Designing and Adding the Missing Piece to the Multi-Domain Jigsaw

Hervé Le Guyader
ENSC
FRANCE

herve.le-guyader@ensc.fr

ABSTRACT

They say war has changed, they say the very nature of conflict has changed, and they're of course right. But what they mean typically falls short as mere observations most often do not lead to conclusions.

Yes, it is true that conflicts can no longer be seen as a series of logically linked events taking place in specific locations, at specific moments in time, involving well defined and identifiable actors, using devices specifically designed for conflict-oriented purposes and whose protagonists seek to obtain – after some violent and kinetic episodes - explicit, tangible quick wins and lasting advantages.

Most people, including public at large, would agree with that statement, but would stop there, somehow intimidated by the consequences of the true sea change that has profoundly modified our geostrategic landscape and this sort of cop-out, at least from public at large, is understandable. After all, who would be comfortable accepting as a fact that life is now to be experienced as a permanent "no-war/no-peace" state. But stopping there, that is being satisfied stating the obvious, isn't going to help.

*For those in charge in our democracies, it's not that "conflicts **can** no longer be seen …", but that "conflicts **must** not be seen …". This shift from one modal verb (**can**) to another (**must**) calls for a series of decisions and actions. In other words, it's time to "close the OODA loop", it's time to boost its Orient and Decide part as enough convincing evidences have been Observed, proving that something was really wrong in today's appreciation of conflictual situation.*

This paper focuses on the "Orient" component of this particular OODA loop and does it for a specific target audience, a "NATO community of interest", looking at a specific concept, the so-called "multi-domain" approach, through a "sort of" prism.

- *NATO, because as a political (civil) and military international institution, it has a unique capability to take democratically based decisions addressing security issues, and to engage considerable military forces to enforce these decisions.*

- *The prism analogy is indeed tempting, to try and reveal the multidomain components of a conflict, just like an optical prism will disperse light and separate it into different component colors.*

1.0 THE DOMAIN FAMILY TREE

1.1 And Then They Were Five

For historical reasons, soon to be followed by industrial reasons, *interested parties* have found it natural to itemize physical environments people would find themselves fighting within, ending up calling them ***domains***, recognizing early on they were far from being mutually exclusive. Greco-Persian wars, 5 centuries BC, for instance, would typically include land and sea domain operations, and it is now well accepted that only multidomain strategies, and multidomain operational and tactical approaches can lead to success.

An interesting point is to look at the very notion of "domain" in the NATO context.

As often, things started fairly smoothly. People had been fighting on land for thousands, and at sea for hundreds, of years so the first two domains, Land and Sea (surface, to start with) were a given.

Then, even if balloons had already been used for observation and propaganda distribution during the Napoleonic wars and the Franco-Prussian conflict of 1870-1871 and planes had been used for bombardment missions during the Italo-Turkish war of 1911-1912, aerial warfare during the First World War marked a rupture with these past examples. It was the first conflict during which aircraft were involved on a large scale and played a significant role[i]. That new theater of operations had enough specificities, when compared to Land and Sea, that making it a third "domain of operations" also became a given, even if, again, an argument could be made (and has been successfully made, at least for NATO) regarding the need to differentiate "air" and "space".

These three first domains share one thing in common: they are of a physical nature, making it easy to intuitively grasp their nature and specificities. Historians, scientists, defense specialists, military and civilian experts, together with practitioners have built considerable knowledge regarding wars waged over land, sea and air.

Then things accelerated with the advent of cybernetics, quickly followed by the recognition of the strategic importance of space and "orbital activities". Progress in dual (civil-military) research and recent conflicts led NATO to add added Cyber[ii] (2016) and Space[iii] (2019) to the list of its operational domains. As a consequence dozens of exercises, executed at a national or coalition level, have given all concerned parties, including industry partners, a chance to optimize and constantly update their readiness level for the five operational domains Land, Sea, Air, Cyber and Space and any combination thereof.

1.2 The Right Toolbox?

So, over hundreds of years, national states and ad hoc coalitions have endeavored to be as efficient as possible dealing with multidomain wars, be they those deciding to go to war, or those being attacked.

For now a bit more than seven decades, NATO has organized itself to fulfill its mission, which is "… *to guarantee the freedom and security of its members through political and military means.*"[iv] and, quite logically, does it through the adoption of a more and more inclusive multidomain-based approach.

Its military strategy is based upon two distinct Strategic Commands at the head of its command structure. Allied Command Transformation (ACT), based in Norfolk, VA, USA, leads the military adaptation of the Alliance, while Allied Command Operations (ACO) whose HQ are located in Mons, Belgium, 6302 kms away from ACT, is responsible for the planning and execution of all NATO military operations.[v]

So, right from the start, the need to constantly challenge status quo and to update military adaptation of the

Alliance through a perpetual transformation process (ACT's role) is a built-in feature for NATO.

Quite understandably, the progresses of science and technology play a pivotal role in that process. Together with ACT, the Science and Technology Organization (STO[vi]), established with a view to meeting to the best advantage the collective needs of NATO, NATO Nations and partner Nations in the fields of Science and Technology, brings its expertise according to the vision of its historical founder, Theodore von Karman, who offered: *"Scientific results cannot be used efficiently by soldiers who have no understanding of them, and scientists cannot produce results useful for warfare without an understanding of the operations."*[vii]

Mere figures combining NATO's available intellectual, industrial, organisational and military resources give to it an undisputable advantage over any adversary and the same can be said for those of its Nations who have been, or currently are, exposed to armed conflicts against state or non-state opponent.

However, as unpleasant and humiliating as it may be, NATO and its members have been keeping on losing wars for the past 70 years, with very few – and not that relevant – exceptions, regardless of how many discrete battles might have been won on the ground,.

As stated above, the sheer definition of war has changed, but that's not the problem. Dozens of papers, lectures, books, have demonstrated that. The problem is that our adversaries, state or non-state actors, have adapted their strategies to avoid direct confrontational engagement, which they reckon would be suicidal, while focusing their efforts on vulnerability points and cracks of our societies. They're doing this with a multidomain approach, even if (i) most of them do not have a significant presence in all 5 domains, (ii) our mobilizable capacities in each of these domains largely surpass theirs, (iii) the pool of talents, knowledge, expertise, accumulated experience in these domains NATO has is greatly superior to theirs.

So, how come do we keep on failing?

For sure, interoperability issues among so many partners, decision-making process hindered by the needs to abide by laws and regulations, overall societal attitude numbed by decades of growing welfare since WWII … may contribute to explain that phenomenon.

But there may be another powerful reason that explains our disadvantage in winning modern wars, and this has to do with our multidomain toolbox. We're missing one (or two) tool/s – call them domain/s -, that our adversaries have well identified and have learned to use to their benefit.

1.3 The Missing Tool

In a quite frustrating manner, this shortage is well known, identified and has been documented in many publications. Chinese "Three warfares" strategy[viii] and Russian's Gerasimov[ix] based doctrine have given a solid foundation to hundreds of researchers, analysts and practitioners for them to try and identify the reasons for our regular failures.

A good illustration of this clear-sightedness is a recent (October 2020) video[x] entitled "The U.S. Army Future Command's Future Operational Environment (FOE)" to be found on the US Army mad scientist website.

The next picture, extracted from this video, sums up the multidomain issue this paper focuses on.

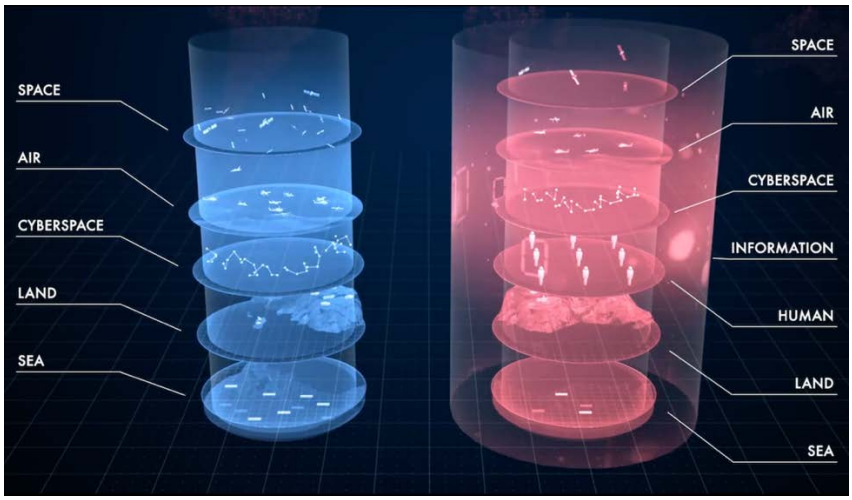

Figure 1-1: https://tinyurl.com/2pdj4eke video snapshot (34 s)

On the left hand side, "our" current five domains. On the right hand side, what the author of the video reckons our adversaries' operational domains are, identifying an "Information domain" and a "Human domain" on top of the five "classic" domains. Of note, the video doesn't even attempt to explain what "Human domain" or "Information domain" are about. Surprisingly enough, its audio content doesn't even pronounce the name of these two newcomers ("human", "information"), but rather generically goes:

"*Adversaries, who view the traditional domains differently than we do will leverage various technologies to disrupt army capabilities and blur the distinction between war and peace, conflict and competition.*"

That website also offers a presentation of what they call "Operational Environment Exploitable Conditions 2028 – Exploitable Conditions Framework", "*a set of 12 conditions in the operational environment (OE) that actors could exploit when competing with the United States and its partners. Understanding these OE conditions and how various actors may exploit them is critical for the U.S. Army to plan, organize, train, and equip the force for success in mitigating or countering potential challenges to U.S. interests* »[xi].

Figure 1-2: https://community.apan.org/wg/gckn/m/mediagallery/380304/download

While not exhaustive in its approach to identifying threats and vulnerabilities, this framework can be put next to General McChrystal's famous "*Afghanistan Stability/COIN Dynamics – Security*" 2009 slide.

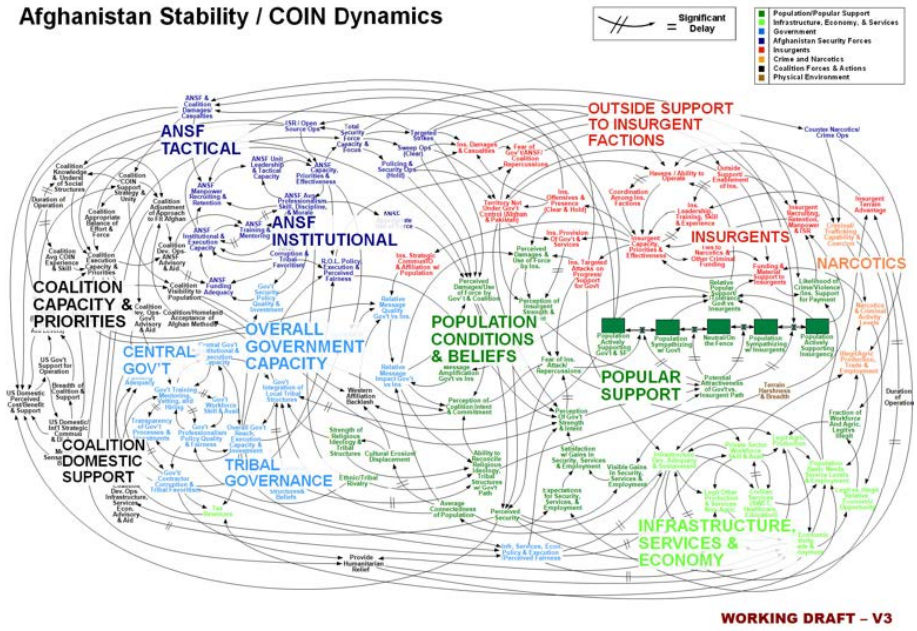

Figure 1-3: https://tinyurl.com/m8ecnvvt

General McChrystal is reported to have commented that slide by saying "When we understand that slide,

we'll have won the war". Twelve years later, he could probably offer a similar remark to the OE Exploitable Conditions chart. In both cases, we have lucid, clear-sighted and more or less user friendly graphic renditions of complex conflict frameworks.

In both cases, reaching that level of synthetic analysis shows how sturdy the research has been, but in both cases, we know this won't suffice. Actually, in the McChrystal Afghanistan case, we know it hasn't sufficed.

"OODA loop wise", these (China, Russia, Afghanistan, US Army Mad Scientist) studies relate to the first ("Observe") and a good chunk of the second ("Orient") quadrants and do a pretty good job at it.

Unfortunately, however valuable these contributions are, they're not going to help unless the last part of the "Orient" quadrant is built and solidly riveted together with the rest of the OODA engine.

In the NATO context, the OODA engine is designed to deliver (the "Decide, Act" part) along NATO's current five domains of operations. Corresponding doctrine, organization, training, materiel, leadership and education, personnel, facilities and interoperability (DOTMLPF-I[xii]) are in line with this five-pronged approach.

Obviously, this is not working and, while recognizing there's no silver bullet that can solve an issue of that magnitude, this paper has one main message:

A multi-domain approach equipped with a mere "five arrows quiver" (land, sea, air, cyber and space) is bound to fail.

There is an urgent need for adding a sixth domain of operations and riveting it as quickly as possible to the other ones through an accelerated DOTMLPF-I update.

In the next part of this paper, we'll first give a stab at defining the word "domain".

Then, we'll then at four conceptual topics (i) What this sixth domain should be about?, (ii) What should it embrace and how should it be named?, (iii) Would it pass the "John Hopkins test?", (iv) What are the main challenges it will need to overcome?

And because we're result oriented, we need to think realistically about implementation. This paper will therefore end with:

- a practical, concrete, actionable-yet-ambitious suggestion for a Project (with a capital p) which can act like a mothership program capable of triggering, framing and guiding the major overhaul that updating DOTMLPF-I will be.
- a suggestion for the role STO might play to facilitate that necessary evolution.

2.0 A MISSING DOMAIN, FINE, BUT WHICH ONE?

2.1 A Domain is a Domain is a Domain[1]

Logically, this second chapter should start with forging a definition of what a (NATO) domain is. Actually, it won't and that, for a couple of reasons:

[1] Borrowing from Gertrude Stein's famous quote « A rose is a rose is a rose », often interpreted as meaning "things are what they are". https://en.wikipedia.org/wiki/Rose_is_a_rose_is_a_rose_is_a_rose

- Surprisingly enough, one would expect such a fundamental concept to be introduced and thoroughly defined somewhere in the 50 odd Allied Joint Publications (AJP) composing the Allied Joint Doctrine, or in the Comprehensive Operations Planning Directive (COPD)[xiii]. Unfortunately, one would be hard pressed to find such a definition or, rather, one definition that would be in line with what we're talking about here, i.e. operational domains such as land, sea, air, cyber, space. What one can find, though, in paragraph 1-7 "The engagement space", p. 26 of the COPD, is a presentation of "*NATO currently recognized six (6) domains under the PMESII construct*". These six domains are (1) Political, (2) Military, (3) Economic, (4) Social, (5) Infrastructure, (6) Information. Interesting, perfectly relevant concepts, but clearly of a different breed, and living on a different level than our land, sea, air, cyber and space family of domains.
- This surprising lack of definition has led many researchers and authors to ask themselves the question "*By the way, what does (or should) one exactly mean by "operational domain*"? Among dozens of propositions, here are three possible definitions given by highly competent authors:

  - A domain is a space in which forces can maneuver to create effects. (Peter Garretson[xiv]),
  - Critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission. (Jared Donnelly and Jon Farley)[xv],
  - 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. (Patrick D. Allen and Dennis P. Gilbert – John Hopkins University)[xvi].

Each of these proposed definitions are interesting, but the third one, although taken from a text whose objective is to advocate an "Information Sphere" to qualify as the next operational domain, is the one that we'll use in this paper. To this writer's, the scientific and academic approach it develops for proving its point is unsurpassed. Besides, the methodological toolkit it has created can be used as the proverbial wall to throw other hypothesis at, to see if they stick.

Lastly, there must be good reasons, and not only academic ones, why significant stakeholders have entered into competition for having their own candidate to become "NATO's 6th domain", "Electromagnetic spectrum", "Information", "Cognitive", "Human" being today jockeying for position.

Maybe the best way to handle the paradox of not finding any official definition for "domain" which, by the way, leads to some questioning regarding the word "multidomain", despite its omnipresence in official texts, **is to cut the Gordian knot and consider the necessity of its existence as an axiom[2]**.

Indeed, a domain is a domain is a domain.

2.2 What Should this Domain be Ready For?

The fact that we keep on losing wars despite an undeniable better and stronger arsenal in the five current domains must mean something, and it's certainly not by keeping on investing trillions of dollars and euros for updating this arsenal that things will change. Of course, maintaining superiority in these domains is necessary but it cannot, it shall not suffice alone. As stated above, "*Adversaries, who view the traditional domains differently than we do will leverage various technologies to disrupt army capabilities and blur the distinction between war and peace, conflict and competition.*"

[2] As defined by the Collins dictionary, an axiom is 1. a self-evident truth that requires no proof, 2. a universally accepted principle or rule, 3. Logic & Math a proposition that is assumed without proof for the sake of studying the consequences that follow from it. https://www.collinsdictionary.com/dictionary/english/axiom

So, something fundamental has to change but, unlike most of adversaries, we have three hurdles to cross:

1. the rules (ethical, democratic, consensus making) we have to abide by,
2. the fundamental interoperability principle at the core of any coalition based initiative,
3. the (free and open) market, profit oriented strategies of our industrial private sector.

So, we know we're missing a domain, we know that adding a domain is a massive task whose inception, conceptualization, lobbying and then consensus building process among partner nations is mandatory to reshuffle the deck at the right political and military level.

Lastly, we know this domain will need to fulfill three obligations:

Obligation #1: We need to create a new domain capable of addressing current shortcomings.

Obligation #2: This new domain must have a multidisciplinary scientific base, combining those Social Sciences and Humanities (SSH) that define the complex Operational Environment today's conflicts develop into.

Obligation #3: Because of the likely rejection response its addition will generate, this 6th domain will have to be hardwired and sturdily clamped to the five existing ones.

2.3 What Should it Embrace, How Should it be Named?

Adding a new domain is no mean task and one has to be very careful and selective when selecting the one which, among today's relevant contenders (Cognitive, EMS, Human, Information …) should be NATO's 6th operational domain.

To this author, the logic is fairly simple: what is the proven, systematically demonstrated, most blatant vulnerability?

The answer is clear: decision making. Not the technological machinery meant to assist it, as most of it is more or less taken care of by the five current domains, but what's at the core of it, **Human decision making**.

It's that "Orient – Decide" vital part of the OODA loop that we ought to focus on for addressing the challenges of a modern Operational environment, i.e. those vulnerabilities the US Army Mad Scientist Lab calls "exploitable conditions".

Then comes the fist-fight between some finalists: should we elect a "Cognitive domain", an "Information domain", a "Human domain"?

To this author, "Information domain", while intuitively highly relevant in this era of growing "digital influence" (social media influence, fake news, deep fake news, more and more convincing avatars, AI assisted propaganda …) can't be NATO's next domain of operations.

The effort for adding a new domain is such that one must prioritize and there's only room for one domain at a time. Information is obviously a key nutriment for feeding our cognitive process, hence contributing to human decision-making but, as a domain, it is ancillary to the Cognitive dimension.

So, should NATO's sixth domain be the "Cognitive domain" or the "Human domain"?

Because of the visibility and marketing appeal of the word "cognitive", "Human domain" is a far harder sell than "Cognitive domain", and there's a strong temptation for going "Cognitive domain" rather than "Human domain". One should therefore address the following question: "*What would we miss, what would be wrong with a Cognitive domain*?"

As this author has co-written a whole essay[xvii] on that subject, let's refer here to the following extract below, part of a fictitious dialog between a 2028 SACT (General Weaver) and Professor Béthany, the latter exposing why NATO's next domain should be Human domain, and not Cognitive domain.

***

"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 those 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 …*"

"*H.P., none of these is addressed by your current five domains, and this is NATO's most serious issue.*"

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

"*No, it's not. Well, actually, cognition is, natively, 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 … 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 behaviour 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****."*

***

To wrap this up, here is a Q&A like final argument for choosing between "Cognitive" and "Human":

- The cognitive dimension is a major part of Human (individual, collective) domain, but is a person/community solely defined by its cognitive capacity?
- For instance, what about neuro/bio/engineering[3], can these technologies affect human decision making?
- Do they represent a potential threat?
- If the answer is « Yes », then, are these threats addressed by the 5 existing domains?
- Would they be addressed by a « Cognitive domain »?

So, yes, a Cognitive domain is a relevant contender but (i) it would not cover for the whole gamut of human-related vulnerabilities, (ii) it is included in the Human domain so, as a choice has to be made for one next domain, the conclusion is clear: it has to be the Human domain.

2.4 Would it Pass the "John Hopkins Test"?

As shown above, the paper "The Information Sphere Domain Increasing Understanding and Cooperation" by Dr. Patrick Allen and Dennis Gilbert, Johns Hopkins University[xviii] 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 are 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.*"

It is therefore tempting to accept this invitation and use this checklist to see how "Human domain" performs vis à vis the six key features that a "new realm" must have to qualify as a domain.

Here are these six features:

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

As a reminder, according to Professor Béthany:

"… 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 … 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] Biotechnology, intimately coupled with AI, Big Data and ML, is advancing at an accelerated pace.

These disciplines co-exist and interact in the crucible from which each of us emerges as an individual. Above that individual level comes the "meta-crucible" in which teams, communities, societies forge their identity. Of course, what comes out from these "crucibles" is not like an unmodifiable plaster casting and modifications to any of the ingredients poured into that crucible will alter – in some way - the individual or the community that's continuously brewing in there.

"Behavior" is probably the one word thats summarize what we're interested in in this context. It encompasses individuality, personality and decision making and, come to think about it, isn't so far from the "Orient-Decide" part of an OODA loop.

It is relatively easy, using the Human domain definition given by Professor Béthnay ("Realm", to use the John Hopkins U. paper wording), to check whether Human domain qualifies as a Domain of operation.

In a nutshell:

1. *Unique capabilities are required to operate in that domain*,
   ➔ "Mind hacking", for instance, requires some fairly sophisticated skills.

2. *A domain is not fully encompassed by any other domain*,
   ➔ Should go without saying. On the other hand, there's an interesting thought to develop that would look at the opposite proposition, i.e. Human domain encompassing all other domains.

3. *A shared presence of friendly and opposing capabilities is possible in the domain*,
   ➔ That's the whole theme of unfriendly influence campaigns against people and communities.

4. *Control can be exerted over the domain*,
   ➔ Every propaganda campaign can be replied to by some counter propaganda, any tampering with neuro integrity can bounce back at its author, any poison may have its antidote.

5. *A domain provides the opportunity for synergy with other domains*,
   ➔ A topic like Cyberpsychology, typical example of scientific discipline belonging to the Human Domain, may lead into better Cyber security training, hence strengthening the Cyber domain.

6. *A domain provides the opportunity for asymmetric actions across domains*.
   ➔ This is to be understood, per the author's writing, as "*opportunities for capabilities in a domain to gain an asymmetric advantage over opposing forces in other domains*." Human domain is, by definition, in the driver's seat[4] when it comes to the "Decide-Act" part of the OODA loop, with direct impacts on other domains.

So, as a conclusion, Human domain does pass the audition.

That the "Information Sphere Domain", subject of the John Hopkins paper, would also qualify is off-topic: we are not looking for possible additional domains, we are looking for NATO's 6th domain, and there can only be one 6th domain.

As a side note, Cognitive domain would fail at the John Hopkins Test, especially on feature #2, as it is fully encompassed by the Human domain.

[4] As of today, the "man in the loop" approach is still favored for Human-Autonomy-Teaming (HAT)

3.0 WHAT ARE THE MAIN CHALLENGES HUMAN DOMAIN WILL NEED TO OVERCOME?

Cyber, in 2016, and Space in 2019 had to fight their way through some real resistance to become *bona fide* NATO domains of operations, but the challenges facing the Human domain are probably of a wider nature and larger magnitude.

A way to start structuring those challenges into tasks is to use the DOTMLPF-I[5] as a "multispectral developer" to plunge Human domain into and realize how multiple, complex and often intertwined the lines of action leading to the desired end states would be.

Mixing "hard sciences" and SSH sciences is certainly a daunting task by itself but, on top of severe technological challenges such as, for instance, visual representation of shared representation of SSH related data, there are three specific and major challenges Human domain will be confronted to. A scientific challenge, a Human Resources challenge, and a business challenge.

3.1 Scientific Challenge

At the conceptual level, Human domain is a multidisciplinary realm (cf. the short list proposed by Professor Béthany supra), that is knowledge associated to it is drawn from different disciplines, while each and every challenge stemming for that domain will require, to be overcome, an interdisciplinary approach to analyze, synthetize and harmonize links between scientific disciplines into a coherent and coordinated whole, that whole being itself conceptualized thanks to a transdisciplinary effort[xix],[xx].

Ask any researcher, any research center, any institution – private or public – in charge of allocating research funds or grants, here are some of the real difficulties invariably cited:

- Evaluation of the research work (jury composition?),
- Methodology (can't be a one-size-fits-all affair): there are considerable differences in methodology used in different disciplines and recognised as acceptable and pertinent by experts in a given field[xxi],
- Training (the present generation of researchers has been trained mostly in maximising the competence of individuals in a well-defined discipline),
- Career progression. The opportunities for finding a scientific journal ready to accept a multidisciplinary paper, hence to enhance one's Google scholar rank[xxii], hence to progress in one's career, get a university chair … are far slimmer than when staying within the confines of one of the 692 well identified, well labelled (siloed?) branches of science[xxiii].

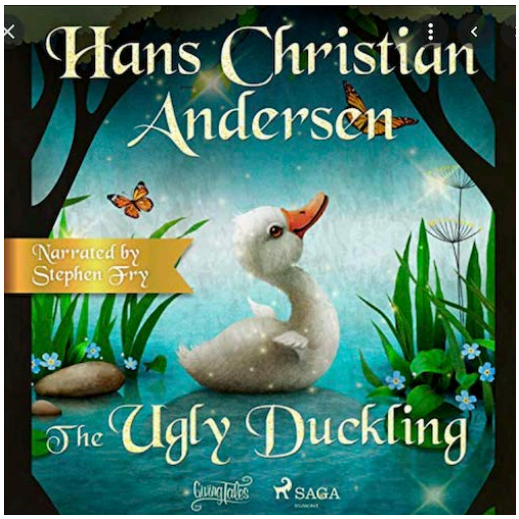

Figure 1-3: https://tinyurl.com/vc3wb59c

As we know, very few are the ugly ducklings[xxiv] lucky enough to turn into successful swans…

As a side note, the trend for encouraging more interdisciplinary projects finds an illustration with the plea for more cross-panel STO activities.

[5] Short for doctrine, organization, training, materiel, leadership and education, personnel, facilities, interoperability.
.

3.2 Human Resources Challenge

This is very much focusing on the TL-I (Training, Leadership, Interoperability) part of the DOTMLPF-I design and implementation.

Human domain's related vulnerabilities and Human domain's related weapons are today's and tomorrow's realities, and that's certainly not reflected at the education/hiring/training/lifelong learning/career evaluation process our forces go through.

Most of the content related to these different steps addresses current 5 domains issues. There is therefore an immediate need for a crash course, probably designed and triggered by those in charge of Transformation all across the NATO alliance.

Additionally, a major update is to be given to military academies, from recruitment procedures to curricula, and to training exercises so that their "multidomain" engine runs on all 6 cylinders.

3.3 Business Challenge

Money talks, as they say and there's a key difference in the respective business models of stakeholders representing the five current domains compared to those involved in the Human domain.

The industrial sectors relative to the defense dimension for the land, sea, air, cyber and space domains have, over the years, decades and sometimes centuries, created some industry juggernauts. Together with their thousands of SME's, they employ hundreds of thousands of highly qualified workers and represent significant chunks of national economies and some crucial exports.

Furthermore, the pervasiveness of digital technologies, the takeoff of Artificial Intelligence, Machine Learning, Big Data, Internet of Objects, have resulted in a growing dual-use (civil/defense-security) innovation-fueled technological sector. Traditional defense industrial stakeholders are absorbing with glutton appetite brains, ideas and products covering the whole TRL scale coming from civilian research, so that they can favorably wage their commercial wars by offering to a never sated market newer and better "devices".

And that's a problem.

Social Sciences and Humanities (SSH) rarely end up building up "devices" that can be put on a shelf, presented at international defense related trade shows, and even more rarely can be traced as the origin of international bribes, data theft and espionage, high scale kompromats.

Besides, and despite the collective trauma caused by terror attacks, some difficulty still lingers on for some SSH scientists to realize the necessity to look at defense and security issues as an existential necessity.

Money does talk indeed and, in the fierce and constant competition for national budget, SSH lobbyists are few and far between, making it difficult for the Human domain to create the momentum that would put it on equal footing with any of the five existing domains when it comes to negotiating public funds.

These difficulties may not exist among our adversaries. Authoritarian regimes make no fuss about resorting to SSH, as just a question of being sensible. Here is a 2013 quote from Russia's chief of General Staff, Valery Gerasimov in his famous article "The Value of Science is in the Foresight"[xxv]:

> *"The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.*

The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.

All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.

Frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals.

The defeat of the enemy's objects [objectives] is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased.

The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."

And for non-state actors, regardless of their motivation, SSH have proven their irresistible price/quality (read: cost/impact-on-their-target) ratio.

One should realize that placing in perspective the existential threat Human domain represents with the combination of these three major challenges (scientific, human resources and business), calls for resolute and immediate action from political and military leaders.

For our democratic, free-market societies, there's no "invisible hand" that will address that threat, decision and action have to come from top leadership.

3.4 The Uniqueness of the Human Domain

And there's yet another challenge our Human domain must meet, this one of a more intellectual nature, due to the uniqueness of its very nature.

No existing domain is orthogonal to the others: planes take off from land or vessels, ships dock in harbours, satellites are filled with Cyber h/w and s/w, special operation forces use whatever tool, technique, device they will see fit to their mission.

There is however a "common sense", intuitive overall understanding of what is meant by the land, sea, air, cyber and space domains and of each domain's unique specifies. One can easily draw something that others will immediately identify as being this or that domain.

Human domain is of a different nature. Human domain is difficult to draw. It is based on SSH sciences which do not fall "naturally" into one of the five existing domains. 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.

Having said that, its borders are, topologically speaking, an interesting challenge to represent graphically.

4.0 AND NOW, WHAT?

It's one thing to try and identify a problem and to, hopefully, convince one's audience of the reality and severity of that problem. It's another thing to contribute addressing it efficiently. This is the purpose of this paper's two final chapters.

As an reminder, the reality and severity of (Human domain related) new types of threat have been well identified at the highest NATO level, as illustrated by this excerpt drawn from item #6 of the London declaration NATO summit, 2019/12/3-4[xxvi]

> "*We are increasing our tools to respond to cyber-attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies. We are stepping up NATO's role in human security*."

More specifically, the specific threat to cognitive security has been addressed in-depth by the 2019 NATO STRATCOM COE "Responding to cognitive security challenges" report[xxvii].

> "… *the risks and threats that social media use may pose to liberal democratic systems. This is followed by a discussion on possible future options for public policy that serves as a conclusion for the research product as a whole. Social media give users the power to spread and receive contaminated information. Threats to cognitive security should not be overlooked. Technological innovations are used to exacerbate deep-seated weaknesses that can destabilize our societies. We hope this anthology will inform the work of researchers and practitioners alike, refining the capabilities of those who are tasked with the safety of our nations and our Alliance*."

On top of these well identified new kinds of threats, some even more ominous ones must not be shied away from, those stemming for **NANOTECHNOLOGY, BIOTECHNOLOGY, INFORMATION TECHNOLOGY AND COGNITIVE SCIENCE** (**NBIC**).

When Kluwer Academic Publishers published in 2003 the NSF/DOC sponsored report "**Converging Technologies for Improving Human Performance**"[xxviii], it created quite a stir, not so much among forward-thinking and open minded scientists who had been taken this convergence for granted for quite some time, but certainly for political leaders looking for gaining an edge in the endless, global competition for power in the largest sense.

Mastering these four families of technologies became a common goal for nations, mostly those who could afford the entry fee. Other actors, in particular rogue organizations, were prompt at realizing the huge benefits they could gain from having access to some NBIC end products and techniques in the asymmetric conflicts they were waging, or fomenting to wage.

Some looked at the seemingly infinite perspectives for human enhancement, all the way up to transhumanism[xxix] and were anticipating with the highest trepidation the advent of the mother of all disruptions, i.e. reaching the point of singularity[6].

[6] The point, resulting from ever-accelerating technological progress, when a sufficient threshold of self-evolving artificial intelligence is reached to result in a superintelligence beyond human conception.

Some others embraced with opened arms, and opened vaults, the possibility to boost their defense strategies with NBIC technologies.[xxx] As we know, the best defense can be … a good offense and the Roman saying "*si vis pacem para bellum*" has kept all of its validity across decades, centuries and now millennia.

This paper is not meant to thoroughly address NBIC related threats, just to illustrate the widening of the threat and vulnerability gamut our societies are exposed to.

The synergy between biotechnology and emerging technologies – in particular AI and Data today, probably quantum tomorrow - and its potential consequences is well identified at the highest level.

Biological weapons, for instance, are described at the World Economic Forum in their "How emerging technologies increase the threat from biological weapons"[xxxi] paper, as the following excerpt will show:

> *"Advances in biotechnology have, for example, made the manipulation of the genetic make-up of organisms—from bacteria to humans— faster, cheaper and easier. However, these developments often interact with or are enabled by other technologies, including by those categorized as 'emerging'.*
>
> *The process of convergence of recent developments in biotechnology with other emerging technologies holds tremendous promise but also increases the possibilities for misuse of biotechnology.*
>
> *Specifically, the convergence of technological developments could affect the development, production or use of biological weapons and thereby challenge governance approaches that aim to prevent the proliferation of biological weapons to both states and non-state actors*."

By the same token, the growing affordability of CRISPR-Cas9 gene editing[xxxii] "genetic scissors" and its military applications [xxxiii] are realities which are well known, regardless of any debate one can have regarding the myths and realities of the super soldier[xxxiv].

Here again, the real issue is not recognizing future and potential threats enough in advance. In other words, the issue does not lie within the "Observe", nor even within the "Observe/first half of Orient" (**O**∅) part of the OODA loop.

The issue resides in the "second half of the Orient/Decide" part **(**∅**D**), that is in the capacity to have a seamless process turning data (Observe's job) into information (**O**∅'s job) and then into actionable knowledge **(**∅**D**'s job) allowing for the right decisions to be made at the right time (second half of **D**ecide and then **A**ct).

What's missing is a clutch.

5.0 MOVING FORWARD

So far, this paper has aimed to demonstrate the urgent necessity of adding a sixth domain to NATO's list of operational domains and to do it at the right ambition level, by opting for a Human domain, despite the many complexities stemming from such a bold decision.

From a pragmatic point of view, a coarse way to categorize these consequences is to consider the DOTMLPF-I acronym and to draw the most exhaustive as possible mind maps resulting from what a "Human domain" would trigger in terms of "to do list" for each the letters composing that acronym.

From that first step, overlaps and possible clusters can be identified among these 8 mind maps so that a

"mother mind map" can be derived, resulting from their trimmed down amalgamation.

The objective of this last paragraph is to propose a proactive and realistic project facilitating this process, paving the way for the advent of Human domain.

The main idea is to take advantage of the size and momentum of what is one of NATO's most important projects for the next 20-30 years, i.e. the design and realization of the Allied Future Surveillance & Control (AFSC), successor to the Airborne Warning & Control System (AWACS).

It is well established that the successor to the AWACS should not be a single flying platform with a stand-alone on-board system, in other terms building a younger and better AWACS is certainly not what's expected, but more likely a Command & Control ***system of systems*** with large cross-domain capabilities.

Here again, the key is to avoid missing one domain in what is, by essence, a multidomain project.

Given the ambition of the AFSC project, the competence level of the contractors, the budgets being put on the table and the far-reaching vision behind the project, there is no question to this writer that AFSC must be designed with the requirement of designing a system of systems up to today's and tomorrow's NBIC induced warfare challenges.

Two key benefits would result from this:

- The most important one is probably to avoid having the AFSC purely and simply missing fulfilling its core mission, which is to **Surveil and Control** all forms of threats the Alliance is and will be confronted to, by creating a system that would be only address threats stemming from the five traditional domains.

  In other words, avoiding designing the AFSC with a native, blatant and fatal blind spot.

- The second one is to benefit from the sheer magnitude and strict schedule of the AFSC project, AWACS being slated for retirement in 2035. Dovetailing the inception of the Human domain to an industrial project will provide this complex research with an existing "project management" frame that will allow both academic and industrial sector to collaborate towards a common and defined goal. Academics will have to apply their respective and multidisciplinary scientific research to concrete implementations, while industrial partners will have to deliver technologies, tools and methods for capturing, ingesting, processing, exploiting and fusing SSH based data with the rest of the (hard science based) informational deluge. In other words, academic and industrial partners will need to leave their "comfort zone" and work together, on an equal footing.

In other words, hit two birds with one stone while one still can.

This can only be realized if and only if the right protagonists are convinced, willing and able to rank it as a top priority in their program of work. It will only work if and only if leadership is built from a balanced multidisciplinary team as, to use an idiom that travels well in many languages "Turkeys don't vote for Christmas (or Thanksgiving)", and "Nur die dümmsten Kälber wählen ihre Metzger selber"!

In that context, and as follow-up to NATO SCI-339[xxxv], a large scale project associating NATO Allied Command Transformation (ACT) and a cross-panel NATO Science @ Technology Organization (STO) RTG would look like a natural and useful endeavor to launch.

Bordeaux, 11 September 2021.

REFERENCES

[i] https://www.bl.uk/world-war-one/articles/aerial-warfare-during-world-war-one
[ii] NATO Warsaw Summit, 8-9 July 2016 https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
[iii] NATO Brussels Summit, 20 November 2019 https://www.nato.int/cps/en/natohq/news_171028.htm
[iv] https://www.nato.int/nato-welcome/index.html
[v] https://www.nato.int/cps/en/natolive/topics_52092.htm
[vi] https://www.sto.nato.int/Pages/organization.aspx
[vii] https://www.sto.nato.int/Pages/agard-history.aspx
[viii] https://en.wikipedia.org/wiki/Three_warfares
[ix] https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf
[x] https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/posts/check-out-the-u-s-army-future-command-s-future-operational-environment-foe-video
[xi] https://community.apan.org/wg/gckn/m/mediagallery/380304/download
[xii] https://en.wikipedia.org/wiki/DOTMLPF
[xiii] https://www.cmdrcoe.org/download.cgf.php?id=9
[xiv] https://othjournal.com/2017/07/10/strategic-domain-development/
[xv] https://www.japcc.org/defining-the-domain-in-multi-domain/
[xvi] https://ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf
[xvii] https://www.innovationhub-act.org/sites/default/files/2021-04/ENG%20version%20v6.pdf
[xviii] https://ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf
[xix] Claverie Bernard, « Pluri-, inter-, transdisciplinarité : ou le réel décomposé en réseaux de savoir », *Projectics / Proyéctica / Projectique*, 2010/1 (n° 4), p. 5-27. DOI : 10.3917/proj.004.0005. URL : https://www.cairn.info/revue-projectique-2010-1-page-5.htm
[xx] https://pubmed.ncbi.nlm.nih.gov/17330451/
[xxi] https://erc.europa.eu/news/supporting-interdisciplinarity-challenging-obligation
[xxii] https://scholar.google.com/citations?view_op=top_venues
[xxiii] https://en.wikipedia.org/wiki/Index_of_branches_of_science
[xxiv] https://www.lrdigital.dk/en/search/?bookType=0&languageCode=eng&query=ugly%20duckling&sort=0
[xxv] https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf
[xxvi] https://www.nato.int/cps/en/natohq/official_texts_171584.htm
[xxvii] https://stratcomcoe.org/publications/responding-to-cognitive-security-challenges/113
[xxviii] https://www.wtec.org/ConvergingTechnologies/Report/NBIC_report.pdf
[xxix] https://en.wikipedia.org/wiki/Transhumanism
[xxx] https://www.innovationhub-act.org/sites/default/files/docs/WoNS.pdf
[xxxi] https://www.weforum.org/agenda/2019/03/how-emerging-technologies-increase-the-threat-from-biological-weapons/
[xxxii] https://en.wikipedia.org/wiki/CRISPR_gene_editing
[xxxiii] https://www.atlanticcouncil.org/blogs/futuresource/gene-editing-in-china-beneficial-science-or-emerging-military-threat/
[xxxiv] https://www.bbc.com/news/world-55905354
[xxxv] https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16856