THE BRAIN IS BOTH THE TARGET AND THE WEAPON

THE STRATEGIC NECESSITY OF NATO'S COGNITIVE WARFARE CONCEPT

by **Tanna M. Krewson**
NATO Allied Command Transformation
Cognitive Warfare Subject Matter Expert;
Architect of NATO's Cognitive Warfare Concept

"Cognitive warfare is not merely an academic exercise or a distant strategic concern. It is the defining security challenge of our time, one that demands both intellectual rigor and practical action from every member of the Alliance community."

Admiral Pierre Vandier
Supreme Allied Commander Transformation

The War Before the War

On August 21, 2013, the world awoke to haunting images from Ghouta, a suburb of Damascus. Civilians — many of them children — were gasping for air, convulsing, and dying in the streets. The evidence pointed to a massive chemical weapons attack by the Assad regime, crossing the "red line" set by U.S. President Barack Obama only a year before.

Almost immediately, the information space was filled with competing narratives. Russian media outlets, diplomats, and proxy influencers, supported by botnets and troll farms, cast doubt on what had happened. Was it a false flag? Could the footage have been staged? In days, what appeared to be a clear-cut atrocity dissolved into ambiguity. These narratives, carried across RT, Sputnik, fringe Western outlets, and social media platforms, tapped into an old wound rooted in public mistrust after the false weapons of mass destruction claims preceding the Iraq War.

This was more than propaganda. It was a deliberate campaign to muddy intelligence, inject doubt into Allied debates, and stall action. Washington hesitated, then backed away from strikes, accepting instead a Russian-brokered deal.[1] Russia's approach in Syria remains one of the clearest examples of how cognitive warfare can target military command and control (C2) at both tactical and strategic levels. By 2015, Russia had paired these narrative operations with electronic and cyber tools — spoofing communications, jamming UAV feeds, and disrupting intelligence, surveillance, and reconnaissance (ISR) — to erode commanders' ability to act decisively. These were not incidental effects but the intended outcomes of an integrated cognitive campaign: victory achieved not through combat, but through paralysed decision-making before the fight began.

The lessons of Ghouta echo today. At the 2025 NATO Communicators Conference in September, participants underscored that adversaries are no longer simply contesting the information space; they are deliberately targeting the Alliance's ability to think, decide, and act. The message was clear: NATO must start taking the cognitive threat seriously, treating it as a contested domain in its own right.

However, this requires more than words. It requires investment in people, training, and capabilities on a scale reflecting the priority adversaries place on cognitive effects. Until NATO develops the ability not just to defend but to contest in this space, it risks repeating the same paralysis that followed Ghouta. That danger captures the essence of cognitive warfare — but to understand it, we must first define it.

What Is Cognitive Warfare?

Despite growing thought leadership in this space, a comprehensive understanding of cognitive warfare remains elusive. It is often mistakenly equated with hybrid warfare; however, while hybrid warfare involves the coordinated use of multiple instruments of power, with information as one of many tools, cognitive warfare differs in its core objective: to target and influence both human and machine cognition. It can be pursued through any domain, by any means, and at any stage in the continuum of competition, with the aim of obscuring truth, inducing decision paralysis, and shaping perceptions and behaviour.

Cognitive warfare is also not a replacement for strategic communications. In this space, information operations (InfoOps), psychological operations (PsyOps), and military public affairs (MilPA) are just a few of the capabilities and functions employed in the daily contest for cognitive advantage. As such, cognitive warfare is not the means by which we fight; it is the fight itself.

This fight is not simply about the proliferation of disinformation or propaganda, nor is it about time-honoured deception and trickery. Cognitive warfare is the deliberate targeting of human and machine cognition to influence how people think, what they feel, and, ultimately, how they act.

In this battlespace, the brain is both the target and the weapon — the terrain and the conduit through which strategic outcomes are won or lost. Emotions, narratives and identities can be engineered en masse and disseminated to others to alter the course of public opinion, destabilize societies, and influence critical decisions, frequently below the threshold of armed conflict. Though seemingly abstract, many of these operations should be viewed as cognitive attacks: orchestrated information activities designed with hostile intent to manipulate perceptions, beliefs, objectives, decisions and behaviours.

However, understanding cognitive warfare solely through a military lens is insufficient. To fully grasp how it functions, the starting point is recognizing its impact on us as individuals, something that does not come easily. After all, cognitive warfare is, at its core, about humans — and humans are notoriously complicated and volatile, making it problematic to predict behaviour, even our own.

How Cognitive Warfare Impacts Us Individually

The challenge for many is that the ambiguities inherent in the cognitive dimension make it difficult for us to see and understand how cognitive warfare operates, particularly at a daily micro level.

However, you only need to walk into a restaurant or café to see the cognitive battlefield. Entire families sit silently at tables — not talking, just scrolling social media feeds comprised of other people's lives, thoughts and opinions. Many of us fall prey to this technological trap because scrolling and posting are often easier than engaging: we're burned out and tired; real-life relationships are hard; and technology is at our fingertips, providing feel-good dopamine surges. This perfect storm of emotional exhaustion, digital ease, and pleasurable brain chemicals makes it easy to believe that our reliance on constant stimulation is harmless. But it is not.

Today's information environment (IE) is intentionally designed to be addictive, to keep us reading headlines, sharing memes, and watching videos. Billion-dollar industries are built upon platforms and algorithms orchestrated to monetize our propensity to check out of our private lives by checking in to social media. However, our increasing digital immersion and fixation on outrage, opinions and chaos is not benign. It is not merely a cultural shift altering how we socialize; it is a strategic vulnerability that primes us for adversarial influence.

In previous generations, people sat with their thoughts. They spent time thinking without distraction in quiet moments, giving their brains the space to have big ideas. But we no longer sit with our thoughts. We sit on our devices, letting the thoughts of others influence us, all while believing we are thinking for ourselves. We outsource our attention and fill our idle moments with a constant stream of memes, headlines, and outrage. The problem is not just distraction; it is infiltration. Because much of the information we consume is not neutral, and what we think are our own thoughts are often just the opposite.

We are being targeted, not randomly but deliberately, and we rarely recognize that the information we consume is a threat. We do not see when it alters our perceptions because we think we have changed our minds based on our own logic. However, often, those changes in belief are unconscious and the result of emotions manipulated by malign actors who benefit from our anger and frustration.

The challenge is that addressing cognitive warfare requires each of us to examine our own behaviour, whether we are civilians, military members, or government officials. It is very easy for us to say:

> *"So, what? I'm on my phone."*
> *"My watch tracks my steps."*
> *"I decompress by scrolling X. My kids enjoy YouTube. TikTok makes my wife laugh. What's the big deal?"*

But, if we step back, what does this dynamic, which stretches across nations and cultures, say about the direction of our societies? And what risks does this persistent access to our data, from our shopping habits and proclivities to our heart rates, pose to us as individuals, leaders, and nations? More importantly, it raises the question: to whom are we giving our time and attention? Do we even know? And what opportunities are we providing adversaries — through influencers, memes, bots, and deepfakes — to shape what we think and how we behave? For most of us, the answer is: we don't know.

"To whom are we giving our time and attention? What opportunities are we providing adversaries — through influencers, memes, bots, and deepfakes — to shape what we think and how we behave? For most of us, the answer is: we don't know."

Why Cognitive Warfare Works

A malign actor who understands the emotional power of symbols such as flags or religious texts will use them to spread their ideas, evoke emotions, and influence people to act in their favour; even better if those symbols can be used to signal a call to action for specific groups. This malign actor can then use information — including knowledge about individuals, how communities are structured, and the meaning of historical events in target populations — to prompt people to react reflexively because they know that we humans are not the rational actors we believe ourselves to be. And that is our primary vulnerability.

While there is debate about the statistics, only 2–15% of human thinking is driven by logical reasoning, with the remaining 85–90% influenced by emotions, instincts, and unconscious processes.[2,3] It is that 85–90% share that makes us reactively click the headline, share the meme, rage about the story, and retreat into digital echo chambers, often without clear awareness.

However, as a society, we continue to overlook the signs that we are being manipulated because this is not about a tangible battle for borders or territory; this is about an intangible battle for our minds. And whilst there is variation in the extent, no one is immune, regardless of rank, education level, age, or IQ.

If I can evoke an emotional reaction in you based on carefully tailored information and imagery, I can also elicit a similar response in others like you. If I can then create a message that rapidly spreads throughout already disenfranchised populations via social media, I can trigger uprisings, movements, riots, and discord. I can make you distrust your systems, hate your leaders, dismiss your family members, and fear your neighbours. And I do not have to use the truth. I can create fake AI-generated videos, fictitious speeches, and fabricated events. I only need to know which symbols will resonate with specific populations, which narratives will tap into existing fears or shame, and which audiences are already vulnerable to my influence. Mere fact-checking will not usurp my ability to guide your perception of reality.

From Targeting Populations to Timing Perception

Skeptics often argue that cognitive warfare is not new, and it isn't. Militaries and governments have used weaponized information and targeted propaganda for centuries. However, what *is* new is the pace of change and the ability of malign actors to infiltrate our daily lives by exploiting the rapidity and reach of technology, as well as their expanding understanding of human behaviour and the brain. There is an increasing asymmetry in capability and agility, and that is why cognitive warfare is so dangerous.

For a moment, picture a future where influence operations are no longer limited to *what* you see but *when* you see it, and in what emotional state. Imagine I have access to your smartwatch data: your heart rate, stress levels, and sleep patterns. With this biometric insight, I do not need to guess when you are most vulnerable — I can know. And by gaining access to or manipulating the platforms that interpret this data, I can time the delivery of content to coincide with moments of heightened emotional or cognitive susceptibility.

If your heart rate spikes, signaling stress, fatigue, or agitation, I can inject targeted messaging into your environment: emotionally charged content, narrative reinforcements, or psychologically primed cues to shape your perception and behaviour. And I can do this at times when the data indicates your executive functioning is compromised: while mindlessly scrolling Instagram late at night, when your heart rate elevates after a fight with your spouse, or when your glucose levels are low before breakfast. This is not just targeting the *who* of influence; it is targeting the *when* and *how*. It enables real-time, individualized microtargeting that bypasses your rational defences and exploits your body's stress response as an entry point for manipulation.

The Engineering Behind Our Dysfunction

This future is not far off — it could well be tomorrow because, while our understanding of human behaviour and neuroscience is relatively young, it is maturing at a rapid pace.

One hundred years ago, we still believed in bloodletting. Fifty years ago, we institutionalized people for manageable conditions such as bipolar disorder. It wasn't until 2003 that the human genome was completely mapped. Over the past 20 to 30 years, our understanding of how the brain interacts with and shapes our realities has expanded rapidly in line with the parallel growth of technology. As a result, the ability to influence how societies function and individuals behave has also evolved.

With this understanding, malign and adversarial actors are not just observing our dysfunction; they are engineering it. And with the power of technology and the hours we dedicate to it, our identities are easily weaponized. The challenge is that many of us have been raised to believe that emotions and beliefs are something we push aside to get on with the business of the day. We grew up singing, "Sticks and stones may break my bones, but words will never hurt me."

Science tells us this is untrue. Words are enormously influential. Emotions, narratives, and worldviews can be powerful enough to make people protest their leaders, align with extremist ideologies, or engage in violent terrorism. What happens if entire populations reject long-held national values not because of genuine disagreement about the values themselves, but because adversaries have succeeded in changing prevailing views about how those values should be applied?

This is not hypothetical; this is the essence of cognitive warfare, and it is happening now. In this new world, society is the vector through which adversaries target political and military systems. They no longer need to target military forces directly if they can stir enough internal discord for citizens to turn against their governments, institutions, and alliances.

And waging this type of warfare is dangerously cost-effective — far cheaper than buying tanks or planes — precisely because it does not require physical force to achieve strategic effects. It targets not terrain but something far more fragile: truth, trust, and the will to act.

We Are All Vulnerable

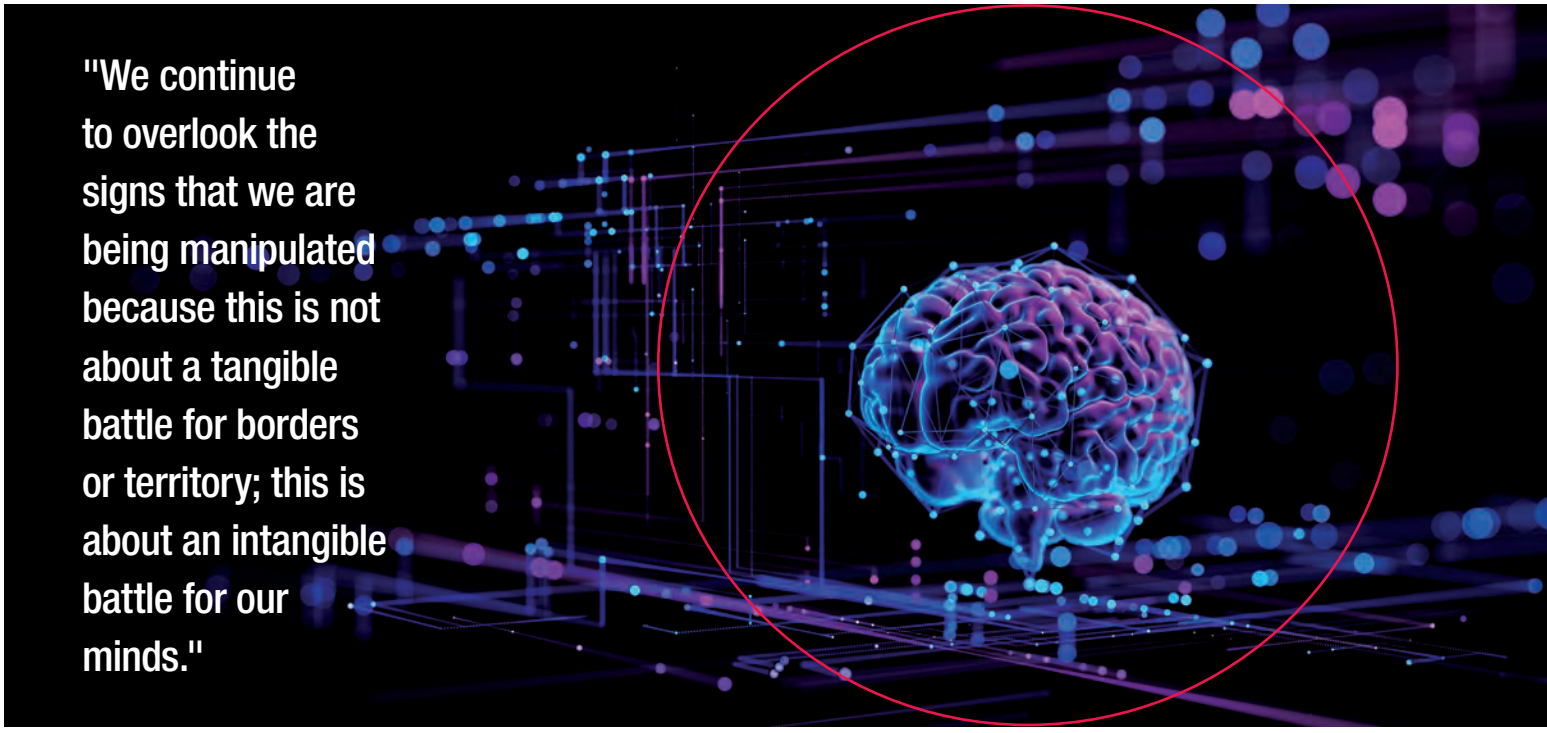
At a NATO Allied Command Transformation (ACT) cognitive warfare simulation event in 2023, national representatives were asked a simple question: Do you believe your country needs to address cognitive warfare? The majority said yes. However, when asked whether they felt personally vulnerable to cognitive warfare, very few did. Their responses were predictable, and they illustrate a fundamental point: how can we, as militaries, nations, and Allies, effectively counter and respond to cognitive warfare if we do not understand how we, as individuals, are vulnerable?

ROBUST PSYCHOLOGICAL and neuroscience research indicates that humans are predisposed to minimizing their own cognitive vulnerabilities while externalizing weaknesses onto others. This protective mechanism helps preserve self-confidence, but it also creates blind spots, impacting our ability to counter and respond to cognitive warfare. More often than not, we assume that the problem is other people: "I'm not vulnerable to influence; they are. I would recognize cognitive warfare."

This is not accurate.

Every individual is a target.

Twenty-four hours a day, our adversaries and competitors utilize trained specialists — and increasingly, machine cognition, AI, and other technologies — to analyze our media habits, affiliations, and identities, creating emotional and behavioural effects from afar. And their goal is clear: to prime and destabilize societies from within long before traditional confrontation occurs.



Real-World Examples

Between 2019 and 2021, ISIL-aligned insurgents in Mozambique's Cabo Delgado province conducted a systematic cognitive warfare campaign, weaponizing platforms such as Facebook, WhatsApp, and Telegram. They distributed graphic propaganda, fabricated footage, and false territorial claims to incite fear and evacuate towns before attacks occurred.[4] These efforts were paired with economic disruption, including strikes on energy infrastructure and supply chains, to amplify perceptions of state failure. Targeted assassinations of local leaders further eroded trust in governance, combining psychological intimidation with physical violence. The campaign glamourized fighters, denigrated the government, and attracted thousands of disenfranchised youths from across the region. By 2020, over 400,000 people were displaced, many fleeing due to fear fueled by online rumours rather than battlefield threats.[5] Cyber disruptions of humanitarian communications paralysed aid delivery, while selective kinetic strikes reinforced the illusion of militant omnipresence. These tactics decimated governance, derailed infrastructure projects, and disrupted humanitarian operations, all without large-scale combat.

China's growing use of AI in influence operations further demonstrates how adversaries are fusing emerging technologies with cognitive effects. Based on research from the New York Times, documents leaked from GoLaxy, a Chinese company tied to state security agencies, reveal how its "Smart Propaganda System" (GoPro) has been deployed in Hong Kong, Taiwan, and inside China to track debates, mine social media profiles, and generate targeted, adaptive propaganda that "feels authentic."[6]

In the 2024 Taiwanese elections, the system recommended narratives designed to exploit divisions in public opinion and weaken the Democratic Progressive Party. These efforts went beyond Russia-style troll farms, using AI to mass-produce and target content at scale. While not all operations proved decisive, the campaigns consistently sought to undermine trust in Taiwan's pro-independence leadership by reframing national identity and amplifying narratives of inevitability around Beijing's influence. GoLaxy's methods highlight the shift from time-intensive, handcrafted propaganda to AI-enabled identity manipulation, something branded as increasingly quicker, cheaper, and more targeted.

Currently, the company claims the ability to track over 180,000 X accounts in Hong Kong, monitor thousands of Western social media posts daily, and build virtual profiles on more than 2,000 U.S. political figures. In Taiwan, these capabilities mean that adversarial messaging can be explicitly aimed at citizens who are already primed by grievances over sovereignty and security. Even when content is factual, its emotional framing and algorithmic amplification create distorted perceptions of consensus and inevitability, crafting an environment where the ultimate target is not facts, but identity itself.[7]

What This Means for NATO

While Allies possess defensive tools such as regulation, legislation, and enforcement to respond to cognitive effects, these measures tend to be fragmented, reactive, and rather slow. This asymmetry in deterrence and defence allows adversaries to undermine societies, weakening national resilience and splintering NATO's collective defence posture.

The traditional visualization of NATO's military capability, holding strong on an eastern or southern flank to prevent a physical advance, is outdated and trapped in a 20th-century perspective.

Information has no borders. These new front lines will not appear on a map. The most straightforward and efficient path to defeating NATO's military capability is not by applying strength against strength but by degrading societal and political support for NATO's military actions before they begin. Our key vulnerabilities are no longer defined by the range and lethality of our weapons but by the openness of our societies.

A Whole-of-Society Problem

Unfortunately, the term "warfare" is somewhat misleading. Responding to cognitive warfare requires us to acknowledge that it cannot be addressed solely through military strength because it is primarily waged through the soft underbelly of society. Our least protected have become our easiest targets and most significant vulnerabilities.

The figure on page 35 illustrates this dynamic by depicting the symbiotic relationship between the military and civil society. The graphic demonstrates the dual nature of the cognitive warfare threat landscape, divided between the comparatively hardened military sphere and the vulnerable civil society domain.

"Information has no borders. Our key vulnerabilities are no longer defined by the range and lethality of our weapons but by the openness of our societies."

"NATO must do more than adapt — it must lead. This demands a full-spectrum, multi-domain approach focused on embedding cognitive warfare into doctrine, training, and operational planning."

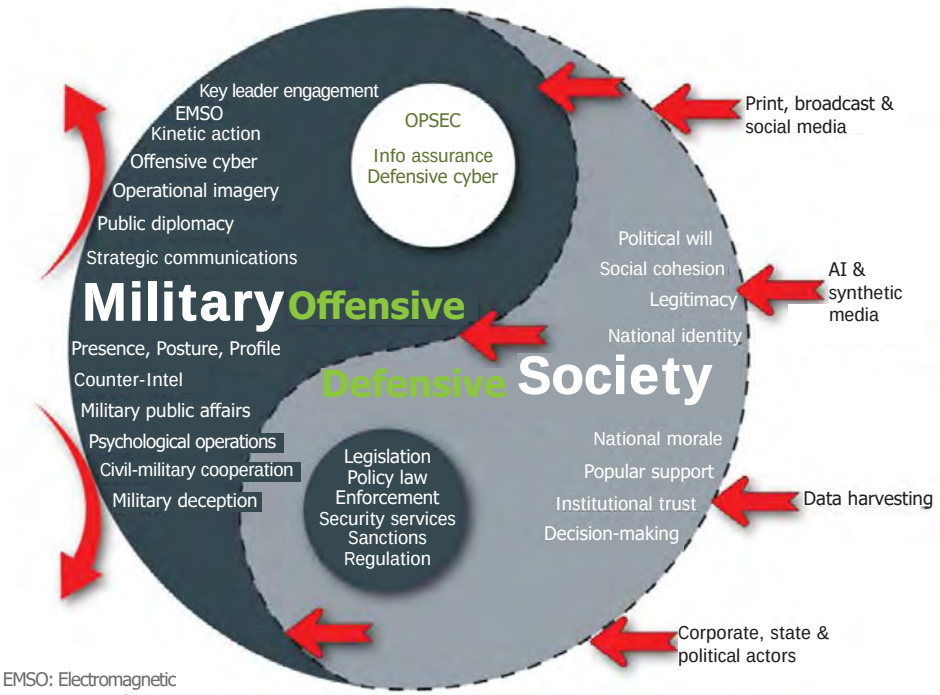
The red arrows represent threats in the information environment (IE) directed at the Alliance, aimed at achieving political and military objectives. The military half of the diagram illustrates traditional capabilities that protect the military instrument of power through tools aimed at adversaries, supported by layered defences such as information assurance, operational security, and defensive cyber. The military operates as a "hard target," fortified by doctrine, infrastructure, and threat awareness. While adversaries may attempt to disrupt military cognition and decision-making, such efforts can be anticipated and neutralized.

In contrast, the civil society half of the diagram is open, decentralized, and exposed. Democratic freedoms and a largely unregulated IE make it a "soft target," vulnerable to adversarial cognitive operations that manipulate perception, polarize opinion, and destabilize communities. These attacks exploit technologies such as AI, media ecosystems, and data harvesting. The dashed line around society reflects its porous boundaries, where adversaries target the accessible, unaware, and unprotected civil domain underpinning NATO's strength.

As a result, the psychological and societal effects of adversarial attacks can bleed into hardened military structures, especially in areas where the civil and military spheres intersect, eroding trust in defence institutions, weakening recruitment, and undermining public support. These attacks are not hypothetical. They degrade readiness, morale and legitimacy, threatening NATO's operational effectiveness.

Even if NATO fielded the strongest and best-resourced militaries in the world, it would not be enough if societies remained vulnerable. Adversaries target the foundations of resilience, knowing that no amount of military power can compensate for a fractured, unstable society. This spillover of effects between civil and military spheres has led to the misconception that cognitive warfare is incompatible with democratic values. However, like warfare in any domain, operations in the cognitive dimension reflect the strategic culture of the actors involved. Democracies need not abandon their principles; they must develop cognitive strategies aligned with their norms while countering adversaries who exploit openness and trust. Upholding democratic integrity while building resilience is not only possible but essential to safeguarding societal cohesion and long-term security.

Below
Graphic adapted from NATO Strategic Communications Centre of Excellence



EMSO: Electromagnetic spectrum operations

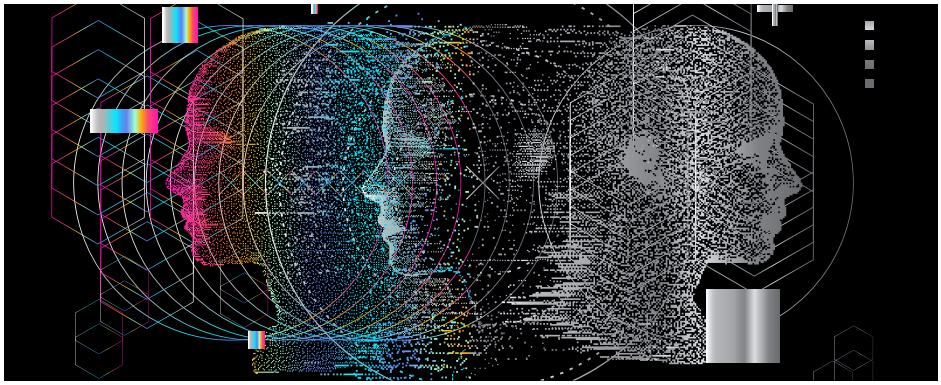
Maintaining Strategic Advantage: The NATO Cognitive Warfare Concept

States within the Alliance are making significant progress toward these goals, including implementing national and regional strategies to counter hostile information activities, enhancing media literacy, and supporting expanded research and development. However, we remain reactive, constrained by outdated legislative, systemic, and conceptual frameworks. The scale of current adversarial information proficiencies exceeds our capabilities — a strategic asymmetry that threatens our ability to act decisively in a crisis.

We face a stark choice: either invest in enhancing cognitive capabilities and adapting traditional perspectives on the role of the military and government within society, or accept that we will fall behind, risking failure to secure cognitive advantage in an increasingly hostile IE. Rapid and decisive action, including a societal paradigm shift, is required to defend our populations, institutions and military forces from degradation in the cognitive dimension.

To accomplish this, NATO must do more than adapt — it must lead. This demands a full-spectrum, multi-domain approach focused on embedding cognitive warfare into doctrine, training, and operational planning; resourcing influence capabilities and behavioural sciences; and uniting uniformed services with civilian institutions across the continuum of competition.

"Facts do not prevail on their own; emotion, identity, and resonance are just as powerful."



These ideas form the basis of NATO's Bilateral Strategic Command (Bi-SC) Cognitive Warfare Concept, a necessary and urgent call to action designed to address functional, legal, ethical, and doctrinal gaps and offer an actionable path forward. The concept acknowledges that cognitive warfare is no longer a supporting function — it is the contest itself. We must strengthen our ability to apply existing instruments of national power in a cohesive, integrated way across all phases of competition; something demonstrated during the early stages of Russia's 2022 invasion of Ukraine. While that unity has evolved with time, Ukraine continues to show what is possible when societies and militaries fight in concert, combining kinetic force with political, economic, diplomatic, and informational power. These hard-earned lessons must not be ignored.

From a strategic communications standpoint, we must also move beyond the assumption that "truth-telling" alone will win the battle for cognitive advantage.

If cognitive warfare has shown us anything, it is that facts do not prevail on their own; emotion, identity, and resonance are just as powerful, if not more so. It is not enough to broadcast our values and fact-check disinformation; we must also address the underlying issues that fuel it by engaging with the full spectrum of perspectives within our societies to deter adversarial weaponization of existing social discord.

Below
The author (right) was one of the speakers at the 2025 NATO Communicators Conference, which underscored that adversaries are no longer simply contesting the information space; they are deliberately targeting the Alliance's ability to think, decide, and act. Photo by HQ SACT PAO

Conclusion: We Are Already in the Fight

As individuals, military and otherwise, we must accept that we are already in the fight. But the front lines are not drawn on maps; they run through our institutions, our societies, and our minds. It is about all of us. There are no bombs, no borders — just the quiet hijacking of our perception. Our adversaries do not need to use expensive missiles and machinery if they can keep us distracted, divided, and emotionally reactive. They understand that influence does not require truth, but only our attention.

If we do not take steps to recognize the ubiquity and seriousness of the cognitive battlespace, which touches every aspect of our military and civilian lives, we will lose more than time; we will also lose readiness. We must invest tonight if we expect to fight tomorrow. If we fail to do so, we may wake up to discover that our thoughts are no longer our own. Not because we lost a war — but because we never appreciated that we were in one. ✧

ENDNOTES

1 BBC, https://www.bbc.com/news/world-middle-east-24091633. U.S. and Russia agree Syria chemical weapons deal
2 V.B. Kahneman, D. (2011). Thinking, fast and slow. Macmillan.
3 Evans, Jonathan St. B. T. & Stanovich, Keith E. (2013). "Dual-Process Theories of Higher Cognition." Perspectives on Psychological Science, 8(3), 223–241.
4 Blaker, L. (2015). The Islamic State's use of online social media. Military Cyber Affairs, 1(1), 4.
5 Svicevic, M., & Bradley, M. M. (2024). Mozambique's Cabo Delgado Conflict. Taylor Francis Limited.
6 New York Times, https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html
7 ibid.