COGNITIVE WARFARE – BEYOND DOMINANCE, MANOEUVRES AND INFORMATION – THE BATTLE FOR THE IMAGINED FUTURE

Colonel Assoc.Prof. Ciprian PRIPOAE-ȘERBĂNESCU, PhD

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2023.4.16

This theoretical paper explores the nascent concept of cognitive warfare in the context of persistently low-intensity forms of confrontation and of an increasingly rich environment in technologies that provide greater opportunities for influence operations. As the hybridity of conflicts has become prevalent, it is of special interest to investigate the relevance of the cognitive warfare concept (CW) in shaping the informational-psychological threats posed by hostile entities. By analysing the current features of CW as presented by various sources, this article aims to contribute to the conceptual development of this notion. The great diversity of definitions suggests a challenge in delineating what is CW, thus the author argues for a threshold between what is a mere, benign influence and what stands as a threat/attack in the cognitive realm, by using a novel approach to cognitive security. Consequently, we will underline what we consider the limits of the current understanding of CW, as presented in current public papers, and make suggestions for a more refined model to think about cognitive warfare based on active inference theory. In conclusion, we will indicate the risks associated with the use of the concept information, and the necessity to integrate CW and cognitive security in a longue durée perspective, one that acknowledges current societal and cultural transformations.

Keywords: hybrid warfare; cognitive warfare; active inference;

INTRODUCTION

Cognitive warfare (CW) has become a new buzzword in the security domain, loosely defined as a confrontation carried on cognitive space to achieve a form of superiority. Along with it, CW brought some other correlated notions, such as cognitive vulnerability, cognitive resilience, or cognitive security. For an adequate treatment of this newcomer in security studies, a careful analysis of the larger context is necessary.

National states and military alliances activate in a geopolitical environment characterised by the interplay between interdependency and strategic competition. As such, governments must operate on a competition continuum in a world where the lines between peace and war are blurred and continuously negotiated. In an ongoing competition held below armed conflict, with hybrid threats tending to become quasi-permanent, authorities must raise awareness of the pervasive, subtle psychosocial effects of the informational-psychological[1] actions carried by hostile actors. More experts and practitioners are concerned with the *"idea of increasing hybridity between different military and non-military means and methods employed by political players to achieve their goals without escalating to an outright open armed confrontation"* (Fridman, Kabernik, Pearce, 2019, p. 2). In this sort of confrontation, the so-called informational dimension, or informational environment is increasingly used to influence various audiences, domestic or foreign, to further promote political and military objectives.

Expanding on the information environment definition, Allen Patrick and Dennis Gilbert introduced the notion of the information sphere, stating *that "cyberspace, cognitive, and information are components of the more encompassing Information Sphere"* (Allen, Gilbert Jr., 2009, p. 5). This assertion is based on the premise that the Information Sphere includes the relationship among these three components that *"define the meaning, context, and value of the Information Sphere, not the three components taken in isolation"* (Ib.). Worth mentioning that through this new concept (information sphere), the gap between classical information operations (IO)

[1] As defined in V. Ryabchuk and V. Nichipor, *"Prognozirovaniye I Predvideniye v Sisteme Planirovaniya Operatsii i Obshchevoyskovogo Boya [Forecasting and Prediction in Operational Planning Systems and Combined Arms Combat]"*, Armeiskii Sbornik [Army Digest], No. 10, October 2012, p. 38.

and cognitive warfare is closing, as the doctrinal limits of IO (to be used only during periods of war, to support kinetic objectives on the battlefield) are extended to include actions during peacetime, and support socio-political objectives.

Information operations have five core capabilities, psychological operations (PSYOPS), electronic warfare (EW), computer network operations, deception, and operational security. In a different approach, information operations are defined as *"a staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capabilities of adversaries, potential adversaries, and audiences in support of mission objectives"* (AJP 10.1, 2023, p. 15). As such, one of the key tenets of IO is the behaviour-centric approach, *"a comprehensive and persistent understanding of audiences"* (Ib., p. 7), an audience defined as *"any individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state"* (Ib., p. 8). Setting audiences at the centre of IO activities suggests the importance and relevance of the cognitive dimension for the influence operations and for the non-kinetic dimension of warfare. As we notice, some of the psychological aspects of audiences were already taken in consideration by IO/PSYOPS, through the centrality of the audience analysis process (TAA). This suggests an overlapping between CW with other related concepts of IO, mostly PSYOPS and cyber warfare, raising the question of the validity and usefulness of a new concept, such as cognitive warfare (CW).

The relevance and importance of CW derive at least from the aforementioned definitions, which underscores the doctrinal limitation of IO, operations that aim to achieve objectives during warfare, on the battlefield, and in support of military objectives. As such, is of interest to recognise the existence of influence operations that are carried out by non-military actors, during peacetime, at the scale of the whole society, aiming to achieve political objectives or even long-term cultural changes.

Another limitation that suggests a different approach to CW is determined by the fact that much of the research in CW is based on cognitive-behavioural school, and on the extensive use of the notion information. It is unclear if the whole psychology of influence operations is entirely represented by using only this approach, so the purpose of this study was to contribute to the conceptual development of CW, firstly by highlighting the current limitation of existing definitions and interpretations, furthermore, to propose a more holistic approach on the *"cognition"*. This will open a new venue for defining cognitive security and cognitive warfare, by using Karl Friston's free-energy principle applied to the field of neuroscience and consciousness studies, as envisaged by Professor Mark Solms.

As such, as an original contribution, we suggest the use of the expression cognitive security to delineate between benign informational influence and cognitive attacks by using the notion of active inference and *"cognitive"* models of the world, therefore improving the operational usage of the CW concept. Moreover, by using a holistic approach to *"cognition"* and the active inference theory, we will be able to introduce and recognise all factors and influences that might undermine cognitive security. In the first section, I will defend the relevance of this new concept (CW), and summarize some of the definitions of CW. For the second part, I will underscore the limitations of the informational-cognitive approach, and advance a new way approach to cognition, cognitive security, and cognitive warfare. My conclusions will underscore the necessity for a new model of mind in conceptualising CW and the role of subtle, long-term socio-cultural transformations in creating vulnerabilities in the context of CW.

WHAT IS *COGNITIVE WARFARE* AND WHY DO WE NEED IT

Actions used mostly for their psychological effects have been carried out since the beginning of human confrontation. Recognising that the human mind has always been a space for battle and dominance, a significant level of disagreement persists on the opportunity, whether the adoption of this new concept would mark any relevant advances for security field, regardless of the level (individual, group/community, society), or domain, economic, military, cultural, or social. What may count as a plausible explanation for the current interest in CW could be the recognition of more robust expertise in the field of information-psychological operations conducted by Russia as part of a larger hybrid confrontation. Enjoying larger freedom for action and expression, unbounded by doctrinal, ethical, or legal constraints, Russia's experts on information-psychological operations have shown a masterclass in deception, disinformation, propaganda, activities conducted over a long period of time with incremental effects. Combining kinetic with information actions, exploiting the blurred limit between war and peace, or transforming the core features of democracies in vulnerabilities, Russia has shown a very intimate knowledge of the human psyche and the dynamics of society.

As most open sources indicate, CW can be situated at the confluence between influence operations and information operations. These two domains are part of the current non-kinetic approach to warfare, so it is important to clarify the nature of influence in the information environment. Different from coercion (use of force), influence is the ability to change, to alter the state of an entity (individual or collective), usually associated with producing effects using immaterial means. This definition inevitably leads us to information operations and information environment, in which the most relevant dimension is the cognitive one. As such, the capacity to influence is reducible to the ability to direct thinking and behaviour, to induce effects, in our case on individual's minds and behaviour, using subtle means. Some voices express the idea that current approaches on influence operations or military specialties (social engineering, propaganda, Information Operations, PSYOPS, StratCom) are enough to cover the field of influence domain. Likewise, the new concept of CW and the subsequent new area (cognitive domain) seems redundant, overloaded, and unnecessary as it can create more confusion and little guidance for practitioners.

Yet, there are reasons that clearly support the idea that influence operations that target how people think, decide, or act tend to become the weapon of choice for political actors and military decision-makers. I will briefly review some of the most relevant and subsequently specify the risks associated with the usage of information notions.

The first feature to be considered regards the level of knowledge accumulated. The advancements made in various fields and disciplines, such as cognitive science, neuroscience, and neurobiology, created the premises for a much more accurate and better understanding of how the brain works, and how the mental processes unfold. The most appealing application of this knowledge is the ability to *predict* the human response (in terms of attitude, emotions, and behaviour) when exposed to specific stimuli and therefore the seductiveness to deliberately exploit specific psychological traits that become targeted *"vulnerabilities"* of the individuals, in order to obtain desired effects. This accurate psychological knowledge combined with AI support made almost ubiquitous the possibility to create well-individualised/tailored messages that basically can target anyone who has access to a smartphone and the Internet[2]. As such, from derailing a rigorous decision-making process to seeding distrust in the government and social institutions, the psychological mechanisms behind influence have become transparent.

[2] Probably the most mediated case is Cambridge Analytica.

The second feature regards the evolution of the Internet and mass media, which have massive epistemic and ontological implications. On the one hand, digital technology made it possible for private, intimate psychological processes to become accessible and open to interference. Due to the intrinsic, bidirectional, and close interactions with the virtual environment, it is easier now than ever to collect relevant data for psychological profiling. As Byung-Chul Han (2017) has nicely framed, individuals have become willingly co-participants involved in the act of self-surveillance. Moreover, the predicted fusion and interconnectivity[3] between the human brain and various devices will generate more ability to collect data and alter the representation of reality, either physical or social. Permeating the human body with sensors and processors will nonetheless affect individuals' identity and their ability to make clear distinctions between the information coming from biological analysers and technological sensors.

On the other hand, with the advent of mass media, the internet, and information technology (ICT), the relationship of humans with reality has become *mediated.* From J. Baudrillard (1994) onwards, communication studies had picked up the postmodernist notions of simulacra and simulation to acknowledge a fundamental change in human society; the increasingly blurred line between reality itself and the simulation of it, the hyperreality. This transition made conceivable concepts and ideas like negotiation of reality, deep-fake, alternative facts, post-truth, and echo-chambers, elevating the human imaginary to the point of a favourite space for influence.

The third and last one connects the matter of mind with the security domain. Thus, the seduction exerted by the knowledge of human minds connected via the Internet with more digital technology will increasingly be exploited by the so-called revisionist entities (governmental or not) to undermine the current status quo of the international system. Taking advantage of the interconnectedness of information technology and the features of hostile informational actions (cheap, fast, deniable, effective), using (new) mass media, malicious actors can crystalise concealed but resilient negative beliefs and resents that will imperil the act of governance and raise difficulties for mobilizing citizens to respond to any future attack.

Resuming the arguments, we advance the hypothesis that influence on the cognitive realm will expand and become increasingly opaque and more affordable

[3] Process associated with transhumanism. The interpenetration between the human body and sensors or processors will likely affect the identity of individuals and their ability to make a clear distinction between information coming from biological analysers and technological sensors.

to many entities, nonetheless even more efficient, posing challenges for national governments to effectively rule their countries. If hybrid warfare will be the standard form of future confrontation, and the informational-psychological aspects of it will dominate the spectrum of threats, then the study of CW, as a form of psychological influence, technologically mediated, is an urgent necessity to respond to future security menaces.

Considering the large spectrum of conflict and the interconnectedness and interdependence of social, political, cultural, diplomatic, and military levels, we have therefore the image of CW as an omnipotent and independent weapon that can be used permanently, without considering his contribution/support to military objectives. Considering all these details, we consider that the battle to influence the human mind will become a prominent and permanent feature of the future human society, during peace and war, which requires special attention.

In what follows, I will introduce the most relevant and used definitions and interpretations of CW, as founded on open sources, and further make a brief analysis.

At the level of the NATO alliance, the HQ ACT Concept Development Branch (https://www.act.nato.int) is currently developing the NATO concept on cognitive warfare. This concept is part of the implementation of the NATO Warfighting Capstone Concept (NWCC), the cognitive warfare concept being an outcome under the WDI Cognitive Superiority Initiative. The Cognitive Warfare Concept is a Line of Delivery (LoD), a *'Jump-Starter'* in SACT's Warfare Development Agenda (WDA), which further highlights the importance attributed.

The first NATO scientific meeting on Cognitive Warfare was held in 2021 at the initiative of the ACT's Innovation Hub. The declared objective was to gain the initiative in this domain by *"establishing a better, shared understanding of the cognitive dimension"* (Masakowski, Blatny, 2023, p. 30). In the summary of Cognitive Symposium, it is stated that *"cognitive warfare is achieved by integrating cyber, information, psychological, and social engineering capabilities. Exploiting information technology, it seeks to create confusion, false representations, and uncertainty with a deluge of information over-abundance or misinformation"* (Cognitive warfare, 2022, p. 21).

Cognitive Warfare is a notion used since the '90s, labelling various understandings of influence operations. In the United States, the notion has been used since 2017 to describe the methods used to "manipulate an enemy or its citizenry's cognition mechanisms in order to weaken, penetrate, influence or even subjugate or destroy it" (Underwood, 2017). CW represents the convergence of Psychological Operations (PsyOps), Information Operations (INFO OPS), and cyber operations with the advance of AI/ML networks that serve as an enabler for the distribution of the adversary's strategic agenda in exploiting human vulnerabilities and shaping human understanding of events (Masakowski, Blatny, p. 72). Cognitive warfare pursues the objective of undermining trust (public trust in electoral processes, trust in institutions, allies, and politicians), therefore the individual becomes the weapon, while the goal is not to attack what individuals think but rather the way they think (Cognitive warfare, p. 12). Cognitive Warfare has the ability to degrade the capacity to know, produce, or thwart knowledge (Cognitive warfare, 2020, p. 6). Cognitive Warfare is a war of ideologies that strives to erode the trust that underpins every society (Ib., p. 7). *"Cognitive Warfare is the most advanced form of manipulation to date, allowing the influence of an individual or a group of individuals on their behavior, with the aim of gaining a tactical or strategic advantage"* (NATO Inovation Hub, 2021, p. 3).

CW is a multidisciplinary approach combining social sciences and innovative technologies to directly alter the mechanisms of understanding and decision-making to destabilise or paralyse an adversary (Pappalardo, 2022). This type of warfare aims at influencing the heuristic of the human brain to win the *"war before the war"* (Takagi, 2022). *"Cognitive warfare is the weaponization of public opinion by an external entity, for the purpose of influencing public and/or governmental policy or for the purpose of destabilizing governmental actions and/or institutions"* (Bernal et al., 2020, p. 10). Dahl described CW as a strategy that impacts the Observation-Orientation-Decision-Action (OODA) loop in terms of decreasing its speed, decreasing its accuracy, or both (Dahl, 1996). *"Cognitive warfare is a strategy that focuses on altering how a target population thinks – and through that how it acts"* (Backes, Swab, 2019).

"*Current and potential adversaries use Cognitive Warfare to influence the behaviours and beliefs of individuals, groups, and populations in order to fracture Western societies. Cognitive Warfare leverages hyper-connectivity, the pervasiveness of data, psychological warfare, and cognitive sciences to affect what and how people think and act"* (NATO Booklet, 2023, p. 26). *"Cognitive warfare is thus an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke* *thought distortion, influence decision-making and hinder action, with negative effects, both at the individual and collective levels"* (Le Guyader, 2022, pp. 3; 1-5). *"CW represents the convergence of a wide range of advanced technologies along with human factors and systems, such as Artificial Intelligence (AI), Machine Learning (ML), Information Communication Technologies (ICT), neuroscience, biotechnology, and human enhancement that are being deliberately used by NATO's adversaries in the 21st-century battlespace"* (Masakowski et al., p. 1).

Some conclusions can be drawn from this plethora of definitions. Some authors focus on the dangers for the immediate /battlefield context decision-making process, while others extend the malign influence beyond the operational area, jeopardizing the very possibility of governing during peacetime. Some definitions are centred around cognitive functions and their intrinsic limitations, while others focus on the contextual advantages obtained from disturbing the cognitive process at the individual or even societal level. Some interpretations seem to suggest that only adversaries use CW, as an offensive weapon, while others hint towards a defensive posture. An interesting aspect is that some definitions focus exclusively on the cognitive level, while others, more ambitious, suggest an influence that affects the general perception of life, the world, or even personal identity.

Explicitly or not, from most of the definitions and interpretations analysed, the security referent object that is threatened by CW, beyond the immediate level of cognition, is the state, more accurately, the reliability of the psycho-social and cultural conditions that make possible the functioning of human society. Additionally, from current definitions turns out that the threats are materialised using opaque communicational forms of influence, mostly projected from the *"outside"* of state boundaries.

A NEW MODEL TO THINK ABOUT COGNITIVE WARFARE

In this section, I will suggest a new definition for CW and a new model to think about *"cognition"* and cognitive warfare using a novel approach to cognitive security. We will underline what we consider the limits of the current understanding of CW, limits induced by the notions of information and cognition.

The most startling aspect of using the notion of information is that it indirectly, converts individuals into just another machinery that processes information, as human society has been recently baptized as the information society that thrives in the information age. Below, I briefly summarise some of the most evident risks associated with the use of the notion *information.*

a) It implicitly encourages the materialistic/physicalism approach centred on the brain and furthermore, the equivalence between the computer and a (computational) brain. Due to the analogy brain-computer, the information notion has become relevant because it is considered that the brain computes data, overlooking that data and information only codify the parameters of a real environment which is vital for satisfying the needs of an embodied human being that experiences reality, not just compute it. However, how people codify their experience with the environment is not a mathematical, logarithmic process, but a very subjective, ambiguous, dynamic, and sometimes paradoxical process.

b) The information experts pretend to adequately describe and model mind functions and consciousness in informational terms using mathematical formulas and statistics when the fundamental traits of the mind (subjectivity, consciousness, intentionality, agency) (Solms, 2021) are beyond any mathematical formula or positivistic treatment/measurement.

c) In the communication discipline/field, the information stays at the bedrock of the cybernetic approach of communications. However, the inadequacy of this informational, mathematical model of communication, and the migration towards a psychological approach is clearly visible in the requirements addressed by the Riga StratCom COE journal (Bolt, Haiden, 2019, p. 43), where the notion of communication is strongly suggested to be associated with the production and exchange of meaning, and not as transmission of messages.

d) It induces the incorrect idea that knowledge derived through information is somehow neutral and objective when, in fact, it is marked by an inherently subjective perspective, and/or by cultural, and historical contexts.

e) Information is mainly used (and trusted) through a subjective process of judgment of the source's credibility, not by the content itself.

f) By using the analogy of the brain that processes/ computes information, the cognitivist paradigm tends to isolate individuals from their containing environment. Individuals are artificially detached from their cultural and historical context, making *"cognition"* decontextualized, thus absurd.

g) It preserves the focus on the technology, therefore on the physical dimension of the informational warfare, hence disregarding the more refined psychologically centred approach used by the adversary.

Moving to the notion of cognition, the Oxford Dictionary of Psychology defines cognition as *"mental activities involved in acquiring and processing information"* (Collman, 2015, p. 143). Under the rubric of information processing, cognition takes various forms, such as attention, perception, memory, thinking, or decision-making. The Merriam-Webster Dictionary defines the notion of cognitive as *"of, relating to, being, or involving conscious intellectual activity (such as thinking, reasoning, or remembering)"* (https://www.merriam-webster.com/dictionary/cognitive). Cognitive is an adjective related to the process of cognition by which *"knowledge and understanding are developed in the mind"* (https://www.oxfordlearnersdictionaries.com/definition/american_english/cognition). Using the computer analogy, cognition is about information acquisition and evaluation, furthermore about the elaboration, or consumption of knowledge. At the individual level is presented as the ability to understand accurately the environment and make optimal, adaptable decisions, while at the societal level, knowledge is considered an enabler of cooperation and social progress. From these definitions, it becomes obvious that the cognitive process is intrinsically linked with information and information processing, inducing the illusion of a process that can be accurately modelled with information theory models.

In this clear, objective theoretical environment, populated by cybernetic-like notions, a simple question has the potential to cause conceptual collapse.

How is possible for a simple string of alphanumerical signs to become a cognitive *threat*?

Most of the adepts of the informational-cognitive approach on CW, and of mind in general, consider that what is threatened is the *"integrity"* of the underlying processes (attention, memory, reasoning, perception), the quality of understanding and of knowledge obtained, a position that highlights again the implicit normative stance, as if cognition could follow a flawless trajectory. The champions of the informational-cognitive paradigm often use two concepts/theories to explain the *"faults"* that appear in the computer-like brain, such as cognitive biases, and cognitive dissonance. The very limitations, critiques and revisions proposed for these two theories open the way for our innovative approach to CW.

In the case of dissonance theory, reviews (Vaidis, Bran, 2019, p. 1189), revisions, and critiques show that dissonance effects are not the result of cognitive inconsistency, pointing toward a much more fundamental role of self (affirmation/esteem) (Aronson, 1992, pp. 303-311), feelings and future consequences (Scher, Cooper, 1989, p. 899), and moral integrity (Steele, Spencer, Lynch, 1993, p. 885), as explanatory resources. Similarly, cognitive biases are vigorously criticised, as they should not be considered errors, as in fact, they have an adaptive role (Gigerenzer, Hoffrage, 1995, p. 684). Moreover, the cognitive bias model is backed by dual process theory, a theory that highlights the role of affects and unconscious levels of the mind, an aspect explicitly stated for implicit bias definition (Noon, 2018, pp. 198-209).

It is obvious that when we try to answer the question of how bits of information become a threat, it is mandatory to acknowledge the active, interpretative stance of the mind, moreover the intricate relation between cognition and other mental processes, and of course the instrumental role of cognition. As we will indicate, the very features which in the *"orthodox"* approach to cognition represent a threat that *"disrupts"/"corrupts"* cognitive process *"integrity"*, in our model represents the key to a genuine understanding of "cognition" and furthermore the CW. Moreover, we will underline the fundamental role of self-identity and consciousness as essential concepts for an adequate model of the mind.

Related to CW is cognitive security, a notion equally ambiguous that was approached by experts in various fields, from informational warfare to communication and security studies. Cognitive insecurity was interpreted in many ways, from a danger for the military decision-making process (altering the OODA loop), to a pervasive symptom of our current society's evolution.

Approached from the perspective of security studies, cognitive security might be considered one of the instances of the shift made by non-conventional schools of thought, such as Copenhagen school, critical theory, or human security, towards psychosocial dimensions of security. Thus, cognitive security marks a net departure from the structured violence paradigm, to unstructured, psychological violence.

Security is an ambiguous term and generically means to be safe from something that might harm, from something (material or not) labelled as a threat. Hence, how *"something"* gets the label *"threat"* and further, how these threats are anticipated is essential for a good explanation of cognitive security, opening the debate on who might be responsible for labelling a threat in the cognitive realm, furthermore, what are the resources to deal with such threats.

With this inquiry, we open our own perspective on what should be considered cognition and what cognitive security should be about. We will indicate what could stand as the threshold between malign and benign influence for a better understanding of CW.

Our approach starts with recognising the intrinsic limitations of the standard cognitive paradigm, namely the reductionist character of it. By isolating the so-called *"cognitive"* functions (attention, memory, reasoning, perception) from other processes of the mind, the cognitive approach ignores some salient, mostly unconscious, *underlying* processes, more significant than *"thinking"*, like creating the experience of self-continuity[4], maintaining the stability of identity, or searching for the meaning of one's existence. These are all-encompassing psychic processes that encapsulate and subordinate cognition. Moreover, the cognitivist approach ignores the instrumental role of cognition. To understand or to know are not ends in themselves but play an adaptive role for humans in natural contexts, both in terms of usefulness/practicality, and satisfaction.

Departing from this narrow perspective, our interpretation of *"cognition"* and furthermore on cognitive security is shaped by a complex, holistic approach, one that grants the fundamental explanatory role to consciousness as an integrative, super ordinate phenomenon. While recognising the role of perception in creating a model of the real world, we must acknowledge the fundamental role of the body (Damasio, 2006) as well in creating this model of the external world and in the generation of consciousness phenomena. If we want to understand *how* people think, as one of the definitions of CW suggests, we hypothesize that one should look for deeper mental processes.

The obvious, next step is to introduce the role of emotions, not only as a necessary condition for thinking, but as the very essence of consciousness (Solms, 2021). While in the orthodox literature, emotions or affects have a parasitical role for *"cognition"*, as threats to its integrity, we adopt the view that cognition is infused by emotions, determining the *"qualia of consciousness"* (Solms, Friston, 2018, p. 3) and implicitly of thinking. Pertaining to consciousness itself, affect could be defined as the means by which organisms register their own states (Damasio, 2010). As neuroscience has proved, without the subcortical projections coming from the upper brainstem, the neocortex, the seat of cognition, would stop (Solms, 2013, pp. 5-19).

With this new perspective on *"cognition"*, we can develop a more refined model of what might constitute a threat to it. Therefore, we propose to substitute cognition, as the referent object of security, with consciousness which reunites

[4] The relevance of this process is indirectly underlined by Anthony`s Giddens expression of *"ontological security"*. In Giddens, Anthony. *"Modernity and self-identity". Social Theory Re-Wired*. Routledge, 512-521.

both affective and rational, cognitive aspects of mind. By doing so I hope also to clarify the relevance of the *awareness* notion, described as the panacea in almost all disinformation papers, suggesting that awareness means more than being mindful of something, but rather it contains an anticipatory and predictive mental stance.

Consciousness is the most complex and bewildering phenomenon in the Universe, the object of study for neuroscientists, psychiatrists, and physicists. Some theories claim to solve Chalmers' *"hard problem of consciousness"* (Chalmers, 2017, pp. 32-42), the leading ones being Global Workspace Theories (GWT) (Baars, 2005, pp. 45-53) or Integrated information theory (IIT) (Tanoni, 2012, pp. 56-90). However, the last and most promising theories that best support the aim of this paper are Karl Friston's active inference theory (Parr, Pezzulo, Friston, 2022) and Mark Solms' (2021) view on the source of consciousness. These two theories combined have, in my view, the biggest explanatory potential, to date, for what mental states are, and what is the function of consciousness. In what follows, I will present the relevance of these theories for cognitive security, and implicitly for the conceptual development of cognitive warfare.

Any individual needs to survive and adapt to the environment, which is nowadays increasingly complex and unpredictable. To do so, individuals must generate predictive models of the environment, taking actions that are guided by an expected value, or as it is known in statistics, by the Bayesian process of active inference (Friston et al., 2023, pp. 1-29) which further leads to homeostasis and survival, as the most basic human needs. Active inference is the necessary process deployed by any ergodic system (including humans) to minimise free-energy and avoid surprising states (Solms, Friston, 2018, p. 5). The principle of minimizing free energy is to reduce the gap between expectations and sensory inputs (Friston, Kilner, Harrison, 2006, p. 5). As such, the fundamental rule for human *"cognition"* is to minimise prediction error, the incongruity between the expectations that result from internal models of the environment and the real world. Any individual, as a living organism, survives within the environment when they reduce the prediction error, *"either by changing their internal models of the world or through action upon the environment itself"* (Solms, 2021, p. 207).

This theory indicates that the brain has an active role in the construction of reality, explaining the subjective contribution to the perception of the environment. So, active inference might be considered the neuroscientific background for humanistic theories, such as phenomenology, symbolic interactionism, and constructivism, models that support the idea that individuals are not passive in their interaction with the world, but actively generate the image of the environment. Moreover, it underpins the hermeneutical, interpretative stance of individuals situated in a communicative situation.

By trying to predict what the sensations are revealing, the brain continuously makes two things, updates/adjusts internal beliefs, and generates inferences and hypotheses. These hypotheses are mental fantasies that best explain the sensorial influx, an aspect that once again indicates the limitation of the *"cognitivist"*, rationalist approach.

Within the active inference theory, precision is an important concept. Precision is a key determinant of free energy minimisation and the enabling – or activation – of prediction errors, it is how the brain represents its degree of confidence in a given source of sensory evidence (Ib., p. 201). Greater precision means minimizing surprise, thus reducing the uncertainty. According to Solms, precision can be also modulated, or optimised by learning from experience (Ib., p. 200), specifically by continuously updating our internal, mental generative model.

Precision optimidation is *"how multiple error signals converging on the PAG were prioritized in the first place, bringing the most salient need to affective awareness, leading to a series of unfolding choices in an expected context, guided by expected precisions"* (Ib., p. 203). Again, underlying the fundamental role of emotions, PAG[5] is described as *"synencephalic bottleneck where action perception and affect come together, where the choices are made about what to do next"* (Merker, 2007, pp. 63-134).

As theorised by Solms and Frinston, precision has two varieties, interoceptive (affective consciousness) and exteroceptive (perceptual consciousness) which are normally conceptualised as goal selection (or motivation) and attention (Solms, Friston, 2018, p. 12). That explains why consciousness itself nothing is more or less than the optimization of precision with respect to free energy (Ib., p. 9). We try to predict the future and this process inevitably induces the feeling of uncertainty.

Returning to the definition of CW, and to our suggested substitution of cognition with consciousness, as the referent object of informational-psychological attacks, we advance a new definition of CW. As such, CW refers to all forms of influence that are purposively designed to alter the precision optimisation mechanism. This entails that through the means of CW the perpetrators aim to increase the amplitude of prediction errors, thus, maximising free energy, a change that pertains to selfhood and identity. This is done by preventing individuals from learning from experience, that is to update their internal generative model. Here's why individuals are unable to make adaptive predictions of the environment, their best guesses about the environment are imprecise, inadequate, and maladaptive. In the absence of precision, we are in the realm of un-reflected thinking, of automated, repetitive actions. Additionally, elements of lived experience remain unelaborated, unintegrated, and further used in the projective process[6] toward the societal milieu.

Unable to adequately infer future states of the environment, individuals become prisoners of a perpetual past that cannot find its development into the future, raising the feeling of uncertainty (towards external background), and incompetence on understanding the environment (toward himself). This approach on mind has several implications for CW. First and foremost, clearly suggest abandoning the cognitive fallacy (Solms, 2021, p. 213), the deeply nested belief that the neo-cortex, cognition, rationality should be prevalent in explaining consciousness and human mental functioning. Secondly, it strongly emphasises the essential role of the affect, prior beliefs, and long-term memory in the perception of reality, but also the role of fantasies. More closely to the commonly used language, the imaginary has a role just as important as rational thinking.

Returning to the question of what cognitive security might be, we have the same approach that underlines the role of a subjective, internal milieu, at the expense of physical, and external features. As such, we suggest the use of the notion "*se-curitas*", which denotes *"a mental state of calm that must be distinguished from salus, which represents safety from physical harm"* (Hamilton, 2013, p. 51), an interpretation that resonates with the Greek notion of *ataraxia*, and clearly suggests the psychological aspect of security. According to these interpretations, *securitas* is obtained through self-care and self-reflection. Through self–knowledge, individuals obtain a form of peacefulness in front of unforeseeable dangers, gaining resilience and tolerance to frustration. *"To secure the self, one must care for the self"* (Ib., p. 54), that is to turn the attention toward the inside, to be aware of our internal model of the world, and how accurately this model predicts future states of the environment.

[5] PAG – Periaqueductal gray formation (along with superior colliculi and midbrain locomotor region) is a sub-cortical brain formation, considered at the centre of decision-making.

[6] Defensive mechanism of attributing negative emotions, and beliefs to someone else in order to protect themselves from inner conflicts and tensions. Blackman, J. *101 Defenses: How the Mind Shields Itself*, Taylor&Francis, USA-UK, 2004, p. 53.

Returning to the challenge of how *"something"* is labelled as a *"threat"*, furthermore how these threats are anticipated, it becomes obvious that one should permanently scrutinise what is the precision of his predictions based on his internal model of the world. So, the question *"How a piece of information becomes a threat"* must turn into *"How my mind is moulded by this information"*.

As it becomes obvious, the most responsible entity is the individual himself, and the resources involved are self-regulation, self-reflection or critical thinking. Although an individual has the privileged access to his own mind, formal and informal institutions must also cope with educating people for more reflexivity. However, this educational process might fail, as can collide with enduring socio-economic tendencies and forces that encourage narcissism/self-centeredness and inhibit elaborate, complex thinking, self-knowledge, or tolerance to frustration[7], furthermore tends to desubjectivise the individuals and create mental vulnerabilities to hostile influences.

CONCLUSIONS

In the current contested environment, the hybridity of confrontation has turned informational-psychological actions into the weapon of choice. The increasing power to engage the human psyche through almost unlimited accessibility and greater susceptibility to various forms of messages renders cognitive warfare and cognitive security a national-state priority. Defending the necessity for this new domain, we choose to analyse in this paper the current development of the fresh concept of *"cognitive warfare"* and offer a new approach to it, starting with the limitations induced using the notion of *"information"* and the cognitive paradigm. We suggest that notions such as information–cognition implicitly encourage the analogy of brain-computer, which furthermore isolates the individual from his cultural and historical context, and induces the appearance of neat, objective knowledge. As cognition is only a fraction of mental activity, subordinated to other higher psychological processes, all definitions centred around the word cognition are at least partial, if not misleading. Informational, cognitive-based discourse on CW although scientifically rigorous, cannot capture the mind's main features, agency, intentionality, and subjectivity. So, escaping from the cognitive spell is essential to catch up with the enemy's refined knowledge and efficiency in informational-psychological warfare.

[7] For a more elaborated and complex perspective, see Bollas, Christopher. *Meaning and Melancholia: Life in the Age of Bewilderment*. Routledge, 2018.

Departing from the classic cognitivist view, we used Friston's active inference theory and Solms' theory on consciousness to develop a more nuanced and complex understanding of mind and CW. Aiming to consider all mental aspects, not just cognition, we introduced active inference theory as applied to the study of mind, therefore taking consciousness as the referent object of security. Underling the subordinate role of cognition to other higher-order mental processes (homeostasis, preserving identity stability, meaning-making) we advanced a more refined model for what the security of mind should be. If the fundamental rule for humansto survive is to minimize prediction error, and the incongruity between the expectations that result from internal models of the environment and the real world, then CW must be defined in relation to this process. As such, as a novel interpretation, CW refers to all forms of influence that are purposively designed to alter the precision optimisation mechanism. This entails that through the means of CW the perpetrators aim to increase the amplitude of prediction errors, thus maximizing free energy, a change that pertains to selfhood and identity. This is achieved by preventing individuals from learning from experience, that is to update their internal generative model. As one of the definitions of CW suggests an influence on how people think (and not what people think), we consider that we formulate an answer to this proposal.

Individuals become unable to make adaptive predictions, their best guesses about the environment are imprecise, inadequate, and maladaptive. Our model strongly emphasises a shift from a theoretical perspective where individuals passively receive external stimuli, to a view that entails that they are involved in the inference process, actively generating hypotheses and predictions based on affects and mental fantasies.

Cognitive security must shift then from truth-telling strategies to an educational process that aims for self-reflection and self-knowledge to understand our internal model of the world, our beliefs, and emotions, and our fantasies. In terms of active inference theory, CW prevents individuals from revising their predictions, admits the error, and further updates their model of the world. Consequently, the cognitive security focus should move from what people know, to how people should inquire what they know in terms of the complexity and plasticity of their own internal model of the environment. Building psychological resilience should aim at developing the ability to tolerate uncertainty, frustration, and contradictions.

Although we find appropriate the initiative for this new domain of CW, we must also recognise a vulnerability. By *"weaponising"*, as the title of this paper suggests, and attributing to an eminently military entity (NATO), the research effort on CW is at the risk of being labelled as purposively militaristic, hostile, and aggressive. A language infused with military jargon has little, if any, contribution to an adequate understanding of CW and raises concerns about its legitimacy, as another expression of a *"securitization approach"* (Buzan, Waever, de Wilde, 1998, p. 25), of a need to use extraordinary means to avoid, apparently, an existential threat for the survival of democratic societies.

BIBLIOGRAPHICAL REFERENCES:

1. AJP 10.1 (2023). Allied Joint Doctrine For Information Operations Edition.
2. Allen, P.D., Gilbert, D.P.Jr. (2009). *The Information Sphere Domain – Increasing Understanding and Cooperation*. *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press, pp. 132-142.
3. Aronson, E. (1992). *The Return of the Repressed: Dissonance Theory Makes a Comeback*. In *Psychological Inquiry,* 3.4, pp. 303-311.
4. Baars, B.J. (2005). *Global Workspace Theory of Consciousness: Toward a Cognitive Neuroscience of Human Experience*. Progress in brain research, 150: 45-53.
5. Backes, O., Swab, A. (2019). *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. Harvard Kennedy School*, https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states, retrieved on 14 September 2023.
6. Baudrillard, J. (1994). *Simulacra and Simulation*. University of Michigan Press.
7. Bernal, A. et al. (2020). *Cognitive Warfare: An Attack on Truth and Thought*. NATO andi Johns Hopkins University: Baltimore MD, USA, p. 10.
8. Blackman, J. (2004). *101 Defenses: How the Mind Shields Itself*. Taylor&Francis, SUA-UK.
9. Bollas, C. (2018). *Meaning and Melancholia: Life in the Age of Bewilderment*. Routledge.
10. Bolt, N., Haiden, L. (2019). *Improving NATO Strategic Communications Terminology*. NATO Strategic Communication Centre of Excellence, p. 43.
11. Buzan, B., Wæver, O., de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.
12. Byung-Chul, H. (2017). *In the Swarms-Digital Prospects*, The MIT Press.
13. Chalmers, D. (2017). *The Hard Problem of Consciousness. The Blackwell companion to consciousness*, 32-42.
14. Claverie, B., Du Cluzel., F. (2022). *„Cognitive Warfare": The Advent of the Concept of „Cognitics" in the Field of Warfare*, 2-1.
15. Claverie, B., Prebot, B., Buchler, N., Du Cluzel, F. (2021). *Cognitive Warfare. First NATO Scientific Meeting on Cognitive Warfare*. Bordeaux, June, NATO-CSO-STO.
16. *Cognitive Warfare* (2021). First NATO scientific meeting on Cognitive Warfare. Bordeaux, 21 June. (see nr. 15).

17. *Cognition Workshop Innovative Solutions to Improve Cognition*. NATO Innovation Hub (2021), https://www.innovationhub-act.org/sites/default/files/2021-07/210601%20Cognition%20Workshop%20Report-%20v3.pdf, p. 3, retrieved on 3 August 2023.
18. Collman, A. (2015). *Oxford Dictionary of Psychology*. Oxford University Press, p. 143.
19. Dahl, A.B. (1996). *Command Dysfunction: Minding the Cognitive War, Technical Report (AU's School of Advanced Air and Space Studies)*, https://apps.dtic.mil/sti/pdfs/ADA360756.pdf, retrieved on 10 September 2023.
20. Damasio, A. (2006). *R. Descartes' Error*. Random House.
21. Damasio, A. (2010). *Self Comes to Mind*. New York. Pantheon.
22. Du Cluzel. F. (2020). *Cognitive Warfare*. Innovation Hub – November.
23. Fridman, O., Kabernik, V., Pearce, J.C. (2019). Eds. *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*. Lynne Rienner Publishers, Incorporated.
24. Friston, K. et al. (2023). *The Free Energy Principle Made Simpler but Not too Simple. Physics Reports* 1024, pp. 1-29.
25. Friston, K., Kilner, J., Harrison, L. (2006). *A Free Energy Principle for the Brain*. *Journal of Physiology*, Paris 100, pp. 70-87.
26. Forgas, J.P. (2013). *"The Affect Infusion Model (AIM): An Integrative Theory of Mood Effects on Cognition and Judgments".* Theories of Mood and Cognition. Psychology Press, pp. 99-134.
27. Giddens, A. (2016). *Modernity and Self-Identity*. *Social Theory Re-Wired*. Routledge, pp. 512-521.
28. Gigerenzer, G., Hoffrage, U. (1995). *How to Improve Bayesian Reasoning without Instruction: Frequency Formats*. In *Psychological Review*, 102.4, 684.
29. Hamilton, J.T. (2013). *Security: Politics, Humanity, and the Philology of Care*. Princeton University Press.
30. Le Guyader, H. (2022). *Cognitive Domain: A Sixth Domain of Operations*. Bernard Claverie, Baptiste Prébot, Norbou Buchler, François du Cluzel (2022). *Cognitive Warfare: The Future of Cognitive Dominance*. NATO Collaboration Support Office, pp. 3, 1-5; 978-92-837-2392-9.
31. Masakowski, Y.R., Blatny, J.M. (2023). *Mitigating and Responding to Cognitive Warfare*. NATO STO Technical Report RDP STO-TR-HFM-ET-356.
32. Merker, B. (2007). *Consciousness without a Cerebral Cortex: a Challenge for Neuroscience and Medicine*. Behavioral and Brain Sciences, vol. 30, pp. 63-134.
33. *NATO Booklet* (2023). ACT 20th Anniversary, p. 26, https://www.act.nato.int/wp-content/uploads/2023/06/NATO-booklet-2023-LR.pdf, retrieved on 23 July 2023.
34. Noon, M. (2018). *Pointless Diversity Training: Unconscious Bias, New Racism and Agency*. *Work, Employment and Society,* 32, pp. 198-209.
35. Pappalardo, D. (2022). *Win the War Before the War? The French Perspective on Cognitive Warfare. War on the Rocks*, 1 August, https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/, retrieved on 23 July 2023.

36. Parr, T., Pezzulo, G., Friston, K.J. (2022). *Active Inference: The Free Energy Principle in Mind, Brain, and Behavior*. MIT Press.
37. Patrick, A.D., Gilbert, D.P. Jr. (2009). *The Information Sphere Domain – Increasing Understanding and Cooperation. The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press, 132-142, p. 5.
38. Ryabchuk, V., Nichipor, V. (2012). *"Prognozirovaniye i Predvideniye v Sisteme Planirovaniya Operatsii i Obshchevoyskovogo Boya [Forecasting and Prediction in Operational Planning Systems and Combined Arms Combat]"*. Armeiskii Sbornik [Army Digest], nr. 10, October, p. 38.
39. Scher, S.J., Cooper, J. (1989). *Motivational Basis of dissonance: The Singular Role of Behavioral Consequences*. *Journal of Personality and Social Psychology* 56.6; 899.
40. Seth, A. (2021). *Being You: A New Science of Consciousness*. Penguin.
41. Solms, M. (2021). *The Hidden Spring: A Journey to the Source of Consciousness*. Profile books.
42. Solms, M. (2013) *The Conscious Id*. *Neuropsychoanalysis* 15.1, pp. 5-19.
43. Solms, M., Friston, K. (2018). *How and Why Consciousness Arises: Some Considerations from Physics and Physiology. Journal of Consciousness Studies*, 25.5-6; 202-238.
44. Steele, C.M., Spencer, S.J., Lynch, M. (1993). *Self-image Resilience and Dissonance: The Role of Affirmational Resources*. *Journal of Personality and Social Psychology* 64.6, 885.
45. Takagi, K. (2022). *The Future of China's Cognitive Warfare: Lessons from the War in Ukraine. War on the Rocks*, 22 July, https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/, retrieved on 23 August 2023.
46. Tononi, G. (2012). *The Integrated Information Theory of Consciousness: An Updated Account*. Archives italiennes de biologie 150.2/3; 56-90.
47. Underwood, K. (2017). *Cognitive Warfare Will Be Deciding Factor in Battle: Lt. Gen. Stewart's Remarks at DoDIIS17*. In *Signal*, The Cyber Edge.
48. Vaidis, D.C., Bran, A. (2019). *Respectable Challenges to Respectable Theory: Cognitive Dissonance Theory Requires Conceptualization Clarification and Operational Tools*. In *Frontiers in Psychology*, 10, 1189.
49. https://apps.dtic.mil/sti/pdfs/ADA360756.pdf, retrieved on 22 August 2023.
50. https://plato.stanford.edu/entries/truth, retrieved on 22 August 2023.
51. https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/, retrieved on 15 September 2023.
52. https://www.innovationhub-act.org/sites/default/files/2021-07/210601%20Cognition%20Workshop%20Report-%20v3.pdf, retrieved on 22 August 2023.
53. https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/, retrieved on 12 August 2023.
54. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind//Allied Command Transformation, retrieved on 22 August 2023.
55. https://www.act.nato.int/wp-content/uploads/2023/06/NATO-booklet-2023-LR.pdf, retrieved on 22 August 2023.

56. https://www.afcea.org/content/cognitive-warfare-will-bedeciding-factor-battle, retrieved on 26 July 2023.
57. https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states, retrieved on 4 July 2023.
58. https://www.futurelearn.com/info/courses/what-is-a-mind/0/steps/5177, retrieved on 22 August 2023.
59. https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf, retrieved on 3 September 2023.
60. https://www.merriam-webster.com/dictionary/cognitive, retrieved on 5 September 2023.
61. https://www.oxfordlearnersdictionaries.com/definition/american_english/cognition, retrieved on 5 September 2023.