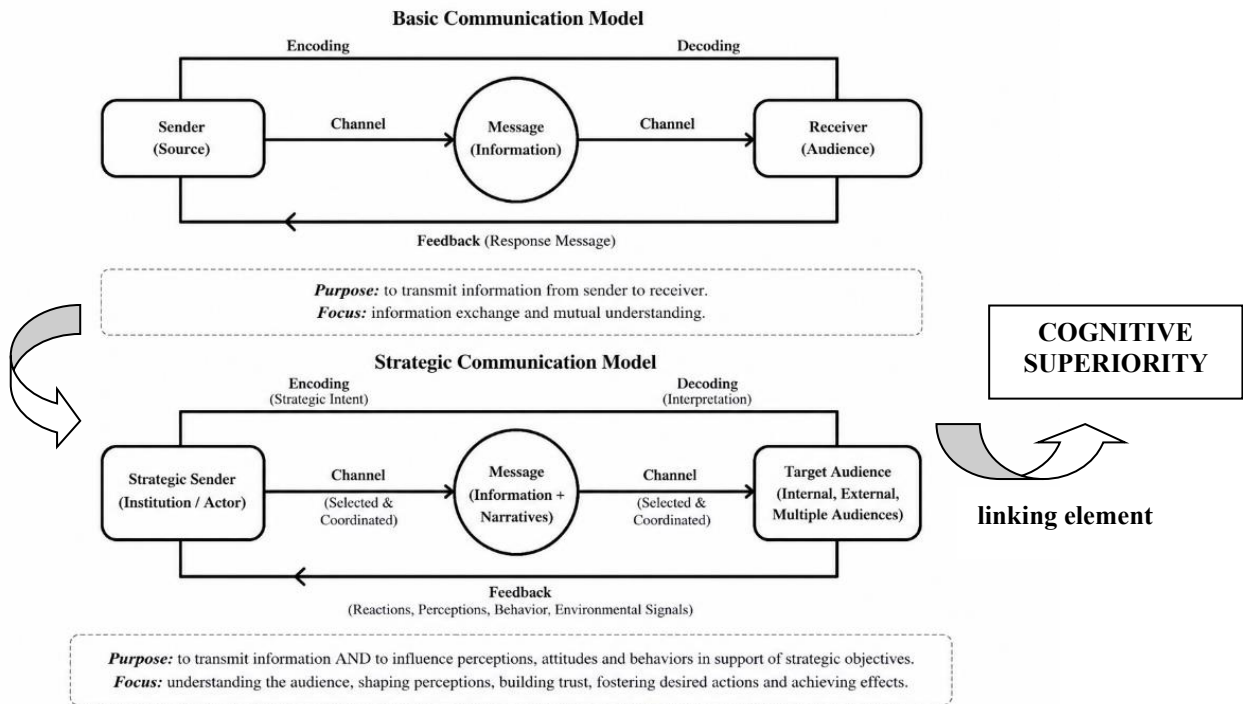


Figure 1: Basic Communication and Strategic Communication Models,
Source: Author

Within NATO, the concept of strategic communication has undergone significant development due to the fact that this field continues to evolve rapidly. Early initiatives took shape in 2009 in response to shortcomings identified in areas such as *public diplomacy* and *public affairs* [5], which were negatively affecting the organisation's credibility in relation to the operation in Afghanistan.

The NATO Strategic Communications Policy (2009) highlighted the need for an integrated approach to communication. The concept was later developed through numerous doctrines and operational directives, culminating in 2023 with the drafting of a NATO military doctrine for strategic communication (AJP-10), intended for member states.

A key milestone in the development of this concept was the establishment, in 2014 in Riga, of the NATO Centre of Excellence for Strategic Communication (NATO StratCom COE). This laid the foundations for the development of the Alliance's strategic communication capabilities.

The definition of strategic communication, as conceived by NATO, involves "*the coordinated and appropriate use of NATO's communications activities and capabilities – public diplomacy, public affairs, military public affairs, information operations and psychological operations, as appropriate – in support of Alliance policies, operations and activities, and in order to achieve NATO aims*" [5].

In the security context following Russia's annexation of Crimea, strategic communication is taking on an increasingly important role as a result of the development of disinformation campaigns and propaganda. Numerous studies have shown how false narratives can influence the perceptions and behaviours of the audience (military personnel, the civilian population, adversaries or allies), destabilising entire societies and eroding public trust in institutions.

Currently, strategic communication has become a core defence capability of the Alliance, particularly in the context of current threats which are no longer merely

military in nature, but directly target the integrity of mental processes and social cohesion.

We start from the premise that *“no rational decision is possible without the involvement of emotions”* [2], as these are an integral part of the cognitive process.

On the one hand, in today’s information environment, characterised by the digitalisation of related technologies, there is a marked tendency towards the superficial processing of information. That is why *“much of human thought and communication is for affiliation and affirmation, not truth-seeking”* [1]. In most cases, people do not react to the information itself, but to the meaning they attribute to it. New technologies exploit this phenomenon through algorithms that memorise individuals’ preferences and emotional states, generating content influenced by user profiles. *“An echo chamber replicates the same information the opinion leader or the source has disseminated, information that is replicated by those whose opinion reflects the same views”* [6], which limits knowledge.

On the other hand, the accurate interpretation of information in the online space has become increasingly complex as a result of the proliferation of content generated by artificial intelligence. Careful verification of the sources providing information is necessary in order to distinguish truth from fiction before forming one’s own perceptions.

In the face of these threats, the human brain becomes the primary target of cognitive hacking, where *“bad actors, foreign governments, extremist groups, and rogue individuals - are working to manipulate the way you think, making you question what’s real and doubt your own beliefs”* [7].

According to AJP-10, at NATO level, strategic communication functions as a central pillar of coherence, serving to ensure constant alignment between actions, images and words: *“coherent StratCom ensures NATO’s actions, images and words are*

consistent with its narrative across the continuum of competition” [8].

Through its fundamental principles, such as: *being grounded in values, being objective-centred, and maintaining credibility*, strategic communication maintains the alignment of actions and narratives, eliminating vulnerabilities that could be exploited by adversaries. It operates through truthful, clear and concise narratives, whilst also serving as a tool for building cognitive resilience. By integrating complementary fields (public diplomacy, public relations, InfoOps, PsyOps and PAO), strategic communication functions both as a defensive mechanism against cognitive threats and as a preventive tool by supporting institutional legitimacy and societal resilience.

From this perspective, it should not be viewed merely as a *reaction* to threats, but rather as a tool for cognitive defence against the manipulation of human actors’ perceptions and behaviours.

Building on the conceptual definition of strategic communication, we shall now illustrate its applicability at NATO level through a case study.

The “Doppelgänger” case (2022–2024)

This is considered one of the most complex disinformation campaigns, coordinated by the Russian Federation with the aim of undermining support for Ukraine and trust in NATO and EU government institutions.

Essentially, the campaign utilised cloned, high-profile websites that mimicked at least 17 credible news organisations, including Der Spiegel, Le Monde, Fox News and The Washington Post [9], among others, with the aim of disseminating false information supporting Russia’s narratives [9]. The media content was rapidly disseminated through bot networks, fake accounts and paid advertising, which created confusion and played on the public’s emotions and perceptions.

The narratives focused on discrediting Ukraine as a corrupt state, undermining Western support, exploiting internal

tensions, portraying Russia as a victim, and delegitimising the West. There was also an attempt to influence the 2024 elections in Europe and the US by exploiting social and political vulnerabilities and amplifying existing discontent. These actions sought to erode public trust in institutions and bolster support for pro-Russian parties. The influence operations primarily targeted Ukraine, the US, Germany, Poland, Italy and France, as well as other regions.

Once the campaign was identified, strategic communication served as the main *defensive weapon* used by the affected states. The role of strategic communication was to expose the operation by bringing known analyses and data to the fore, countering the narrative, and coordinating with digital platforms to limit the spread of this phenomenon. The states involved aligned their strategic communication objectives within a unified deterrence framework. NATO contributed by providing support to strengthen national resilience. At the same time, the NATO StratCom COE assessed the campaign's impact on the collective security of the states. In the context of strategic communication, coordination between governments and public institutions is also relevant in terms of the narratives conveyed to raise public awareness and deter the campaign. The Doppelgänger campaign demonstrates that, in the digital age, cognitive superiority is achieved not only through technology, but through the capacity of strategic communication to protect the *brand of truth* [10].

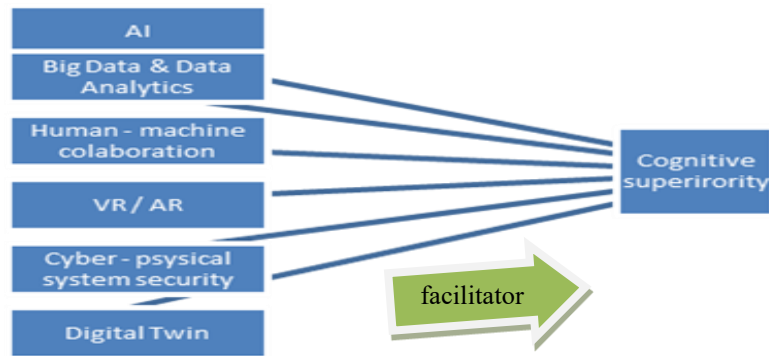
4. Digitalisation and associated technologies – a catalyst for cognitive security 5.0

The architecture of modern conflicts has expanded beyond traditional physical

domains into cyberspace and, ultimately, into the cognitive domain. This transition has taken place gradually and is closely linked to the process of digitalisation. Whilst conflict initially moved into cyberspace as a result of the development of dual-use and emerging technologies, digitalisation has created the conditions for a subsequent stage in which information becomes a primary vector of influence. Rapid technological changes have shaped both the information environment and the processes of human cognition by extending their impact on perceptions and cognitive processes. We are witnessing the emergence of new scientific paradigms.

Weaponization of Neurosciences is a new concept involving the convergence of the fields of Nanobiology, Biotechnology, Information Technology and Cognitive Sciences (NBIC). The fusion of these four fields aims to achieve *human-technology symbiosis* [7].

Industry 5.0 represents a new stage of industrialisation, bringing the human factor to the fore as a central element in advanced technological ecosystems. This paradigm can influence social stability and is based on the interaction between humans and machines, sustainability and resilience, as an integrated and coherent system in which the two dimensions - *human cognition* and *emerging technologies*, co-evolve. In the context of cognitive warfare, we can speak of cognitive superiority as a result of the ability to control and integrate these complex systems. Beyond strategic communication, the associated technologies represent another important catalyst for cognitive superiority (Figure 2).



*Figure 2: Industry 5.0 components and cognitive superiority,
Source: Author*

5. Conclusion

The contemporary security environment is marked by an unprecedented diversity of threats, which are constantly evolving and converging towards the cognitive dimension. To understand these new forms of threats, a multidisciplinary approach is needed, involving psychological, biological, socio-economic, and technological dimensions. It is important to leverage the opportunities offered by new technologies, but we must also be prepared to counter the risks that may arise from their use. The conceptualization of cognitive warfare within NATO is an important step, but continuous adaptation is necessary due to the dynamics of the technological and informational environment in which it operates. Attackers are using advanced technologies and artificial intelligence to monitor our emotions in real time, knowing that they are, in fact, the engine of our actions. By manipulating feelings, they can create confusion or digital “paralysis” turning information into a weapon that directly targets our ability to think critically. To defend ourselves, we must build “mental immunity” by training our discernment before we are exposed to manipulation. This resilience is only achieved when the whole of society collaborates to protect truth and public trust.

Based on the research results, we conclude that the effective use of strategic communication represents an indispensable strategic capability for managing complex threats. Integrating strategic communication (StratCom) as a central command function is imperative for achieving and maintaining cognitive superiority in the contemporary security architecture. At the same time, technology is not an auxiliary element, but a necessary condition for the efficiency of strategic communication in the 5.0 context. Without technology, strategic communication remains a tool of the past. The intervention of technology focuses on information collection and processing, as well as cognitive protection, through technologies for detecting disinformation, deepfakes, and influence operations. Resilience is no longer just a defensive capability, but an active strategic asset; StratCom success depends on transforming public trust from an abstract concept into a concrete barrier against manipulation. Thus, cognitive superiority becomes the ultimate guarantor of sovereignty in a borderless information space.

A future research direction could be a bibliometric study that, by analysing the intersection of strategic communication, technology, and cognitive superiority, would offer continuity to this study.

References

- [1] Hartley III, Dean, S. & O. Jobson, Kenneth. Cognitive Superiority: Information to Power. Edition 1. Switzerland AG: Springer Cham; 2021. 10-11. <https://doi.org/10.1007/978-3-030-60184-3>. Accessed April, 02, 2026.
- [2] Waltzman, Rand. Future Challenges to Cognitive Superiority. Arlington, VA: Irregular Warfare Center (IWC); (May 12, 2025). Available at: <https://irregularwarfarecenter.org/publications/perspectives/future-challenges-to-cognitive-superiority/>, Accessed April, 08, 2026.
- [3] Allied Command Transformation. Protecting the Alliance Against the Threat of Cognitive Warfare. Norfolk, VA: NATO's Strategic Warfare Development Command; (n.d.). Available at: <https://www.act.nato.int/activities/cognitive-warfare/>. Accessed April, 06, 2026.
- [4] Blatny, Janet M. & Søndergaard, Steen. NATO Chief Scientist Research Report on Cognitive Warfare. NATO Science & Technology Organization (STO); (December 19, 2025). Available at: <https://www.sto.nato.int/document/cognitive-warfare/>. Accessed April 14, 2026.
- [5] NATO. NATO Strategic Communication Policy SG (2009) 0794. NATO Unclassified. (September 14, 2009). Available at: <https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf>. Accessed April 14, 2026.
- [6] Popescu, Maria-Magdalena. Disinformation deconstructed - Cognition Security and Digital Control. Bulletin of the Transilvania University of Braşov. 2021; Vol. 14(63). 125. <https://doi.org/10.31926/but.ssl.2021.14.63.1.12>. Accessed April, 08, 2026.
- [7] Drnec, Kim. Cognitive Warfare is Manipulating Your Thoughts and Destroying Democracies. Applied Cognitive Effects Newsletter – Perception, Cognitive Warfare. (December, 2025). Issue (4). 11. Available at: https://www.act.nato.int/wp-content/uploads/2025/12/20251219_CogWar-Newsletter-December.pdf. Accessed April, 08, 2026.
- [8] NATO Standardization Office (NSO). Allied Joint Doctrine for Strategic Communications AJP-10, Edition A, Version 1. NATO Unclassified. (2023). Available at: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf. Accessed April, 08, 2026.
- [9] Alaphilippe, Alexandre et.al. Doppelganger - Media clones serving Russian propaganda. (2022). Available at: <https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf>. Accessed April, 08, 2026.
- [10] Mârzac, Elena & Panța, Rodica. Comunicarea strategică – Ghid conceptual. Republic of Moldova: Platform for Security and Defense Initiatives; (2024). Available at: https://pisa.md/wp-content/uploads/2026/01/Comunicare-strategica_-Ghid-conceptual.pdf. Accessed April, 08, 2026.