Cognitive Domain: A Sixth Domain of Operations

Hervé Le Guyader

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

www.sto.nato.int

Cognitive Warfare: The Future of Cognitive Dominance

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021.
Symposium organized by the Innovation Hub of NATO-ACT and ENSC,
with the support of the French Armed Forces Deputy Chief of Defence,
the NATO Science and Technology Organization / Collaboration
Support Office, and the Region Nouvelle Aquitaine.

Scientific Editors
B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel.

Chapter 3 – COGNITIVE DOMAIN: A SIXTH DOMAIN OF OPERATIONS?

Hervé Le Guyader[1]

"The sixth domain, a domain where influence and mind control make it possible for the adversary to avoid frontal confrontation, always costly, often risky."

3.1 INCEPTION OF A SIXTH DOMAIN

The concept for a sixth domain of operations emerged at the beginning of 2020. It was introduced as the first recommendation in the essay "Weaponization of neurosciences" (Le Guyader, 2000) written for the "Warfighting 2040" study ran by Allied Command Transformation (ACT).

Its executive summary offered the three following recommendations:

- "Human mind" should be NATO's next domain of operations;
- AWACS successor must address Nanotechnology, Biotechnology, Information technologies, Cognitive technologies (NBIC); and
- Global security is what's at stake today.

After this first publication, ACT asked for a follow up essay to be written in the same so-called "FICINT" (intelligent fiction) style, to further develop the idea for a sixth domain of operations to be added to the five existing ones (land, sea, air, cyber, space).

A second essay, "Cognitive: A Sixth Domain of Operations" was then published in a bilingual (English/French) version (Cole and Le Guyader, 2020; Le Guyader and Cole, 2020).[2]

With this essay, part of the larger "Cognitive Warfare" study led by ACT's Innovation Hub, the concept of this sixth domain of operations reached NATO's highest echelons, together with the third recommendation presented by the previous essay ("Global Security Is What's at Stake Today"). Of note, general media followed suit and started addressing the sixth domain issue (Le Guyader, 2021; Orinx and Struye de Swielande, 2021).

Having said that, precisely defining the scope of this sixth domain is still debated – should it be restricted to a mere "Cognitive domain," or should it rather address a more ambitious "Human Domain"?

The essay "Cognitive, A Sixth Domain of Operations?" clearly favors that second option (Human Domain), as illustrated by the following excerpt from its first chapter (Tallinn chat and walk), an exchange between General Weaver (SACT) and Professor Béthany:

> *Is this 'Human Domain' just another label for the 'Cognitive Domain' that I keep hearing about?"* asked General Weaver.

[1] Hervé Le Guyader is a graduate engineer from ENSEEIHT (École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications – Toulouse FR). Founder and former director of the European Center for Communication (Centre Européen de la Communication), he then joined ENSC (Ecole Nationale Supérieure de Cognitique Institut Polytechnique de Bordeaux FR) as Head of Innovation. As a distinguish member of the STO IST panel, he partakes in activities led by the NATO ACT Innovation Hub. He is currently a sworn judiciary cyber expert for the Court of Appeal and the Administrative Court of Appeal of Bordeaux FR.

[2] English and French are the two official languages of NATO.

Béthany saw Weaver's gaze wander to the rooftop architecture, a sign that his interest was waning because, his friend knew, he was already convinced of the relevance of the "Cognitive Warfare" concept.

"No, it's not. Well, actually, cognition is naturally included in the Human Domain but a Cognitive Domain would be far too restrictive, as tempting as it may be. I know the human brain, this extraordinary piece of 'connected flesh'," Béthany made another finger quote gesture, *"this unbeatable 'thinking machine' has been luring some into advocating the Cognitive Domain should become NATO's sixth domain of operations. I know this from experience; they tried to corral me into their little club but, believe me, this would be a half-baked decision. Cognition is of course crucial to any decision-making process and key to any individual or organization's behavior but, as discomforting as it may sound, 'cog-weapons' only fill one drawer of the arsenal our adversaries are designing right now.*

Adding a Cognitive Domain to NATO's list of domains of operations would certainly look cool and make headlines, but relief would be very short-lived."

"But, what do you really mean by Human Domain?" General Weaver asked, a bit unsettled.

"Well, the Human Domain is the one defining us as individuals and structuring our societies. It has its own specific complexity compared to other domains, because of the large number of sciences it's based upon. I'll list just a few and, trust me, these are the ones our adversaries are focusing on to identify our centers of gravity, our vulnerabilities. We're talking political science, history, geography, biology, cognitive science, business studies, medicine and health, psychology, demography, economics, environmental studies, information sciences, international studies, law, linguistics, management, media studies, philosophy, voting systems, public administration, international politics, international relations, religious studies, education, sociology, arts and culture …"

3.2 FOUR KEY QUESTIONS

3.2.1 What Exactly Does NATO Mean by "Domain of Operations"?

Paradoxically, while it's relatively easy to find such a definition at the national level (US, in particular), one is hard pressed to find the one used by NATO in its literature, even in the 50 odd documents part of its doctrine. Of note, the word "domain" is introduced in its "Comprehensive Operations Planning Directive" (Collective, 2010) document, but the domains identified there correspond to the acronym PMESII, i.e., the Political, Military, Economic, Social, Infrastructure and Information domains.

Some authors have attempted to address this surprising shortcoming, offering in particular:

- A domain is a space in which forces can maneuver to create effects (Garreston, 2017).
- The sphere of influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects (Allen and Gilbert, 2018).
- Critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission (Donnelly and Farley, 2019).

Interestingly, several candidates are today jockeying for position to become "NATO's sixth domain of operations." Next to "Cognitive Domain" and "Human Domain," "Electromagnetic Spectrum (EMS) Domain" or "Information Domain" have quite a few motivated advocates.

3.2.2 Would Human Domain Address All 6 Criteria Selected by the Johns Hopkins University?

The paper "The Information Sphere Domain Increasing Understanding and Cooperation," by Dr. Patrick Allen and Dennis Gilbert, of Johns Hopkins University, has introduced an elaborate and robust methodology for assessing whether "a field" can be considered as a war fighting domain.

While their point was to advocate the merits of what they call the "information sphere," the authors "offer for discussion what they consider to be the six key features of a domain," adding "The authors posit that if a domain has these six features, it qualifies as a domain, and if it does not have all six features, it should not qualify as a domain. This checklist of features can then be used as criteria to determine whether a new realm, such as the Information Sphere, qualifies as a domain:

- Unique capabilities are required to operate in that domain;
- A domain is not fully encompassed by any other domain;
- A shared presence of friendly and opposing capabilities is possible in the domain;
- Control can be exerted over the domain;
- A domain provides the opportunity for synergy with other domains;
- A domain provides the opportunity for asymmetric actions across domains.

The Human Domain clearly addresses these six features, but the second criterium "A domain is not fully encompassed by any other domain" probably would disqualify a Cognitive Domain, in particular if a competition between both candidates were to happen, as one can certainly argue that Cognitive Domain is, by construction, a (significant, of course) part of the Human Domain.

3.2.3 What Would Be Wrong With a "Cognitive Domain"?

Besides the arguments presented by Professor Béthany in the excerpt quoted above, several points need to be made:

- Adding a domain of operation is a highly complex task and its selection among several candidates has to be fierce and rigorous: there can only be one sixth domain!
- The cognitive dimension is, of course, a key component of the Human Domain both at individual and collective level, but is a person, is a community solely defined by its cognitive capacities?
- What about, for instance, biotechnologies, nanotechnologies?
- Don't these two technologies represent some potential threat and, should the answer be yes, are these threats addressed by the five existing domains?
- Would they be addressed by a "Cognitive Domain"?

3.2.4 What Risk Would One Take if Sticking to the Five Existing Domains?

Dr. Bryan H. Wells, NATO chief scientist, in his presentation at the ICMCIS'21 conference (Wells, 2021) eloquently presented what he sees as being the most relevant major technology trends and their accelerating synergies with Emerging and Disruptive Technologies (EDT), together with their respective timelines (see Figure 3-1). There are some fundamental human considerations attached to each of these technologies, to each of these synergies, and sticking to a purely technological approach to them would cause an existential issue. As happens with any existential issue, its nature is multidisciplinary and addressing it requires an interdisciplinary approach in order to be correctly tackled. That approach needs to put Social Sciences and Humanities (SSH) on an equal footing with the so-called "hard sciences."

Further illustrating the dual "hard sciences / social sciences and humanities" approach are these various ways of naming modern forms of warfare, such as: "hybrid," "under the radar," "ambiguous," "war and peace," "no-war."

As a reminder, China, with its "Three Warfares" strategy 1) Public opinion warfare, 2) Psychological warfare, 3) Legal warfare; and Russia (Gerasimov, 2013) have long made it clear – and public – that they fully intended to use the Human Domain to their advantage and to add it to their own multidomain strategies.

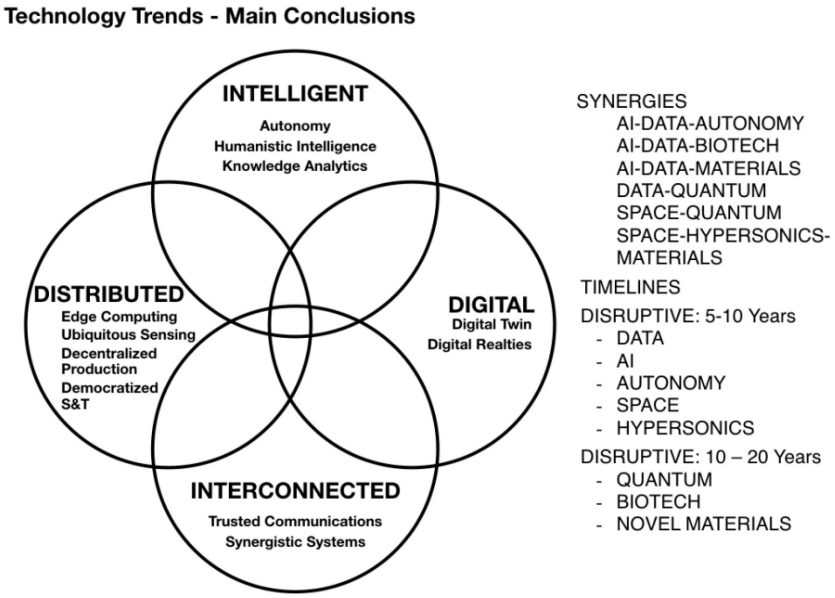

Figure 3-1: Technology Trends, Synergies and Timelines (Wells, 2021).

3.2.5 The Uniqueness of a Human Domain

Two points need first to be made:

- No existing domain is orthogonal to the others: planes take off from land or vessels, ships dock in harbors, satellites are filled with Cyber hardware and software, special operation forces use whatever tool, technique, device they will see fit to their mission.
- The industrial sectors relative to the defence dimension of the five current domains have created over the years, decades and sometimes centuries, some industry juggernauts. Together with thousands of SMEs, they employ hundreds of thousands of highly qualified workers and represent significant chunks of national economies and some crucial exports.

Human Domain is of a different nature. It is based on SSH sciences which do not fall "naturally" into one of the five existing domains and do not typically offer "off the shelf" devices. These sciences rather are to be found, simultaneously, in all five current domains. Their applications constitute a basic tenet of modern warfare as they provide key ingredients to modern threats.

SSH precede, explain, and lead to all domains. They're both inside and outside each of them and, taken as a whole, they embrace, encompass all of the five existing domains.

Human Domain IS a domain as such, but it is also the "womb" for all other domains whose existence is solely based on and justified by this 6th domain.

3.2.6 And Now, What?

As a reminder, an operational approach always needs to be designed to turn a "domain" into a "domain of operation" proper. This translates into the design of main Lines of Action corresponding to the each of the letters of the DOTMLPF-I acronym (cf: Fly, 2009), that is "doctrine," "organization," "training," "materiel," "leadership," "personnel," "facilities," and "interoperability."

Three different challenges have to be met so that the operational suggestion we wish to make here can be followed.

- A scientific challenge, because of the necessary interdisciplinarity of the approach (in particular, the combination of "hard" and "SSH" sciences);
- A technical challenge: the solution will of course be based on a "system of systems," but the issues associated with i) Multi-domain fusion, with the drastic timescale differences within each and between all domains (Human Domain attacks can go from one picosecond to several generations); ii) Computer aided (AI, ML, BD …) visualization; iii) Decision-making assistance, are bound to be quite arduous;
- A human resource challenge, both in terms of hiring (the right persons), of career progression and of (lifelong) education and training.

The Allied Future Surveillance and Control (AFSC) project would provide a unique and concrete opportunity to address these three challenges and, to put it bluntly, to prevent it from missing a significant share of the threats the Alliance faces today and will be facing onwards, part of the continuum of threats its core mission demands to "surveil and control."

AFSC will replace the retiring AWACS in 2035. Given its ambition, the competence level of its contractors, the budgets allocated and the far-reaching vision behind the project, AFSC must be designed with the requirement of building a system of systems up to today's and tomorrow's NBIC induced warfare challenges. Its multidomain coverage must address all six domains.

3.3 REFERENCES

Allen, P.D., Gilbert, D.P. (2018). The Information Sphere Domain Increasing Understanding and Cooperation. Tallinn (Estonia): The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. https://www.ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf.

Cole, A., Le Guyader, H. (2020). Cognitive, a 6th Domain of Operations? FICINT document. Norfolk (VA, USA): NATO ACT innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-04/ENG%20version%20v6.pdf.

Collectif (2010). Allied Command Operations – Comprehensive Operations Planning Directive (COPD). Brussels (Belgique): Supreme Headquarters Allied Power Europe. https://info.publicintelligence.net/NATO-COPD.pdf.

Donnelly, J., Farley, J. (2019). Defining the 'Domain' in Multi-Domain. Shaping NATO for Multi-Domain Operations of the Future, Joint Air and Space Power Conference, Berlin (Germany) 8 – 10 October 2019. Kalkar (Germany): Joint Air Power Competence Centre. https://www.japcc.org/defining-the-domain-in-multi-domain/.

Fry, S.A. (Ed.) (2009). Joint Department of Defense Dictionary of Military and Associated Terms – Joint Pub 1-02. Washington (DC, USA): Department of Defense. https://web.archive.org/web/20091012193530/; http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

Garretson, P. (2017). USAF Strategic Development of a Domain. Over The Horizon (OTH) Journal, 10 June 2017. Montgomery (AL, USA): Air Command and Staff College. https://othjournal.com/2017/07/10/strategic-domain-development/.

Gerasimov, V. (2013). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Military-Industrial Kurier, 27 February 2013. Translation from Russian to English by R. Coalson, Military Review, 1, 2016. http://www.theatlantic.com/education/archive/2015/10/complex-academic-writing/412255/.

Le Guyader, H. (2000). Weaponization of Neuroscience. Technical Report. Norfolk (VA, USA): NATO ACT innovation Hub. https://www.innovationhub-act.org/sites/default/files/docs/WoNS.pdf.

Le Guyader, H. (2021). Le Domaine Cognitif de la Manipulation est Devenu un Terrain de Conflit. Paris (France): Le Monde, 6 May 2021. https://www.Lemonde.Fr/Idees/Article/2021/05/06/Le-Domaine-Cognitif-De-La-Manipulation-Est-Devenu-Un-Terrain-De-conflit_6079291_3232.html.

Le Guyader, H., Cole, A. (2020). Cognitif, un Sixième Domaine d'Opérations ? FICINT document. Norfolk VA, USA: NATO ACT Innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-04/FR%20version%20v6.pdf.

Lee, C. (2019). News from AUSA Global: Army Fleshing Out Updated Modernization Strategy. National Defense, NDIA's Business & Technology Magazine, 26 March 2019. Arlington (VA, USA): National Defense Industrial Association. http://www.nationaldefensemagazine.org/articles/2019/3/26/army-looks-to-modernize-dotmlpf-in-modernization-strategy.

Orinx, K., Struye de Swielande, T. (2021). Carte Blanche: la Guerre Cognitive et les Vulnérabilités des Démocraties. Brussels (Belgium): Le Soir, 11 May 2021. https://plus.lesoir.be/371510/article/2021-05-11/carte-blanche-la-guerre-cognitive-et-les-vulnerabilites-des-democraties.

Wells, B.H. (2021). Emerging and Disruptive Technologies: Challenges and Opportunities. Scientists Discuss Future CIS Technologies for Defence in Global Online Conference. 21st International Conference on Military Communication and Information Systems ICMCIS'2021. Virtual Edition: 4 – 5 May 2021. Brussels (Belgium): NATO Communications and Information Agency (NCIA). https://www.ncia.nato.int/about-us/newsroom/scientists-discuss-future-cis-technologies-for-defence-in-global-online-conference.html.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
		ISBN 978-92-837-2392-9	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Cognitive Warfare: The Future of Cognitive Dominance

7. Presented at/Sponsored by

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021. Symposium organized by the Innovation Hub of NATO-ACT and ENSC, with the support of the French Armed Forces Deputy Chief of Defence, the NATO Science and Technology Organization / Collaboration Support Office, and the Region Nouvelle Aquitaine.

8. Author(s)/Editor(s)	9. Date
B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel	March 2022
10. Author's/Editor's Address	**11. Pages**
Multiple	118

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cognition; Cognitive bias; Cognitive domain; Cognitive war; Cognitive warfare; Cyber-psychology; Human

14. Abstract

This document, published by the NATO-CSO, brings together articles related to the presentations given during the first Symposium on Cognitive Warfare, held in Bordeaux, France, in June 2021, on the initiative of the NATO-ACT Innovation Hub and the Bordeaux-based ENSC, with the support of the French Armed Forces Joint Staff, the NATO-STO-CSO, and the Region Nouvelle Aquitaine. This first Symposium reflected on human cognition, its strengths and weaknesses, its collaborative organization for military decision-making, its relation with and dependence on digital technology, and its social and political dimensions within the context of fierce international competition. The Supreme Allied Commander for Transformation (SACT) and the French Armed Forces Vice-Chief of Defence expressed their views on the topic. This first Symposium was the starting point of a series of meetings and workshops further exploring the subject, on the initiative of NATO CSO and ACT.