The 21st-Century Game Changer

COGNITIVE WARFARE

Although most of the cognitive attacks remain below the threshold of armed conflict, the effects can be lethal and multi-domain, affecting all five domains of warfare.

"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."

Major General Robert H. Scales (Retired), Ph.D.
Former Commandant of the U.S. Army War College

by **Commander Cornelis van der Klaauw**
Royal Netherlands Navy
Subject Matter Expert,
Strategic Communications
and Information Operations
NATO Joint Warfare Centre

Introduction

This article aims to raise awareness of a new NATO concept that is in its infancy, but that will have a significant impact on individuals, groups, societies and the way future wars are fought: cognitive warfare.

As part of the NATO Warfighting Capstone Concept and using the Warfare Development Agenda as a framework for the delivery, Headquarters Supreme Allied Commander Transformation (HQ SACT) initiated the development of a Cognitive Warfare Concept in 2021. The concept is part of the Warfare Development Imperative of cognitive superiority. The aim of the concept is to seize the initiative in the cognitive dimension through enabling a shared understanding and appreciation of the dimension looking 10 to 20 years into the future. This needs to be accomplished through defensive and proactive measures that ensure the Alliance's protection and enhance our cognitive processes. An exploratory concept is foreseen for 2023, while the final concept is to be approved by NATO's Military Committee in 2024.

The cognitive warfare concept is a means to engage more effectively, ensure preparedness and, in doing so, maintain credibility and deterrence capability against adversaries across all domains of warfare. This article will describe what cognitive warfare is and why it is important to NATO.

Furthermore, it will explain the most important ways and means used in cognitive warfare as well as the actors who engage it in. Based on this, the article will examine how the Alliance can best protect itself against the impact of cognitive activities. Finally, we will conclude with a look at expected future developments.

Why It Matters

Cognitive warfare is a structured and well-considered approach to target the human cognition of individuals, groups and societies in a way that affects their decision-making processes and ultimately their behaviour.

While cognitive effects are not measurable in the typical sense, they do affect how we think, what we feel and how we act using brain-centred technologies that aim to destabilize structures, create distrust, and fracture and break social cohesion, for example through amplifying pre-existing social differences in order to undermine democracies and weaken our rule-based systems.

Allied Command Transformation explains cognitive warfare as including "activities conducted in synchronization with other instruments of power to affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary."

Why is it a priority for the Alliance to improve its understanding of cognitive warfare? Is countering cognitive attacks actually a military task? It is. The reasoning for this can be found in Article 3 of the Washington Treaty, NATO's founding document. It establishes the principle of resilience:

> "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."

Article 3 includes supporting the continuity of government and the provision of essential services, among them resilient civil communications systems. This means that cognitive resilience, as an aspect of promoting and enhancing

civil preparedness, requires that NATO plays a key role — but only in support of its member nations' own efforts and not as a standalone actor. NATO nations differ in their cultural, social, technological and governmental structures and with that, their susceptibility to cognitive attacks. A tailored approach is needed to provide the right support to the nations.

There is an additional reason why NATO is developing a concept for cognitive warfare: A cognitive attack directly targets the minds of civilians, meaning non-combatants. As that is a violation of the Law of Armed Conflict.

Unlike psychological operations, cognitive activities are not directed at our conscious mind, but at our subconscious mind, the main drivers of our behaviour: emotions. This takes place through hyper-personalized targeting integrating and exploiting neuroscience, biotechnology, information and cognitive techniques (NBIC), mainly using social media and digital networks for neuro-profiling and targeting individuals. We need to realize that individuals are at the centre of all military operations and strategic-political decision-making.

Although they often sound like ideas from a science-fiction film, cognitive attacks are not science fiction anymore. They are taking place already now, and these attacks will continue to become more sophisticated. Several countries are developing NBIC capabilities and collecting data for use in targeting the cognitive dimension. These activities are supported by aspects such as datamining and data analytics, and are further combined with artificial intelligence.

Although most of the cognitive attacks remain below the threshold of armed conflict, the effects can be lethal and multi-domain, affecting all five domains of warfare. Furthermore, these attacks are people-centric, meaning they have human cognition as their centre of gravity, and in principle that is a continuous, never-ending battle. Although not proven to be a cognitive attack, the so-called Havana syndrome, a cluster of adverse symptoms reported by U.S. intelligence and military personnel stationed abroad in recent years, could well be an instance of the use of cognitive capabilities.

China is globally one of the leading nations in the scientific development of NBIC capabilities. China conducts human research and experiments that are deemed unethical according to Western standards, but these experiments nevertheless attract scientists from all over the world. Within the context of the Chinese "three warfares" strategy, an integrated people-centric, psychological and legal approach, the Chinese have developed a database with the profiles of more than two million prominent individuals worldwide that may be used to influence decision-making processes.

"Only five to ten percent of the decisions we make are rational decisions; for the rest, we rely on our subconscious decision-making, which is strongly influenced by repetition, automatisms, biases and fallacies."

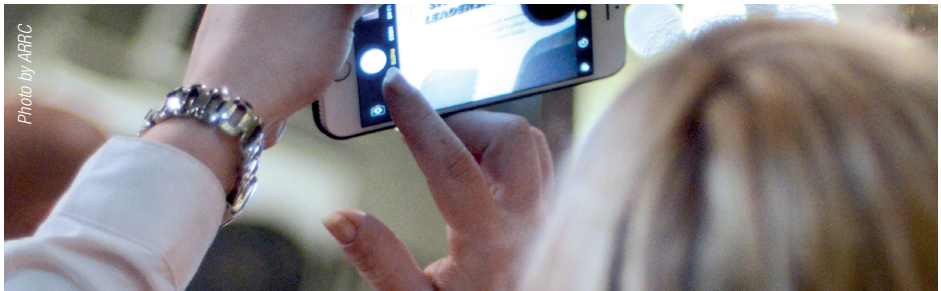


Photo by ARRC

LOOKING AT COGNITIVE activities in more detail, we can identify long-term campaigns taking place over several years, but also one-off activities. What both have in common is a structured approach to achieve a specific aim without the target becoming aware of an attack. Generally the damage is already done before the target realizes that it has been targeted.

The reason why cognitive attacks go unnoticed by their targets is that cognitive activities bypass the conscious mind and directly target the subconscious of a person. In fact, within the subconscious mind, the primary target is the amygdala. From an evolutionary point of view, the amygdala is the oldest part of the brain. Before we go more into detail on the ways and means used for cognitive activities, we will briefly look at the functions of our conscious and subconscious mind as well as the relationship between the two.

As the term suggests, our subconscious mind exists "beneath" our conscious mind. Contrary to the conscious mind, the subconscious mind is always active; it never sleeps. It regulates our basic organic functions, our emotions and, surprisingly enough, most of our decision-making. The reason why most of our decisions are made by our subconscious is that our conscious mind uses a lot of energy, which causes it to reach the limits of its capacity quickly. Actually only five to ten percent of the decisions we make are rational decisions; for the rest, we rely on our subconscious decision-making, which is strongly influenced by repetition, automatisms, biases and fallacies. We tend to then use our conscious mind to justify, rationalize and explain our emotionally driven decision-making and behaviour.

What cognitive attacks then do is exploit these emotions, automatisms, biases and fallacies in a way that affects our processes of making meaning of our surroundings, affecting not what we think but how we think. Adversaries do this in different ways, integrating and exploiting NBIC techniques. In this context we need to consider that both biases (non-rational shortcuts acceptable in normal situations) and fallacies (conclusions without evidence, based on assumptions) are commonly uniform across cultures and therefore easier to exploit.

The preferred way to do this is via social media and digital networks, as these are our primary environment for sharing all sorts of information, and they have increasingly

become our main source for news. However, there are more aspects that make social media an ideal vector for cognitive activities. Social media weaken our cognitive abilities as the content can easily stir up emotions and forces us to react quickly. Social media platforms are designed to foster addictive behaviour. On average, we are exposed to digital information systems between five and seven hours a day. Internet use disorder is now a recognized mental disorder. Furthermore, social media are ideal for collecting personal information and for carrying out data analysis and datamining. Drawing up a person's digital profile is a quick and relatively simple process that can be carried out with limited means. The effects of the digital age are far-reaching: A paper copy of the newspaper does not know what we read; our tablets, however, do. The advertisement in the paper does not know what we bought and where; our smartphones do. The newspaper editor does not know what article we found interesting and shared with friends; our social network does.

Closely related to and often fully integrated with social media are our smart devices. Smart devices collect all manner of personal physiological information such as blood pressure, heart and breathing rate, skin temperature and so on. All this information is relevant to target people in the right moment, for example when they are tired, hungry, stressed or angry.

Looking to digital networks, gaming platforms, with their more than three billion gamers worldwide, are ideal venues for cognitive activities. The platforms contain all kinds of sub-cultures that are in turn linked to non-gaming groups who can create their own games or modify existing games to infiltrate the gamers' lives without any control or regulations of the content of the games. An aspect that, in this context, should not be overlooked is that the lines between physical, digital and mental personas are becoming blurrier and with that, the difference between reality and fiction is also becoming unclear. Virtual reality environments in particular drive this trend.

Digital spaces have also been known to breed echo chambers. Within them, people concentrate on a narrative that supports their beliefs and desires while ignoring information that is not aligned with their narratives. The result is closed micro-societies vulnerable to group thinking, polarization and generation of distrust. This becomes more likely when the time to think about the information is limited; the less time is available, the more people tend to unquestioningly follow a narrative aligned with their beliefs.

> "In cognitive warfare, the ultimate aim is to **alter our perception of reality** and deceive our brain in order to **affect our decision-making**."

In addition, it should be noted that echo chambers are an excellent venue to collect personal information that can be used for micro-targeting of individuals.

Furthermore, emerging technologies such as synthetic media, deepfakes, artificial intelligence and datamining create opportunities to collect and process information that can be used for cognitive activities. One of these emerging technologies is the Metaverse. The Metaverse is able to replicate the physical world and provide a highly immersive social experience through the use of headsets, body suits and haptic equipment. At the same time, it can provide a significant amount of physical and mental information that can be used for psychological and emotional manipulation or, in the hands of adversaries, microtargeting of individuals.

Who becomes a target for cognitive attacks? Some people are more vulnerable than others. The most vulnerable are individuals who feel a lack of belonging, feel marginalized, think they lack the ability to express their grievances or believe they are deprived of their rights. Usually this is combined with a lack of trust in governance and social structures. These perceptions can stem from ethical, racial, religious, economic or even historical reason. Vulnerabilities are also the key when it comes to understanding how we can protect ourselves against a cognitive attack.

In Western societies, there are four fundamental vulnerabilities to consider:

- **Government structure:** The Western liberal democratic structure is vulnerable to cognitive attacks and at the same time limits the opportunity to detect and defend against these attacks.

- **The media and information landscape:** Limited means or lack of willingness to share information openly, especially in combination with low literacy or underdeveloped critical thinking skills, opens up a critical vulnerability that can be exploited by adversaries.

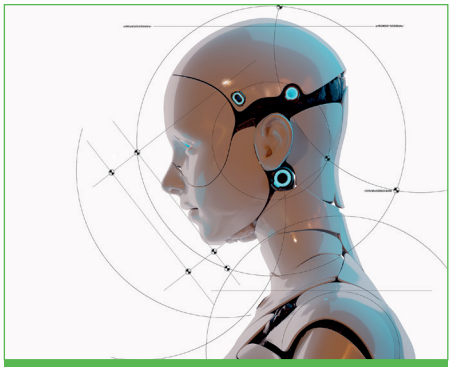
- **Social structures:** Fragmented social structures and particularly echo chambers are vulnerable to false and misleading narratives. The lack of communication between people that only exchange information within their own communities is an easily exploited vulnerability.

• **Increasing level of populism:** People who feel that they are not being heard or properly represented in institutions and that the "elite" is disregarding their concerns see populism as the solution to their problems, making them especially vulnerable to cognitive manipulation.

Knowing one's vulnerabilities is important, but knowing when a cognitive attack is taking place is just as vital. This requires a high level of awareness and a basic understanding of the different methods used. For example, it is essential to maintain awareness about the information we unknowingly share that can be used against us. At the same time, technological solutions can help to identify cognitive attacks through algorithms and artificial intelligence, but also with real-time pattern and signature recognition. General awareness and technological solutions may alert us to cognitive attacks in good time and help us in determining the best way to respond. This brings us to the subject of creating cognitive resilience.

Within the Cognitive Warfare Concept, cognitive resilience is defined as "the capacity to withstand and recover quickly from an adversarial cognitive attack through the effective preparation of groups and individuals." In order to create cognitive resilience, we must look at the current ways in which cognitive activities are conducted, and by which means. In order to keep the initiative, we need to anticipate possible future developments. Currently such future developments include ways to read thoughts and emotions, which can enable measurements of the effect of cognitive activities. Based on the result, models can be developed to improve decision-making, but also to identify weaknesses to exploit.

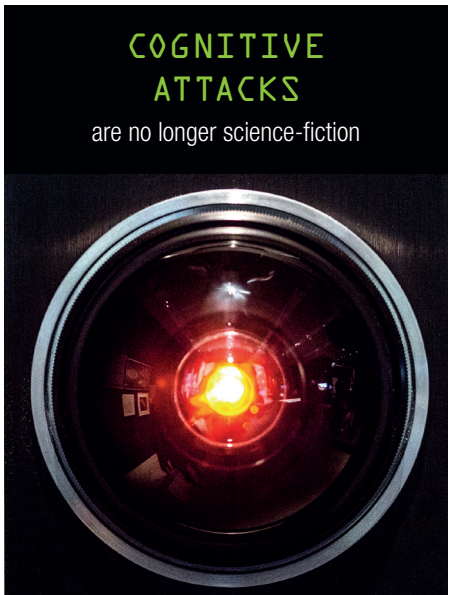
THERE ARE OTHER RAPID developments in the fields of nanotechnology, biotechnology and information technology. In nanotechnology we see the development of nanorobotics, nanosensors and nanoenergy sources making in-body processes possible. Bioartefacts linked to nanorobotics can stimulate perception, cognition and behaviour. In the field of biotechnology, there are encouraging developments in bioengineering, biogenomics and neuropharmacology. One of the most promising projects is the development of embedded synthetic DNA or sDNA. This can be a useful alternative to silicon semiconductors. Currently it is possible to store 2.14 × 106 bytes of data on sDNA. This organic material could enable human-machine interfaces and is often seen as the 47th human chromosome.



"Neural nanotechnology can be used to bring nano-sized robots close to a neuron via the bloodstream and make it possible to link the human brain directly to a computer, making use of artificial intelligence in the process."

In the field of neurocomputing, implants can be used to improve hearing and vision. Furthermore, neural nanotechnology can be used to bring nano-sized robots close to a neuron via the bloodstream and make it possible to link the human brain directly (i.e. not intercepted by our senses) to a computer, making use of artificial intelligence in the process. But we must keep in mind that this is a two-way street: such an artificial intelligence will, in turn, be linked to a human brain.

Below
HAL 9000, a sentient computer from the film "2001: A Space Odyssey."
Photo by Hethers, Shutterstock



In April 2013, U.S. President Obama announced the launch of the White House initiative Brain Research Through Advancing Innovative Neurotechnologies (BRAIN). Its goal was to support innovation that would further our understanding of the brain; Russian commentators perceived it as a project to "hack the human brain."

In 2016 Elon Musk started the neurotechnology company Neuralink, which aims to develop a brain-computer interface to extend the abilities of people with paralysis. Of course, such an interface may also be used to extend the abilities of people without disabilities, for instance to improve their performance on the battlefield. Future developments include innovation in artificial intelligence, machine intelligence and means to enhance human brainpower, either through alteration of genes or directly, by linking the brain through physical peripherals or anatomically internalized products.

IN CONCLUSION, it is important to reiterate that cognitive warfare is no longer science-fiction. Cognitive warfare is a fact of the modern age and everyone, whether civilian or military, is a potential target. Cognitive attacks are aimed at exploiting emotions rooted in our subconscious, bypassing our rational conscious mind. This is achieved by exploiting biases, fallacies, emotions and automatisms, but also through nanotechnology, biotechnology and information technology.

In cognitive warfare, the ultimate aim is to alter our perception of reality and deceive our brain in order to affect our decision-making. We are commonly unaware of such attacks before it is too late and they have already affected their targets. Therefore, we must protect ourselves by raising awareness and developing a system of indicators and warnings that can provide real-time information. The use of artificial intelligence can show us the preferred way to react to a possible cognitive attack.

The human mind is becoming the battlefield of tomorrow, and this means that every person is a potential target. Warfare is no longer a purely military concept; it has become much broader and more complex. In the future, there will only be one rule in warfare: There are no rules. While other domains can provide tactical and operational victories, the human domain is the only domain in which we can secure a full victory. ✦