The Cognitive Warfare Concept

Bernard Claverie[1], François du Cluzel[2]

The views expressed in this article are those of the authors and do not reflect the official views of their respective institution.

> *"Cognitive warfare is now with us. The main challenge is that it is essentially invisible; all you see is its impact, and by then ... it is often too late."*

Cognitive warfare is now seen as its own domain in modern warfare. Alongside the four military domains defined by their environment (land, maritime, air and space) and the cyber domain that connects them all, recent events that upset the geopolitical balance of power have shown how this new warfare domain has emerged and been put to use.

It operates on a global stage, since humankind as a whole is now digitally connected. It uses information technology and the tools, machines, networks and systems that come with it. Its target is clear: our intelligence, to be considered both individually and as a group.

Attacks are defined, structured and organized to alter or mislead the thoughts of leaders and operators, of members of entire social or professional classes, of the men and women in an army, or on a larger scale, of an entire population in a given region, country or group of countries. Cognitive aggression is boundless. It can have a variety of objectives and will adapt itself to other strategies being used: territorial conquest (a bordering region, peninsula or group of islands for instance), influence (elections, stirring up popular unrest), service interruptions (national or local administrations, hospitals, emergency services, and sanitation, water or energy supplies) or transportation (airspaces, maritime chokepoints…), information theft (through involuntary disclosure or the sharing of passwords…) etc.

[1] - Bernard Claverie is a University Professor, Honorary Director and Founder of the *Ecole Nationale Supérieure de Cognitique* at the Bordeaux *Institut Polytechnique* and a researcher at the *Centre National de Recherche Scientifique* (CNRS) — UMR5218 — Bordeaux University.

[2] - François du Cluzel is a retired Lieutenant-Colonel of the French Army and Head of Innovative Projects within Allied Command Transformation Innovation Hub in Norfolk Virginia.

Cognitive warfare is the art of using technological tools to alter the cognition of human targets, who are often unaware of any such attempt - as are those entrusted with countering, minimizing, or managing its consequences, whose institutional and bureaucratic reactions are too slow or inadequate.

A Few Definitions

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 distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels.

This is obviously related to the concept of cyber warfare that uses digital information tools to gain control, alter or destroy said tools. However, cognitive warfare goes beyond information to target what individual brains will do with this information. It therefore extends beyond the human consequences of cyber warfare involving computer engineering, robotics and programmes; a cognitive effect is not a by-product of action, but its very objective.

Though technological tools are a medium towards an effect, this *objective* is independent of the technologies used to achieve it. One way of thinking about it is as a "psychological-social-technical warfare" on the one hand and of a form of "influence warfare" on the other, using cyber means. In the military context specifically, it involves the use of a strategy intended to carry out a combat, surveillance and/or security actions.

Other definitions exist for related concepts. 'Cognitive combat' is related to the actual, local and temporary use of tactical tools to affect cognition. This within a larger strategy designed to engage cognitive targets. For offensive actions, it is characterized by an approach centred on harassment, the systematic exploitation of weaknesses, whereas in a defensive posture it involves the development of resilient and preventative capabilities using similar tools. The notion of "cognitive conflict" is a notion that could be utilized when the context is generalized and the confrontation of cognitive processes is the rule. But that notion is still to be theorized.

Cognitive Warfare is all around us.

Cognitive Warfare is already being used, with more or less success and not necessarily under that name, by a number of state and non-state players, institutions or companies, including terrorist organizations, aggressive religious movements, etc. These actors include specialized and highly-competent units working for digital intelligence services, as well as industry agencies and companies engaged in competition with others or in the more routine area of marketing and manipulation of potential clients. In all these cases, the object is to dominate, establish one's superiority, or even conquer and destroy. Today these practices have reached such a level that political leaders can no longer ignore their importance.

The term « Cognitive Warfare » has been used with that meaning in the United States since 2017, to describe in particular the modes of action available to a state or influence group seeking to "manipulate an enemy or its citizenry's cognition mechanisms in order to weaken, penetrate, influence or even subjugate or destroy it". While that broad mission has always formed a part of the art of war, here we have a new discipline that requires further elucidation. It is the combination of the newer cyber techniques associated with information warfare and the human components of soft power, along with the manipulation aspects of psychological operations (or PSYOPS). They usually involve a biased presentation of a reality, usually digitally altered, intended to favour one's own interests. New communication tools now offer infinite possibilities, opening the way to new methods and new objectives. This increased complexity should encourage potential victims to develop a constant posture of resilience, even if in most cases, victims usually realize they were attacked too late.

This approach to Cognitive Warfare has caught the eye of armed forces across the world and includes both strategic and operational aspects, some of which are more developed than others. It is not currently covered by established ethical considerations and doctrines. Cognitive Warfare expanded considerably with the arrival of digital strategic decision-making assistants, new operational domains and the invasion of big data and analytics, in the realm of information, wargaming and the conduct of operations. It is now spreading to all areas where digital information is used, including the quiet implementation of offensive and defensive uses, cognitive attrition, and defensive measures intended to protect target populations. It is a mix of well-thought out attack processes as well as counter and preventative measures.

Theorization

New theories are being developed, including those dealing with resilience or the weaknesses of neurosciences, the exploitation of cognitive biases and the likelihood of cognitive errors, the manipulation of perceptions, how our attention spans can be overwhelmed or steered, and cognitive stresses induced. All of these have predictable consequences on our mental acuity, social relations and motivations and on the efficiency of organizations.

These early conceptual efforts caught the attention of many researchers and military thinkers. Including, among many others, neuro-ethicist James Giordano[3] who has described the brain as the site for the battlefields of the 21st century and studied the *weaponization of neuroscience*s. General Goldfein[4] has stated that we have moved on to wars of attrition to wars of cognition, Colonel Banach[5] has talked about the idea of virtual warfare, Lieutenant General Stewart[6] of the Defense Intelligence Agency, saw modern warfare as a cognitive battleground, and General Desclaux[7] described the command and control strategic processes as a cognitive triangle involving knowledge dominance, cyber confidence and decision superiority, all of which serving to guide strategy to achieve the commander's objectives. As the cognitive aspects of the planning and conduct of is operations is becoming increasingly vital, Colonel Remanjon of NATO's Allied Command Transformation has studied whether the human brain is now the ultimate battlefield.

And the theoretical underpinnings of the sixth domain of warfare have recently been developed, linking the *technium* to the *noosphere*[8] seen as the

[3] James Giordano is a professor in the Georgetown Department of Neurology in Washington D.C. and the Director of the Neuroethics Studies Programme at the O'Neill-Pellegrino Center for Clinical Bioethics.

[4] David Goldfein was a former general and Chief of Staff of the US Air Force, member of the Joint Staff and a military advisor in the Council of National Security and to the Secretary of Defense and President of the United States.

[5] Steve Banach is a colonel in the US Army and former director of the School of Advanced Military Studies (SAMS) at Leavenworth (Kansas, USA).

[6] Vincent R. Stewart is a former Lieutenant General of the Marine Corps and Director of the Defense Intelligence Agency (DIA).

[7] Gilles Desclaux is a retired Lieutenant General in the French Air Force. He commanded air operations during the war in Lybia and is now a frequent contributor to C2 work being conducted in industry.

[8] As defined by Kelly (2011): all the information available to human brains.

global representation of human intelligence as mediated through technologies, in a recent book on Cognitive Superiority by Dean S. Hartley[9] and Kenneth Jobson[10] (2021).

Basic Principles

Cognitive Warfare is where all the elements of information warfare - to include the operational aspects of psychology and neurosciences, based on systemics and complexity - for military action. It sits at the intersection of two operational fields that hitherto were managed separately: PSYOPS and influence operations (soft power) on the one hand, and cyber operations (cyber defence) intended to degrade or destroy physical information assets on the other. This intersection makes it possible to unite concepts and points of views from different scientific, military or intelligence communities of interest, bringing about an interdisciplinary approach to how new technologies impact humankind.

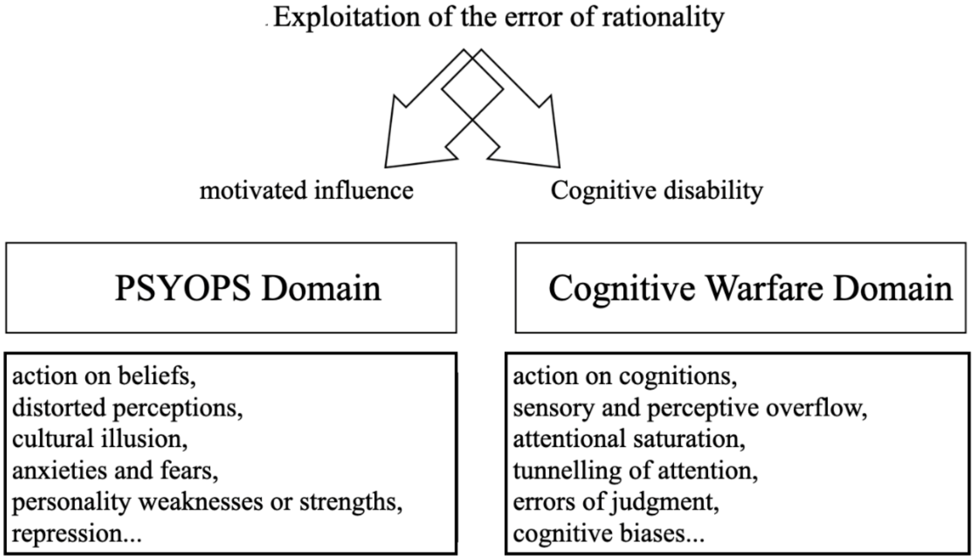


Fig.1:Differences between cognitive warfare and PSYOPS (including, in broad terms actual psychological operations and other non-kinetic actions such as influence operations and civil-military cooperation (CIMIC)

The main goal is not to serve as an adjunct to strategy or to defeat an enemy without a fight, but to wage a war on what an enemy community thinks, loves or believes in, by altering perceptions. It is a war on how the enemy thinks, how its minds work, how it sees the world and develops its conceptual thinking. The effects sought are an alteration of worldviews, and

[9] Dean S. Hartley III Director of Hartley Consulting at Oak Ridge (TN, USA) and honorary president of a number of other consulting firms.

[10] Kenneth O. Jobson is a psychiatrist and the creator of the *International Psychopharmacology Algorithm,* and is particularly active in biotechnologies.

thereby affect their peace of mind, certainties, competitiveness and prosperity.

The stated objective is to attack, exploit, degrade or even destroy how someone builds their own reality, their mental self-confidence, their trust in processes and the approaches required for the efficient functioning of groups, societies or even nations. Although its technical aspects (cyber) are somewhat different, it is a companion to psychological operations (PSYOPS).

Levels of Action

Cognitive Warfare can be studied from two points of view: a global one and one based on the available tools. The first is intended to contribute to a culture which seeks to manipulate minds or on the other end of the spectrum to build up resilience and global security. It is both intended to inform and train those most likely to be targeted by ill-intentioned actions or intentions, and use cognitive tools to counter such actions.

The cognitive dimension is based both on a knowledge of the psychology of players involved, of the psychosociology of specific populations or groups, and the influence of culture on the decision-making and rationality of various players. The second level is related more specifically to various fields of cognition, including for instance the decision/indecision dichotomy, cognitive errors and biases, perceptions and illusions, cybernetics and the absence or loss of control, influence and soft power, psychology and cyber psychology, interactions between users and systems, robotics and drones, autonomy and the ethics associated with new technologies, motivation and loss thereof (giving up and despair), morality and the clash of values, psychology and religion, the urgency of psychiatric support in cases of post traumatic care or after someone has snapped, cybersecurity and human reliability, and the cognitive aspects of Command and Control (C2) which involve a considerable number of other considerations, including multi-domain and multicultural aspects.

A Defensive Posture

This kind of cognitive approach cannot be defined along the traditional categories of instruments of war, but rather as a tool for interfering with individual or massed targets, seeking to achieve effects at various scales, from the single person all the way to an entire social/technical environment.

These capabilities and effects can be used before, during and after kinetic actions, while remaining outside current international definitions of what constitutes an act of war. These non-kinetic actions will deliver imbalances that will benefit their stewards and hinder those targeted. But now they may become part and parcel of a global, discreet or even invisible action, or specific, precise and undetectable actions, or as only components of one or several aggressive operations, all of which requires we learn the dangers posed and how to develop defensive techniques and effective deterrent options or ways of dealing with the consequences.

Moving towards a Human Domain?

What are the consequences? The information era has morphed into a network era, since the world is increasingly defined by its interconnections. This evolution has grown more complex as our physical, digital and mental personas have merged within these human enhancement networks. They are typical of the human domain, where the ability to solve complex problems is dependent on how information is represented, understood and developed. This domain must take into account the strengths, limitations, vulnerabilities and diversity of those involved in decision-making or when applying rules and procedures.

From a defensive point of view, the challenges are many: whether they involve ensuring the cognitive security of individuals, facilitating the efficient running of state structures, establishing and maintaining cognitive superiority for decisive action or to improve competitiveness, developing and certifying the performance of intelligent systems or artificial intelligence systems intended to augment human labour, improve the collective intelligence of Human-Autonomy Teaming (HAT), improve complex and shared decision-making. Guaranteeing an advantage in the human domain will require new approaches which are better able to combine humans and technology, while managing both technical and psychological consequences.

Means of Action

Over the last twenty years or so, the design of digital tools has taken into account the differences and characteristics of users in order to encourage their spontaneous use. This has led some to think about how these guided approaches can be manipulated to allow for greater integration of human users within the system. The intention has gone from facilitating the user experience to instigating or even dictating how they behave.

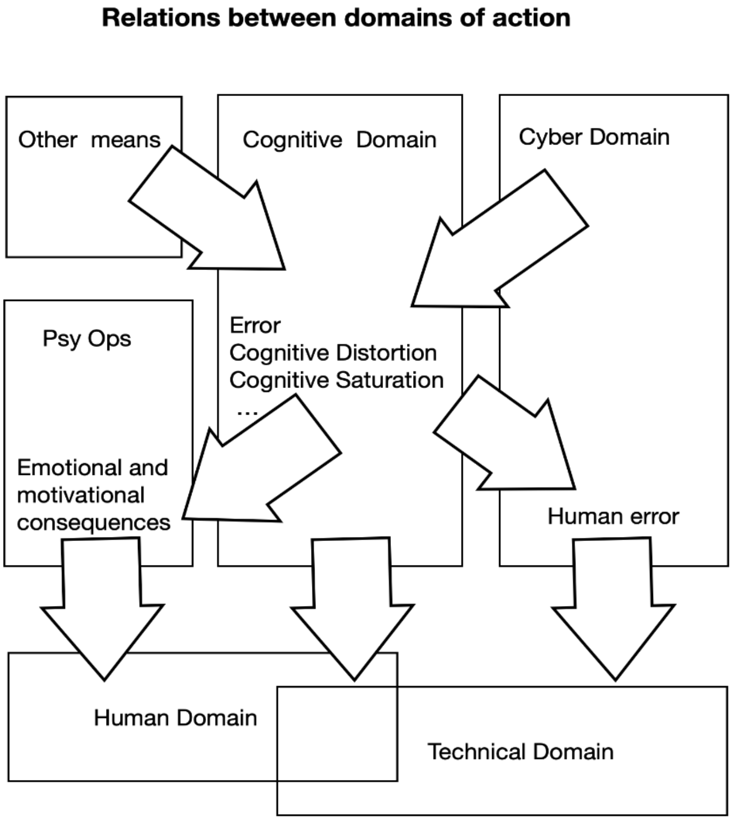


Figure 2: Complementarity of human and technical domains and how they interact with other domains

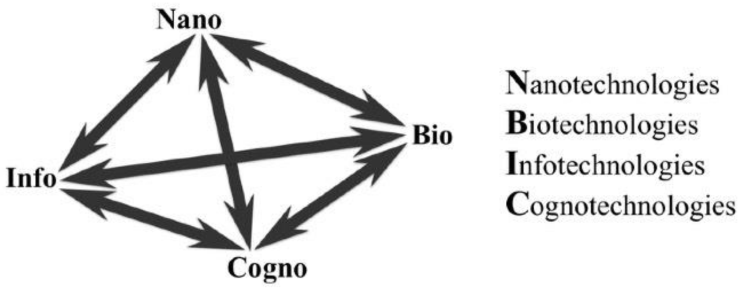
From the attacker's point of view, the most efficient action – albeit the hardest to execute– is to encourage the use of digital tools that can disrupt or affect all levels of an enemy's cognitive processes. The various decision-making stages are targeted, starting with how information is taken in, which can be overwhelmed, how it is then filtered, which can be side-stepped, by altering how representations are constructed, by influencing memory storage, leading to inadequate decisions or by paralyzing the taking of action and making it difficult to alter objectives. Each of these phases is now understood, codified or even replaced by digital tools. They can therefore be targeted.

Consequences may be found at three potential levels: (i) the influence over psychological, relationship, motivational dimensions, or by sowing doubt or consolidating certainties, or causing chronic consequences, (ii) in the cyber domain by factorizing or inducing human errors directly, to affect the network, the information it carries or human-system interfaces, (iii) or by targeting individual cognitive abilities directly, in particular those whose cognitive capabilities are chronically altered.

This kind of warfare will assume new dimensions as we develop wearable technologies and connected objects, and in particular the likely potential of the internalization of these new tools with the appearance of the augmented soldier.

Preparing the Future with Mobile Cyber Capabilities.

NBIC is a scientific project bringing together four heretofore distinct domains: nanotechnology (*nano-robot technology, nano-sensors, nanostructures, energy...),* biotechnology *(bio-genomic technology,* CRISPR-*Cas9, neuropharmacology*...), information technology *(computer science, microelectronics...*) and cognitive technology (*cognitive science and neuropsychology).* The project was formalized with the encouragement of the US Defence Department in 2002 and subsequently taken up by major international institutions and a number of nations, to bring together future technologies.



NBIC technologies tetrahedron

Figure 3: Convergent technologies as defined by the US DOD in the Roco and Bainbridge Report (2012).

The object is to encourage the development of tools and adapt or improve humans through an anthropo-technical approach to develop a hybridized man-system to meet health, security, defence objectives and prepare them for specific bioenvironments (space, sea, deserts, etc.). Today, this project has led to the partial convergence of domains, mostly through pairing information technology and health nanotechnologies, new chemical cognition enhancers, embedded electronics, etc. Ultimately, the goal is that it will lead to an augmented human operator (or even a hybrid one), injected with amplifying substances or nanotechnologies, providing informational resilience and superiority. A number of enhanced soldier projects are already underway.

Information, of course, can imply cyber threats and information distortion or manipulation. And a connected brain, in particular a soldier's connected brain, will lead to offensive and defence forms of 'cognitive warfare'. Many writers have already imagined what threats might emerge. Most of them remain science-fiction, but some projects are benefiting from real resources, programmed and in some cases tested, with for instance neurocomputing implants and perception augmenting technical hybrids (vision and hearing), or even genomic modifications.

Beyond traditional and existing threats associated with cognitive warfare as used by allied or competing nations, or those that might be developed by unofficial entities (such as terrorists or entities seeking cultural or religious domination), we need to think about the future of NBIC, and how it might influence human cognition, by distracting, saturating or even taking over and modifying objectives. We should also mention the issue of these implants' obsolescence and their exploitation.

Conclusion

The cyber world is now all-encompassing, ever-present and no decision or action can be executed without the tools it provides. This obviously affects the cognition of those who use them and will impact individuals and groups, at all levels, both psychologically, with human consequences, and technically when human errors impact systems. This is a fast-growing domain and new paths are constantly pushing back the limits of our knowledge and what potential uses might be developed. It is imperative we try to anticipate threats born of future technologies and learn more about those being developed today.

These threats are increasingly common and their consequences, more often than not, will have global repercussions, requiring NATO and its member Nations to think about cognitive warfare's varied dimensions. To anticipate them will mean acquiring the means to go beyond a reactive posture. If militaries remain reactive, it will lead to losing the technological initiative that is so vital to military strategy today.

Bibliography

Claverie, B. (2021). *Des théories pour la cognition : Différences et Complémentarité des Paradigmes*. Paris (France): L'Harmattan.

Cole, A., Le Guyader, H., (2020). *Cognitive : a 6th Domain of Operations*. Norfolk (VA, USA) : Innovation Hub, NATO ACT Edition.

Devilliers, L. (2021). "Désinformation : les Armes de l'Intelligence Artificielle". *Pour La Science*, 523, 26-33.

Remanjon, J. (2021), " Le cerveau sera-t-il l'ultime champ de bataille?", Revue de la Défense Nationale.

Hartley, D.S.III, Jobson, K.O. (2021). *Cognitive Superiority: Information to Power*. New-York (NY, USA): Springer.

Kelly, K. (2011). *What technology wants*. New York (NY, USA): Penguin Books. ISBN: 978-0143120179.

Roco, M.C., Bainbridge, W.S. (2003). *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. New-York (NY, USA) : Springer-Verlag.

Underwood K. (2017). "Cognitive Warfare Will Be Deciding Factor in Battle: Lt. Gen. Stewart's remarks at DoDIIS17". *Signal, The cyber edge*. https://www.afcea.org/content/cognitive-warfare- will-be-deciding-factor-battle. https://youtu.be/Nm-lVjRjLD4.

Wall, T. (2010). "U.S. Psychological Warfare and Civilian Targeting". *Peace Review* 22, 3: 288– 294.