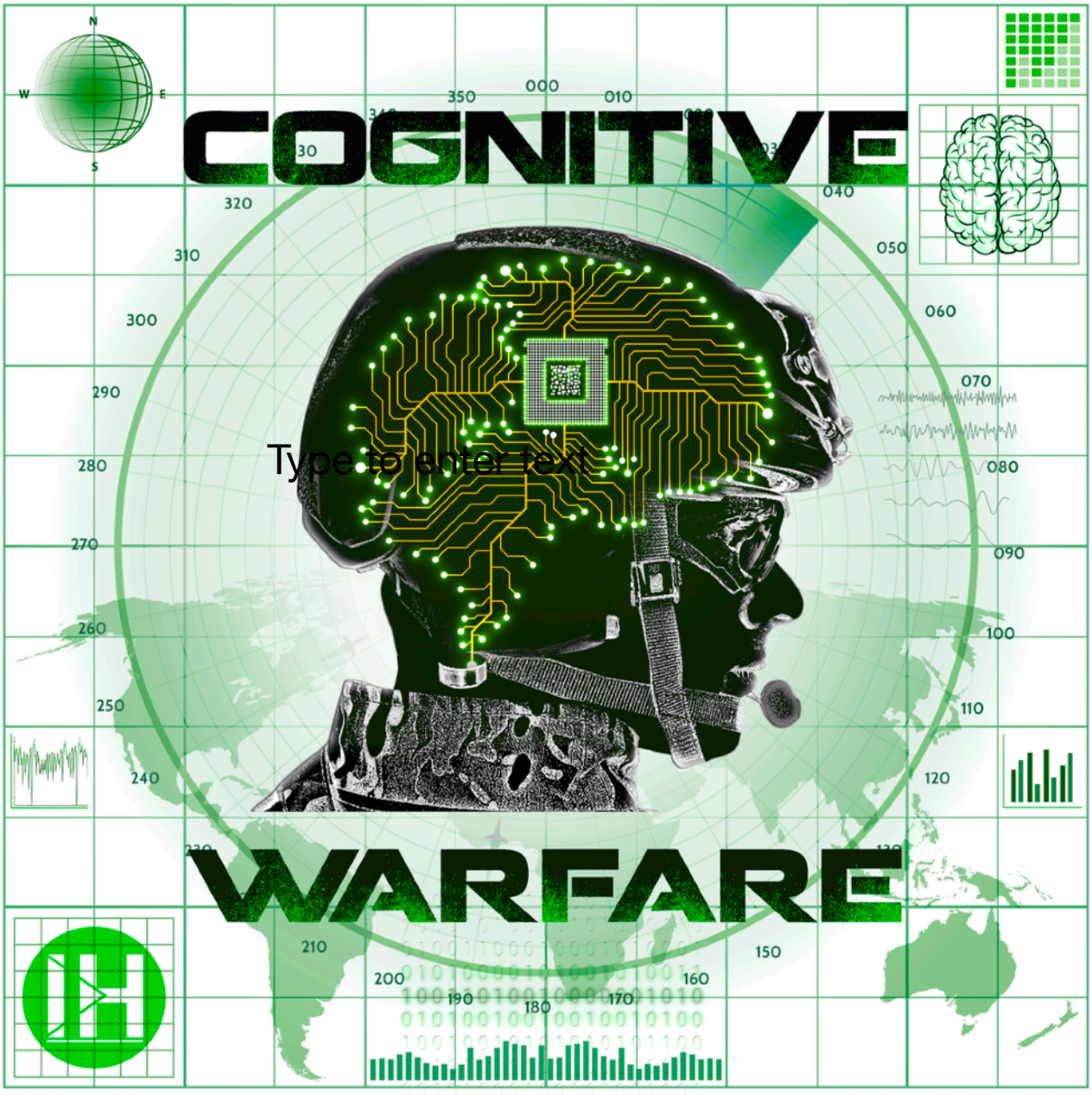


June-November 2020
François du Cluzel

Executive Summary **4**
Introduction **5**
The advent of Cognitive Warfare **6**
From Information Warfare to Cognitive Warfare 6
Hacking the individual 7
Trust is the target 8
Cognitive Warfare, a participatory propaganda 8
Behavioural economy 9
Cyberpsychology 11
The centrality of the human brain **12**
Understanding the brain is a key challenge for the future 12
The vulnerabilities of the human brain 13
The role of emotions 15
The battle for attention 15
Long-term impacts of technology on the brain 16
The promises of neurosciences 17
The militarisation of brain science **19**
Progress and Viability of Neuroscience and Technology (NeuroS/T) 19
Military and Intelligence Use of NeuroS/T 20
Direct Weaponisation of NeuroS/T 21
Neurodata 22
The neurobioeconomy 23
Towards a new operational domain **25**
Russian and Chinese Cognitive Warfare Definition 26
It's about Humans 28
Recommendations for NATO 32
Definition of the Human Domain 32
Impact on Warfare Development 34
Conclusion **36**
Bibliography and Sources **37**
Annex 1 ..... **38**
Nation State Case Study 1: The weaponisation of neurosciences in China 38
Annex 2 ..... **41**
Nation State Case Study 2: The Russian National Technology Initiative 41

This is Allied Command Transformation (ACT) sponsored study but the views and opinions expressed in this publication strictly reflect the discussions held on the Innovation Hub forums. They do not reflect those of ACT or its member Nations, so none of them can be quoted as an official statement belonging to them.

Executive Summary

As written in the Warfighting 2040 Paper, the nature of warfare has changed. The majority of current conflicts remain below the threshold of the traditionally accepted definition of warfare, but new forms of warfare have emerged such as Cognitive Warfare (CW), while the human mind is now being considered as a new domain of war.

With the increasing role of technology and information overload, individual cognitive abilities will no longer be sufficient to ensure an informed and timely decision-making, leading to the new concept of Cognitive Warfare, which has become a recurring term in military terminology in recent years.

Cognitive Warfare causes an insidious challenge. It disrupts the ordinary understandings and reactions to events in a gradual and subtle way, but with significant harmful effects over time. Cognitive warfare has universal reach, from the individual to states and multinational organisations. It feeds on the techniques of disinformation and propaganda aimed at psychologically exhausting the receptors of information. Everyone contributes to it, to varying degrees, consciously or sub consciously and it provides invaluable knowledge on society, especially open societies, such as those in the West. This knowledge can then be easily weaponised. It offers NATO's adversaries a means of bypassing the traditional battlefield with significant strategic results, which may be utilised to radically transform Western societies.

The instruments of information warfare, along with the addition of "neuro-weapons" adds to future technological perspectives, suggesting that the cognitive field will be one of tomorrow's battlefields. This perspective is further strengthened in by the rapid advances of NBICs (Nanotechnology, Biotechnology, Information Technology and Cognitive Sciences) and the understanding of the brain. NATO's adversaries are already investing heavily in these new technologies.

NATO needs to anticipate advances in these technologies by raising the awareness on the true potential of CW. Whatever the nature and object of warfare, it always comes down to a clash of human wills, and therefore what defines victory will be the ability to impose a desired behaviour on a chosen audience. Actions undertaken in the five domains - air, land, sea, space and cyber - are all executed in order to have an effect on the human domain. It is therefore time for NATO to recognise the renewed importance of the sixth operational domain, namely the Human Domain.

Introduction

Individual and organisational cognitive capabilities will be of paramount importance because of the speed and volume of information available in the modern battlespace. If modern technology holds the promise of improving human cognitive performance, it also holds the seeds of serious threats for military organisations.

Because organisations are made up of human beings, human limitations and preferences ultimately affect organisational behaviour and decision-making processes. Military organisations are subject to the problem of limited rationality, but this constraint is often overlooked in practice[1].

In an environment permeated with technology and overloaded with information, managing the cognitive abilities within military organisations will be key, while developing capabilities to harm the cognitive abilities of opponents will be a necessity. In other words, NATO will need to get the ability to safeguard her decision-making process and disrupt the adversary's one.

This study intends to respond to the three following questions:

- Improve awareness on Cognitive Warfare, including a better understanding of the risks and opportunities of new Cognitive / Human Mind technologies;
- Provide 'out-of-the-box' insight on Cognitive Warfare;
- And to provide strategic level arguments to SACT as to recommend, or not, Cognitive / Human Mind as an Operational Domain.

The advent of Cognitive Warfare

From Information Warfare to Cognitive Warfare

Information warfare (IW) is the most related, and, thus, the most easily conflated, type of warfare with regards to cognitive warfare. However, there are key distinctions that make cognitive warfare unique enough to be addressed under its own jurisdiction. As a concept, IW was first coined and developed under US Military doctrine, and has subsequently been adopted in different forms by several nations.

As former US Navy Commander Stuart Green described it[2] as, "Information operations, the closest existing American doctrinal concept for cognitive warfare, consists of five 'core capabilities', or elements. These include electronic warfare, computer network operations, PsyOps, military deception, and operational security."

Succinctly, Information Warfare aims at controlling the flow of information.

> "Conflicts will increasingly depend on/and revolve around, information and communications— (…) Indeed, both cyberwar and netwar are modes of conflict that are largely about "knowledge"—about who knows what, when, where, and why, and about how secure a society"
> **John Arquilla and David Ronfeldt**
> The Advent of Netwar, RAND, 1996

Information warfare has been designed primarily to support objectives defined by the traditional mission of military organisations - namely, to produce lethal kinetic effects on the battlefield. It was not designed to achieve lasting political successes.

As defined by Clint Watts, cognitive Warfare opposes the capacities to know and to produce, it actively thwarts knowledge. Cognitive sciences cover all the sciences that concern knowledge and its processes (psychology, linguistics, neurobiology, logic and more).[3]

Cognitive Warfare degrades the capacity to know, produce or thwart knowledge. Cognitive sciences cover all the sciences that concern knowledge and its processes (psychology, linguistics, neurobiology, logic and more).

Cognitive Warfare is therefore the way of using knowledge for a conflicting purpose. In its broadest sense, cognitive warfare is not limited to the military or institutional world. Since the early 1990s, this capability has tended to be applied to the political, economic, cultural and societal fields.

Any user of modern information technologies is a potential target. **It targets the whole of a nation's human capital.**

> "Big Data allows us to develop fabulous calculation and analysis performances, but what makes it possible to respond to a situation is reason and reason is what enables to take a decision in what is not calculable, otherwise we only confirm the state of affairs."
> **Bernard Stiegler**

The most striking shift of this practice from the military, to the civilian, world is the pervasiveness of CW activities across everyday life that sit outside the normal peace-crisis-conflict construct (with harmful effects). Even if a cognitive war could be conducted to complement to a military conflict, it can also be conducted alone, without any link to an engagement of the armed forces. Moreover, cognitive warfare is potentially endless since there can be no peace treaty or surrender for this type of conflict.

Evidence now exists that shows new CW tools & techniques target military personnel directly , not only with classical information weapons but also with a constantly growing and rapidly evolving arsenal of neuro-weapons, targeting the brain. It is important to recognise various nations' dedicated endeavours to develop non-kinetic operations, that target the Human with effects at every level - from the individual level, up to the socio-political level.

Hacking the individual

The revolution in information technology has enabled cognitive manipulations of a new kind, on an unprecedented and highly elaborate scale. All this happens at much lower cost than in the past, when it was necessary to create effects and impact through non-virtual actions in the physical realm. Thus, in a continuous process, classical military capabilities do not counter cognitive warfare. Despite the military having difficulty in recognising the reality and effectiveness of the phenomena associated with cognitive warfare, the relevance of kinetic and resource-intensive means of warfare is nonetheless diminishing.

Social engineering always starts with a deep dive into the human environment of the target. The goal is to understand the psychology of the targeted people. This phase is more important than any other as it allows not only the precise targeting of the right people but also to anticipate reactions, and to develop empathy. Understanding the human environment is the key to building the trust that will ultimately lead to the desired results. Humans are an easy target since they all contribute by providing information on themselves, making the adversaries' sock-puppets[4] more powerful.

> "Social engineering is the art and science of getting people to comply to your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behaviour and it is far from foolproof"
>
> **Harl**, People Hacking, 1997

In any case NATO's adversaries focus on identifying the Alliance's centres of gravity and vulnerabilities. They have long identified that the main vulnerability is the human. It is easy to find these centres of gravity in open societies because they are reflected in the study of human and social sciences such as political science, history, geography, biology, philosophy, voting systems, public administration, international politics, international relations, religious studies, education, sociology, arts and culture…

Cognitive Warfare is a war of ideologies that strives to erode the trust that underpins every society.

Trust is the target

Cognitive warfare pursues the objective of undermining trust (public trust in electoral processes, trust in institutions, allies, politicians…).[5], therefore the individual becomes the weapon, while the goal is not to attack what individuals think but rather t*he way they think*[6].

It has the potential to unravel the entire social contract that underpins societies.

It is natural to trust the senses, to believe what is seen and read. But the democratisation of automated tools and techniques using AI, no longer requiring a technological background, enables anyone to distort information and to further undermine trust in open societies. The use of fake news, deep fakes, Trojan horses, and digital avatars will create new suspicions which anyone can exploit.

It is easier and cheaper for adversaries to undermine trust in our own systems than to attack our power grids, factories or military compounds. Hence, it is likely that in the near future there will be more attacks, from a growing and much more diverse number of potential players with a greater risk for escalation or miscalculation. The characteristics of cyberspace (lack of regulation, difficulties and associated risks of attribution of attacks in particular) mean that new actors, either state or non-state, are to be expected[7].

As the example of COVID-19 shows, the massive amount of texts on the subject, including deliberately biased texts (example is the Lancet study on chloroquine) created an information and knowledge overload which, in turn, generates both a loss of credibility and a need for closure. Therefore the ability for humans to question, normally, any data/information presented is hampered, with a tendency to fall back on biases to the detriment of unfettered decision-making.
It applies to trust among individuals as well as groups, political alliances and societies.

"**Trust, in particular among allies, is a targeted vulnerability**. As any international institution does, NATO relies on trust between its partners. Trust is based not only on respecting some explicit and tangible agreements, but also on 'invisible contracts,' on sharing values, which is not easy when such a proportion of allied nations have been fighting each other for centuries. This has left wounds and scars creating a cognitive/information landscape that our adversaries study with great care. Their objective is to identify the '**Cognitive Centers of Gravity**' of the Alliance, which they will target with 'info-weapons'."[8]

Cognitive Warfare, a participatory propaganda[9]

In many ways, cognitive warfare can be compared to propaganda, which can be defined as "a set of methods employed by an organised group that wants to bring about the active or passive participation in its actions of a mass of individuals, psychologically unified through psychological manipulations and incorporated in an organisation."[10]

The purpose of propaganda is not to "program" minds, but to influence attitudes and behaviours by getting people to adopt the right attitude, which may consist of doing certain things or, often, stopping doing them.

> "New tools and techniques, combined with the changing technological and information foundations of modern societies, are creating an unprecedented capacity to conduct virtual societal warfare."
>
> **Michael J. Mazarr**

Cognitive Warfare is methodically exploited as a component of a global strategy by adversaries aimed at weakening, interfering and destabilising targeted populations, institutions and states, in order to influence their choices, to undermine the autonomy of their decisions and the sovereignty of their institutions. Such campaigns combine both real and distorted information (misinformation), exaggerated facts and fabricated news (disinformation).

> "Modern propaganda is based on scientific analyses of psychology and sociology. Step by step, the propagandist builds his techniques on the basis of his knowledge of man, his tendencies, his desires, his needs, his psychic mechanisms, his conditioning — and as much on social psychology as on depth psychology."
>
> **Jacques Ellul**, Propaganda, 1962

Disinformation preys on the cognitive vulnerabilities of its targets by taking advantage of pre-existing anxieties or beliefs that predispose them to accept false information. This requires the aggressor to have an acute understanding of the socio-political dynamics at play and to know exactly when and how to penetrate to best exploit these vulnerabilities.

Cognitive Warfare exploits the innate vulnerabilities of the human mind because of the way it is designed to process information, which have always been exploited in warfare, of course. However, due to the speed and pervasiveness of technology and information, the human mind is no longer able to process the flow of information.

Where CW differs from propaganda is in the fact that everyone participates, mostly inadvertently, to information processing and knowledge formation in an unprecedented way. This is a subtle but significant change. While individuals were passively submitted to propaganda, they now actively contribute to it.

The exploitation of human cognition has become a massive industry. And it is expected that emerging artificial intelligence (AI) tools will soon provide propagandists radically enhanced capabilities to manipulate human minds and change human behaviour[11].

Behavioural economy

"Capitalism is undergoing a radical mutation. What many describe as the **'data economy'** is in fact better understood as a 'behavioural economics'".

Behavioural economics (BE) is defined as a method of economic analysis that applies psychological insights into human behaviour to explain economic decision-making.
As research into decision-making shows, behaviour becomes increasingly computational, BE is at the crossroad between hard science and soft science[12].
Operationally, this means massive and methodical use of behavioural data and the development of methods to aggressively seek out new data sources. With the vast amount of (behavioural) data that everyone generates mostly without our consent and awareness, further manipulation is easily achievable.
The large digital economy companies have developed new data capture methods, allowing the inference of personal information that users may not necessarily intend to disclose. The excess data has become the basis for new prediction markets called targeted advertising.
"Here is the origin of surveillance capitalism in an unprecedented and lucrative brew: behavioural surplus, data science, material infrastructure, computational power, algorithmic systems, and automated platforms", claims Soshanna Zuboff[13].
In democratic societies, advertising has quickly become as important as research. It has finally become the cornerstone of a new type of business that depends on large-scale online monitoring.
The target is the human being in the broadest sense and it is easy to divert the data obtained from just commercial purposes, as the Cambridge Analytica (CA) scandal demonstrated.
Thus, the lack of regulation of the digital space - the so-called "data swamp"- does not only benefit the digital-age regimes, which "can exert remarkable control over not just computer networks and human bodies, but the minds of their citizens as well"[14].
It can also be utilised for malign purposes as the example of the CA scandal has shown.

> "Technology is going on unabated and will continue to go on unabated. […] Because technology is going so fast and because people don't understand it, there was always going to be a Cambridge Analytica."
> **Julian Wheatland**
> Ex-Chief Operating Officer of Cambridge Analytica

CA digital model outlined how to combine personal data with machine learning for political ends by profiling individual voters in order to target them with personalised political advertisements.
Using the most advanced survey and psychometrics techniques, Cambridge Analytica was actually able to collect a vast amount of individuals' data that helped them understand through economics, demographics, social and behavioural information what each of them thought. It literally provided the company a window into the minds of people.
The gigantic collection of data organised via digital technologies is today primarily used to define and anticipate human behaviour. Behavioural knowledge is a strategic asset. "Behavioural economics adapts psychology research to economic models, thus creating more accurate representations of human interactions."[15]
"Cambridge Analytica has demonstrated how it's possible […] to leverage tools to build a scaled-down version of the massive surveillance and manipulation machines"[16]

As shown by the example of Cambridge Analytica, one can weaponise such knowledge and develop appropriate offensive and defensive capabilities, paving the way for virtual societal warfare.[17] A systematic use of BE methods applied to the military could lead to better understanding of how individuals and groups behave and think, eventually leading to a wider understanding of the decision-making environment of adversaries. There is a real risk that access to behavioural data utilising the tools and techniques of BE, as shown by the example of Cambridge Analytica, could allow any malicious actor- whether state or non-state- to strategically harm open societies and their instruments of power.

Cyberpsychology

Assuming that technology affects everyone, studying and understanding human behaviour in relation to technology is vital as the line between cyberspace and the real world is becoming blurry.

The exponentially increasing impact of cybernetics, digital technologies, and virtuality can only be gauged when considered through their effects on societies, humans, and their respective behaviours.

Cyberpsychology is at the crossroads of two main fields: psychology and cybernetics. All this is relevant to defense and security, and to all areas that matter to NATO as it prepares for transformation. Centered on the clarification of the mechanisms of thought and on the conceptions, uses and limits of cybernetic systems, cyberpsychology is a key issue in the vast field of Cognitive Sciences. The evolution of AI introduces new words, new concepts, but also new theories that encompass a study of the natural functioning of humans and of the machines they have built and which, today, are fully integrated in their natural environment (anthropo-technical). Tomorrow's human beings will have to invent a psychology of their relation to machines. But the challenge is to develop also a psychology of machines, artificial intelligent software or hybrid robots.

Cyber psychology is a complex scientific field that encompasses all psychological phenomena associated with, or affected by relevant evolving technologies. Cyber psychology examines the way humans and machines impact each other, and explores how the relationship between humans and AI will change human interactions and inter-machine communication[18].

* * * *

Paradoxically, the development of information technology and its use for manipulative purposes in particular highlights the increasingly predominant role of the brain.

The brain is the most complex part of the human body. This organ is the seat of intelligence, the interpreter of the senses, the initiator of body movements, the controller of behaviour and the centre of decisions.

The centrality of the human brain

For centuries, scientists and philosophers have been fascinated by the brain, but until recently, they considered the brain to be almost incomprehensible. Today, however, the brain is beginning to reveal its secrets. Scientists have learned more about the brain in the past decade than in any previous century, thanks to the accelerating pace of research in the neurological and behavioural sciences and the development of new research techniques. For the military, it represents the last frontier in science, in that it could bring a decisive advantage in tomorrow's wars.

Understanding the brain is a key challenge for the future

Substantial advances have been made in recent decades in understanding how the brain functions. While our decision-making processes remain centered on Human in particular with its capacity to orient (OODA loop), fed by data, analysis and visualisations, the inability of human to process, fuse and analyse the profusion of data in a timely manner calls for humans to team with AI machines to compete with AI machines. In order to keep a balance between the human and the machine in the decision-making process, it becomes necessary to be aware of human limitations and vulnerabilities. It all starts with understanding our cognition processes and the way our brain's function.

Cognitive Science
Discipline associating psychology, sociology, linguistics, artificial intelligence and neurosciences, and having for object the explicitation of the mechanisms of thought and information processing mobilised for the acquisition, conservation, use and transmission of knowledge.

Neuroscience
Trans-disciplinary scientific discipline associating biology, mathematics, computer science, etc., with the aim of studying the organisation and functioning of the nervous system, from the point of view of both its structure and its functioning, from the molecular scale down to the level of the organs.

Over the past two decades, cognitive science and neuroscience have taken a new step in the analysis and understanding of the human brain, and have opened up new perspectives in terms of brain research, if not indeed of a hybridisation, then of human and artificial intelligence. They have mainly made a major contribution to the study of the diversity of neuro-psychic mechanisms facilitating learning and, as a result, have, for example, challenged the intuition of "multiple intelligences". No one today can any longer ignore the fact that the brain is both the seat of emotions the interactive mechanisms of memorisation, information processing, problem solving and decision-making.

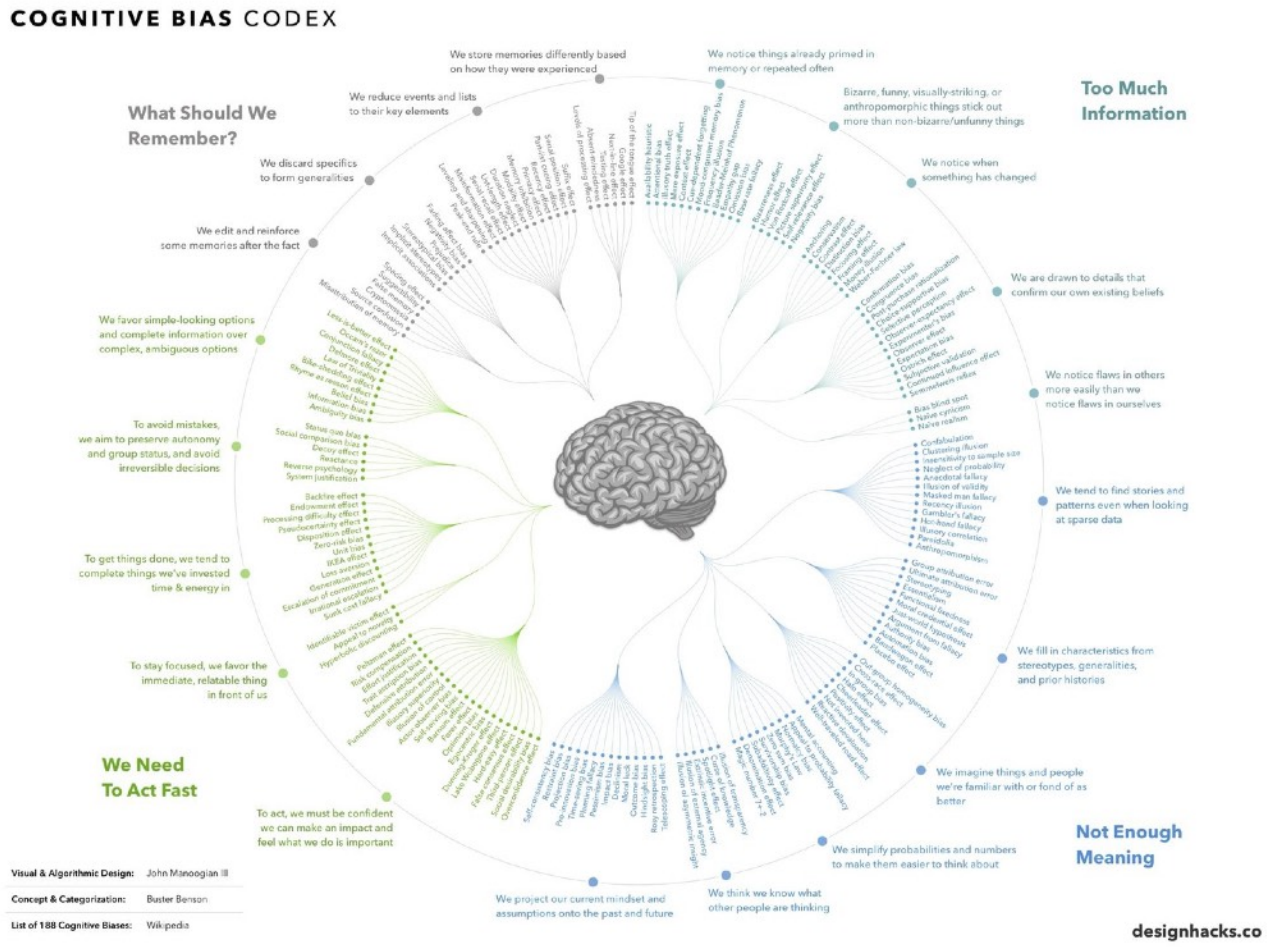
The vulnerabilities of the human brain

"In the cognitive war, it's more important than ever to know thyself."[19]

Humans have developed adaptations to cope with cognitive limitations allowing more efficient processing of information. Unfortunately, these same shortcuts introduce distortions in our thinking and communication, making communication efforts ineffective and subject to manipulation by adversaries seeking to mislead or confuse. These cognitive biases can lead to inaccurate judgments and poor decision making that could trigger an unintended escalation or prevent the timely identification of threats. Understanding the sources and types of cognitive biases can help reduce misunderstandings and inform the development of better strategies to respond to opponents' attempts to use these biases to their advantage.

In particular, the brain:

- is unable to distinct whether particular information is right or wrong;
- Is led to take shortcuts in determining the trustworthiness of messages in case of information overload;
- is led to believe statements or messages that its already heard as true, even though these may be false;
- accepts statements as true, if backed by evidence, with no regards to the authenticity of the that evidence.



Those are, among many others, the cognitive bias, defined as a systematic pattern of deviation from norm or rationality in judgment.[20]

There are many different cognitive biases[21] inherently stemming from the human brain. Most of them are relevant to the information environment. Probably the most common and most damaging cognitive bias is the confirmation bias. This is the effect that leads people to look for evidence that confirms what they already think or suspect, to regard facts and ideas they encounter as further confirmation, and to dismiss or ignore any evidence that seems to support another point of view. In other words, "*people see what they want to see*"[22].

Cognitive biases effect everyone, from soldiers on the ground to staff officers, and to a greater extent than everyone admits.

It is not only important to recognise it in ourselves, but to study the biases of adversaries to understand how they behave and interact.

As stated by Robert P. Kozloski, "The importance of truly "knowing yourself" cannot be understated. Advances in computing technology, particularly machine learning, provide the military with the opportunity to know itself like never before. Collecting and analysing the data

generated in virtual environments will enable military organisations to understand the cognitive performance of individuals."[23]

Ultimately, operational advantages in cognitive warfare will first come from the improvement of understanding of military cognitive abilities and limitations.

The role of emotions

In the digital realm, what allows the digital industries and their customers (and notably advertisers) to distinguish individuals in the crowd, to refine personalisation and behavioural analysis, are emotions. Every social media platform, every website is designed to be addictive and to trigger some emotional bursts, trapping the brain in a cycle of posts. The speed, emotional intensity, and echo-chamber qualities of social media content cause those exposed to it to experience more extreme reactions. Social media is particularly well suited to worsening political and social polarisation because of their ability to disseminate violent images and scary rumours very quickly and intensely. "The more the anger spreads, the more Internet users are susceptible to becoming a troll."[24]

At the political and strategic level, it would be wrong to underestimate the impact of emotions. Dominique Moïsi showed in his book "The Geopolitics of Emotion"[25], how emotions - hope, fear and humiliation - were shaping the world and international relations with the echo-chamber effect of the social media. For example, it seems important to integrate into theoretical studies on terrorist phenomena the role of emotions leading to a violent and/or a terrorist path.

By limiting cognitive abilities, emotions also play a role in decision-making, performance, and overall well-being, and it's impossible to stop people from experiencing them. "In the face of violence, the very first obstacle you will have to face will not be your abuser, but your own reactions."[26]

The battle for attention

Never have knowledge and information been so accessible, so abundant, and so shareable. Gaining attention means not only building a privileged relationship with our interlocutors to better communicate and persuade, but it also means preventing competitors from getting that attention, be it political, economic, social or even in our personal life.

This battlefield is global via the internet. With no beginning and no end, this conquest knows no respite, punctuated by notifications from our smartphones, anywhere, 24 hours a day, 7 days a week.

> "We are competing with sleep"
>
> **Reed Hastings**
> CEO of Netflix

Coined in 1996 by Professor B.J. Fogg from Stanford University, "captology"[27] is defined as the science of using "computers as technologies of persuasion".

The time has therefore come to adopt the rules of this "attention economy", to master the technologies related to "captology", to understand how these challenges are completely new. Indeed, this battle is not limited to screens and design, it also takes place in brains, especially in the way they are misled. It is also a question of understanding why, in the age of social networks, some "fake news", conspiracy theories or "alternative facts", seduce and convince, while at the same time rendering their victims inaudible.
Attention on the contrary is a limited and increasingly scarce resource. It cannot be shared: it can be conquered and kept. The battle for attention is now at work, involving companies, states and citizens.
The issues at stake now go far beyond the framework of pedagogy, ethics and screen addiction. The consumption environment, especially marketing, is leading the way. Marketers have long understood that the seat of attention and decision making is the brain and as such have long sought to understand, anticipate its choices and influence it.
This approach naturally applies just as well to military affairs and adversaries have already understood this.

Long-term impacts of technology on the brain

As Dr. James Giordano claims, "the brain will the battlefield of the 21st century".[28]

And when it comes to shaping the brain, the technological environment plays a key role.

The brain has only one chance to develop. Damage to the brain is very often irreversible. Understanding and protecting our brains from external aggression, of all kinds, will be one of the major challenges of the future.

According to the neuroscientist Maryanne Wolf, humans were not meant to read and the invention of printing changed the shape of our brains[29]. It took years, if not centuries, to assess the consequences - social, political or sociological for example - of the invention of printing. It will likely take longer before understanding accurately the long-term consequences of the digital age but one thing everyone agrees on is that the human brain is changing today faster than ever before with the pervasiveness of digital technology.

There is a growing amount of research that explores how technology affects the brain. Studies show that exposure to technology shapes the cognitive processes and the ability to take in information. One of the major findings is the advent of a society of 'cognitive offloaders', meaning that no one memorises important information any longer. Instead, the brain tends to remember the location where they retrieved when it is next required. With information and visual overload, the brain tends to scan information and pick out what appears to be important with no regard to the rest.

One of the evolutions already noticed is the loss of critical thinking directly related to screen reading and the increasing inability to read a real book. The way information is processed affects brain development, leading to neglect of the sophisticated thought processes. Brains will thus be different tomorrow. It is therefore highly probable that our brains will be radically

transformed in an extremely short period, but it is also likely that this change will come at the expense of more sophisticated, more complex thinking processes necessary for critical analysis.

In an era where memory is outsourced to Google, GPS, calendar alerts and calculators, it will necessarily produce a generalised loss of knowledge that is not just memory, but rather motor memory. In other words, a long-term process of disabling connections in your brain[30] is ongoing. It will present both vulnerabilities and opportunities.

However, there is also plenty of research showing the benefits of technology on our cognitive functions. For example, a Princeton University[31] study found that expert video gamers have a higher ability to process data, to make decisions faster or even to achieve simultaneous multitasks in comparison to non-gamers. There is a general consensus among neuroscientists that a reasoned use of information technology (and particularly games) is beneficial to the brain.

By further blurring the line between the real and the virtual, the development of technologies such as Virtual Reality (VR), Augmented Reality (AR) or Mixed Reality (MR) has the potential to transform the brain's abilities even more radically[32]. Behaviours in virtual environments can continue to influence real behaviour long after exiting VR.[33]

Yet, virtual environments offer the opportunity to efficiently complement live training since it can provide cognitive experience that a live exercise cannot replicate.

While there are concerns and research on how digital media are harming developing minds, it is still difficult to predict how the technology will affect and change the brain, but with the ubiquity of IT, it will become increasingly crucial to carefully detect and anticipate the impacts of information technology on the brain and to adapt the use of information technology.

In the long-term, there is little doubt that Information Technologies will transform the brain, thus providing more opportunities to learn and to apprehend the cyber environment but also vulnerabilities that will require closely monitoring in order to counter and defend against them and how to best exploit them.

The promises of neurosciences

“Social neuroscience holds the promise of understanding people’s thoughts, emotions and intentions through the mere observation of their biology.”[34]

Should scientists be able to establish a close and precise correspondence between biological functions on the one hand and social cognitions and behaviours on the other hand, neuroscientific methods could have tremendous applications for many disciplines and for our society in general. It includes decision-making, exchanges, physical and mental health care, prevention, jurisprudence, and more.

This highlights how far neurosciences occupies a growing place in medical and scientific research. More than just a discipline, they articulate a set of fields related to the knowledge of the brain and nervous system and question the complex relationships between man and his

environment and fellow human beings. From biomedical research to cognitive sciences, the actors, approaches and organisations that structure neuroscience are diverse.

Often convergent, they can also be competitive.

While the discoveries and challenges of the neurosciences are relatively well known, this field raises both hope and concern. In a disorganised and, at times, ill-informed way, "neuroscience" seems to be everywhere. Integrated, sometimes indiscriminately, in many debates, they are mobilised around the issues of society and public health, education, aging, and nourish the hopes of an augmented man.

* * * *

Today, the manipulation of our perception, thoughts and behaviours is taking place on previously unimaginable scales of time, space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities that every individual must learn to deal with. Many actors are likely to exploit these vulnerabilities, while the evolution of technology for producing and disseminating information is increasingly fast. At the same time, as the cost of technology steadily drops, more actors enter the scene.

As the technology evolves, so do the vulnerabilities.

The militarisation of brain science

Scientists around the world are asking the question of how to free humanity from the limitations of the body. The line between healing and augmentation becomes blurred. In addition, the logical progression of research is to achieve a perfect human being through new technological standards.

In the wake of the U.S. Brain Initiative initiated in 2014, all the major powers (EU/China/Russia) have launched their own brain research programs with substantial fundings. China sees the brain **"as the HQ of the Human body and precisely attacking the HQ is one of the most effective strategies for determining victory or defeat on the battlefield"[35].**

The revolution in NBIC (Nanotechnology, biotechnology, information technology, and cognitive science) including advances in genomics, has the potential for dual-use technology development. A wide range of military applications such as improving the performance of soldiers, developing new weapons such as directed energy weapons are already discussed.

Progress and Viability of Neuroscience and Technology (NeuroS/T)

Neuroscience employs a variety of methods and technologies to evaluate and influence neurologic substrates and processes of cognition, emotion, and behaviour. In general, brain science can be either basic or applied research. Basic research focuses upon obtaining knowledge and furthering understanding of structures and functions of the nervous system on a variety of levels by employing methods of the physical and natural sciences. Applied research seeks to develop translational approaches that can be directly utilised to understand and modify the physiology, psychology, and/or pathology of target organisms, including humans. Neuroscientific methods and technologies (neuroS/T) can be further categorised as those used to assess, and those used to affect the structures and functions of the nervous system, although these categories and actions are not mutually exclusive. For example, the use of certain drugs, toxins, and probes to elucidate functions of various sites of the central and peripheral nervous system can also affect neural activity.

NeuroS/T is broadly considered a natural and/or life science and there is implicit and explicit intent, if not expectation to develop and employ tools and outcomes of research in clinical medicine. Neuroscientific techniques, technologies, and information could be used for medical as well as non-medical (educational, occupational, lifestyle, military, etc.) purposes[36].

It is questionable whether the uses, performance enablements, and resulting capabilities could (or should) be used in intelligence and/or diplomatic operations to mitigate and subvert aggression, violence, and conflict. Of more focal concern are uses of research findings and products to directly facilitate the performance of combatants, the integration of human-machine interfaces to optimise combat capabilities of semi-autonomous vehicles (e.g., drones), and development of biological and chemical weapons (i.e., neuroweapons).

Some NATO Nations have already acknowledged that neuroscientific techniques and technologies have high potential for operational use in a variety of security, defense and intelligence enterprises, while recognising the need to address the current and short-term ethical, legal and social issues generated by such use[37].

Military and Intelligence Use of NeuroS/T

The use of neuroS/T for military and intelligence purposes is realistic, and represents a clear and present concern. In 2014, a US report asserted that neuroscience and technology had matured considerably and were being increasingly considered, and in some cases evaluated for operational use in security, intelligence, and defense operations. More broadly, the iterative recognition of the viability of neuroscience and technology in these agenda reflects the pace and breadth of developments in the field. Although a number of nations have pursued, and are currently pursuing neuroscientific research and development for military purposes, perhaps the most proactive efforts in this regard have been conducted by the United States Department of Defense; with most notable and rapidly maturing research and development conducted by the Defense Advanced Research Projects Agency (DARPA) and Intelligence Advanced Research Projects Activity (IARPA). To be sure, many DARPA projects are explicitly directed toward advancing neuropsychiatric treatments and interventions that will improve both military and civilian medicine. Yet, it is important to note the prominent ongoing – and expanding – efforts in this domain by NATO European and trans-Pacific strategic competitor nations.

As the 2008 National Research Council report[38] stated, "… for good or for ill, an ability to better understand the capabilities of the body and brain… could be exploited for gathering intelligence, military operations, information management, public safety and forensics". To paraphrase Aristotle, every human activity and tool can be regarded as purposed toward some definable "good". However, definitions of "good" may vary, and what is regarded as good for some may present harm to others. The potential for neuroS/T to afford insight, understanding, and capability to affect cognitive, emotional, and behavioural aspects of individuals and groups render the brain sciences particularly attractive for use in security, intelligence, and military/warfare initiatives.

To approach this issue, it is important to establish four fundamental premises.

- **Firstly**, neuroS/T is, and will be increasingly and more widely incorporated into approaches to national security, intelligence gathering and analysis, and aspects of military operations;
- **Secondly**, such capabilities afford considerable power;
- **Thirdly**, many countries are actively developing and subsidising neuroS/T research under dual-use agendas or for direct incorporation into military programs;
- **Fourthly**, these international efforts could lead to a "capabilities race" as nations react to new developments by attempting to counter and/or improve upon one another's discoveries.

This type of escalation represents a realistic possibility with potential to affect international security. Such "brinksmanship" must be acknowledged as a potential impediment to attempts to develop analyses and guidelines (that inform or prompt policies) that seek to constrain or restrict these avenues of research and development.

Neuroscientific techniques and technologies that are being utilised for military efforts include:

1. Neural systems modelling and human/brain-machine interactive networks in intelligence, training and operational systems;
2. Neuroscientific and neurotechnological approaches to optimising performance and resilience in combat and military support personnel;
3. Direct weaponisation of neuroscience and neurotechnology.

Of note is that each and all may contribute to establishing a role for brain science on the 21st century battlescape.

Direct Weaponisation of NeuroS/T

The formal definition of a weapon as "a means of contending against others" can be extended to include any implement "…used to injure, defeat, or destroy". Both definitions apply to products of neuroS/T research that can be employed in military/warfare scenarios. The objectives for neuroweapons in warfare may be achieved by augmenting or degrading functions of the nervous system, so as to affect cognitive, emotional and/or motor activity and capability (e.g., perception, judgment, morale, pain tolerance, or physical abilities and stamina) necessary for combat. Many technologies can be used to produce these effects, and there is demonstrated utility for neuroweapons in both conventional and irregular warfare scenarios.

At present, outcomes and products of computational neuroscience and neuropharmacologic research could be used for more indirect applications, such as enabling human efforts by simulating, interacting with, and optimising brain functions, and the classification and detection of human cognitive, emotional, and motivational states to augment intelligence or counterintelligence tactics. Human/brain-machine interfacing neurotechnologies capable of optimising data assimilation and interpretation systems by mediating access to – and manipulation of – signal detection, processing, and/or integration are being explored for their potential to delimit "human weak links" in the intelligence chain.

The weaponised use of neuroscientific tools and products is not new. Historically, such weapons which include nerve gas and various drugs, pharmacologic stimulants (e.g., amphetamines), sedatives, sensory stimuli, have been applied as neuroweapons to incapacitate the enemy, and even sleep deprivation and distribution of emotionally provocative information in psychological operations (i.e., PSYOPS) could rightly be regarded as forms of weaponised applications of neuroscientific and neurocognitive research.

Products of neuroscientific and neurotechnological research can be utilised to affect

1) memory, learning, and cognitive speed;
2) wake-sleep cycles, fatigue and alertness;
3) impulse control;
4) mood, anxiety, and self-perception;
5) decision-making;
6) trust and empathy;
7) and movement and performance (e.g., speed, strength, stamina, motor learning, etc.).

In military/warfare settings, modifying these functions can be utilised to mitigate aggression and foster cognitions and emotions of affiliation or passivity; induce morbidity, disability or suffering; and "neutralise" potential opponents or incur mortality.

Neurodata

The combination of multiple disciplines (e.g., the physical, social, and computational sciences), and intentional "technique and technology sharing" have been critical to rapid and numerous discoveries and developments in the brain sciences. This process, advanced integrative scientific convergence (AISC), can be seen as a paradigm for de-siloing disciplines toward fostering innovative use of diverse and complementary knowledge-, skill-, and tool-sets to both de-limit existing approaches to problem resolution; and to develop novel means of exploring and furthering the boundaries of understanding and capability. Essential to the AISC approach in neuroscience is the use of computational (i.e., big data) methods and advancements to enable deepened insight and more sophisticated intervention to the structure and function(s) of the brain, and by extension, human cognition, emotion, and behaviour[39].

Such capacities in both computational and brain sciences have implications for biosecurity and defense initiatives. Several neurotechnologies can be employed kinetically (i.e., providing means to injure, defeat, or destroy adversaries) or non-kinetically (i.e., providing "means of contending against others," especially in disruptive ways) engagements. While many types of neuroS/T have been addressed in and by extant forums, treaties, conventions, and laws, other newer techniques and technologies – inclusive of neurodata – have not. In this context, the term "neurodata" refers to the accumulation of large volumes of information; handling of large scale and often diverse informational sets; and new methods of data visualisation, assimilation, comparison, syntheses, and analyses. Such information can be used to:

- more finely elucidate the structure and function of human brain;
- and develop data repositories that can serve as descriptive or predictive metrics for neuropsychiatric disorders.

Purloining and/or modifying such information could affect military and intelligence readiness, force conservation, and mission capability, and thus national security. Manipulation of both civilian and military neurodata would affect the type of medical care that is (or is not)

provided, could influence the ways that individuals are socially regarded and treated, and in these ways disrupt public health and incur socio-economic change.

As the current COVID-19 pandemic has revealed, public – and institutional public health – responses to novel pathogens are highly variable at best, chaotic at worst, and indubitably costly (on many levels) in either case. To be sure, such extant gaps in public health and safety infrastructures and functions could be exploited by employing "precision pathologies" (capable of selectively affecting specific targets such as individuals, communities;, domestic animals, livestock, etc.) and an aggressive program of misinformation to incur disruptive effects on social, economic, political, and military scales that would threaten national stability and security. Recent elucidation of the Chinese government's Overseas Key Individuals Database (OKIDB), which, via collaboration with a corporate entity, Shenzhen Zhenua Data Technology, has amassed data to afford "insights into foreign political, military, and diplomatic figures…containing information on more than 2 million people…and tens of thousands who hold prominent public positions…" that could be engaged by "Beijing's army of cyberhackers".

Digital biosecurity – a term that describes the intersection of computational systems and biological information and how to effectively prevent or mitigate current and emerging risk arising at this intersection – becomes ever more important and required. The convergence of neurobiology and computational capabilities, while facilitating beneficial advances in brain research and its translational applications, creates a vulnerable strategic asset that will be sought by adversaries to advance their own goals for neuroscience. Hacking of biological data within the academic, industry, and the health care systems has already occurred – and neurodata are embedded within all of these domains.

Thus, it is likely that there will be more direct attempts at harnessing neurodata to gain leverageable informational, social, legal, and military capability and power advantage(s), as several countries that are currently strategically competitive with the U.S. and its allies invest heavily in both neuro- and cyber-scientific research programs and infrastructure. The growing fortitude of these states' quantitative and economic presence in these fields can – and is intended to – shift international leadership, hegemony, and influence ethical, technical, commercial and politico-military norms and standards of research and use. For example, Russian leadership has declared interest in the employment of "genetic passports" such that those in the military who display genetic indications of high cognitive performance can be directed to particular military tasks.

The neurobioeconomy

Advancements in neuroS/T have contributed to much growth in the neuro-bioeconomy. With neurological disorders being the second leading cause of death worldwide (with approximately 9 million deaths; constituting 16.5% of global fatalities), several countries have initiated programs in brain research and innovation.

These initiatives aim to:

1) advance understanding of substrates and mechanisms of neuropsychiatric disorders;
2) improve knowledge of processes of cognition, emotion, and behaviour;
3) and augment the methods for studying, assessing, and affecting the brain and its functions.

New research efforts incorporate best practices for interdisciplinary approaches that can utilise advances in computer science, robotics, and artificial intelligence to fortify the scope and pace of neuroscientific capabilities and products. Such research efforts are strong drivers of innovation and development, both by organising larger research goals, and by shaping neuroS/T research to meet defined economic, public health, and security agendas.

Rapid advances in brain science represent an emerging domain that state and non-state actors can leverage in warfare. While not all brain sciences engender security concerns, predominant authority and influence in global biomedical, bioengineering, wellness/lifestyle, and defense markets enable a considerable exercise of power. It is equally important to note that such power can be exercised both non-kinetic and kinetic operational domains, and several countries have identified neuroS/T as viable, of value, and of utility in their warfare programs. While extant treaties (e.g., the BTWC and CWC[40]) and laws have addressed particular products of the brain sciences (e.g., chemicals, biological agents, and toxins), other forms of neuroS/T, (e.g., neurotechnologies and neuroinformatics) remain outside these conventions' focus, scope, and governance. Technology can influence, if not shape the norms and conduct of warfare, and the future battlefield will depend not only upon achieving "biological dominance", but achieving "mental/cognitive dominance" and "intelligence dominance" as well.

It will be ever more difficult to regulate and restrict military and security applications of neuroS/T without established standards and proper international oversight of research and potential use-in-practice.

* * * *. *

In sum, it is not a question of whether neuro S/T will be utilised in military, intelligence, and political operations, but rather when, how, to what extent, and perhaps most importantly, if NATO nations will be prepared to address, meet, counter, or prevent these risks and threats. In this light (and based upon the information presented) it is, and will be increasingly important to address the complex issues generated by the brain sciences' influence upon global biosecurity and the near-term future scope and conduct of both non-kinetic and kinetic military and intelligence operations.[41]

Towards a new operational domain

The advent of the concept of "cognitive warfare" (CW) brings a third major combat dimension to the modern battlefield: to the physical and informational dimensions is now added a cognitive dimension. It creates a new space of competition, beyond the land, maritime, air, cybernetic and spatial domains, which adversaries have already integrated.

In a world permeated with technology, warfare in the cognitive domain mobilises a wider range of battle spaces than the physical and informational dimensions can do. Its very essence is to seize control of human beings (civilian as well as military), organisations, nations, but also of ideas, psychology, especially behavioural, thoughts, as well as the environment. In addition, rapid advances in brain science, as part of a broadly defined cognitive warfare, have the potential to greatly expand traditional conflicts and produce effects at lower cost.

Through the joint action it exerts on the 3 dimensions (physical, informational and cognitive), cognitive warfare embodies the idea of combat without fighting dear to Sun Tzu ("The supreme art of war is to subdue the enemy without fighting"). It therefore requires the mobilisation of a much broader knowledge. Future conflicts will likely occur amongst the people digitally first and physically thereafter in proximity to hubs of political and economic power.[42]

The study of the cognitive domain, thus centred on the human being, constitutes a new major challenge that is indispensable to any strategy relating to the combat power generation of the future.

Cognition is our "thinking machine". The function of cognition is to perceive, to pay attention, to memorise, to reason, to produce movements, to express oneself, to decide. To act on cognition means to act on the human being.

Therefore, defining a cognitive domain would be too restrictive; a human domain would therefore be more appropriate.

While actions taken in the five domains are executed in order to have an effect on the human domain[43], cognitive warfare's objective is to make everyone a weapon.

To turn the situation around, NATO must strive to define in a very broad sense and must have a clear awareness of the meanings and advances of international actors providing NATO with specific strategic security and broader challenges in the field of cognitive warfare.

Russian and Chinese Cognitive Warfare Definition

Russian Reflexive Control

In 2012, Vladimir Karyakin added: "The advent of information and network technologies, coupled with advances in psychology regarding the study of human behaviour 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."[44]

Russian CW falls under the definition of the Reflexive Control Doctrine. It is an integrated operation that compels an adversary decision maker to act in favour of Russia by altering their perception of the world[45].

This goes beyond "pure deception" because it uses multiple inputs to the decision maker using both true and false information, ultimately aiming to make the target feel that the decision to change their behaviour was their own:

- The Reflexive Control is ultimately aimed at the target's decision making.

- The information transmitted must be directed towards a decision or position.

- The information must be adapted to the logic, culture, psychology and emotions of the target.

The reflexive control has been turned into a broader concept taking into account the opportunities offered by new IT technologies called 'Perception Management'. It is about controlling perception and not managing perception.

The Russian CW is based on an in-depth understanding of human targets thanks to the study of sociology, history, psychology, etc. of the target and the extensive use of information technology.

As shown in Ukraine, Russia used her in-depth knowledge as a precursor and gained a strategic advantage before the physical conflict.

Russia has prioritised Cognitive Warfare as a precursor to the military phase.

* * * *

China Cognitive Warfare Domain

China has adopted an even broader definition of CW that includes the systematic utilisation of cognitive science and biotechnology to achieve the "mind superiority."

China has defined the Cognitive Domain of Operations as the battlefield for conducting ideological penetration (…) aiming at destroying troop morale and cohesion, as well as forming or deconstructing operational capabilities"

It encompasses six technologies, divided across two categories (Cognition, which includes technologies that affect someone's ability to think and function; and subliminal cognition that covers technologies that target a person's underlying emotions, knowledge, willpower and beliefs).

In particular, "Chinese innovation is poised to pursue synergies among brain science, artificial intelligence (AI), and biotechnology that may have far-reaching implications for its future military power and aggregate national competitiveness."[46]

The goal of cognitive operations is to achieve the "mind superiority" by using information to influence an adversary's cognitive functions, spanning from peacetime public opinion to wartime decision-making.[47]

> "The sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness, the human brain will become a new combat space."
>
> **He Fuchu**, "The Future Direction of the New Global Revolution in Military Affairs.

Chinese strategists predict that the pace and complexity of operations will increase dramatically, as the form or character of warfare continues to evolve. As a result, People's Liberation Army (PLA) strategists are concerned about the intense cognitive challenges that future commanders will face, especially considering the importance of optimising coordination and human-machine fusion or integration. These trends have necessarily increased the PLA's interest in the military relevance not only of artificial intelligence, but also of brain science and new directions in interdisciplinary biological technologies, ranging from biosensing and biomaterials to human enhancement options. The shift from computerisation to intelligentisation is seen as requiring the improvement of human cognitive performance to keep pace with the complexity of warfare"[48].

As part of its Cognitive Domain of Operations, China has defined "Military Brain Science (MBS) as a cutting-edge innovative science that uses potential military application as the guidance. It can bring a series of fundamental changes to the concept of combat and combat methods, creating a whole new "brain war" combat style and redefining the battlefield."[49] The pursuit of advances in the field of MBS is likely to provide cutting edge advances to China.The development of MBS by China benefits from a multidisciplinary approach between human sciences, medicine, anthropology, psychology etc. and also benefits from "civil" advances in the field, civilian research benefiting military research by design.

It's about Humans

A cognitive attack is not a threat that can be countered in the air, on land, at sea, in cyberspace, or in space. Rather, it may well be happening in any or all of these domains, for one simple reason: humans are the contested domain. As previously demonstrated, the human is very often the main vulnerability and it should be acknowledged in order to protect NATO's human capital but also to be able to benefit from our adversaries's vulnerabilities.

> "Victory will be defined more in terms of capturing the psycho-cultural rather than the geographical high ground. Understanding and empathy will be important weapons of war."
> **Maj. Gen. Robert H. Scales**

"Cognition is natively included in the Human Domain, thus a cognitive domain would be too restrictive", claimed August Cole and Hervé Le Guyader in "NATO's 6th domain" and:

"*…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 (…) and these are those our adversaries are focusing on to identify our centres of gravity, our vulnerabilities*."[50].

The practice of war shows that although physical domain warfare can weaken the military capabilities of the enemy, it cannot achieve all the purposes of war. In the face of new contradictions and problems in ideology, religious belief and national identity, advanced weapons and technologies may be useless and their effects can even create new enemies. It is therefore difficult if not impossible to solve the problem of the cognitive domain by physical domain warfare alone.

The importance of the Human Environment

The Human Domain is not solely focusing of the military human capital. It encompasses the human capital of a theatre of operations as a whole (civilian populations, ethnic groups, leaders…), but also the concepts closely related to humans such as leadership, organisation, decision-making processes, perceptions and behaviour. Eventually the desired effect should be defined within the Human Domain (aka the desired behaviour we want to achieve: collaboration/ cooperation, competition, conflict).

"To win (the future) war, the military must be culturally knowledgeable enough to thrive in an alien environment"[51].

In the 21st century, strategic advantage will come from how to engage with people, understand them, and access political, economic, cultural and social networks to achieve a position of relative advantage that complements the sole military force. These interactions are not reducible to the physical boundaries of land, air, sea, cyber and space, which tend to focus on geography and terrain characteristics. They represent a network of networks that define power and interests in a connected world. The actor that best understands local contexts and builds a network around relationships that harness local capabilities is more likely to win.

For the historian Alan Beyerchen, social sciences will be the amplifier of the 21st century's wars.[52]

In the past wars, the problem was that the human factor could not be a significant amplifier simply because its influence was limited and difficult to exploit; humans were considered more as constants than as variables. Certainly, soldiers could be improved through training, selection, psychological adaptation and, more recently, education. But in the end, the human factor was reduced to numbers. The larger the army, the greater the chance of winning the war, although the action of a great strategist could counterbalance this argument. Tomorrow, to have better soldiers and more effective humans will be key.

Last, the recent developments in science, all kinds of science, including science related to the human domain, have empowered anyone, whether individuals or committed minorities, with potential devastating power at their disposal. It has created a situation never seen before in the history of mankind[53], where individuals or small groups may jeopardise the success of military operations.

The crucible of Data Sciences and Human Sciences

The combination of Social Sciences and System Engineering will be key in helping military analysts to improve the production of intelligence for the sake of decision-making[54].

The Human Domain of Operations refers to the whole human environment, whether friend of foe. In a digital age it is equally important to understand first NATO's own human strengths and vulnerabilities before the ones of adversaries.

Since everyone is much more vulnerable than before everyone needs to acknowledge that one may endanger the security of the overall. Hence, a deep understanding of the adversary's human capital (i.e. the human environment of the military operation) will be more crucial than ever.

"If kinetic power cannot defeat the enemy, (…) psychology and related behavioural and social sciences stand to fill the void.[55]"

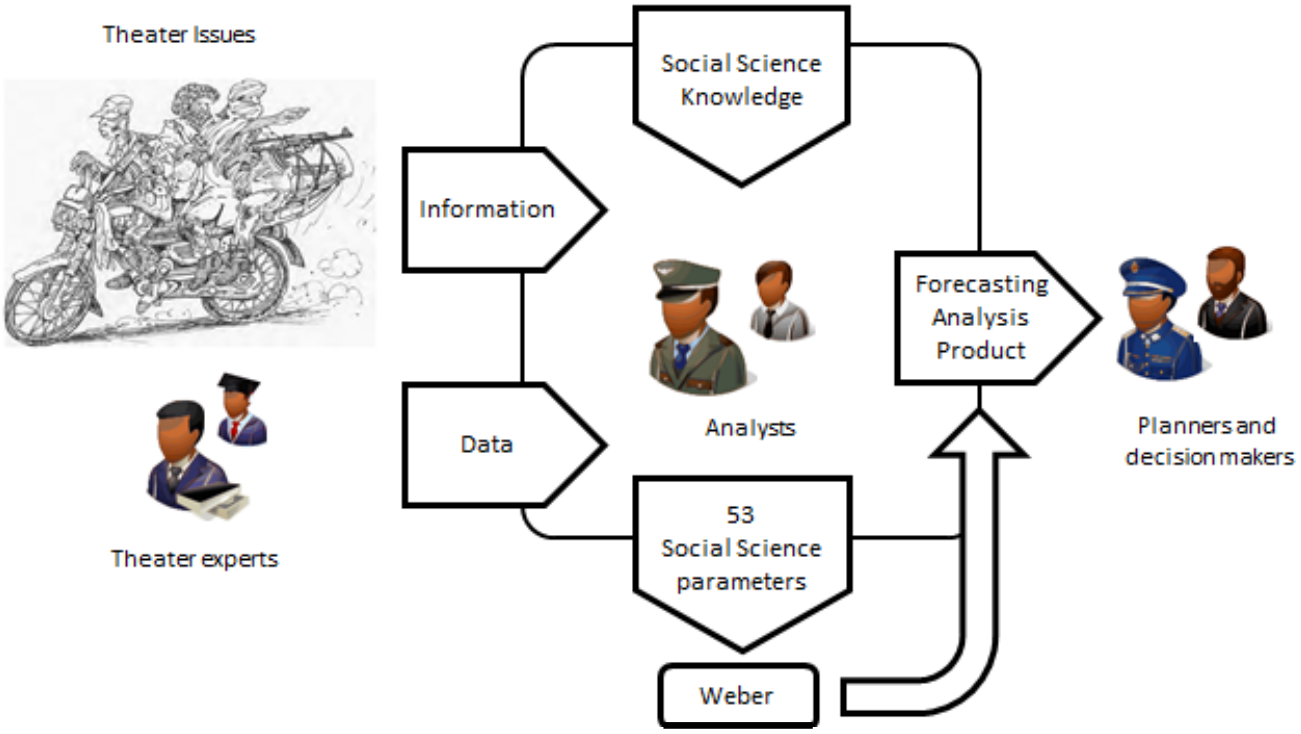
"Achieving the strategic outcomes of war will necessarily go through expanding the dialogue around the social sciences of warfare alongside the "physical sciences" of warfare..(…) it will go through understanding, influence or exercise control within the "human domain".[56]

Leveraging social sciences will be central to the development of the Human Domain Plan of Operations. It will support the combat operations by providing potential courses of action for the whole surrounding Human Environment including enemy forces, but also determining key human elements such as the Cognitive center of gravity, the desired behaviour as the end state. Understanding the target's goals, strengths, and vulnerabilities is paramount to an operation for enduring strategic outcomes.

The deeper the understanding of the human environment, the greater will be the freedom of action and relative advantage.

Psychology and social sciences have always been essential to warfare, and while warfare is moving away from kinetic operations, they might be the new game changer. Psychology, for instance, can help to understand the personal motives of terrorist groups and the social dynamics that make them so attractive to the (mostly) young men who join their ranks.

As an example, the picture below depicts a methodology (called Weber) applied to the study of terrorist groups in Sahel. It combines Social Sciences and System Engineering in order to help predicting the behaviours of terrorist groups. The tool allows the decision-makers to assess the evolution of actors through behavioural patterns according to several criteria and social science parameters, and ultimately to anticipate courses of action.[57]



The analysis, turned towards understanding the other in the broad sense (and often non-Western), cannot do without anthropology. Social and cultural anthropology is a formidable tool for the analyst, the best way to avoid yielding to one of the most common biases of intelligence, ethnocentrism, i.e. the inability to get rid of mental structures and representations of one's own cultural environment.

Cognitive sciences can be leveraged to enhance training at every level, especially in order to improve the ability to make decisions in complex tactical situations. Cognitive sciences can be employed in the creation of highly efficient and flexible training programs that can respond to fast-changing problems.

Legal and ethical aspects

Legal aspects

The development, production and use of Cognitive Technologies for military purposes raise questions as to whether, and to what extent, existing legal instruments apply. That is, how the relevant provisions are to be interpreted and applied in light of the specific technological characteristics and to what extent international law can sufficiently respond to the legal challenges involved with the advent of such technology.

It is essential to ensure that international law and accepted norms will be able to take into account the development of cognitive technologies. Specifically, to ensure that such technologies are capable of being used in accordance with applicable law and accepted international norms. NATO, through its various apparatus, should work at establishing a common understanding of how cognitive weapons might be employed to be compliant with the law and accepted international norms.

Equally, NATO should consider how the Law of Armed Conflict (LoAC) would apply to the use of cognitive technologies in any armed conflict in order to ensure that any future development has a framework from which to work within. Full compliance with the rules and principles of LoAC is essential.

Given the complexity and contextual nature of the potential legal issues raised by Cognitive technologies and techniques, and the constraints associated with this NATO sponsored study, further work will be required to analyse this issue fully. Therefore, it is recommended that such work be conducted by an appropriate body and that NATO Nations collaborate in establishing a set of norms and expectations about the use and development of Cognitive technologies. The immediate focus being how they might be used within extant legal frameworks and the Law of Armed Conflict.

Ethics

This area of research - human enhancement and cognitive weapons – is likely to be the subject of major ethical and legal challenges, but we cannot afford to be on the back foot when international actors are already developing strategies and capabilities to employ them. There is a need to consider these challenges as there is not only the possibility that these human enhancement technologies are deliberately used for malicious purposes, but there may be implications for the ability of military personnel to respect the law of armed conflict.

It is equally important to recognise the potential side effects (such as speech impairment, memory impairment, increased aggression, depression and suicide) of these technologies. For example, if any cognitive enhancement technology were to undermine the capacity of a subject to comply with the law of armed conflict, it would be a source of very serious concern. The development, and use of, cognitive technologies present numerous ethical challenges as well as ethical benefits, such as recovery from Post traumatic Stress Disorder (PTSD). Policy makers should take these challenges seriously as they develop policy about Cognitive Technologies, explore issues in greater depth and determine if other ethical issues may arise as this, and other related, technology develops.

Recommendations for NATO

The need for cooperation

While the objective of Cognitive Warfare is to harm societies and not only the military, this type of warfare resembles to "shadow wars" and requires a whole-of-government approach to warfare. As previously stated, the modern concept of war is not about weapons but about influence. To shape perceptions and control the narrative during this type of war, battle will have to be fought in the cognitive domain with a whole-of-government approach at the national level. This will require improved coordination between the use of force and the other levers of power across government. This could mean changes to how defence is resourced, equipped, and organised in order to offer military options below the threshold of armed conflict and improve the military contribution to resilience.

For NATO, the development of actions in the cognitive domain also requires a sustained cooperation between Allies in order to ensure an overall coherence, to build credibility and to allow a concerted defense.

Within the military, expertise on anthropology, ethnography, history, psychology among other areas will be more than ever required to cooperate with the military, in order to derive qualitative insights from quantitative data, as an example. In other words, if the declaration of a new field of combat consecrates the new importance of humans, it is more about rethinking the interaction between the hard sciences and the social sciences. The rise of cognitive technologies has endowed human with superior analysis and accuracy. In order to deliver timely and robust decisions, it will not be a question of relying solely on human cognitive capacities but of cross engineering systems with social sciences (sociology, anthropology, criminology, political science...) in order to face complex and multifaceted situations. The modelisation of human dynamics as part of what is known as Computational Social Science will allow the use of knowledge from social sciences and relating to the behaviour of social entities, whether enemies or allies. By mapping the human environment, strategists and key military leaders will be provided reliable information to decide on the right strategy.

Definition of the Human Domain

Thus defined by NATO's major adversaries, the mastery of the field of perceptions is an abstract space where understanding of oneself (strengths and weaknesses), of the other (adversary, enemy, human environment), psychological dimension, intelligence collection, search for ascendancy (influence, taking and conservation of the initiative) and capacity to reduce the will of the adversary are mixed.

Within the context of multi-domain operations, the human domain is arguably the most important domain, but it is often the most overlooked. Recent wars have shown the inability to achieve the strategic goals (e.g. in Afghanistan) but also to understand foreign and complex human environments.

Cognitive warfare was forced upon the Western liberal democracies by challenging international actors who have strategised to avoid the military confrontation, thus blurring the line between peace and war by targeting the weakest element: humans. CW which includes the increasing use of NBICs for military purposes may provide a sure way of military dominance in a near future.

The Human Domain of operations could tentatively be defined as **"the sphere of interest in which strategies and operations can be designed and implemented that, by targeting the cognitive capacities of individuals and/or communities with a set of specific tools and techniques, in particular digital ones, will influence their perception and tamper with their reasoning capacities, hence gaining control of their decision making, perception and behaviour levers in order to achieve desired effects."**

"Military power is of course one essential segment of security. But global security refers to a broad range of threats, risks, policy responses that span political, economic, societal, health (including cognitive health!) and environmental dimensions, none of these being covered by your current domains of operations! Some international actors already use weapons that precisely target these dimensions, while keeping their traditional kinetic arsenal in reserve as long as they possibly can. NATO, if it wishes to survive, has to embrace this continuum and claim as its responsibility, together with its allies to, seamlessly, achieve superiority all across it."[58]

Raising awareness among Allies

While advances in technology have always resulted in changes in military organisations and doctrines, the rapid advancements in technology, in particular in brain science and NBIC, should force NATO to take action and give a greater consideration to the emergence of the threats that represents Cognitive Warfare. Not all NATO nations have recognised this changing character of conflicts. Declaring the Human as sixth domain of operations is a way to raise awareness among the NATO Nations. NATO should consider further integrating Human situational awareness in the traditional situation awareness processes of the Alliance.

Anticipating the trends

There is evidence that adversaries have already understood the potential of developing human-related technologies. Declaring the Human Domain as a sixth domain of operations has the potential to reveal possible vulnerabilities, which could otherwise amplify rapidly. It is not too late to face the problem and help keep the dominance in the field of cognition.

Delays in declaring the Human Domain as a domain of operations may lead to fight the last war.

Given that the process of declaring a new domain of operations is a lengthy process and given the sensitivity of the topic, NATO needs to be fast in focusing on political/military responses while capacity/threats of our opponents are still low.

Finally, ethical problems should be raised. Since there is no agreed international legal framework in the field of neurosciences, NATO may play a role in pushing to establish an international legal framework that meets the NATO Nations' ethical standards.

Accelerating information sharing

Accelerated information sharing among Alliance members may help faster integration of interoperability, to assure coherence across multi-domain operations. Information sharing may also assist some nations in catching up in this area. In particular, surveillance of ongoing international activities in brain science, and their potential dual-use in military and intelligence operations should be undertaken and shared between Allies along with identification and quantification of current and near-term risks and threats posed by such enterprises.

Establishing DOTMLPFI components upstream

The first step is to define the "human domain" in military doctrine and use the definition to conduct a full spectrum of capability development analysis, optimising the military for the most likely 21st century contingencies. Since the Human Domain complements the five others, each capability development should include the specificities of modern threats, including those related to cognitive warfare and, more generally, the sixth domain of operations. The Human Domain is not an end in itself but a means to achieve our strategic objectives and to respond to a type of conflict that the military is not accustomed to dealing with.

Dedication of resources for developing and sustaining NATO Nations capabilities to prevent escalation of future risk and threat by:

1) continued surveillance;
2) organisational and systemic preparedness;
3) coherence in any/all entities necessary to remain apace with, and/or ahead of tactical and strategic competitors' and adversary's capabilities in this space.

Impact on Warfare Development

By essence, defining a new domain of operations and all the capabilities and concepts that go along with it, is part of ACT's mission.

ACT should lead a further in-depth study with a focus on:

- Advancements on brain science initiatives that may be developed and used for non-kinetic and kinetic engagements.
- Different ethical systems that govern neuroscientific research and development. This will mandate a rigorous, more granular, and dialectical approach to negotiate and resolve issues and domains of ethical dissonance in multi- and international biosecurity discourses.
- Ongoing review and evaluation of national intellectual property laws, both in relation to international law(s), and in scrutiny of potential commercial veiling of dual-use enterprises.
- Identification and quantification of current and near-term risks and threats posed by such enterprise(s)
- Better recognizing the use of social and human sciences in relation with "hard" sciences to better understand the human environment (internal and external)
- Include the cognitive dimension in every NATO exercises by leveraging new tools and techniques such as immersive technologies

Along with those studies, anticipating the first response (such as the creation of a new NATO COE or rethink and adapt the structure by strengthening branches as required) and defining a common agreed taxonomy (Cognitive Dominance/Superiority/Cognitive Center of Gravity etc…) will be key tasks for ACT to help NATO keep the military edge.

Conclusion

Failing to thwart the cognitive efforts of NATO's opponents would condemn Western liberal societies to lose the next war without a fight. If NATO fails to build a sustainable and proactive basis for progress in the cognitive domain, it may have no other option than kinetic conflict. Kinetic capabilities may dictate a tactical or operational outcome, but victory in the long run will remain solely dependent on the ability to influence, affect, change or impact the cognitive domain.

> "Today's progresses in nanotechnology, biotechnology, information technology and cognitive science (NBIC), boosted by the seemingly unstoppable march of a triumphant troika made of Artificial Intelligence, Big Data and civilisational "digital addiction" have created a much more ominous prospect: an embedded fifth column, where everyone, unbeknownst to him or her, is behaving according to the plans of one of our competitors."
>
> **August Cole, Hervé Le Guyader**
> NATO's 6th Domain

Because the factors that affect the cognitive domain can be involved in all aspects of human society through the areas of will, concept, psychology and thinking among other, so that particular kind of warfare penetrates into all fields of society. It can be foreseen that the future information warfare will start from the cognitive domain first, to seize the political and diplomatic strategic initiative, but it will also end in the cognitive realm.

Preparing for high-intensity warfare remains highly relevant, but international actors providing NATO with specific strategic security challenges have strategised to avoid confronting NATO in kinetic conflicts and chose an indirect form of warfare. Information plays a key role in this indirect form of warfare but the advent of cognitive warfare is different from simple Information Warfare: it is a war through information, the real target being the human mind, and beyond the human per se.

Moreover, progresses in NBIC make it possible to extend propaganda and influencing strategies. The sophistication of NBIC-fueled hybrid attacks today represent an unprecedented level of threat inasmuch they target the most vital infrastructure everyone relies on: the human mind[59].

Cognitive warfare may well be the missing element that allows the transition from military victory on the battlefield to lasting political success. The human domain might well be the decisive domain, wherein multi-domain operations achieve the commander's effect. The five first domains can give tactical and operational victories; only the human domain can achieve the final and full victory. "Recognising the human domain and generating concepts and capabilities to gain advantage therein would be a disruptive innovation."[60]

Bibliography and Sources

Essays

August Cole, Hervé Le Guyader, *NATO 6th Domain of Operations*, September 2020

Dr. James Giordano, *Emerging Neuroscience and Technology (NeuroS/T): Current and Near-Term Risks and Threats to NATO Biosecurity*, October 2020

Article

Nicolas Israël and Sébastien-Yves Laurent, "Analysis Facing Worldwide Jihadist Violence and Conflicts. What to do?" September 2020

Online Collaboration with Johns Hopkins University

"*Cognitive Biotechnology, Altering the Human Experience*", Sep 2020
"*Cognitive Warfare, an attack on truth and thoughts*", Sep 2020
Under the direction of **Professor Lawrence Aronhnime**
Contributors: **Alonso Bernal, Cameron Carter, Melanie Kemp, Ujwal Arunkumar Taranath, Klinzman Vaz, Ishpreet Singh, Kathy Cao, Olivia Madreperla**

Experiments

DTEX (Disruptive Technology Experiment) - 7 October 2020
NATO Innovation Hub Disruptive Technology Experiment (DTEX) on disinformation.
Under the direction of **Girish Sreevatsan Nandakumar** (Old Dominion University)

Hackathon "Hacking the Mind"
Run by **Dr. Kristina Soukupova and the Czech Republic Defense and Security Innovation Hub**, October 2020.
https://www.hackthemind.cz

Annex 1

Nation State Case Study 1: The weaponisation of neurosciences in China

As described in the Five-Year Plans (FYPs) and other national strategies, China has identified and acknowledged the technical, economic, medical, military, and political value of the brain sciences, and has initiated efforts to expand its current neuroS/T programs. China utilises broader strategic planning horizons than other nations and attempts to combine efforts from government, academic, and commercial sectors (i.e., the "triple helix") to accomplish cooperation and centralisation of national agendas. This coordination enables research projects and objectives to be used for a range of applications and outcomes (e.g., medical, social, military). As noted by Moo Ming Poo, director of China's Brain Project, China's growing aging population is contributing to an increasing incidence and prevalence of dementia and other neurological diseases. In their most recent FYP, China addressed economic and productivity concerns fostered by this aging population, with a call to develop medical approaches for neurological disorders and to expand research infrastructure in neuroS/T.

This growing academic environment has been leveraged to attract and solicit multi-national collaboration. In this way, China is affecting international neuroS/T through

1) research tourism;
2) control of intellectual property;
3) medical tourism;
4) and influence in global scientific thought. While these strategies are not exclusive to neuroS/T; they may be more opportunistic in the brain sciences because the field is new, expanding rapidly, and its markets are growing, and being defined by both share- and stake-holder interests.

Research tourism involves strategically recruiting renowned, experienced scientists (mostly from Western countries), as well as junior scientists to contribute to and promote the growth, innovation, and prestige of Chinese scientific and technological enterprises. This is apparent by two primary efforts. First, initiatives such as the Thousand Talents Program (launched in 2008) and other programs (e.g., Hundred Person Program, Spring Light Program, Youth Thousand Talents Program, etc.) aim to attract foreign researchers, nurture and sustain domestic talent, and bring back Chinese scientists who have studied or worked abroad. Further, China's ethical research guidelines are, in some domains, somewhat more permissive than those in the West (e.g., unrestricted human and/or non-human primate experimentation), and the director of China's Brain Project, Mu-Ming Poo, has stated that this capability to engage research that may not be (ethically) viable elsewhere may (and should) explicitly attract international scientists to conduct research in China.

Second, China continues to engage with leading international brain research institutions to foster greater cooperation. These cooperative and collective research efforts enable China to

achieve a more even "playing field" in the brain sciences. China leverages intellectual property (IP) policy and law to advance (and veil) neuroS/T and other biotechnologies in several ways. First, via exploitation of their patent process by creating a "patent thicket". The Chinese patent system focuses on the end-utility of a product (e.g., a specific neurological function in a device), rather than emphasising the initial innovative idea in contrast to the U.S. system. This enables Chinese companies and/or institutions to copy or outrightly usurp foreign patents and products. Moreover, Chinese patent laws allow international research products and ideas to be used in China "for the benefit of public health," or for "a major technological advancement." Second, the aforementioned coordination of brain science institutions and the corporate sector establishes compulsory licensing under Chinese IP and patent laws. This strategy (i.e., "lawfare") allows Chinese academic and corporate enterprises to have economic and legal support, while reciprocally enabling China to direct national research agendas and directives through these international neuroS/T collaborations. China enforces its patent and IP rights worldwide, which can create market saturation of significant and innovative products, and could create international dependence upon Chinese neuroS/T. Further, Chinese companies have been heavily investing in knowledge industries, including artificial intelligence enterprises, and academic book and journal partnerships. For example, TenCent established a partnership with Springer Nature to engage in various educational products. This will allow a significant stake in future narratives and dissemination of scientific and technological discoveries.

Medical tourism is explicit or implicit attraction and solicitation of international individuals or groups to seek interventions that are either only available, or more affordable in a particular locale. Certainly, China has a presence in this market, and at present, available procedures range from the relatively sublime, such as using deep brain stimulation to treat drug addiction, to the seemingly "science-fictional", such as the recently proposed body-to-head transplant to be conducted at Harbin Medical University in collaboration with Italian neurosurgeon Sergio Canavero. China can advance and develop areas of neuroS/T in ways that other countries cannot or will not, through homogenising a strong integrated "bench to bedside" capability and use of non-Western ethical guidelines.

China may specifically target treatments for diseases that may have a high global impact, and/or could offer procedures that are not available in other countries (for either socio-political or ethical reasons). Such medical tourism could create an international dependence on Chinese markets as individuals become reliant on products and services available only in China, in addition to those that are "made in China" for ubiquitous use elsewhere. China's growing biomedical industry, ongoing striving for innovation, and expanding manufacturing capabilities have positioned their pharmaceutical and technology companies to prominence in world markets. Such positioning – and the somewhat permissive ethics that enable particular aspects and types of experimentation – may be seductive to international scientists to engage research, and/or commercial biomedical production within China's sovereign borders.

Through these tactics of economic infiltration and saturation, China can create power hierarchies that induce strategically latent "bio-political" effects that influence real and perceived positional dominance of global markets.

China is not the only country that has differing ethical codes for governing research. Of note is that Russia has been, and continues to devote resources to neuroS/T, and while not uniformly allied with China, has developed projects and programs that enable the use of neurodata for non-kinetic and/or kinetic applications. Such projects, programs, and operations can be conducted independently and/or collaboratively to exercise purchase over competitors and adversaries so as to achieve greater hegemony and power.

Therefore, NATO, and its international allies must

4) recognise the reality of other countries' science and technological capabilities;
5) evaluate what current and near-term trends portend for global positions, influence, and power;
6) and decide how to address differing ethical and policy views on innovation, research, and product development.

Annex 2

Nation State Case Study 2: The Russian National Technology Initiative[61]

Russian President Vladimir Putin has explicitly stated intent to implement an aggressive modernisation plan via the National Technology Initiative (NTI). Designed to grant an overmatch advantage in both commercial and military domains against Russia's current and near-term future key competitors, the NTI has been viewed as somewhat hampered by the nation's legacy of government control, unchanging economic complexity, bureaucratic inefficiency and overall lack of transparency. However, there are apparent disparities between such assessment of the NTI and its capabilities, and Russia's continued invention and successful deployment of advanced technologies.

Unlike the overt claims and predictions made by China's scientific and political communities about the development and exercise of neuroS/T to re-balance global power, explication and demonstration(s) of Russian efforts in neuroS/T tend to be subtle, and detailed information about surveillance and extent of such enterprise and activity is, for the most part, restricted to the classified domain. In general, Russian endeavours in this space tend to build upon prior work conducted under the Soviet Union, and while not broad in focus, have gained relative sophistication and capability in particular areas that have high applicability in non-kinetic disruptive engagements. Russia's employments of weaponised information, and neurotropic agents have remained rather low-key, if not clandestine (and perhaps covert), often entail nation-state or non-state actors as proxies, and are veiled by a successful misinformation campaign to prevent accurate assessment of their existing and developing science and technologies.

Military science and technology efforts of the USSR were advanced and sustained primarily due to the extensive military-industrial complex which, by the mid-1970s through 1980s, is estimated to have employed up to twenty percent of the workforce. This enabled the USSR to become a world leader in science and technology, ranked by the U.S. research community as second in the world for clandestine S&T programs (only because the overall Soviet system of research and development (R&D) was exceptionally inefficient, even within the military sector). The collapse of the USSR ended the Soviet military-industrial complex, which resulted in significant decreases in overall spending and state support for R&D programs. Any newly implemented reforms of the post-Soviet state were relatively modest, generating suboptimal R&D results at best. During this time, Russian R&D declined by approximately 60% and aside from the Ministries' involvement with the military sector, there was a paucity of direct cooperation between Russian R&D institutions and operational S&T enterprises. This limited interaction, was further compounded by a lack of resources, inability to bring new technology to markets, absent protections for intellectual property, and "brain drain" exodus of talented researchers to nations with more modern, cutting-edged programs with better pay and opportunities for advancement.

Recognising the inherent problems with the monoculture of the Russian economic and S&T ecosystems, the Putin government initiated a process of steering Russia toward more lucrative, high-tech enterprises. The NTI is ambitious, with goals to fully realise a series of S&T/R&D advancements by 2035. The central objective of the NTI is establish "the program for creation of fundamentally new markets and the creation of conditions for global technological leadership of Russia by 2035." To this end, NTI Experts and the Agency for Strategic Initiatives (ASI) identified nine emerging high-tech markets for prime focus and penetrance, including neuroscience and technology (i.e., what the ASI termed "NeuroNet"). Substantive investment in this market is aimed at overcoming the post-Soviet "resource curse", by capitalising on the changes in global technology markets – and engagement sectors – to expand both economic and military/intelligence priorities and capabilities. According to the ASI, NeuroNet is focused upon "distributed artificial elements of consciousness and mentality", with Russia's prioritisation of neuroS/T being a key factor operative in influence operations directed and global economies and power. Non-kinetic operations represent the most viable intersection and exercise of these commercial, military, and political priorities, capabilities, and foci of global influence and effect(s).

Notes

[1] Robert P. Kozloski, https://www.realcleardefense.com/articles/2018/02/01/knowing_yourself_is_key_in_cognitive_warfare_112992.html, February 2018

[2] Green, Stuart A. "Cognitive Warfare." *The Augean Stables* , Joint Military Intelligence College, July 2008, www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare.pdf.

[3] Clint Watts, (2018) Messing with the Enemy, HarperCollins

[4] As defined by Wikipedia, a sock puppet or sockpuppet is an online identity used for purposes of deception. It usually refers to the Russian online activism during the US electoral campaign 2016. https://en.wikipedia.org/wiki/Sock_puppet_account

[5] https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf

[6] Dr Zac Rogers, in Mad Scientist 158, (July 2019), https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you/

[7] August Cole-Hervé Le Guyader, NATO 6th Domain of Operation, 2020

[8] Ibid.

[9] Alicia Wanless, Michael Berk (2017), Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications: https://www.researchgate.net/publication/329281610_Participatory_Propaganda_The_Engagement_of_Audiences_in_the_Spread_of_Persuasive_Communications

[10] Jacques Ellul, (1962) Propaganda, Edition Armand Colin

[11] Matt Chessen, The MADCOM Future: How AI will enhance computational propaganda, The Atlantic Council, Sep 2017

[12] https://en.wikipedia.org/wiki/al_economics

[13] Shoshana Zuboff, (2019) The Age of Surveillance Capitalism, Public Affairs

[14] Peter W. Singer, Emerson T. Brooking (2018) LikeWar The Weaponisation of Social Media, HMH Edition page 95

[15] Victoria Fineberg, (August 2014) Behavioural Economics of Cyberspace Operations, Journal of Cyber Security and Information Systems Volume: 2

[16] Shoshana Zuboff, (2019) The Age of Surveillance Capitalism, Public Affairs

[17] Michael J Mazarr, (July 2020) Survival: Global Politics and Strategy, Virtual Territorial Integrity: The Next International Norm, in Survival: Global Politics and Strategy, IISS

[18] Bernard Claverie and Barbara Kowalczuk, Cyberpsychology, Study for the Innovation Hub, July 2018

[19] Dr Zac Rogers, in Mad Scientist 158, (July 2019), https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you/

[20] Haselton MG, Nettle D, Andrews PW (2005). "The evolution of cognitive bias.". In Buss DM (ed.). *The Handbook of Evolutionary Psychology*

[21] Wikipedia lists more than 180 different cognitive biases: https://en.wikipedia.org/wiki/Cognitive_bias

[22] Lora Pitman (2019)"The Trojan horse in your Head: Cognitive Threats and how to counter them" ODU Digital Commons

[23] Robert P. Kozloski, https://www.realcleardefense.com/articles/2018/02/01/knowing_yourself_is_key_in_cognitive_warfare_112992.html, February 2018

[24] Peter W. Singer, Emerson T. Brooking (2018) LikeWar The Weaponisation of Social Media, HMH Edition page 165

[25] Dominique Moïsi (2010) The Geopolitics of Emotion, Edition Anchor.

[26] Christophe Jacquemart (2012), Fusion Froide Edition

[27] Fogg, B.J. (2003). Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers.

[28] https://mwi.usma.edu/mwi-video-brain-battlefield-future-dr-james-giordano/

[29] Maryanne Wolf, (2007)"Proust and the Squid: The Story and Science of the Reading Brain" HarperCollins

[30] Bernard Stiegler, https://www.observatoireb2vdesmemoires.fr/publications/video-minute-memoire-vers-une-utilisation-raisonnee-du-big-data 2019

[31] https://pphr.princeton.edu/2017/04/30/are-video-games-really-mindless/

[32]*"Never has a medium been so potent for beauty and so vulnerable to creepiness. Virtual reality will test us. It will amplify our character more than other media ever have."* Jaron Lanier, (2018) Dawn of the New Everything: Encounters with Reality and Virtual Reality, Picador Edition

[33] Philosopher Thomas Metzinger: https://www.newscientist.com/article/2079601-virtual-reality-could-be-an-ethical-minefield-are-we-ready/

[34] Gayannée Kedia, Lasana Harris, Gert-Jan Lelieveld and Lotte van Dillen, (2017) From the Brain to the Field: The Applications of Social Neuroscience to Economics, Health and Law

[35] Pr. Li-Jun Hou, Director of People's Liberation Army 202nd Hospital, (May 2018), Chinese Journal of Traumatology,

[36] For more on the definition of "dual use" in neuro S/T, see Dr. James Giordano's essay October 2020

[37] National Research Council and National Academy of Engineering. 2014. Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues.

[38] Ibid.

[39] Giordano J. (2014). Intersections of "big data", neuroscience and national security: Technical issues and derivative concerns. In: Cabayan H et al. (eds.) *A New Information Paradigm? From Genes to "Big Data", and Instagrams to Persistent Surveillance: Implications for National Security*, p. 46-48. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

[40] Biological and Chemical Weapons Conventions

[41] DeFranco JP, DiEuliis D, Bremseth LR, Snow JJ. Giordano J. (2019). Emerging technologies for disruptive effects in non-kinetic engagements. *HDIAC Currents* 6(2): 49-54.

[42] Parag Khanna, *Connectography: Mapping the Future of Global Civilisation* (New York Random House, 2016)

[43] Megan Bell, *An Approachable Look at the Human Domain and why we should care* (2019), https://othjournal.com/2019/06/17/an-approachable-look-at-the-human-domain-and-why-we-should-care/

[44] Vladimir Vasilyevich Karyakin, (2012) "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

[45] GILES, SHERR et SEABOYER (2018), Russian Reflexive Control, Royal Military College of Canada, Defence Research and Development Canada.

[46] Elsa B. Kania, Prism Vol.8, N.3, 2019

[47] Nathan Beauchamp-Mustafaga, China Brief, (Sep 2019) https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/

[48] Ibid.

[49] Hai Jin, Li-Jun Hou, Zheng-Guo Wang, (May 2018)Military Brain Science - How to influence future wars, Chinese Journal of Traumatology

[50] August Cole, Hervé Le Guyader, NATO 's 6th Domain, September 2020

[51] Maj. Gen. Robert H. Scales, (2006), http://armedforcesjournal.com/clausewitz-and-world-war-iv/

[52] Alan Beyerchen, "Clausewitz, Nonlinearity and the Unpredictability of War," *International Security*, 17:3 (Winter, 1992)

[53] August Cole, Hervé Le Guyader, NATO 's 6th Domain, September 2020

[54] "Analysis Facing Worldwide Jihadist Violence and Conflicts. What to do?" Article for the Innovation Hub, Nicolas Israël and Sébastien-Yves LAURENT, September 2020

[55] https://www.psychologytoday.com/us/blog/head-strong/201408/psychology-and-less-lethal-military-strategy

[56] Generals Odierno, Amos and Mc Raven, Strategic Landpower, NPS Publication 2014

[57] "Analysis Facing Worldwide Jihadist Violence and Conflicts. What to do?" Article for the Innovation Hub, Nicolas Israël and Sébastien-Yves LAURENT, September 2020

[58] August Cole, Hervé Le Guyader, NATO 6th Domain of Operations, September 2020

[59] Hervé Le Guyader, the Weaponisation of Neurosciences, Innovation Hub Warfighting Study February 2020

[60] Ibid.

[61] Ibid.