Weaponization of neurosciences

Hervé LE GUYADER

Ecole Nationale Supérieure de Cognitique, Bordeaux, FRANCE

Table of contents

Disclaimer **2**

Executive Summary **2**

Brussels, July 17, 2026, NATO Summit: "Human mind", the 6th domain of operation **3**

The road to the Summit **4**

2018: French German Forum Research Summit 4
2018: IST-159 Exploitation of Cyberspace For Intelligence project 4
2019: Responding to cognitive security challenges, the "Hacking humans" report 5
2021 Horizon Europe 5
The writing was on the wall 5
2022: Davos EEC Global Risks report to include Malicious Mind Hacking 6
2024: "Five brains initiative" 7

Norfolk, we have a problem **9**

NBIC, a cornucopia of new tricks for old habits 10
From "Hybrid war", "Three warfares", to "non-obvious wars" 11
One thousand blades, one thousand cuts 13
Toughening and speeding up the response 16
2030: Addendum to the 2026 Summit declaration 19

Meanwhile… **19**

The "One Belt One Road initiative" (OBOR), aka "Belt and Road Initiative" (BRI) or "Silk road" 19
Silk road… 19
Polar silk road… 21
… and African rare earths… 22
2039: The two incidents 24
Nkombwa Hill (Zambia) 24
Vardø, Kirkenes (Norway) 27

Article 5 triggered **30**

Conclusion **31**

Annex: Recommendations **32**

Disclaimer

This is a work of fiction. Names, characters, businesses, places, events and incidents are either the products of the author's imagination or used in a fictitious manner. The views and opinions expressed in this essay are those of the author and do not necessarily reflect the official policy or position of any institution. Examples of analysis performed within this article are only examples, based on limited source information.

Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Executive Summary

While it has been said that ***everything could be weaponized***, neurosciences and, more broadly speaking, Nanotechnology, Biotechnology, Information Technology and Cognitive Sciences (NBIC) are clearly providing state and non-state actors some true game changers.

The story narrated in this essay begins in 2018 with weak, and not so weak signals, and ends in 2040 with NATO triggering Article 5 because of NBIC attacks on some of its allied Nations. During these 22 years, pivotal decisions are taken at NATO Summits, fundamental choices are made for the design of the successor to the Alliance's main surveillance and control system, and NATO manages to embark a large number of nations, far beyond its core allied nations, into a pragmatic educational program on global security.

All of this because of the "Weaponization of neurosciences" challenging topic that was to be addressed.

This essay uses fiction and mixes actual facts and events, fairly logical foresights and some fictitious extrapolations drawn from a couple of long term key geostrategic initiatives launched by today's big players. Of course, the roles played in this story by those big players could be interchanged, albeit with some work.

Using a few dramatization tricks, at the cost of being a bit provocative to try and keep the reader's interest doesn't mean not being serious at voicing out one's deep beliefs.

In this particular case:

- Yes, "Human mind" should be NATO's next domain of operation,
- Yes, AWACS successor must address NBIC,
- Yes, global security is what's at stake today, and it will take more than professionals of the defense, security and military sectors to address it efficiently.

However difficult it will be.

Brussels, July 17, 2026, NATO Summit: "Human mind", the 6th domain of operation

Excerpt from the Brussels Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 16-17 July 2026.

Article 11 … *To stay secure, we must look to the future together. We are addressing the breadth and scale of new technologies to maintain our technological edge, while preserving our values and norms. We will continue to increase the resilience of our societies, as well as of our critical infrastructure and our energy security. To effectively do so, NATO and Allies, within their respective authority, must constantly take stock of the pace and breadth of scientific research being conducted, in particular outside the Alliance. Nanotechnology, Biotechnology, Information Technology and Cognitive Sciences (NBIC), whose development rate is staggering, have an immense potential to deeply transform our societies, but the dual nature of this potential poses a new set of challenges to our security.*

For decades, NATO and Allies, and our competitors too had been used to operate in a three-dimensional environment, where air, land and sea represented familiar, distinct but interoperable operational context.

The 2014 Wales Summit identified that Cyber-attacks presented a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. By way of consequence, NATO and Allies agreed that cyber defense was part of NATO's core task of collective defense.

The 2016 Warsaw Summit then recognized cyberspace as a domain of operations in which "NATO must defend itself as effectively as it does in the air, on land, and at sea"[1].

Three years later, the 2019 London Summit declared, in the article #6[2] *of its final declaration, Space as an operational domain for NATO, recognizing its importance in keeping us safe and tackling security challenges, while upholding international law. Of note, the same article also stated "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. We recognize that China's growing influence and international policies present both opportunities and challenges that we need to address together as an Alliance."*

Progresses in NBIC make it today possible for our competitors to develop new ways to reach their offensive objective. While propaganda and influencing strategies have always existed, the depth and sophistication of NBIC-fueled hybrid attacks today represent an unprecedented threatening level inasmuch they target the most vital infrastructure we rely on: the human mind.

We therefore recognize the human mind as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, at sea, in cyberspace and in space.

[1] https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[2] https://www.nato.int/cps/en/natohq/official_texts_171584.htm

The road to the Summit

Reaching a consensus across all Nations for taking such a radical decision was not an easy feat. Getting to that point took more than 8 years, and yet it soon proved that it was just the first step in realizing the real sea change, i.e. a NBIC fueled, massive onslaught on NATO nations.

It first took a series of studies, reports, local, bilateral and multilateral initiatives to identify and then zoom in on one particular issue, rapidly referred to as the "***Hacking the mind***" threat.

To name a few:

2018: French German Forum Research Summit[3]

A regular bilateral forum for French and German research ministries and main stakeholders, aiming at reaching a high-level vote on research and innovation policy strategies and priorities. Its 2018 edition had identified Global Security/Civil Security (GS/CS) as one of the six mains strands research investment should be focusing on. Logically, four "expectable, albeit perfectly justified" GS/CS research themes were selected for funding:

1. Radicalization and the fight against terrorism,
2. Rights and freedoms in the field of civil security,
3. Critical infrastructure protection and resilience,
4. Protection against emerging infections and biological threats,

French and German members of the High-Level Expert Group had actually identified a fifth theme, cross-cutting not only at the disciplinary level, but also at the societal level:

5. Education and Information towards a shared culture on global and civil security.

But resistance to change finally prevailed and that 5th, disruptive, theme was not followed up on. But seeds were sown.

2018: IST-159 Exploitation of Cyberspace For Intelligence project

NATO's STO[4]'s IST[5] panel had embarked on an ambitious project, whose goal was to "*understand the cognitive layer of cyberspace and investigate potentially relevant methods and technologies for use by intelligence analysts in order to provide situational awareness, indicators and warning, and intelligence to commanders*".
To achieve that goal, eight scientific objectives had been identified:

1. Exploration of attack vectors and effects of cyberattacks at the cognitive layer,
2. Intelligence opportunities in this layer,
3. Defense options and techniques,
4. Operational effects and countermeasures,

[3] https://www.internationales-buero.de/en/6th_forum_franco-german_research_cooperation_2018.php
[4] Science and Technology Organization (STO), https://www.nato.int/cps/en/natohq/topics_88745.htm
[5] Information Systems Technology (IST) panel, https://www.sto.nato.int/Pages/technical-team.aspx?k=(*)&s=Search%20IST%20Activities&View={2C52FF39-CB1C-4A13-8129-6976E923EDEC}&FilterField1=ACTIVITY%5FPANEL&FilterValue1=IST

5. Exploration of relevant technologies and tools,
6. Cyber ISR,
7. Fake News Recognition,
8. Combine SM exploitation and NW-Analysis.

Although successful in reaching its scientific objectives, the project's impact was hampered by the difficulty to widely communicate its findings outside the restricted community it had been developed within but, here again, seeds had been sown.

2019: Responding to cognitive security challenges, the "Hacking humans" report

Edited by NATO STRATCOM COE[6] this report, although not creating the "wake-up call" it should have, accurately highlighted the massive threat NATO nations, in particular, were exposed to. Quote from its conclusion:

> *"… 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*."

Another good example of what could/should have been a wake-up call for Defense and (global) Security stakeholders.

2021 Horizon Europe

Horizon Europe[7] 2021-2027, was the 100 B€ budget European Union's seven-year research and innovation program. Based upon three pillars ((1) Excellent Science, (2) Global Challenges and European Industrial Competitiveness, (3) Innovating Europe), its second pillar had identified "Civil Security for Society" as one of its six clusters.

But, here again, it proved too difficult to overcome institutional hurdles and silo syndrome, and no significant project that would have created sustainable synergy between the relevant actors (NATO, EDA[8], European Commission) ended up making any lasting impact.

The writing was on the wall

Playing with human perceptions, emotions, feelings, awareness, triggering decisions through massive, or more customized propaganda campaigns have always been there, part of our context, be it at peace or at war. After all, advertisers, politicians and PSYOPS planners are continuously manipulating people into changing their perceptions of reality and making choices that ultimately do not benefit them.

[6] https://www.stratcomcoe.org/
[7] https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en
[8] https://www.eda.europa.eu/

Closely linked to the development of the internet, of social media, of big data, of artificial intelligence, and to their combined ability for using personal data, oh-so nicely and blindly, offered by hundreds of millions of users, the "art" of mental manipulation was propelled to a new level, as illustrated by the ***Stanford Persuasive Technology Lab***[9]**,** created as early as in **1997**.

Fast forward a decade, and this initiative spurred the development of an entire industry, cleverly blending cognitive sciences, in particular cognitive biases[10] and information technologies, turning startups into stock market juggernauts in just a few years.
Societal risks associated to this exponential development were rapidly identified, sometimes by insiders from these very tech company-turned whistleblowers, as exemplified by this **2015** quote from a Google ex-employee who happened to, also, be a Stanford Persuasive Technology Lab alumnus:

"*Never before has a handful of people working at a handful of tech companies been able to steer the thoughts and feelings of a billion people," he said in a recent talk at Stanford. "There are more users on Facebook than followers of Christianity. There are more people on YouTube than followers of Islam. I don't know a more urgent problem than this."*[11]

It didn't take long for state and non-state actors to jump onto that bandwagon, to develop aggressive strategies, such as influencing electoral processes, in particular the **2016** US and the **2017** FR presidential elections.

2013-2014 At the battlefield level, this new arrow to the "hybrid warfare" quiver played a role in the Ukraine conflict, in particular aiming at influencing external perceptions on its reality. The then used strategy targeted perception and narratives, capable of influencing domestic and foreign audiences in order to erode public support for the sanctions against Russia pushed by the US.

Studies run by intelligence and defense agencies were prompt in analyzing and reporting the breadth, depth and resolve of Digital Influence Machines (DIM), such as the Russian IRA (Internet Research Agency), with its "Trolls from St. Petersburg" and its expertise in using social networks for influencing opinion.[12]

Late 2019, in Mali and neighboring countries, WhatsApp and Facebook fake news campaigns managed to convince some that France was actually shipping motorbikes and weapons to terrorist groups, so that it could justify its presence in the Sahel region.

2022: Davos EEC Global Risks report to include Malicious Mind Hacking

Dozens of similar evidences around the globe that "*something serious was going on*", jeopardizing every day a bit more global and civil security, made the issue more and more visible on decision makers' radar, to such an extent that, at the December 2022 World Economic Forum in Davos, "Malicious Mind Hacking" made an explosive entry into the Global Risks Report both in terms of Likelihood and of Impact.

[9] http://captology.stanford.edu/go/welcome?from=
[10] https://en.wikipedia.org/wiki/List_of_cognitive_biases and
https://en.wikipedia.org/wiki/List_of_cognitive_biases#/media/File:Cognitive_bias_codex_en.svg
[11] https://www.wired.com/story/phone-addiction-formula/
[12] https://edition.cnn.com/2019/04/18/tech/internet-research-agency-mueller-report/index.html

Of note, Cyber related issues, which had been featuring in previous editions of the Global Risks Report at the "Likelihood" level, were swept away in 2020 and 2021 by *environmental related risks*. Malicious mind hacking first entry into the report boasted a highly visible and commentated 3rd place.

Perhaps more surprising to a majority of observers, the "Weapons of mass destruction" topic, which had quite justifiably featured in the top three in terms of "Impact" in the seven previous editions, became the subject of heated debate as to whether or not it should now include Social Networks and other digital services in their taxonomy, because of their massive, exponentially growing and addictive use by society at large.

"*Hey, GAFAM, NATU, BATX, kudos for your* ***Weapons of mass cretinization****!*" some valiant activists, standing in the mud and melting snow that Davos winters were now the synonym of, were shouting, doing their best to get media's attention.

2024: "Five brains initiative"

The accumulation of evidence for the threat posed by some digital products and services to human cognition, and unanimously alarming reports issued by think tanks, defense and security agencies, prompted five nations to create the "***Five brains initiative***". This core set of concerned nations pledged to mobilize budget, to share data, knowledge and research agenda, with one objective: drafting within a year a doctrine and ad hoc rules of engagement for reacting when confronted to aggressions labelled as "***Malicious mind hacking***".

The Five brains initiative quickly gathered momentum, fueled by the results of research projects led by NATO STO and NATO ACT[13], with additional help from Centers of Excellence[14] and a precious "out of the box" collaboration from the broad, non-NATO, non-military international community managed by ACT's Innovation Hub[15].

Spokespersons from the five founding members, France, Germany, Japan, Norway and USA, soon to be joined by partners from Africa, Middle East and Asia, were keen on explaining how crucial this reaction was by hammering the message:

"***Each and every day, we are losing battles we don't even know we were engaged in. This can't last, this won't last***".

Quite expectedly, ICT major players (the GAFAM, NATU, BATX actors), mobilized their best lobbyists to oppose, or at least mitigate, this campaign. They did a great job at demonstrating the obvious and real benefits their products and services were providing, but their delaying tactics and reluctance to modify their economic models was undermined by two contributing factors: in-house activists and the worldwide spread of rules inspired by the 2016 European General Data Protection Regulation (GDPR[16]).

The explosive combination of these two factors proved too difficult to fend off as general public understood that blindly giving away their personal data was the modern equivalent to leaving a post-it

[13] Allied Command Transformation (ACT), https://www.act.nato.int/
[14] https://www.act.nato.int/centres-of-excellence
[15] https://www.act.nato.int/innovationhub
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR

with your password on your desk. The latter gives access to your computer, the former to you, as a unique person, and to your most intimate control levers, a much more frightening prospect.

It took some blood, lots of sweat and sometimes tears, but this series of initiatives, this series of fact-based studies and plain observations, the global pressure build-up achieved at the diplomatic level by the Five Brains and their allies led up to the Brussels, July 17, 2026, NATO Summit declaration, where the Human Mind became NATO's 6th domain of operation.

And that was good.

But not quite enough.

Norfolk, we have a problem

As it turned out, preparation to the 2026 Summit had not been as exhaustive and sturdy as it should have been. Years of under-budgeting and under-staffing had taken their toll and Article 11, the "***Mind hacking***" article, was one key casualty.

Enthusiastic accolades were shared and raucous applause heard across the world but, soon enough, once the dust had settled, impartial observers were prompt to identify two main fault lines:

- **I**C, and not **NBIC**
  While Article 11 had correctly presented NBIC, as a whole, as being the issue to address, only one and a half (or thereabout) out of its four components had been in reality looked into with the necessary rigor: **Information** (technologies) and their own, specific capacity to tamper with human **Cognition**. But **Nano**, **Bio** technologies, and their own impact on **Cognition** (hence the 1.5 vs. 2.5 approximation) had, in reality, been put on the backburner.

- Doctrine? Rules of engagement? Training? DOTMLPFI[17]?
  Under public and diplomatic pressure, NATO had managed to reach consensus among nations on this fairly disruptive concept of Human mind as a domain of operations and to pull off a unanimous decision but, unlike the five first domains of operation, "***NBIC warfare against human mind***" was pretty much *terra incognita*, most certainly in terms of lessons learned.
  People had been fighting for hundreds of years on land, at sea, for a little bit more than a century in the air, for a few decades in cyberspace and space. Historians, scientists, defense specialists, military and civilian experts and practitioners had built considerable knowledge regarding wars waged over land, sea and air. More recent conflicts had added Cyber and even Space warfare data and analysis to the mix, and dozens of exercises, executed at the coalition (NATO) level had allowed for all concerned parties to optimize their readiness level.

  But human mind as domain of operation??? What's the equivalent to the "smoking gun", how can it be detected, identified, attributed to … something, somebody??? Where is my OODA loop??? My C4ISR?, What are the ad hoc CCIR[18]'s???

And then, the real killer issue: ***What would cause triggering Article 5?***

Adversaries and competitors were merciless in overtly mocking NATO's apparent unpreparedness, stressing the "existential risks this "*marketing rather than strategic*" decision was creating for the human race". More covertly, troll farms[19], fake news factories[20] and 50 Cent Army[21] worked double, triple, quadruple shifts to make sure gullible (remember Weapons of Mass Cretinization?) folks would go down streets and avenues around the world with new, anti-NATO slogans.
Ironically, the same time pressure that had prompted NATO to issue its declaration in 2026, in an admittedly rushed out fashion, ended up also applying to its competitors who, in turn, made a series of bad moves that ended up in "incidents". Epitomizing the NBIC threat and serious enough in their disastrous

[17] https://en.wikipedia.org/wiki/DOTMLPF
[18] http://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/CCIR2.pdf
[19] https://www.collinsdictionary.com/us/submission/17707/troll+farm
[20] https://www.bbc.com/future/article/20190528-i-was-a-macedonian-fake-news-writer
[21] https://en.wikipedia.org/wiki/50_Cent_Party

consequences, these incidents managed to make triggering Article 5 a near "*no-brainer*", as commentators later on found amusing to say, with the bravery of those who are out of range.

But it took 10 years to get there.

NBIC, a cornucopia of new tricks for old habits

When Kluwer Academic Publishers published in 2003 the NSF/DOC-sponsored report entitled "**Converging Technologies for Improving Human Performance NANOTECHNOLOGY, BIOTECHNOLOGY, INFORMATION TECHNOLOGY AND COGNITIVE SCIENCE**" [22], 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 technologies became a common goal for all nations, mostly those who could afford the price of the ticket. 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[23] and were anticipating with the highest trepidation the advent of the mother of all disruptions, i.e. reaching the point of singularity[24].

Some others embraced with opened arms, and opened vaults, the possibility to boost their defense strategies with NBIC technologies.

The **hybrid warfare** concept, theorized a long time ago and, in quite a few places applied with success, would never be the same.

The Wikipedia article[25] on Hybrid Warfare would read as early as 2020:

> **Hybrid warfare** is a military strategy which employs political warfare and blends conventional warfare, irregular warfare and cyberwarfare with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution. Hybrid warfare can be used to describe the flexible and complex dynamics of the battlespace requiring a highly adaptable and resilient response.

By the same token, while adding some significant complexity and sophistication, the Chinese "**Three Warfares**" approach, combining (i) opinion warfare, (ii) psychological warfare and (iii) legal warfare, to supplement PLA's more traditional means and methods, felt greatly invigorated by NBIC's boundless horizons promises, from nano-scale to … well, global, worldwide level!

---

[22] https://www.wtec.org/ConvergingTechnologies/Report/NBIC_report.pdf
[23] https://en.wikipedia.org/wiki/Transhumanism
[24] 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.
[25] https://en.wikipedia.org/wiki/Hybrid_warfare

From "Hybrid war", "Three warfares", to "non-obvious wars"

It has been said that the two drivers for human behavior were "*sacred rules and utilitarian values*"[26], in that order. This certainly applies to many institutions and businesses, with their "Vision Statement", "Mission Statement" approach, leading to *programs and action plans*, each of them in turn materialized by *projects*, but also to states or "aspiring states" alike.
Russia and China were probably among those nation states scoring the highest in that respect. Apart from NATO Nations and considering their amount of resources and the firm resolve authoritarian regimes are always in a better position to exert than democratic ones, Russia and China, indeed, were prime candidates for harnessing the potential of NBIC technologies to serve their "vision" with disruptive "utilitarian" projects.

And sure they did.

Chicken and egg: It is difficult to tell which came first between "*Hybrid war*", popularized by Russia in the Ukraine war, but whose theoretical underpinnings (to be also found in NATO) originated much earlier, and the "*Three Warfares*" strategy, more easily traceable to China.

In 2003, the Central Military Commission (CMC) had approved the guiding conceptual umbrella for information operations for the People's Liberation Army (PLA) - the "Three Warfares" (san zhong zhanfa - 三种战法). The concept is based on three mutually-reinforcing strategies:

1) coordinated use of strategic psychological operations, influencing foreign decision-makers and how they approach China policy,

2) overt and covert media or public opinion warfare, attempts to shape public opinion both domestically and internationally manipulation,

3) legal warfare designed to manipulate strategies, defense policies, and perceptions of target audiences abroad, shaping the legal context for Chinese actions, including building the legal justification for Beijing's actions and using domestic laws to signal Chinese intentions.[27, 28]

In 2005, Lieutenant General Mattis and Lieutenant Colonel Hoffman coined the expression "Hybrid War" in a US Naval Institute magazine[29]. They wrote:

"In Hybrid Wars we can expect to simultaneously deal with the fall out of a failed state that owned but lost control of some biological agents or missiles, while combating an ethnically motivated paramilitary force, and a set of radical terrorists who have now been displaced. We may face remnants of the fielded army of a rogue state in future wars, and they may employ conventional weapons in very novel or nontraditional ways. We can also expect to face unorthodox attacks or random acts of violence by sympathetic groups of non-state actors against our critical infrastructure or our transportation networks. We may also see other forms of economic war or crippling forms of computer network attacks against military or financial targets.

[26] http://www.ccnl.emory.edu/greg/Berns_Sacred_Values_FinalPrinted.pdf
[27] https://www.globalsecurity.org/military/library/report/2008/2008-prc-military-power03.htm
[28] sources : https://css.ethz.ch/en/services/digital-library/articles/article.html/195268/pdf and https://warontherocks.com/2018/01/chinas-three-warfares-perspective/
[29] https://pdfs.semanticscholar.org/4346/95e7b8867944550936d28092653feb8b0c34.pdf

The kinds of war we will face in the future cannot be won by focusing on technology; …"

In 2013, Russia's chief of General Staff, Valery Gerasimov in his famous article[30] "*The Value of Science is in the Foresight*" then went as far as writing:

> "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."

Indeed, it became obvious that the lines between War and Peace would be from now on always fuzzy and blurred and that, rather than traditional war waging, NATO nations had to realize they were now exposed to a permanent background of "***non-obvious warfare***".

In other words, and to paraphrase Clausewitz, "*Peace is a mere continuation of war with other means*".

Key to non-obvious warfare is ambiguity, inasmuch the target should not be aware he/she is targeted, let alone by whom, and the new *spectrum of conflict* would from now on go from ambiguous, non-obvious warfare all the way to NBC[31], Armageddon like, conflict.

NBIC, and in particular converging BIC technologies in order to design what became referred to as "neuroweapons"[32] became a R&D top priority for nations both inside and outside the Alliance, as their possibilities seemed endless, for a cost performance ratio they could afford.
Hundreds of projects were funded, dozens of them actually turning in operational realities. The most threatening ones stayed under the radar until, in 2039, "something" happened.

---

[30] https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf
[31] NBC: Nuclear, Biological, Chemical
[32] for the sake of simplicity, let's say that neuroweapons are weapons that specifically target the brain or the central nervous system in order to affect the targeted person's mental state, mental capacity and ultimately the person's behaviour in a specific and predictable way.

One thousand blades, one thousand cuts

Neuroscience/NBIC weaponization potential can be coarsely structured along:

- human enhancement technologies,
- intelligence and security applications,
- performance degradation technologies or neuroweapons

Each of these broad entries can then be further analyzed and detailed for each of their segments contributing to shaping the whole spectrum of conflict, from non-obvious warfare up to full-blown NBC conflict, but this particular chapter will focus on the low-intensity but constant onslaught that can be performed thanks to Information and Cognitive Sciences technologies. The last chapter of this paper will provide an illustration to issues more directly linked to human enhancement and performance degradations applications.

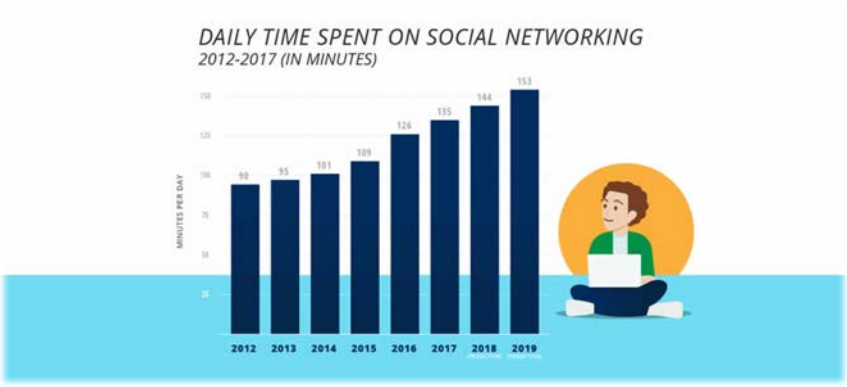
As early as 2009, Major-General Vladimir Belous could write: "*Provocative programming will be designed to affect not only the people's intelligence but primarily their senses, especially with the public's low political awareness, insufficient information and unpreparedness for such warfare.*
The objectives of such activities would be to make the adversary either incapable of effective resistance or to shape their consciousness in such a way as to manipulate them into not wanting to resist at all"[33]

In 2012, Vladimir Karyakin added: "*the advent of information and network technologies, coupled with advances in psychology regarding the study of human behavior and the control of people's motivations, make it possible to exert a specified effect on large social groups but [also] to also reshape the consciousness of entire peoples*." [34]

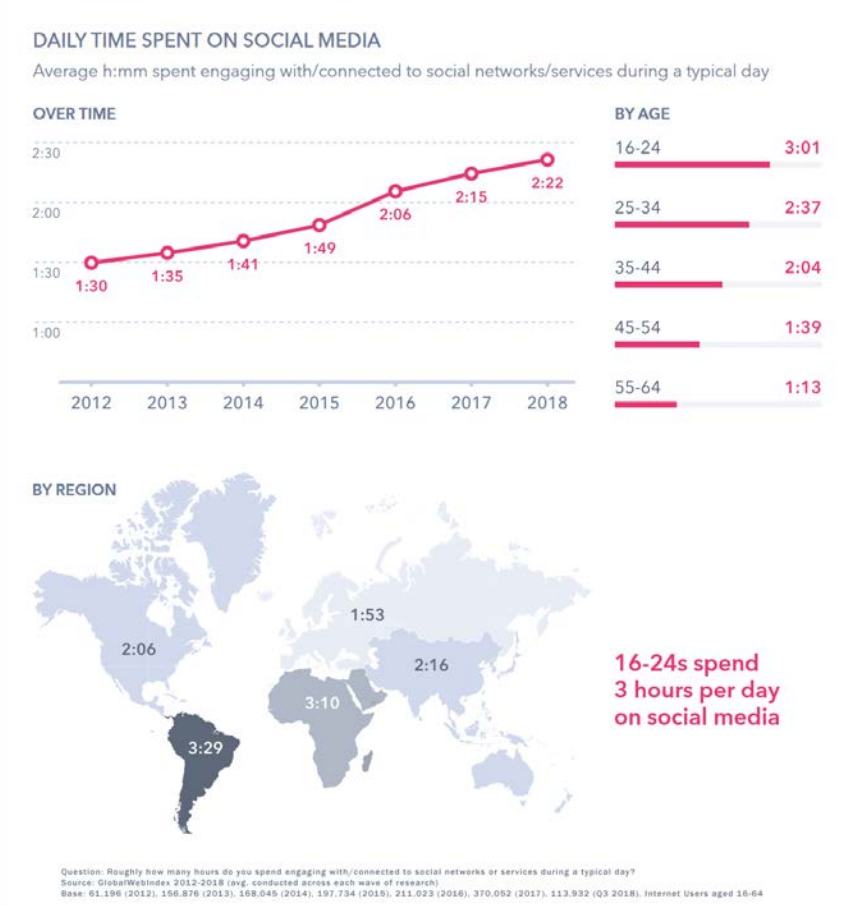
At the time when Belous and Karyakin formulated these thoughts, social networks were already spreading their wings[35] and starting to showing their power.

While 100% accurate data can be hard to trust 100%, the following picture gives a reasonably accurate indication of the level of addiction to social networks, especially in the Western World[36]:

[33] Belous, V. (2009) 'Weapons of the 21st Century', International Affairs, vol. 55, no. 2, pp. 64–82
[34] Vladimir Vasilyevich Karyakin, "The Era of a New Generation of Warriors—Information and Strategic Warriors—Has Arrived," Moscow, Russia, Nezavisimaya Gazeta Online, in Russian, April 22, 2011, FBIS SOV, September 11, 2012.
[35] Facebook reached the one billion monthly active members on September 14, 2012 https://www.wsj.com/articles/SB10000872396390443635404578036164027386112
[36] methodology presented in this article: https://www.broadbandsearch.net/blog/average-daily-time-on-social-media

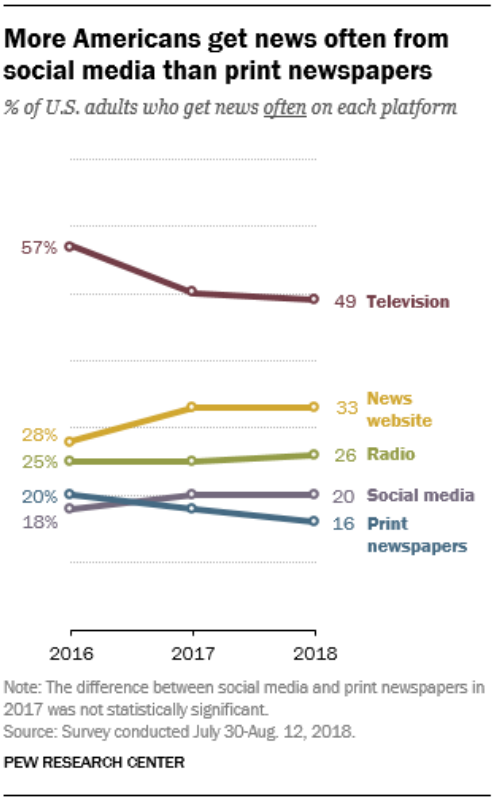


The picture above is fairly consistent with the one below providing some geographical differentiation:[37]



[37] https://www.digitalinformationworld.com/2019/01/how-much-time-do-people-spend-social-media-infographic.html

Be it as it may, these studies can't illustrate what counts most, i.e. the impact of messages read by users of these social networks. Relevant survey based studies can simply show trends in terms of users' approach to sourcing news and information, like this Pew Research Center survey (limited to the US).

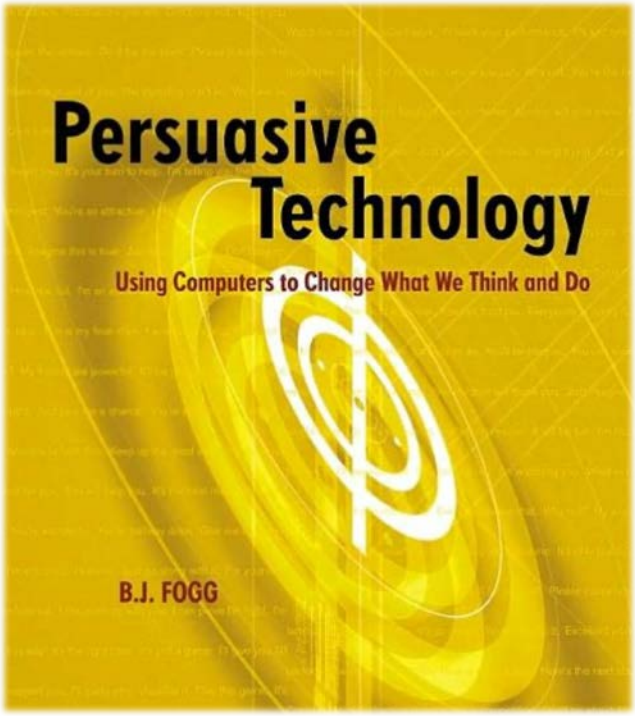


If one combines social media, blogs and news websites (fuzzy border between the latter two), "born digital news" content is therefore, by a growing margin, a large winner. At least in the US, at least in 2018.

But again, this will not show the impact of digital content absorbed by the users' brain.

Remember Stanford Persuasive Technology Lab and its aptly named http://**captology**.stanford.eu website? so

Well then, maybe you should read what follows, the abstract of the book that Lab's founder, Dr. B.J. Fogg wrote, published in 2003:



Can computers change what you think and do? Can they motivate you to stop smoking, persuade you to buy insurance, or convince you to join the Army? "Yes, they can," says Dr. B.J. Fogg, director of the Persuasive Technology Lab at Stanford University. Fogg has coined the phrase "Captology"(an acronym for computers as persuasive technologies) to capture the domain of research, design, and applications of persuasive computers. In this thought-provoking book, based on nine years of research in captology, Dr. Fogg reveals how Web sites, software applications, and mobile devices can be used to change peoples attitudes and behavior. Technology designers, marketers, researchers, consumers-anyone who wants to leverage or simply understand the persuasive power of interactive technology-will appreciate the compelling insights and illuminating examples found inside. Persuasive technology can be controversial-and it should be. Who will wield this power of digital influence? And to what end? Now is the time to survey the issues and explore the principles of persuasive technology, and B.J. Fogg has written this book to be your guide.

Mastering computer science AND neurosciences, opened new pathways to the old archaic pleasure and reward circuit in more and more customized way, thanks to all the personal data users had been blindly giving away was the key to success.

And the GAFAM, NATU, BATX of the world, with help coming from some of the brightest brains, became absolute masters in the art of creating addiction.

In 2017, Netflix CEO Reed Hastings has claimed that the streaming giant's biggest rivals weren't Amazon, YouTube or even traditional broadcasters. According to Mr. Hastings, our need for sleep is actually its main barrier.

> "*You know, think about it, when you watch a show from Netflix and you get addicted to it, you stay up late at night,*" he said.
>
> "*We're competing with sleep, on the margin. And so, it's a very large pool of time*.""[38]

Such "Digital Addiction & Indoctrination Tools", a perfect example of dual-use technology, were quickly embraced as the Holy Grail by non-obvious warfare enthusiasts who saw in these tools a remarkable double-edge sword: one edge addressing the "sacred rules" (peoples, communities, national cultures and beliefs), i.e. the very roots of society, the other edge in charge of severing, day after, users' attention spans, memory, reasoning skills, net result being a growing overall intellectual laziness.

The beauty of this strategy is that the victims of its combined attack are typically not aware that they are been targeted, while each and every individual's faculty of critical thinking is under constant attack.
The other beauty of it is that there is no need to invest in armies of Manchurian candidates[39]. This strategy of "***One thousand cuts***[40]", unintentionally made possible at remarkably low cost by IT behemoths was indeed doing a wonderful job at creating millions of "*potentially useful digital idiots*", to paraphrase the "*useful idiot*" expression apocryphally attributed to V.I. Lenin.

Indeed, Five Brains initiative spokespersons were right saying "***Each and every day, we are losing battles we don't even know we were engaged in."***

Toughening and speeding up the response

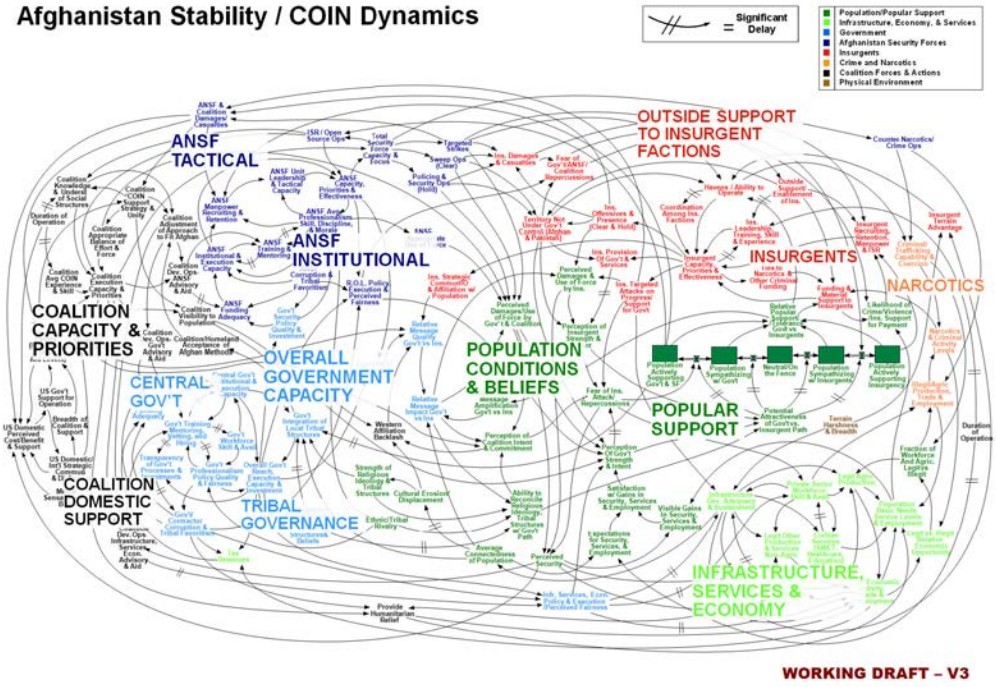
Spurred by the Five Brains[41] initiative, backed up by the findings of projects vigorously led by NATO ACT and STO, whose roadmaps had been tailored for, and budgets significantly raised for focusing on the NBIC overall issue, major decisions were made at the highest level.

[38] https://www.independent.co.uk/life-style/gadgets-and-tech/news/netflix-downloads-sleep-biggest-competition-video-streaming-ceo-reed-hastings-amazon-prime-sky-go-a7690561.html
[39] https://en.wikipedia.org/wiki/The_Manchurian_Candidate
[40] https://www.investopedia.com/terms/d/death-1000-cuts.asp
[41] At that point, rather a "brain hive", as soon nicknamed and referred to, due to the growing number of participating nations and bodies, aware of the threat and determined to address it.

One decision epitomized that profound sea change in collective awareness: The heavy spin given to the design of the Allied Future Surveillance and Control (AFSC) project, the successor to the E-3 Airborne Early Warning and Control System (AWACS) in view of its retirement in 2035.

In a nutshell, at the core of the AFSC system of systems, the NBIC component, including the **influence** issue, was to be addressed at the same level that all other types of threats. Logical decision, in a way, since "human mind" had been made a domain of operation, but a whole new level of ambition and expectations to be met by industry players aspiring to play a role in this project.

General Stanley A. McChrystal's 2009 famous slide and provocative comment "*When we understand that slide, we'll have won the war*" was now going to feature on each contractor's desk.



Maybe even more pivotal was a radical decision made by most NATO nations, joined by interested nations from Partnership for Peace (PfP), Mediterranean Dialogue (MD), Partners across the Globe … programs.

Inspired by previous bilateral initiatives such as the 2018 French-German Research Forum, and fully aware that in this constant world environment of non-obvious war, ***security*** could no longer be left to defense and security professionals alone, these nations embarked on a massive collective project, entitled "**Towards a shared culture on global defense and security**", aiming at creating a citizen level new critical competence: awareness, vigilance and readiness for new forms of threat.

After yet another Cambridge Analytica[42] type scandal, after the gross anti-government exploitation of yet another devastating heatwave in Australia, after new "coming outs" from insiders-now-whistleblowers regarding, not only big data/AI fed massive surveillance but also NBIC more hidden, surreptitiously growing neuroweapons, these nations came out with a common understanding which they summarized as:

[42] https://en.wikipedia.org/wiki/Cambridge_Analytica

“General public and, to some degree, institutions including administrations are not sufficiently informed and aware about NBIC related threats and about their consequences for each and every citizen and institution, especially in case of an actual emergency, of a partial or global crisis. Lessons learned from research in civil security are often largely misinterpreted, implemented in a wrong way by institutions and emotionalized by people, media and politicians. Possible reasons for this situation are the increasing role of post-factual culture and a severe lack of knowledge.

Furthermore, this phenomenon is intensified by a growing difficulty faced by all actors of the society. It is more and more difficult for their own situation awareness to keep pace with the evolution of a society where technology allows for and yields an exponential growth (i) in data production, (ii) in information (real or fake) production and availability, and also (iii) in terms of complexity and gamut of associated risks.

It is therefore becoming vital to develop an enlightened awareness, understanding and overall attitude for (i) threat evaluation, (ii) resilience, (iii) deterrence and, if necessary, (iv) retaliation, all contributing to shaping what is now a mandatory “defense and security state of mind”.

In order to reach that priority objective, participant nations commit to the following main lines of actions:

- Increase in a sustainable way the information level of the population, based on regularly updated NBIC focuses SWOT analysis,
- Enhance the civil security literacy of populations and administrations,
- Integrate defense and security issue in all stages of education (from schools to universities, continuing education, (e-) learning and teaching material,
- Heighten awareness of the general public regarding the complexity of decisions that need to be made by decision makers in defense and security scenarios.”

2030: Addendum to the 2026 Summit declaration

Testimony to the seachange in the collective mind set, the Oslo Summit (16-17 May 2030) declaration did some fine-tuning of Article #11 of the Brussels 2026 Summit declaration, by just adding 10 words to it, demonstrating NATO and its allied Nations' understanding NBIC had profoundly changed rules.

The article thus became:

"Progresses in NBIC make it today possible for our competitors to develop new forms of strategies to reach their offensive goals. While propaganda and influencing strategies have always existed, the depth and sophistication of NBIC-fueled hybrid attacks represent an unprecedented threatening level inasmuch they target the most vital infrastructure we rely on: the human mind, ***as symbolizing the uniqueness of each and every human person***[43].

We therefore recognize the human mind as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, at sea, in cyberspace and in space."

Meanwhile…

The "One Belt One Road initiative" (OBOR)[44], aka "Belt and Road Initiative" (BRI) or "Silk road"

Silk road…

Slated for completion on 1st October, 2049 to coincide with the 100th anniversary of the People's Republic of China, this global development strategy adopted by the Chinese government in 2013 and involving infrastructure development and investments in nearly 70 countries and international organizations in Asia, Europe and Africa, was bound to be the ultimate playground for some serious seasoning with Three Warfares spices.

And seasoning it did, the geopolitical spread and extent of the project providing irresistible appeal for:

1) coordinated use of strategic psychological operations influencing foreign decision-makers and how they approach China policy,

2) overt and covert media or public opinion warfare, attempts to shape public opinion both domestically and internationally manipulation,

3) legal warfare designed to manipulate strategies, defense policies, and perceptions of target audiences abroad, shaping the legal context for Chinese actions,

i.e. the pillars of the three-pronged Three Warfares strategy.

---

[43] For context and background information on what the authors of the declaration meant when using the word "*person*", the reader may wish to read "The category of the person, Anthropology, philosophy, history, Published by the Press Syndicate of the University of Cambridge"
http://www.urbanlab.org/articles/self/Carrithers%20et%20al.%20(1986),%20The%20Category%20of%20the%20Person.pdf#page=8

[44] https://en.wikipedia.org/wiki/Belt_and_Road_Initiative

Source: David Foster, Yahoo Finance[45]

China had established its first overseas military base in Djibouti in 2017, allowing Chinese Foreign Ministry spokesman Geng Shuang to offer to the world a splendid example of "*Three warfare parlance*" by going for record as saying "*The completion and operation of the base will help China better fulfill its international obligations in conducting escorting missions and humanitarian assistance ... It will also help promote economic and social development in Djibouti*[46]".

[45] https://finance.yahoo.com/news/china-new-silk-road-us-192303366.html
[46] https://www.mic.com/articles/181986/china-establishes-its-first-overseas-military-base

Experts agreed that the ports built or heavily renovated through the BRI can be dual-use for commercial and military purposes, while US DoD explained in its annual report to Congress "**Military and Security Developments Involving the People's Republic of China 2019**"[47]:

*China's leaders are leveraging China's growing economic, diplomatic, and military clout to establish regional preeminence and expand the country's international influence. China's advancement of projects such as the **"One Belt, One Road" Initiative (OBOR) will probably drive military overseas basing through a perceived need to provide security for OBOR projects.***

… China launched the Asian Infrastructure Investment Bank (AIIB) in 2016, with 57 founding members, to promote infrastructure building in the region. China has used OBOR, Xi's signature program, to enhance its global role by financing hundreds of billions of dollars' worth of major infrastructure projects throughout Asia, Africa, Latin America, the Middle East, and parts of Europe.

*China's leaders increasingly seek ways to leverage China's growing economic, diplomatic, and military clout to establish regional preeminence and expand its international influence. For example, **China's advancement of global economic projects will probably drive new PLA overseas** basing through a perceived need to provide security for OBOR projects.*

***Some OBOR investments could create potential military advantages for China, should China require access to selected foreign ports** to pre-position the necessary logistics support to sustain naval deployments in waters as distant as the Indian Ocean, Mediterranean Sea, and Atlantic Ocean to protect its growing interests.*

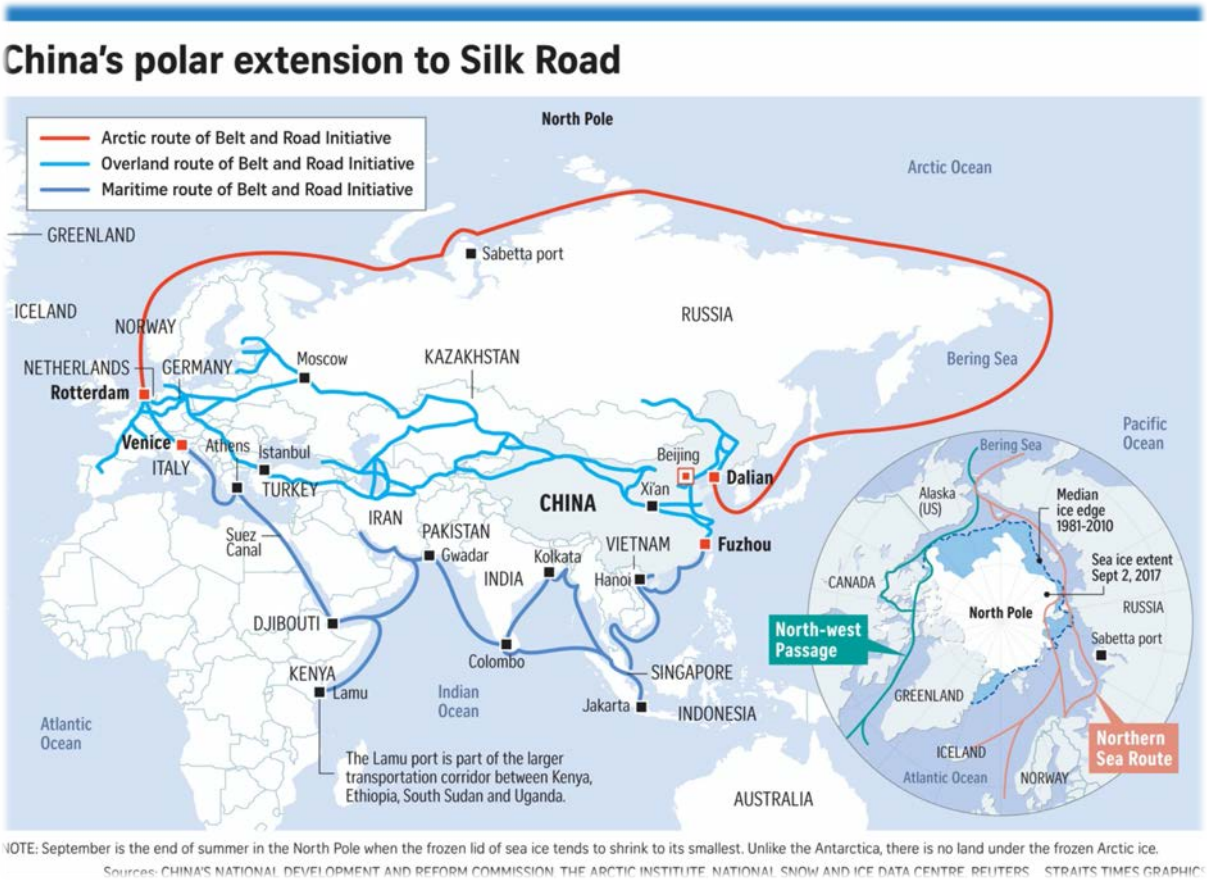
Polar silk road…

With a little help from global warming allowing for new trade routes to emerge in the region, it was only natural for China to look at the Artic region as a highly palatable ingredient for supplementing its BRI strategy.

The State Council Information Office of the People's Republic of China released in January 2018 its "China's Artic Policy" white paper[48], introducing a "**Polar Silk Road**", as per by the following excerpt:

"The Silk Road Economic Belt and the 21st-century Maritime Silk Road (Belt and Road Initiative), an important cooperation initiative of China, will bring opportunities for parties concerned to jointly build a "Polar Silk Road", and facilitate connectivity and sustainable economic and social development of the Arctic."

[47] https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf
[48] http://www.scio.gov.cn/m/32618/Document/1618217/1618217.htm



https://www.straitstimes.com/asia/east-asia/chinas-polar-ambitions-cause-anxiety

China's diplomatic skills and efforts, and long term strategy proved once again successful as, despite its geographical distance, it was given in 2013 the opportunity to join the Arctic Circle Council as one of its 13 observers. They could then sit and work next to the permanent status members, i.e. the eight Arctic States (Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden and the USA), together with the six organizations representing Arctic indigenous peoples.

"*Near-Arctic state*", "*a continental state close to the Arctic Circle*", an "*Arctic stakeholder*", were some of the formulas used by China to define itself in, again, perfect "Three warfare parlance"[49].

… and African rare earths…

Although China only contains one third of the world's rare earths reserves, it accounted in 2019 for 80% of US import of raw minerals, as it controls nearly all off the facilities to process the material[50].

[49] http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/620231/EPRS_BRI(2018)620231_EN.pdf

[50] https://www.reuters.com/article/us-usa-rareearths-pentagon-exclusive/exclusive-pentagon-eyes-rare-earth-supplies-in-africa-in-push-away-from-china-idUSKCN1T62S4

Africa's largely untapped potential, with the exception of Rainbow Rare Earths[51] which began operating in Burundi in 2017 and Mkango Resources[52], which at that time had just started developing a rare earths mine and processing facility in Malawi, looked like a most tempting continent for both the US and China to compete for these much in demand elements, crucial for high tech and military equipment.

Rare earth deposits of Africa: Harmer, Robin & Nex, Paul (2016), p.384[53]

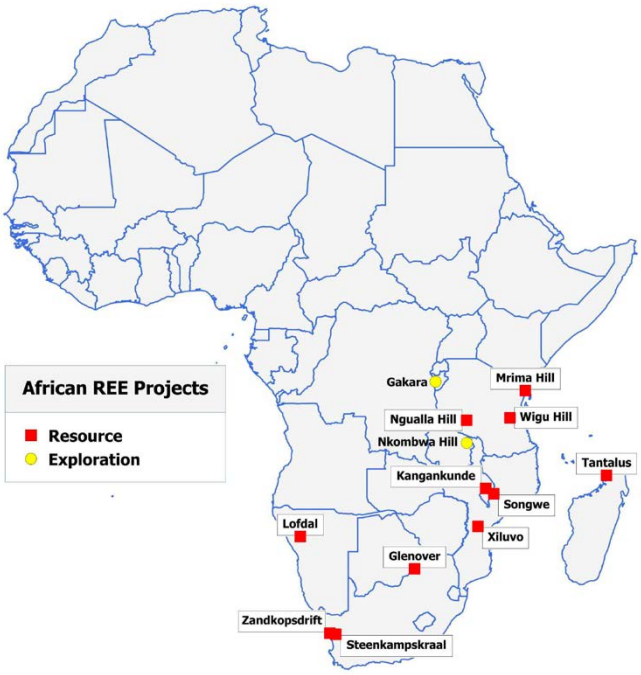


Figure 1: Map showing locations of the African REE projects included in the review.

The US were looking for diversifying their sources while China was interested in securing its leadership position while leveraging upon their BRI massive investments engaged in Africa.

"*If you put yourself in China's shoes, this is their main weapon in the trade war*" Mark Seddon, an Argus metals analyst[54] was caught saying.

And although rare earths were only one of the many subjects of potential dispute in an international competition for getting access to African wealth (strategic location, oil, rare earth metals, fish, arable land …), it's an incident caused by that "ore rush", coinciding with a seemingly unrelated incident up in the Arctic Region, that triggered Article 5.

[51] http://rainbowrareearths.com/
[52] https://www.mkango.ca/
[53] https://www.researchgate.net/publication/305918070_Rare_Earth_Deposits_of_Africa
[54] see [46]

2039: The two incidents

Nkombwa Hill (Zambia)

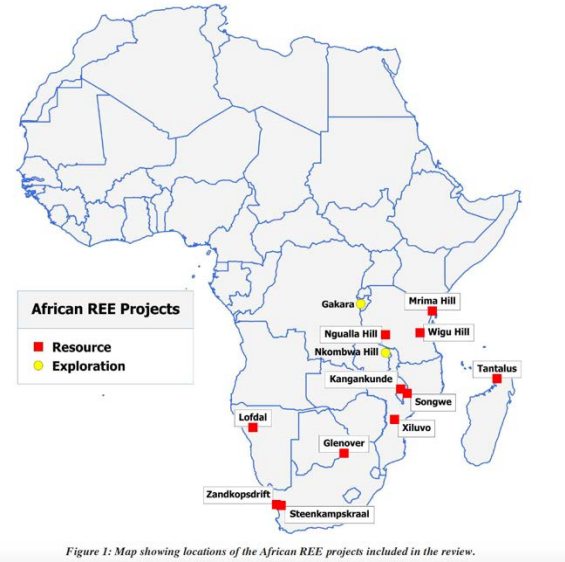
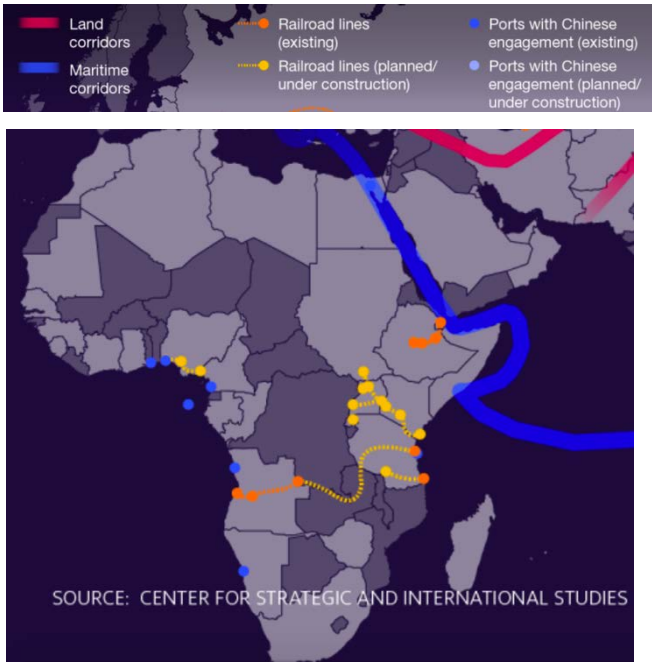


Figure 1: Map showing locations of the African REE projects included in the review.

Rare earth deposits of Africa, Harmer, Robin & Nex, Paul. (2016). Episodes. 39. 381., p. 384[55]



China's new Silk Road[56]
Source: David Foster, Yahoo Finance

Worth a thousand words, the similarity between the two maps above explains why tensions could only be expected between both (US and China) parties in that part of the world.

Expected, of course were the usual illustrations from both sides of some now well-oiled "three warfare" tricks and magic, and classic debt-trap diplomacy, used in particular to lure local authorities into some irresistible deals.

What was *kind of* expectable was that prospectors and mining engineers would roam the grounds around spots already identified, and that they would be escorted by special forces and S.O.F. in some kind of a mutual deterrence,

What had also been identified as a potential hazard was a possible brawl, caused by the explosive cocktail of extreme heat and humidity, testosterone and stress caused by prospecting rush.

What was not expected at all, though, was what autopsies revealed after what became known as the Nkombwa Hill[57] incident of 22 March, 2039.

[55] https://www.researchgate.net/publication/305918070_Rare_Earth_Deposits_of_Africa
[56] https://finance.yahoo.com/news/china-new-silk-road-us-192303366.html
[57] https://www.proactiveinvestors.com/companies/news/14460/african-consolidated-resources-agrees-jv-for-nkombwa-hill-rare-earth-project-17573.html

Rising 1100 feet (335m) above the surrounding savannah, this extinct volcano, "Nkombwa Mountain" impresses in its imposing massif.[58]

After a series of "close-shaving" encounters, where the Chinese team had demonstrated some astounding capacity in their ability to camouflage and quickly retreat while carrying what seemed like crushing loads of armament and communication gear, all hell broke loose in the evening of 22 March, 2039 in the savannah, on the foothills of the Nkombwa mountain.

When medics finally got to the deadly skirmish site, and after having taken care of US and Australian personnel, a young doctor took a look at the other bodies, badly wounded or worse still laying around.

And froze.

"*There's something wrong with these guys*", said Dr. Fishman, fresh out of Cambridge, MA, with his Harvard-MIT Health Sciences and Technology[59] PhD.

And wrong indeed it was.

While the brain monitoring and brain stimulation integrated in their helmets to help controlling mental state and alert of dangers was not too much of a surprise (DARPA had been funding similar projects for quite some time), the posture and behavior of the severely injured survivors could only be depicted as … supra-human.

What Dr. Fishman was looking at was a living proof that Chinese research in gene editing and military oriented CRISPR-Cas9[60] based manipulations had not stopped with the arrest of He Jiankui on 30 December 2019 and his three years' imprisonment plus RMB 3 million fine sentenced by the Shenzhen Nanshan District People's Court[61].

[58] https://www.africanagronomix.com/phosphate
[59] https://hst.mit.edu/
[60] https://en.wikipedia.org/wiki/CRISPR_gene_editing
[61] https://en.wikipedia.org/wiki/He_Jiankui

What he was looking at on that 23 March 2039 morning, was the proof that the successor to the Airborne Early Warning and Control System (AWACS)[62] had been doing a good job at identifying and keeping track of NBIC related emerging threats.

What he was looking at, as it was demonstrated by further in-depth exams, was that this 17 years old "man" had come out from a gene-editing, CRISPR-Cas9 tinkering based lab or, rather, farm, with traits, muscles, built-in night vision[63], resistance to sleep deprivation, to thirst, extreme heat and humidity that made "him", indeed, supra-human.

What he was looking at was proof that alarming reports dating as far as 2017[64] had been right when identifying the gene-editing threat as a possible game-changer in defense matters.

It took longer for experts to understand how these creatures had been retro-fitted with AI and biomaterials to "brain control" their weapons in what proved to be a highly-sophisticated man-machine teaming optimization, yet utterly failed experiment. That failure was good news for US and Australian folks, save for two Rare Earth International (REI)[65] engineers, in what could otherwise have been a total massacre.

What should have been a simple "commercial dispute" turned out to start an international crisis, as all fingers pointing at China, accused to have blatantly violated all ten points of the Nuremberg Code[66].

[62] see chapter « toughening and speeding up the response » in this document.
[63] https://phys.org/news/2019-08-nanoparticles-humans-built-in-night-vision.html
[64] https://www.atlanticcouncil.org/blogs/futuresource/gene-editing-in-china-beneficial-science-or-emerging-military-threat/
[65] http://www.rareearthmetalsinternational.com/
[66] https://en.wikipedia.org/wiki/Nuremberg_Code

Vardø, Kirkenes (Norway)

A couple of weeks after, 7500 miles up North somewhere in Lapland in a region encompassing the Norwegian county of Troms og Finnmark[67] and the Russian Kola Peninula[68], an even more severe incident took place, involving this time Norway, Finland, USA, Russia and China.

Norway, Finland and Russia have been sharing borders up there for several decades, but China and the US happened to have a presence, albeit less visible, for reasons summarized below.

China: As shown a few pages above, China had been prompt identifying the strategic importance of the Arctic Region vis à vis its *Silk Road* initiative, adding to the initial vision the *Polar Silk Road* element.

But, to develop this new opportunity, China had a few options.

The following excerpt from the European Parliament's China's Arctic policy briefing "*How China aligns rights and interests*"[69] perfectly sets the scene for presenting China's two options for their future shipping routes across the Arctic, the Northwest Passage and the Northern Sear Route:

China's interest in shipping routes across the Arctic as an alternative to the traditional southern maritime route through the Suez Canal is linked to its efforts to reduce its reliance on energy supplies from the Middle East by drawing more on Russian energy supplies. It also seeks to enhance its energy security by avoiding the US-monitored Malacca Strait chokepoint, as well as the pirate-infested Horn of Africa. Equally important is that alternative Arctic shipping routes such as the Northern Sea Route (NSR), the Northwest Passage and the Transpolar Route are much shorter (up to 35 %) than the traditional maritime route, requiring less fuel and producing less CO2 emissions. On the other hand, additional fees arise from passing through Russian waters with ice-breaker escorts and so far the NSR, for example, is only passable for a few months per year. Other challenges include the unpredictability of Arctic weather conditions, ice floes, and tonnage limitations. These constraints make Arctic shipping routes less suited for transit container shipping that relies on on-time delivery within a tight schedule. The routes are better suited for destination shipping, i.e. the transport of bulk goods such as minerals, LNG, gas and oil from points of extraction to markets outside the Arctic.

[67] https://en.wikipedia.org/wiki/Troms_og_Finnmark
[68] https://en.wikipedia.org/wiki/Kola_Peninsula
[69] http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/620231/EPRS_BRI(2018)620231_EN.pdf

Other disadvantages are the lack of purpose-built shipping fleets, variable seasonal conditions, limited satellite coverage, poor shore-side infrastructure and search-and-rescue capabilities, and high insurance premiums.

For reasons laid out in the European Parliament document above, there were very good reasons for China to look at using the Northern Sea Route along Russia, then stop and unload at the "right" port so that they could, from there, proceed down South to the rest of Europe by train.

- Hence the 2017 agreement between Russia and China to cooperate on the Northern Sea Route[70],
- Hence envisioning Kirkenes, Norway, as a massive new container terminal on the Barents Sea coast and, from there, considering a (to be built) 300-mile railway to the city of Rovaniemi in Finland, going then all the way down South to Helsinki and continuing from there to Tallinn, Estonia via a (to be built) tunnel under the Baltic sea[71],
- Hence a very much needed buy-in from Norwegian and Finnish governments, especially after a binational working group study[72] had concluded late 2018 that the project, estimated to cost more than $3 billion, would not be "financially feasible.", and also would "affect in many ways the Sámi culture and livelihoods, for example reindeer husbandry and its structure, reindeer grazing, and pastures."

In other words … another perfect playground for China to flex its Three Warfare influence muscle.
USA: Not far away from Kirkenes, in the city of Vardø, the United States and Norway had initiated a cooperation back in the 1950s on a radar system. Globus I was fielded at the end of the 1980s and, at the end of the 2010s, a new and more powerful radar system, Globus III was set up[73] in a new location at Vårberget (city of Vardø). Operated and controlled by the Norwegian Intelligence Service (NIS), one of the largest employers in that Northern part of Norway, Globus (I, II and III) had nevertheless always been identified by Russia as a major problematic neighbor.

The major modernization[74] underwent by Globus, rumored to play a key role in the surveillance and control system put in place by NATO to replace it AWACS, turned out to be just too much for Russia's comfort, whose most important military bases were situated on the Kola Peninsula, Mourmansk and Severomorsk, the naval and air base main administrative base of the Russian Northern Fleet[75].

In true Hybrid Warfare style, authorities then decided it was time to do something, ideally to both critically undermine regional support for the radar base and to degrade health condition of some "troublemakers".

[70] https://www.cnbc.com/2018/02/06/russia-and-china-battle-us-in-race-to-control-arctic.html
[71] http://www.xinhuanet.com/english/2018-03/10/c_137029993.htm
[72] http://julkaisut.valtioneuvosto.fi/handle/10024/161367
[73] https://en.wikipedia.org/wiki/Globus_II
[74] https://forsvaret.no/etjenesten/globus-modernization
[75] https://en.wikipedia.org/wiki/Northern_Fleet and https://commons.wikimedia.org/w/index.php?curid=11033173

From blunder/s to tragedy

The geographic proximity between **Vardø**, **Kirkenes** and **Mourmansk/Severomorsk,** but also the growing pressure for meeting deadlines (as a reminder, Silk Road was due for completion on 1st October, 2049, to coincide with the 100th anniversary of the People's Republic of China) probably looked good enough reasons for **黑色的水 Черная вода**, the security arm of the joint venture created by China and Russia for the Polar Silk Road project, to cut some corners and, while at it, experiment "things".

Except, cost-killers at **黑色的水 Черная вода** thought it would be an even better idea to save some money by hiring, this time, a new and price competitive hackers' startup and give them *carte blanche* for an "*all-inclusive package*" covering just about everything from:

- Fake news/deep fakes smearing campaigns against Norwegian and Finnish national politicians to undermine their credibility and their willingness for them to oppose to the Kirkenes-Helsinki railway,

- Fake news regarding the health hazard to Vardø population that would be caused by electromagnetic radiation from Globus radar,

- More fake news/deep fakes to demoralize US personnel in Vardø and their family left at home.

Progresses in stylometry[76] and successes achieved by the new NATO's surveillance and control system, together with a remarkable citizen participation, resulting from the worldwide campaigns against mind hacking coordinated by a majority of Nations after the NATO 2030 Oslo Summit, made it possible to identify the hackers and trace back to their payer.

That, in itself, could have triggered Article 5, as (Norwegian) NATO Secretary General Jens Stoltenberg had clearly stated during his intervention at the "Future of NATO" roundtable[77] during Word Economic Forum 2020 in Davos:

"*… a cyber-attack on any of our allies can trigger Article 5*", specifying "*the response doesn't have to be restricted to cyber, but can use any of the other domains*", while also adding "*we will not give the advantage to a potential adversary to precisely define what a red line is*".

[76] https://en.wikipedia.org/wiki/Code_stylometry
[77] https://www.weforum.org/events/world-economic-forum-annual-meeting-2020/sessions/the-future-of-nato starting at 35'20''

What did trigger Article 5 was the lethal effect of bioweapons that S.O.F. subcontractors of 黑色的水 **Черная вода** used for "*taking care of the Sámi issue*".

China's national strategy of military-civil fusion had indeed highlighted biology as a priority, and (ret.) general Zhang Shibo and former president of the National Defense University, had been quoted for saying: "*Modern biotechnology development is gradually showing strong signs characteristic of an offensive capability*" including the possibility that "*specific ethnic genetic attacks*" could be employed.

Furthermore, the 2017 edition of *Science of Military Strategy* a textbook published by the PLA's National Defense University that is considered to be relatively authoritative, debuted a section about biology as a domain of military struggle, similarly mentioning the potential for new kinds of biological warfare to include "*specific ethnic genetic attacks*."[78]

Black market had made it possible for the mercenaries to covertly source some of these bioweapons and to start testing them on some of the most vocal and organized Sámi reindeer herders opposed to the Kirkenes-Helsinki railway.

Officially unbeknownst to their payer, let alone, to Russian and Chinese authorities, that initiative, on Wednesday, 6 April 2039, proved lethal to most of their targets, "*a question of dose-response problem, it was supposed to just tranquilize them*" said, cynically, surviving perpetrators once identified and captured after most of them had succumbed for simply handling the products.

Article 5 triggered

The African and Arctic incidents had been the last straw on the proverbial camel's back. This time, NATO and its allies didn't buy the fig leaf of deniability, the "proxy" factor (黑色的水 **Черная вода** and its subcontractors) as new, blockchain based and quantum computing boosted traceability tools fed on data provided by NATO's new surveillance and control system made it clear who had really been pulling the strings.

[78] this paragraph is taken from https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/

Conclusion

Three points in this essay deserve, to this author's humble opinion, to be taken on board and to be turned into concrete actions:

Point # 1: Human mind should be seriously considered becoming NATO's 6th domain of operation.

➔ Working today on Doctrine, Rules of engagement, DOTMLPFI, Training and exercise addressing that domain should become priorities.

Point # 2: The follow-on to the E-3 Airborne Early Warning and Control System (AWACS) must obviously address all domains of operations. Not including Human mind would be a major mistake.

➔ Its design must address NBIC threats, including the influence issue briefly raised in this essay, as disrupting as it may look.

Point # 3: Security is not merely a military issue. Global security is a society issue, but the public at large is simply not aware of it.

➔ NATO, Nations and their partners must realize that the constant undermining (the "one thousand cuts" reality) they are suffering from, together with the unique opportunities NBIC offer to their competitors for hybrid, ambiguous warfare, create existential threats that cannot be addressed just by professional defense and security personnel. Together with industry, NATO, Nations and their partners must be deadly serious at designing and launching Education and Information programs towards a shared culture on global and civil security.

As difficult as it may be.

Annex: Recommendations

This is an annex to the main "Weaponization of neurosciences" essay, aimed at providing some recommendations related to the three main points summarized in its conclusion.
Going too far without interacting first with NATO, based on its reaction to the paper, would probably be unrealistic and useless, so here are some fairly concrete recommendations for the two first main points raised by the essay. The third point raises some strategic and geopolitical issues that clearly need to be better appreciated in order to provide plausible recommendations.

Point # 1: Human mind as NATO's 6th domain of operation.

Reaching that level may be a long shot but, whether or not that objective is achievable, the reality of the human mind hacking threat is undeniable and NATO must react in a concrete manner, and do it quickly.

The code name proposed for NATO's response is: "***Human mind hacking: Light, camera, action!"***, a three-year project.

- **Light**: Because it is a developing and complex subject, Human mind hacking needs light being shed on it to be made clearer and more decipherable.

  This will start with an exhaustive state of the art study addressing the nature, plausibility, development of that threat, together with an impact assessment of attacks already perpetrated. That particular task may be coordinated by the Innovation Hub. Evidence gathering, structuration of the study do not raise any particular issue and can be distributed among several military and non-military int'l partners, but particular attention must be given to the quality of the deliverables so that they lend themselves well to the two next steps of NATO response.

  This is a 10-month effort, going from April 2020 till February 2021. Updates every six month.

- **Camera**: Because the relevance and potential impact of the Human mind hacking issue address the full gamut of stakeholders, from leaders to first responders involved in complex, hybrid crises, from their awareness and understanding of the situation to decision-making process, cameras (figuratively speaking, of course) are needed to capture and broadcast in the most efficient manner the takeaways from the study summarized above, and to do it with messages customized to targeted audiences.

  While this effort must start immediately (April 2020) and be sustained for the whole duration of the project with regular updates to the material that will be generated, a first production of communication material will have to be out by September 2020.

- **Action**: Led by ACT, and starting in April 2020, this third pillar to the project has two primary objectives

  - As an *in itinere* work package, from Month 1 and for the three years' duration of the initial effort: setting in motion the production of the entire DOTMLPFI and coordinating its progresses,
  - As an immediate priority: Make sure that each and every exercise, wargame scenario, training material … includes Human mind hacking material generated by the ("light" and "camera") two other components of the project.

Point # 2: Allied Future Surveillance & Control (AFSC)

This is obviously a major project for NATO in terms of strategic importance and in terms of budget. Even if the current AWACS has benefited from many updates along its existence, AFSC's design faces unique challenges because of the complexity of today's conflicts (see main report re: hybrid, complex warfare …), let alone the exponential growth of (NBIC) technologies.
In other words, AFSC, in whatever shape/s or form/s this "*system of systems*" will take, will epitomize the depth and sophistication of NATO's understanding of tomorrow's conflicts.

I am convinced that addressing all possible threats is a vital necessity.

My recommendation is to extend that mind set to the whole design process.

Point # 3: Security is not merely a military issue. Global security is a society issue.

To develop that point and come out with concrete recommendations capable of providing some added value and not merely "state the obvious" would necessitate a better understanding of how NATO and chiefs of government, but also NATO and large international institutions work together and craft common agendas.

One point, though, goes without saying: the communication material put together by the "***Human mind hacking: Light, camera, action!"*** project needs to be designed with these partners in mind.

Considering the geographical and political breadth of this issue, this is probably the most challenging point of the "Weaponization of neurosciences" recommendations to address.