HUMANITARIAN LAW & POLICY

“Cognitive warfare”: why the human brain should not become a battlefield

February 5, 2026, Analysis / Conduct of Hostilities / IHL / Law and Conflict / New Technologies / Related bodies of law / Weapons

15 mins read

Pierrick Devidal
Policy Adviser, ICRC

Militaries are gearing up for confrontation on a new battlefield: the human brain.

While psychological operations aimed at deceiving enemies or manipulating soldiers and civilian populations have long been part of the military playbook, “cognitive warfare” marks a conceptual shift in which human cognition is framed as a “sixth domain” of military competition, alongside land, sea, air, cyber, and space.

In this post, ICRC Policy Adviser Pierrick Devidal offers an overview of the concept of “cognitive warfare” and examines the humanitarian concerns it raises. He argues that if our brains are to be treated as future battlefields, now is the time to consider how the risks can be prevented and mitigated.

For some military commentators, “cognitive warfare” is “the *ultimate* domain of military confrontation between major powers” and “the *game changer* of the 21st century”. Some *predict* that “the human mind is becoming the battlefield of tomorrow, and this means that every person is a potential target”. Others see “cognitive warfare” as another buzzword repackaging old concepts for strategic purposes. Either way, technological innovation and advances in neuro-, bio-, information and cognitive (NBIC) sciences are enabling new military capabilities that are gaining significant *attention* among governments.

This shift is occurring in the context of broader changes in contemporary warfare. Instilling uncertainty and mistrust in the data and information that have become critical to multidomain military coordination, sometimes described as “*mosaic warfare*”, is now a highly valued strategic capability. “Cognitive warfare” seeks to strengthen that capability through *technological convergence*.

A confusing concept, with the brain as the “target”

There is no commonly agreed definition of the concept of "cognitive warfare". Depending on who uses the term, in which context, and in which language, it can refer to a *wide range* of tools, means and methods aimed at influencing perceptions, emotions, beliefs, decision-making, and actions through the human brain, in order to enhance militaries' strategic advantage over an adversary.

For example, *NATO research defines* "cognitive warfare" as "the art of using technological tools" "to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder actions with negative effects". Chinese strategists tend to use the term "*intelligentized warfare*" in the context of the *"Three Warfares"* approach. Russian military doctrine refers to "*mental warfare*", a term closely linked to '*reflexive control*' concepts. Other expressions, such as "*neuro warfare*" or "*integrated information warfare*" are also in use, adding to the general terminological confusion.

Within strategic discourse, the concept is often framed through *related notions* such as "information warfare" and psychological or influence operations. "Cognitive warfare," however, is best understood as an umbrella term bundling these different forms of military capabilities and operations. While traditional psychological and information operations focus on *what* the target thinks or believes, cognitive operations also aim at influencing *how* they think by affecting the physiological triggers of reactions.

Interference with cognitive and sensory processes through technological means – such as directed sound, light, or radiofrequency energy, or brain stimulation through neural interfaces – builds on manipulated information to trigger action. For example, a large gathering of civilians could be disrupted by the spread of false information on social media about an impending attack, combined with the simultaneous use of a sound canon to provoke a physiological reaction and trigger panic, causing the crowd to disperse.

A key point in this respect is that it is now possible to leverage *neuro-data* to engineer cognitive functions and to "*hack*" the human brain through *neurotechnologies* (such as *brain-computer interfaces* or connected virtual headsets) or *nootropics* and *neuroceuticals* (e.g. chemical substances such as "brain boosters", "smart drugs" or "cognitive enhancers" that impact attention, memory or self-control brain functions). For example, a person wearing *brain-reading earphones* may generate neuro-data indicating a state of excitement or fatigue, which can then be exploited for manipulation through digital interfaces in real time.

While, outside of the context of warfighting, NBIC innovations are creating immense opportunities for medical *progress* – along with no less significant *ethical* questions – they are also enabling increasingly sophisticated manipulation techniques that carry a physical dimension of risk. Recent *reports* of devices generating "anomalous health episodes" through *radio waves* offer just one illustration of their potential impact.

Beyond information and psychological operations, cognitive operations are directed not only at the "data" and software" of human cognition, but also at its "hardware": the brain.

The multiple dimensions of the cognitive domain

Another dimension of "cognitive warfare" is its reliance on a systemic approach, connecting NBIC technologies with cyber and AI tools to enhance the speed, impact and scale of military action while reducing visibility, attributability, and costs. Cognitive operations seek to create convergence and "*enhance synergies*" between different tools and techniques to generate a physical effect on the brain functions of the humans targeted. The objective is to induce them *to act* in line with military aims while preserving the target's impression of self-control. For example, creating an information vacuum through a cyber operation while overwhelming the target's sensory system with loud noises and simulating an emergency risk situation through fake radio calls could lead a military commander to panic and take the wrong decision.

Cognitive operations can also *combine* horizontal (e.g., leveraging family or intra-community relations) and vertical (e.g., using authority and power relationships) vectors of influence. These influencing efforts can be aimed at specific individuals (e.g., military commanders, political leaders, or influential public figures), groups (e.g., political parties, social movements, civil society organizations), or entire populations (e.g. by leveraging *national* institutions or socio-cultural characteristics). Effects multiply and can impact the *whole of society*. Examples of wide-scale manipulation through exploitation of data-based psychological profiles for microtargeting influence operations on social media, such as the famous *Cambridge Analytica* scandal, illustrate the risks.

These multilayered operations are deliberately hard to detect, leading some to characterize them as an "*invisible*" form of warfare. It is indeed difficult to point to real-life examples with certainty, or to distinguish theoretical from real applications of means and methods that are meant to be unattributable. Yet when looking at current events, it is not difficult to see why some believe that people, communities and societies are being manipulated by external interests to act against their own.

The science is no more a fiction

The potential use of technologies such as "*neuro-weapons*" or *brain-computer interfaces* for military purposes may sound like a science-fiction *scenario* of a dystopian future. But military commentators warn that "cognitive attacks are not science fiction anymore. They are "taking place already *now*", allegedly "all around *us*".

While such statements could be exaggerations designed for strategic purposes, it is difficult to ignore the significant military *efforts*, and *financial investments*, that are *taking place* in the cognitive domain. Increased polarization of politics and informational ecosystems, the development of "*total defense*" strategies against "*hybrid threats*", and progress and massive financial capitalization in *NBIC* technologies are creating strong incentives for "cognitive warfare" development.

For now, existing *strategies* are mostly framed around cognitive "*resilience*" or "*performance*" rather than offensive capabilities, but the line between defense and offense purposes can be a very thin one. The potential for *repurposing* is significant, and technological safeguards seem to be inexistant. The *cognitive arms race* is accelerating under the usual pretense that adversaries' action must be *matched*, risking a race to the bottom in terms of *ethics*, with potentially dangerous consequences.

The tech myth of "clean wars"

Some advocates of "cognitive warfare" argue that it could help to "*win the war before the war*," reducing the need for direct military confrontation and, in turn, saving lives by limiting the scale and human cost of kinetic hostilities. This is a wishful claim. The promise of "*clean wars*" achieved through technological innovation has so far proved a *myth*, sustained in part by the economic and political interests that benefit from *techno-solutionism*.

"Cyber warfare" was similarly pitched by some as a way to reduce the need for "boots on the ground". Drones and AI-guided weapons were presented as tools for more precise targeting and greater protection of civilians. Yet in ongoing conflicts, soldiers continue to be deployed in large numbers to frontlines. Entire cities continue to be destroyed, children continue to be killed and maimed on an unimaginable scale, and civilian populations and infrastructure continue to face gruesome attacks. In practice, "cognitive warfare" is layered *on top* of kinetic warfare. It creates *more* risk for civilians and combatants, not less.

The concept of “cognitive warfare” also expands the domain of so-called “hybrid” military operations below the threshold of armed conflict, and explicitly includes civilians as potential targets. As a result, it contributes to *blur*ring the boundary between war and peace, between what is civilian and what is military, and between what is a legitimate military target and what is not. However, in law, the (red) lines that protect civilians and limit the means and methods of warfare during armed conflict are clear. And within or outside of armed conflict, cognitive operations must comply with applicable *human rights law*, including the rights to privacy and self-determination.

Attempts to “*blur* the lines” are manipulations that *serve* a worrying *tendency* to “*weaponize everything*” and present existing rules and safeguards as obstacles to military objectives. It is critical to respect the law to prevent the potentially devastating consequences of “cognitive warfare”.

The potentially devastating impacts of “cognitive warfare”

Undoing humanness, agency and control

Cognitive modifications can *help* sustain or impair vigilance and focus; improve or deteriorate memory, coordination and reaction time; and increase or reduce stress and fatigue. They are specifically designed interferences with situational and emotional awareness, critical reasoning and judgement capacities. They target the *core* of the brain’s cognitive functions and human agency. The rhetorical questions about the humanness of those who are subject to those ‘*enhancements*’ are significant, leading some legal scholars to *question* whether such modifications can turn humans into “*weapons*”.

It is not difficult to understand the military interest in methods that promise both tactical and strategic advantages, defensive and offensive capabilities, from the frontlines of the battleground to the “*battle of narratives*”. Yet this perceived military interest can be short-sighted. When soldiers are cognitively or *biologically modified* to be more aggressive and “*combat fit*”, and when their sense of empathy and humanity towards others is deliberately manipulated for combat purposes, how will they behave towards civilians and others protected by international humanitarian law (IHL)? And if their agency and sense of control are undermined, what guarantees exist that they will recover their full cognitive abilities once an operation ends, or when they return to their families and civilian life?

Militaries are already *outpaced* in their ability to keep control of the *cyber*, *AI* and *neuro*– technologies at their disposals. The technological challenges to their cognitive *agency* can have serious consequences on the conduct of hostilities and *respect* for IHL. “Cognitive warfare” techniques risk further altering soldiers’ sense of control in ways that jeopardize their ability to follow orders or rules of engagement. And while they may not be in a position to truly consent to use, or be used for, cognitive operations, they remain accountable for them.

Humans are, arguably, already often cognitively overwhelmed and getting *number* and *dumber* because of the impact of the “attention economy” technologies on our ability to think. Increasing reliance on AI is leading to “*cognitive offloading*”, gradually eroding intellectual abilities and undoing essential elements of what it means to be human(e). Faced with new, more advanced cognitive manipulation techniques, we may be in real trouble.

Unpredictable reverberating effects

It has been said that “cognitive warfare” is like a “*Molotov cocktail*” for the brain. Once it is used (or becomes accessible to non-state or criminal actors), it may light a fire that is difficult, if not impossible, to control. By combining cognitive modifications (e.g., ‘*go pills*’ to increase aggressiveness and combat resilience) and psychological manipulations techniques (e.g., use of popular digital *services* to manipulate people’s emotions), cognitive operations create a cumulative domino effect.

Messing with brain functions has inevitable side effects and longer-term *consequences* on people and societies that cannot be predicted. At the level of individuals, cognitive damage may be permanent and irreversible. When people are manipulated to be paranoid, angry, radicalized and violent, how does one mitigate the risks for their safety and dignity? And when the war ends, how do you build peace and maintain security with individuals and communities who have been cognitively formatted to trust nothing and no one?

At the societal level, the secondary effects may be profound, systemic and long-lasting. Cognitive operations target the enemy’s “*fabric of trust*” to create confusion, fragmentation and tension. The potential society-wide effects are however unpredictable and unlikely to stop at borders. By eroding the trust of soldiers, cognitive operations can impact their ‘will and morale’ and jeopardize discipline and chains of command – essential tools to ensure respect for IHL. By instrumentalizing morality and legitimacy to affect the trust of populations, such operations may fragment the cement of the social contract on which governments are built. By introducing division, polarization and dehumanization of the “other” within communities, they may poison the glue of social cohesion. By leveraging corruption and inequalities, they can undo the systemic trust that underpins functioning economies. Without social contracts, cohesion and trust, societies can simply not function.

Through “cognitive warfare”, it is expected that the enemy will eventually fall apart from within, without having to shoot a bullet. But the reverberating effects of destroying cognitive functionalities and the social fabric of trust are difficult to identify and effectively mitigate. And it is very *unclear* if militaries are adequately equipped to prevent and mitigate these deeply disruptive potential secondary impacts.

Responding to the convergence of risks through compliance and prevention

As states prepare for potential large-scale armed conflicts across the world, the idea that the miliary battlefield could expand to the human brain is profoundly alarming. As discussed above, “cognitive warfare” threatens core elements of human integrity and agency and undermines essential tenets of IHL and militaries’ ability to comply with it. Cumulatively, its secondary impacts are unpredictable and potentially devastating. As military strategies and investments in the cognitive domain develop, it is essential to seize the moment to build effective safeguards against a “cognitive arms race” that threatens the integrity of our brains and what defines our humanity. We should begin by:

- Ensuring that military cognitive operations comply with IHL principles and rules, including those governing conduct of hostilities. As it is in fact not a new domain of warfare, “cognitive warfare” does not emerge in a legal vacuum, and the techniques and methods it encompasses are regulated by existing legal frameworks, notably IHL. Using information, psychological, cyber or AI means to manipulate and deceive the enemy is not prohibited, provided such use complies with IHL. Military technology must fit the law, not the other way around.
- Developing militaries’ ability to build effective “cognitive warfare” risk prevention and mitigation frameworks at both the doctrinal and operational level. The capacity to understand and measure secondary impacts and reverberating effects on individuals and societies is essential to ensuring the legality of such operations.
- Respecting international *human rights law obligations* that protect people’s physical and cognitive integrity, their rights to self-determination, health and freedom of thought from undue interferences, including through neuro- and biotechnologies and “cognitive warfare” related techniques.
- Leveraging medical, scientific and military ethics to inform behaviour in the cognitive domain and when relevant, building new *legislation* to protect “*neuro-rights*” and preserve people’s cognitive security and agency against dangerous commercial or military experimentations.

“Cognitive warfare” relies on a convergence of technological, scientific and psychosocial layers of action. That same convergence applies to the risks it creates. These risks do not operate in isolation; they accumulate, interact, and amplify one another. Ongoing cooperation, regulatory and *governance* initiatives in the fields of *IHL*, *digital information environments*, *artificial intelligence*, *information and communication technologies*, and *neuro*– and *bio*technologies offer an opportunity to build a similarly convergent approach to prevention and risk mitigation.

The time to act is now, while we still have the cognitive capacity and freedom to do so.

See also

- Terry Hackett and Alexis Comninos, *Outsourcing humanity? International law, humane treatment, and artificial intelligence in detention…*, November 13, 2025
- Anna M. Gielas, *Warfare at the speed of thought: can brain-computer interfaces comply with IHL?*, August 21, 2025
- Ruben Stewart, *The shifting battlefield: technology, tactics, and the risk of blurring lines in warfare – Humanita…*, May 22, 2025
- Joanna L D Wilson, *AI, war and (in)humanity: the role of human emotions in military decision-making*, February 20, 2025
- Ruben Stewart, *Algorithms of war: The use of artificial intelligence in decision making in armed conflict*, October 24, 2023

Tags: AI, Artificial Intelligence, Civilians, conduct of hostilities, Cyber and Information Operations, ethics, Gender and IHL, human rights, international human rights law, international humanitarian law, Legal Review of Weapons, Means and Methods of Warfare, military, modern warfare

Bridging IHL and WPS: untapped potential to advance the wellbeing of women in conflict settings

13 mins read

Analysis / Conduct of Hostilities / IHL / Law and Conflict / New Technologies / Related bodies of law / Weapons Jessica Anania

The International Criminal Court recently issued its first conviction for gender persecution as a crime …

Deaths and separations in migration: lessons from migrant women and children

11 mins read

Analysis / Conduct of Hostilities / IHL / Law and Conflict / New Technologies / Related bodies of law / Weapons

Magdalena Arias Cubas, Sanjana Bhardwaj & Simon Robins

Many women and children are exposed to violence, exploitation and other risks, including death and …