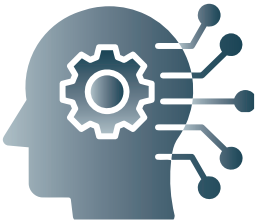
NATO OTAN

Science & Technology Organization (STO)

Cognitive Warfare

NATO Chief Scientist Research Report



NATO Chief Scientist Research Report

The Chief Scientist Research Reports (CSRRs) provide NATO's senior political and military leadership with clear, evidence-based insight into science & technology (S&T) developments. These reports translate complex research results into actionable analysis to help the Alliance anticipate potential technological disruption, identify likely capability gaps, and adapt strategically in order to shape the future security environment and battlespace.

As the senior scientific advisor to NATO leadership, the Chief Scientist provides the evidence base that supports planning, policy, and decision-making, leveraging cutting-edge research from the NATO Science & Technology Organization (STO). The CSRRs contribute to scientific awareness, supporting long-term reflection, and ensure that S&T considerations are factored into broader defence planning and policy development. The CSRRs are decision-support tools that help connect the Alliance's knowledge base with real-world priorities. They guide senior leaders in translating knowledge into action and reinforcing NATO's ability to respond with agility and coherence to emerging security challenges.

At the core of NATO's scientific community is the STO, the Alliance's principal body for cooperative defence S&T. Governed by the NATO Science & Technology Board (STB), the STO conducts a multinational Programme of Work and acts as the hub for scientific collaboration among Allied and Partner Nations. It brings together national experts who pursue applied research, experimentation, prototype testing, and analysis. By fostering interoperability and information exchange, the STO enables NATO to derive decisive advantages across all Instruments of Power from the nations' combined investment in NATO's shared knowledge base.

Table of Content

Disclaimer: The research and analysis underlying this report and its conclusions were conducted by the NATO Science & Technology Organization (STO). This report does not represent the official opinion or position of NATO or individual governments.

Foreword

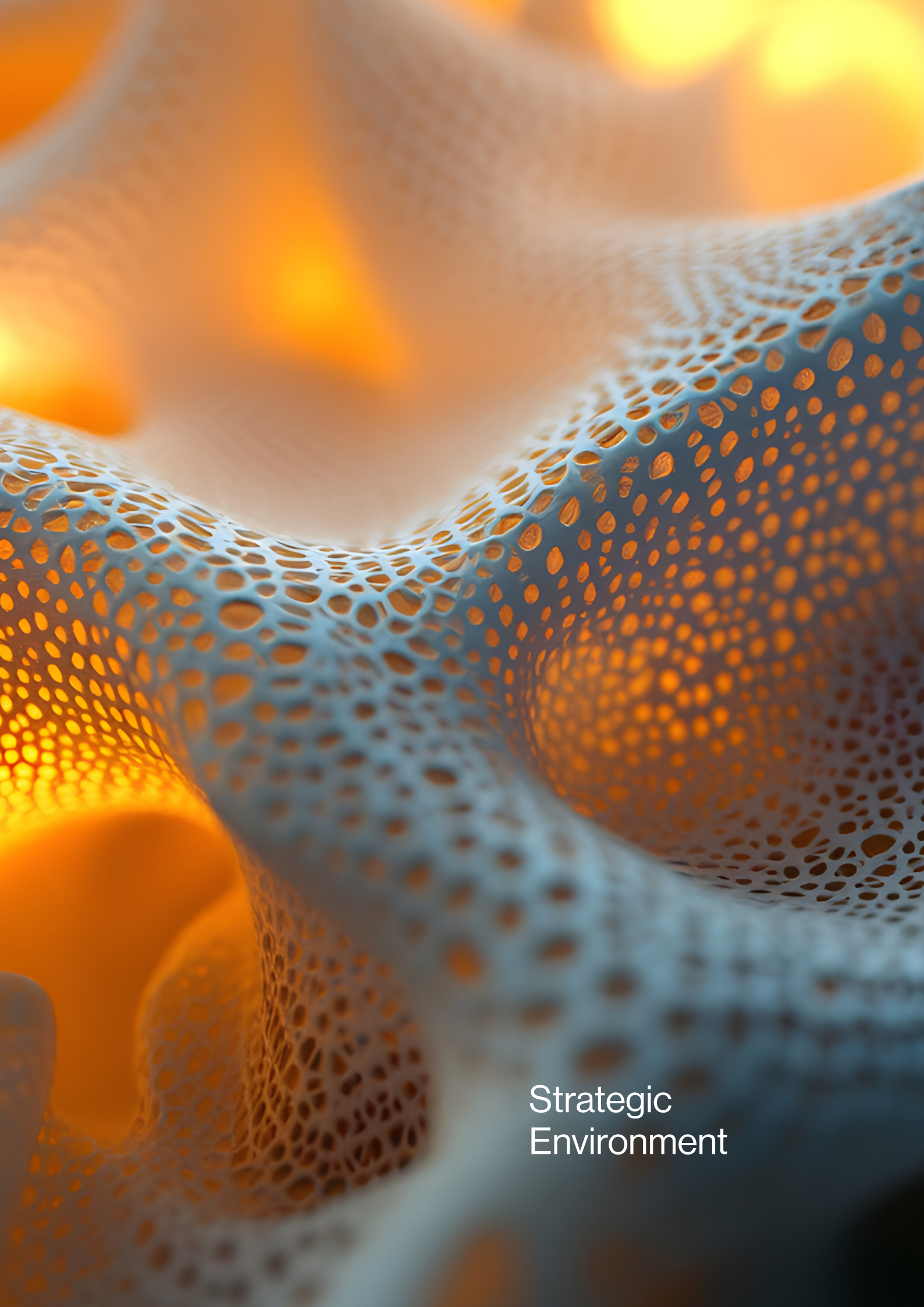
Understanding human behaviour and the thinking that guides it is crucial for strategic and military decision-making. Whether to improve our own situational awareness, judgement and planning, or to better predict, manipulate and make sense of adversary behaviour, NATO increasingly recognises the need to better its understanding of human cognition. With the advent of advanced Artificial Intelligence tools and the growing threat of hybrid attacks that manipulate public opinion, it has never been more important to invest in our ability to defend against and conduct Cognitive Warfare, now and in the future.

In recognition of this, NATO has articulated its commitment to improving Cognitive Warfare capabilities. The 2021 NATO Warfighting Capstone Concept outlines five long-term Warfare Development Imperatives to achieve NATO's core mission, two of which – Cognitive Superiority and Influence & Power Projection – build heavily on principles of Cognitive Warfare. NATO's 2022 Strategic Concept highlights that "ensuring national and collective resilience is critical to all our core tasks and underpins our efforts to safeguard our nations, societies and shared values". Technology able to alter human behaviour – for example, via information processing, communications or social media – can be used to target both military personnel and civilians. Collaboration between civilian and defence stakeholders is therefore essential to detect, mitigate, and respond to cognitive attacks.

The NATO Science & Technology Organization (STO) plays a pivotal role in enhancing NATO's operational readiness. Through evidence-based research, the STO has been addressing Cognitive Warfare to support military and political leadership in effective decision-making and cognitive superiority over adversaries during peace, crisis and conflict. In 2022, the NATO Science & Technology Board recognised Cognitive Warfare as a strategic research challenge for its Collaborative Program of Work (CPoW). Since then, 20 research activities related to Cognitive Warfare have been established, bringing together the joint competence of over 200 experts from 26 NATO Allies and Partners. A Community of Interest on Cognitive Warfare has also been established, meeting frequently to discuss and identify research needs.

This report aims to present insights from this work to enable NATO Allies to combat Cognitive Warfare. It also seeks to raise awareness of and identify key research gaps that can be addressed following the STO's CPoW Challenge on Cognitive Warfare. The STO's activities outlined three overall functions of Cognitive Warfare, and highlighted S&T needs and emerging capabilities that need attention to build further knowledge and understanding to defend against Cognitive Warfare; i) to degrade capabilities of adversaries, reducing their ability to influence and change Allies' behaviour and thereby ensuring Allied decision-making ability and cognitive superiority; ii) to improve human and technological cognition, enhancing cognitive capabilities above the current baseline; and iii) to be resilient withstanding and recovering operational performance and retain performance in the face of cognitive threats. Undoubtedly, Cognitive Warfare will remain a key research theme for ongoing and future work within the STO to support NATO's core mission.

Mr Steen Søndergaard
NATO Chief Scientist



Strategic Environment

NATO is navigating an unpredictable strategic environment where strategic competitors and potential adversaries exploit the openness and interconnectedness of Western societies, targeting the security of Allies' citizens through hybrid tactics.

NATO's evolving defence and security environment, along with its strategic decision-making capabilities, is also significantly influenced by Science and Technology (S&T) (Fact Box 1). Public trust in science, in institutions, and in governments is fragmenting, as NATO Allies and Partners experience malicious campaigns aimed at influencing public opinion through propaganda and disinformation (such as deepfakes), even leading to election interference. Significant challenges to NATO security in the near future include social instability, climate change and mass migration.[1]

Many threat actors, some of whom consider themselves at war with NATO, have long used weaponised tactics to influence our sense- and decision-making capabilities. Propaganda, deception, interference, and manipulation are tactics NATO's adversaries use to alter Allied citizens' perceptions and behaviour to their advantage. These actors exploit the freedoms and protections enshrined in democracies, thus waging Cognitive Warfare.

Before Russia's full-scale invasion of Ukraine on 24 February, 2022, Russia used conflicting narratives and false flags to destabilise and influence decisions. The war showed that modern interstate warfare can be both a war of attrition, with significant material and human costs, and a war involving the human mind through access to digital information technology. The war has highlighted the importance of the "cognitive dimension" in warfare, and where society shapes the security environment.

Military commanders recognize the growing importance of human cognition in modern warfare. Adversaries exploit vulnerabilities in the Observe, Orient, Decide, and Act (OODA) military decision-making framework to target cognitive weaknesses. Technological advancements have made it easier to manipulate human cognition, exploiting the complexities of human behaviour. The digital information environment amplifies the potential to mislead and disrupt societies, from citizens to military leaders. Social media and other digital tools shape the Information Environment (IE), influencing cognition. The COVID-19 pandemic highlighted the impact of disinformation in social media, showing how weaponised information threatens decision-making.

Fact Box 1: Macro Trends shaping the defence and security landscape[2]

NATO STO has identified six Macro Trends that impact and are impacted by S&T, shaping NATO's strategic landscape: Evolving Competition Areas, Race for 'Artificial Intelligence (AI) and Quantum Superiority, Biotechnology Revolution, Resource Divide, Fragmenting Public Trust, and Technology Integration & Dependencies.

Cognitive Warfare is both a military and societal issue. Advances in neurobiology, AI, biotechnology, and human-computer integration increase the potential for cognitive attacks. While Cognitive Warfare is not new, technology and digital platforms enhance its reach and effectiveness. NATO stands on the threshold of advanced disruptive technologies affecting cognition and human life, both during war and peacetime. Understanding the socio-cognitive-technical context and integrating emerging disruptive technologies (EDTs) is crucial for NATO's decision-making superiority.

NATO must therefore invest in S&T to defend Allies against Cognitive Warfare. This includes understanding the science, challenges and opportunities of Cognitive Warfare against adversaries. Enhanced knowledge of the relationship between cognition and technology, and its potential weaponisation, is essential. A broader understanding of threat actors, the information environment, and the technological, defence, and societal implications is vital for countering Cognitive Warfare.

[1] NATO Science and Technology Trends 2025 2045 Vol 1. https://sto-trends.com/.
[2] Ibid.

The re-emergence of Cognitive Warfare

During the 5th century BC, the Chinese military general and strategist Sun Tzu described a set of skills related to warfare and military methods, famously known as The Art of War. This work has profoundly influenced both East Asian and Western military theory and strategy[3]:

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." ... "The whole secret lies in confusing the enemy, so that he cannot fathom our real intent."
> *- Sun Tzu on the Art of War*

Modern Cognitive Warfare retains these strategies but extends them through technological approaches, targeting a broader audience beyond the armed forces. This form of warfare has re-emerged due to the fact that adversaries can now access technologies that can target large segments of the population. Several elements of Sun Tzu's strategic thinking are captured in today's military decision-making OODA loop.

Literature proposes various definitions of Cognitive Warfare.[4] Du Cluzel describes Cognitive Warfare as the "manipulation of the enemy's cognition" aimed at weakening, influencing, delaying, and even destroying the enemy.[5] Cognitive Warfare influences human decision-making and extends its reach to the public, society, and the military. Information is weaponised across numerous platforms to target individuals, governments, and mass consciousness, justifying adversaries' strategic objectives. Cognitive Warfare can also be described as the use of all knowledge, strategies, and available tools to impact human behaviour through cognition, with the end goal of manipulating and altering decision-making. Most recently, NATO has defined Cognitive Warfare as the fight for Cognitive Superiority. Contesting in this environment comprises deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain and protect cognitive advantage.[6]

Figure 1 provides an overall illustration of Cognitive Warfare.

[3] Sun, T. [496 BC] (1910). Sun Tzu on the Art of War. Trans. L. Giles. London: Luzac and Co.
[4] Cowles, N. and Verrall, N. (2023). The Cognitive Warfare concept: A short introduction. Defence Science and Technology Laboratory, UK, DSTL/TR146721 v1.
[5] Du Cluzel, F. (2021). Cognitive Warfare, a Battle for the Brain. STO-MP-AVT-211, STO-MP-HFM-334.
[6] 2025 Cognitive Warfare. https://www.act.nato.int/activities/cognitive-warfare/

The Main Aspects of Cognitive Warfare

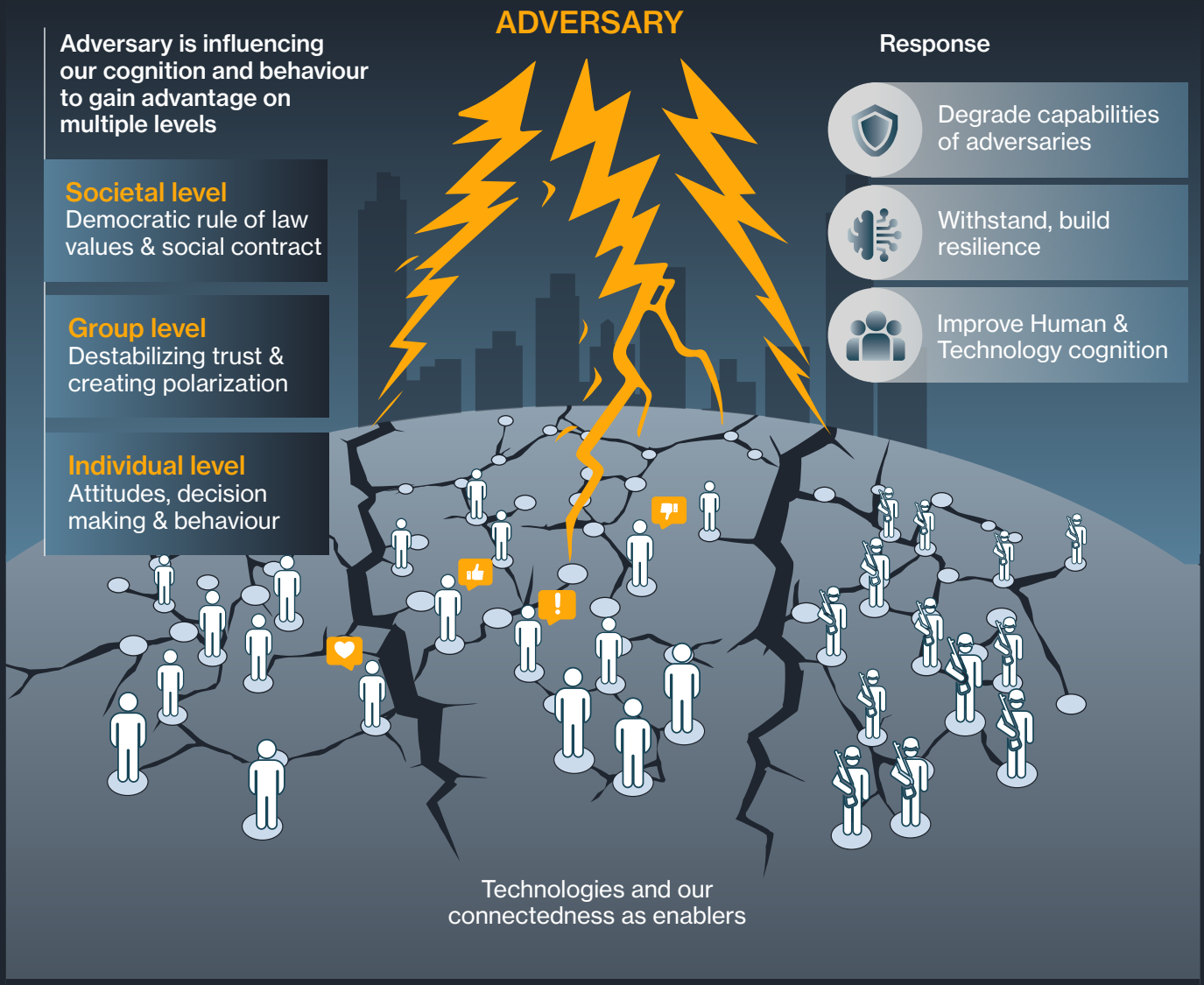


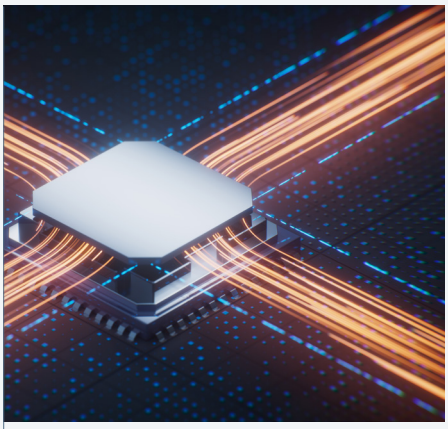
Figure 1. Illustration of the main aspects of Cognitive Warfare. The lightning bolts indicate that Cognitive Warfare may target human (military and civilian population) as well as artificial cognition. The left part shows various effects at individual, group, and societal levels. The connectedness between individuals (connected dots) is increased by modern technologies, facilitating the spread of information, enabling new forms of deception (e.g., deepfakes), and often replacing human cognition. The right part of the figure shows three main responses to Cognitive Warfare: degrading adversaries' capabilities, increasing resilience to withstand attacks, and improving human and technological cognition. (Illustration by Prof Dr José Kerstholt, Organisation for Applied Scientific Research (TNO), The Netherlands).

Cognitive Warfare can be used offensively against NATO and Allied nations through influence-related capabilities such as Information Operations (InfoOps), Psychological Operations (PsyOps), media operations, messaging and deterrence, Strategic Communication (STRATCOM), and engagement activities.[7] Cognitive Warfare has footprints in several areas and capability planning within NATO (Fact Box 2). It represents the convergence of PsyOps, InfoOps, and cyber operations with the advancement of Artificial intelligence/Machine learning networks, enabling the distribution of adversaries' strategic agendas by exploiting human vulnerabilities and shaping human understanding of events.[8]

Additionally, Allies' Open-Source Intelligence (OSINT) and Human Intelligence (HUMINT) consider human cognition. Some communities discuss use of Social Media Intelligence (SOCMINT).[9] This underscores the crucial need for NATO to prepare against deliberate actions where technological advances are used to achieve adversaries' goals. However, the NATO STO studies described in this report approach Cognitive Warfare from a purely defensive posture. As Cognitive Warfare targets both military and civilian populations, a whole-of-government and -society approach is needed to ensure strategies and capabilities to defend against this type of warfare.

Fact Box 2: Traditional tools encountering cognition include military tactics and approaches through Psychological Operations (PsyOps), Information Operations (InfoOps), as part of Strategic Communication (STRATCOM) functions.[10]

Psychological Operations (PsyOps): Psychological Planned activities using communication methods and other means directed at approved audiences to influence perceptions, attitudes, and behaviour, affecting political and military objectives. These operations are based on distinct planning and preparations towards targeted and specific objectives.



Information Operations (InfoOps): A military function providing advice and coordinating military information activities to create desired effects on the will, understanding, and capability of adversaries, potential adversaries, and other North Atlantic Council-approved parties in support of Alliance mission objectives. InfoOps is one of several tools to conduct Cognitive Warfare, differentiating from the information environment where warfare/actions take place.

Strategic Communication (STRATCOM): Integration of communication capabilities and information staff functions with other military activities (including Public Affairs, PsyOps, and InfoOps) to shape the information environment in support of NATO aims and objectives. STRATCOM is considered in the planning process, reflected in operations design, expressed in the commander's intent, and applied during execution and targeting.

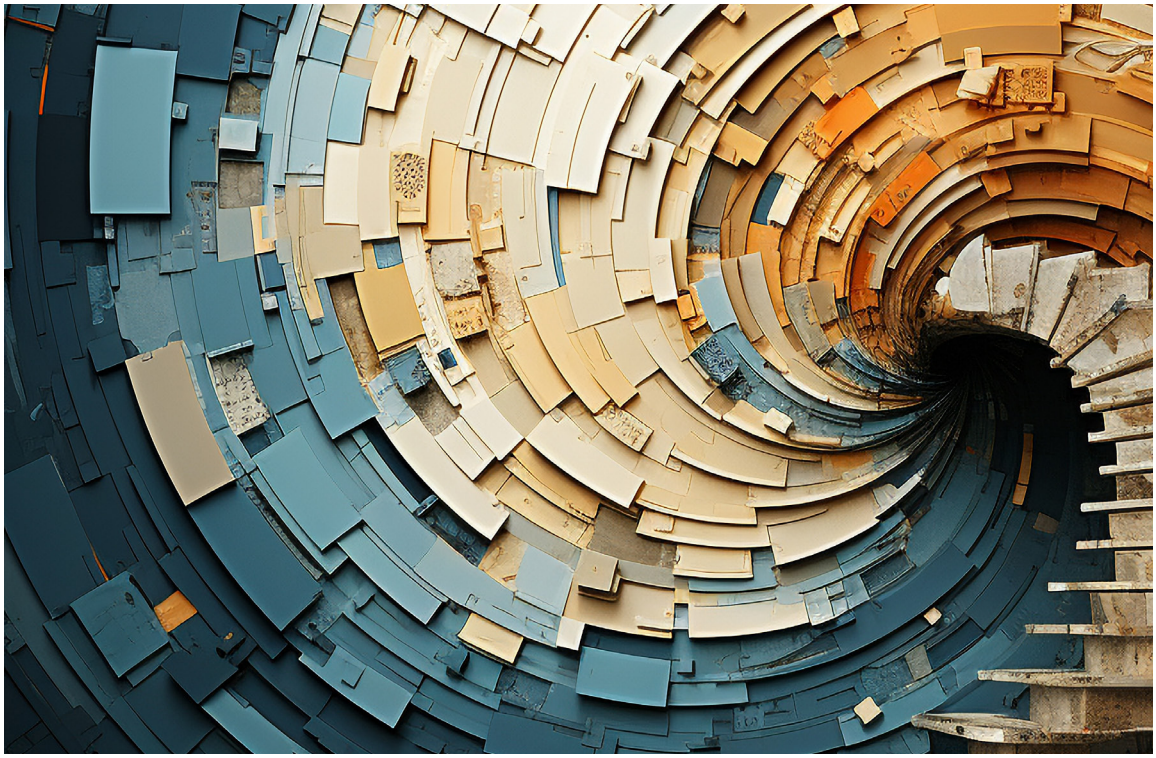
[7] See note 4.
[8] Guyader, H. (2022). "Cognitive Domain: A Sixth Domain of Operations". In Claverie, B., Prébot, B., Beuchler, N. and du Cluzel, F. (Eds.). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 2021. NATO STO.
[9] https://www.sciencedirect.com/topics/computer-science/social-medium-intelligence.
[10] AJP-3 ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS, Edition C Version 1 FEBRUARY 2019.

Cognitive Warfare is broader than InfoOps, PsyOps, STRATCOM, and cyber operations, differing from these operational tactics by:

- Aiming to alter human behaviour through cognitive effects using any means, including advanced technologies, without necessarily knowing the outcome of the behavioural change.
- Not necessarily targeting specific audiences and objectives.
- Not being a solely military challenge nor mission-oriented.
- Often being designed to create chaos and complexity below the threshold of armed conflict.
- Creating a cognitive battlespace using multiple actions or interference to manipulate adversaries.

Despite the fact that "cognition" is not recognized as a separate domain like the traditional domains (Maritime, Land, Air, Space, and Cyber), Cognitive Warfare is a cross-cutting effect dimension. NATO's Multi-Domain Operations (MDO) Concept, which pushes for orchestrating military activities across all operating domains and environments and synchronisation between military and non-military activities, includes the Information Environment and thus the cognitive dimension.

NATO works closely with Allies and partners to understand, counter and build resilience against information threats. NATO's approach to counter such threats include proactive measures and response options through increasing understanding of the information environment, preventing information threats, mitigating information incidents and recovering stronger from such threats.[11] In total, these efforts imply that research-based knowledge and understanding of Cognitive Warfare and the cognitive dimension will be needed in the years to come.



[11] NATO (2024), "Resilience, civil preparedness and Article 3", 13 November, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.

NATO's Approach to Cognitive Warfare

The 2021 NATO Warfighting Capstone Concept (NWCC) outlines five Warfare Development Imperatives (WDIs) to achieve NATO's core missions: Cognitive Superiority, Layered Resilience, Influence and Power Projection, Cross-Domain Command, and Integrated Multi-Domain Defence.[12] Cognitive Superiority involves understanding the operating environment and potential adversaries relative to the Alliance's own capabilities, capacities, and objectives (Fact Box 3). Cognitive Warfare is central to the Cognitive Superiority WDI and has implications for the others. Understanding future warfighting in a multi-region, multi-dimensional (physical, virtual, and cognitive), and multi-domain operating environment necessitates an understanding of Cognitive Warfare.

The 2022 NATO Strategic Concept underscores NATO's responsibility to ensure collective defence through a 360-degree approach, strengthening deterrence and defence across all domains and threats. It highlights the importance of military and civilian collaboration. The Strategic Concept also emphasizes the need to safeguard societies and nations, enhancing national and collective resilience to fulfil the Alliance's core tasks.

In 2020, the Allied Command Transformation (ACT) Innovation Hub began exploring Cognitive Warfare as a new form of warfare and suggesting NATO consider a sixth operational domain, the "Human Domain".[13] In June 2021, France hosted the first NATO scientific meeting on Cognitive Warfare.[14]

The 2021 NATO Innovation Challenge on Countering Cognitive Warfare focused on identifying *"innovative tools and measures to assess and protect against attacks on the cognitive domain of NATO forces and their Allies."*[15] Building on several NATO initiatives, an emphasis on providing a sound S&T-base to support NATO in countering the impacts of Cognitive Warfare was identified.

Fact Box 3: NATO Warfare Capstone Concept 2021, Cognitive Superiority.

Improving the Alliance's situational awareness and strategic anticipation has been an important dimension of the Alliance's strengthened deterrence and defence posture. Fundamental to the Alliance's ability to shape, contest and fight is expanding knowledge and understanding, with a view to ultimately achieving cognitive superiority. This understanding needs to be connected across all-domains, and enabled by technology, in order to maximize commanders' ability to anticipate, think, decide and act. Efforts to build better situational awareness and understanding with a view to achieving cognitive advantage over potential adversaries is a priority for the Alliance.

[12] 2021 NATO Warfighting Capstone Concept. https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/
[13] Du Cluzel, F. 2021. "Cognitive Warfare". Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf .
[14] Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (Eds.). (2021). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 2021. NATO STO. https://hal.archives-ouvertes.fr/hal-03635898/document .
[15] NATO Allied Command Transformation (ACT) (2021), "NATO Innovation Challenge Fall 2021 – Countering Cognitive Warfare", 8 October, https://www.act.nato.int/articles/innovation-challenge-2021-2-countering-cognitive-warfare .

STO research activities on Cognitive Warfare

The first two STO activities related to Cognitive Warfare were “Social Media Exploitation for Operations in the Information Environment” (IST-177 RTG, 2019-2023) and “Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices” (SAS-161 RTG, 2020-2023). These studies focused on the information environment and hybrid warfare.

In 2022, the NATO Science & Technology Board (STB) recognised Cognitive Warfare as a strategic research challenge within STO’s Collaborative Program of Work (CPoW), led by Norway. CPoW Challenges are mechanisms used annually by the STB to signal areas of strategic importance for Allies. They are led by one or more Nations and revolve around an overarching problem statement, aiming to generate collaboration and new STO research activities in the short- and medium-term. These challenges typically last one year and involve expert workshops to translate specific demands into actionable scientific collaboration.

The STO Human Factors and Medicine (HFM) Science & Technology Committee (STC) initially identified various aspects of Cognitive Warfare through a Specialist Team (HFM-ST-356), involving NATO ACT and seven Allied Nations, providing insights and frameworks for the CPoW Challenge on Cognitive Warfare.[16] This Specialist Team defined the goal of Cognitive Warfare as “exploiting facets of cognition to disrupt, undermine, influence, or modify human decision-making” and established a model to reflect the multifaceted and multidimensional nature of Cognitive Warfare (Figure 2). This model was reviewed at the NATO ACT Tide Sprint Conference in 2022 and provides a framework for S&T needs, priorities, and future investments.

The House Model identified seven S&T areas as essential knowledge fields to understand adversarial approaches and mitigate the effects of Cognitive Warfare on NATO’s democratic values. These areas are independent S&T fields that can become interdependent when operationalised and viewed through the lens of NATO’s defence against Cognitive Warfare. Cognitive Warfare involves using knowledge for conflicting purposes as well as developing mitigation and response strategies to reduce vulnerabilities. Thus, the House Model can be used to view Cognitive Warfare from both a BLUE team (bottom-up) and a RED team (top-down) approach. The seven knowledge areas of the House Model (Fact Box 4) are composed of i) four cross-cutting knowledge areas acting as force multipliers (bars), and ii) three knowledge pillars for which the four cross-cutting areas are force multipliers. Both the pillars and bars are built upon NATO’s legal and ethical frameworks.

[16] Masakowski, Y. R. and Blatny, J.M. (Eds). Mitigating and Responding to Cognitive Warfare. 2023. NATO STO. STO-TR-HFM-ET-356.

S&T Approach

Understand Adversary Actions/Intent Used to Inform How We Might Counter Cognitive Warfare

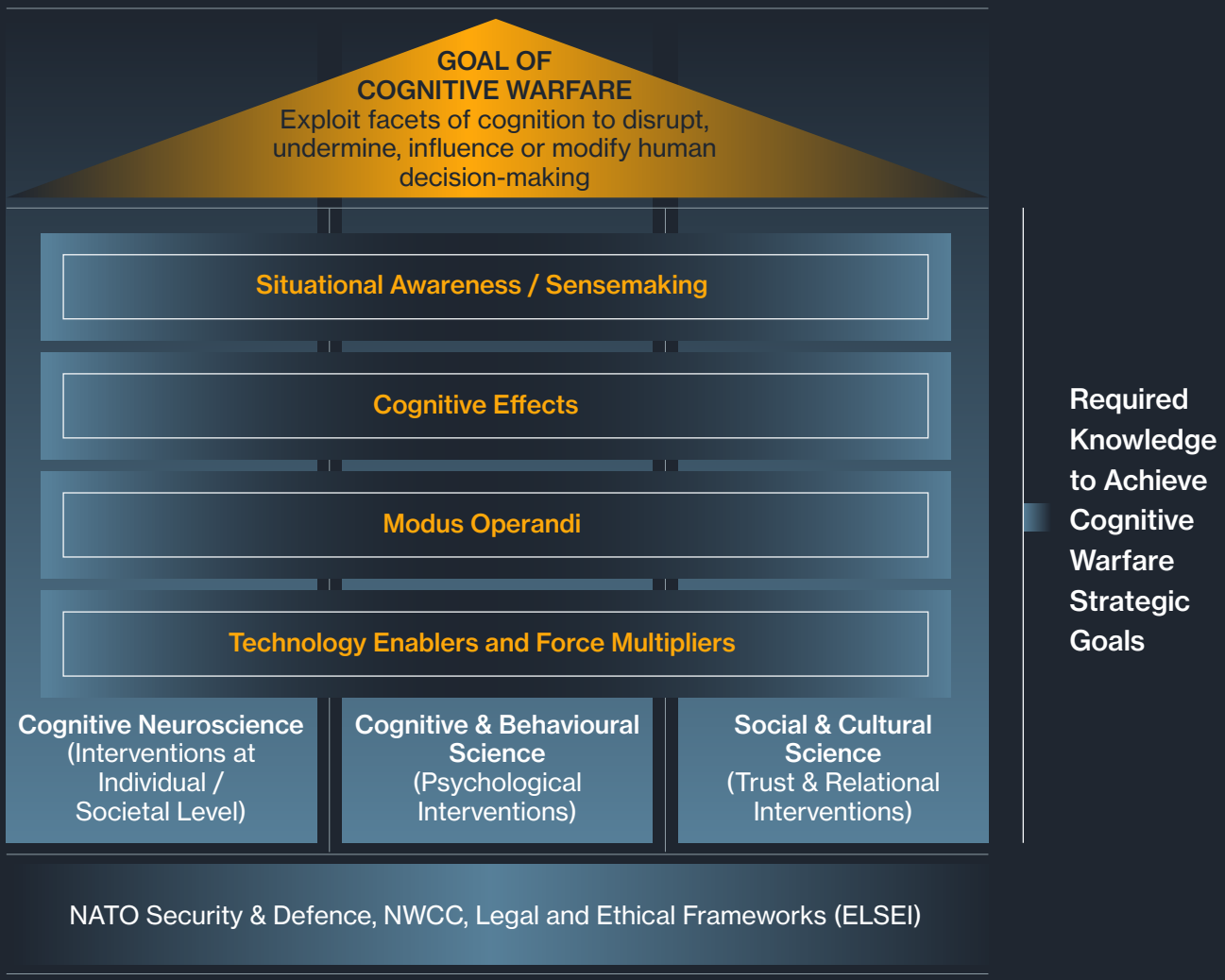


Figure 2. The House Model Developed by NATO STO HFM-ST-356 identified seven S&T knowledge areas. The goal of Cognitive Warfare is to exploit facets of cognition to disrupt, undermine or modify human decision-making. The House Model reflects the multifaceted and multidimensional nature of Cognitive Warfare. Cognitive Warfare achieves overt and covert objectives below and above the threshold of war, affecting how we think, act, and make decisions by exploiting facets of cognition to disrupt, undermine, influence, or modify human decision-making. Modern technological enablers act as force multipliers. Novel methods and ways of operating (modus operandi, see Fact Box 4) allow adversaries to deliver cognitive effects that target Allies' situational awareness and ability to make sense of events by penetrating and permeating the conscious and subconscious of individuals and the collective.[18]

[85] Ibid.

Fact Box 4. Mitigating and Responding to Cognitive Warfare.

Understanding the seven S&T knowledge areas identified in the House Model (STO HFM-ST-356) is crucial. See Figure 2.

1. Situational Awareness / Sense-making: S&T is needed to understand the factors that enable or block attempts to make sense of ambiguous situations and evolving non-linear events, as sense-making informs and is a prerequisite to decision-making.

2. Cognitive Effects: S&T is needed to understand how an actor may try to affect a target audience to achieve the desired goal. This includes doctrinal effect verbs (e.g., distort, distract, degrade), as well as the impact of neurobiology on cognitive functions, emulative functions, or triggering social contagion.

3. Modus Operandi: S&T is needed to understand and examine adversary methods and stratagems to generate desired effects on the target audience and identify opportunities for intervention. This includes understanding the synchronisation of activities by adversaries to psychologically prime and target.

4. Technology Enablers and Force Multipliers: S&T is needed to understand technological advances that enable actors to pursue their goals. This aspect addresses a broad range of emerging and disruptive technologies, especially big data, artificial intelligence, information and communication technologies, neurobiology, and biotechnology.

5. Cognitive Neuroscience: S&T is needed to understand the physiological and neurological mechanisms of reasoning, sense-making, and decision-making.

6. Cognitive & Behavioural Science: S&T is needed to understand the psychological knowledge on sense-making, decision-making, social interaction, human behaviour, emotion, communication, and trust.

7. Social & Cultural Science: S&T is needed to understand interdisciplinary approaches to better comprehend structural and institutional factors in social, cultural, economic, and political contexts that shape and empower individual and collective behaviour.

A warfighter's cognitive abilities are crucial in the modern battlespace. There is a need to process enormous amounts of data and information rapidly and accurately, ensuring that the information gathered is trustworthy, accurate, and dependable. Errors in processing can have cascading consequences for effective decision-making in the operational environment. The House Model is linked to the operational OODA military decision framework (Figure 3), as Cognitive Warfare can be viewed through the lens of this decision cycle. Cognitive Warfare can target the OODA loop, impacting a commander's decision. Thus, the House Model highlights the important synergy between research and operational communities.

The Observe-Orient-Decide-Act (OODA) Loop Decision Cycle

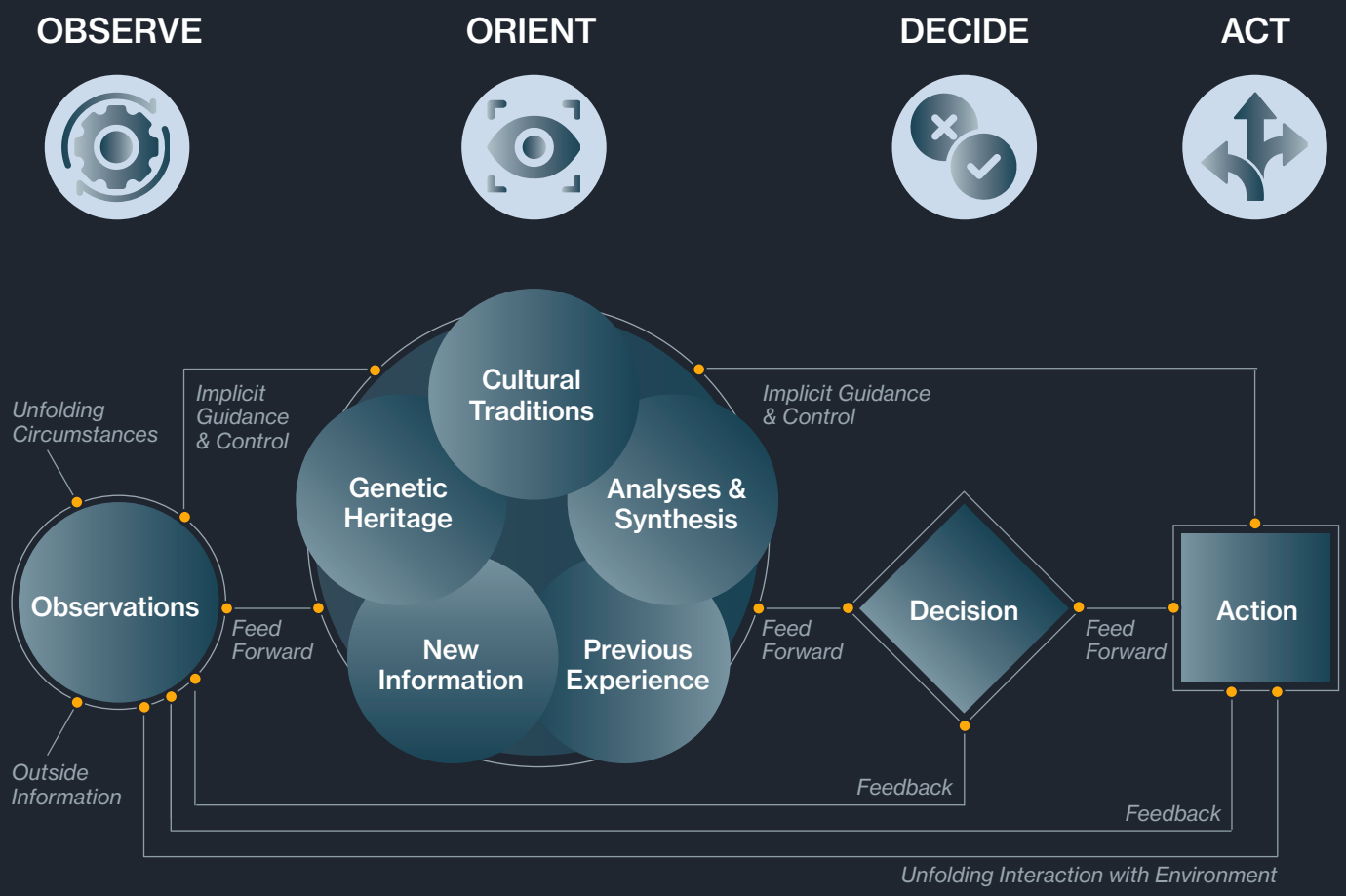


Figure 3. The Observe-Orient-Decide-Act (OODA) Loop Decision Cycle (John Boyd, 1976). The OODA loop is a means for understanding the decision-making process through a 4-step approach. For the military, the OODA loop serves as a framework for decision-making. The OODA loop allows decision-makers to adapt to changes as they gather information in real time. **Observe** – Data collection phase from multiple sources, i.e., aggregation of information from all sources. **Orient** – Filter, analyse, and enrich information, i.e., information is analysed, evaluated, and prioritized. **Decide** – Actionable insights enable best available response, i.e., choosing between options and courses of action. **Act** – Execute decision, determine if action was correct.

[15] The sum is 53 because the activity SAS-HFM-ET-GD is aligned both with R2 and R7.

As a follow-up to HFM-ST-356 and the CPoW Challenge on Cognitive Warfare, a STO workshop was held in November 2022 at the Norwegian Defence Research Establishment (FFI). The workshop identified the CPoW problem statement on Cognitive Warfare (Fact Box 5) and four critical components to increase knowledge and provide mitigation strategies[18]:

- Technology-enabled tactics, techniques, procedures and tools to influence human decision-making at an individual and/or societal level.
- Altering human behaviour to align with an adversaries' political, social, economic, or military objectives.
- Means (i.e., training, technology, policy) to defend and better secure the cognitive battlespace.
- Resilience and a whole-of-society perspective.

The workshop aimed to raise further awareness, obtain a common understanding of Cognitive Warfare, and succeeded in setting the scene for new STO activities, based on the seven knowledge areas of the House Model. Over 75 participants from 16 nations, across the STO STCs, attended the workshop and took a deep dive into Cognitive Warfare to outline a forward-looking research agenda. Subsequently, six STO activities were approved at the STB Spring meeting in 2023. In the aftermath of HFM-ST-356, and within a short period from an S&T perspective, 17 additional STO research activities on Cognitive Warfare were identified and initiated (as of April 20, 2025) (Figure 4). All the research activities aim to obtain an in-depth understanding of the seven S&T knowledge areas identified by HFM-ST-356 and strengthen the knowledge itself looking toward achievable results.

Fact Box 5. CPoW Cognitive Warfare – Problem Statement.

Based on the STO HFM-ST-356 study and the STB CPoW Challenge on Cognitive Warfare, a total of 20 STO activities have been initiated on Cognitive Warfare, five of which are cross-Committee activities. As of April 2025, eleven activities have been completed, five are ongoing, three are planned, and two are submitted for STB approval. Six of the STO activities are publicly releasable, 14 are classified (Figure 4).

26 Allied and Partner Nations, along with five associated NATO organizations – ACT, Strategic Communications Centre of Excellence (STRATCOM CoE), Counter-Improvised Explosive Devices Centre of Excellence (C-IED CoE), Combined Air Operations Centres (CAOC), and Joint Analysis and Lessons Learned Centre (JALLC) – have participated or are currently participating in these 20 STO activities.

Cognitive Warfare Activities

IST-177-RTG (Completed)
Social Media Exploitation for Operations in the Information Environment

IST-195-RSY (Completed)
Societal Challenges for Operations in the Information Environment

HFM-345 RTG (Completed)
Operations Security and Susceptibility to Influence in the Information Environment

HFM-356 ST (Completed)
Mitigating and Responding to Cognitive Warfare

HFM-361 RSY (Completed)
Mitigating and Responding to Cognitive Warfare

HFM-377-RSY (Completed)
Meaningful Human Control in Information Warfare

HFM-MSG-ET-212 (Completed)
Evaluation Criteria and Use Cases for Information Operation/Social Media Simulators

HFM-ET-214 (Completed)
Cognitive Security: Building and Maintaining Resistance to Offensive Cognitive Strategies

HFM-ET-215 (Completed)
The Ethical and Legal Challenges of Cognitive Warfare

HFM-ET-216 (Completed)
Methods and Weapons of Adversary Cognitive Warfare

SAS-161-RTG (Completed)
Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices

HFM-373-RTG (Active)
Technology Enablers and Force Multipliers for CogWar: From Monitoring and Assessment to AI-based Assistance and Automation Systems

HFM-374-RTG (Active)
COGARMY: COGnitive Training and Teamwork Assessment of ARMY Personnel

SAS-185-RTG (Active)
Indicators and Warnings for Cognitive Warfare in Cyberspace

HFV-IST-416-ST (Active)
NATO Full Spectrum Cognitive Warfare

HFM-SAS-406-RTG (Planned)
The Ethical and Legal Challenges of Cognitive Warfare

HFM-IST-SCI-410 RTG (Planned)
Information Operations and Social Media Simulators Evaluation

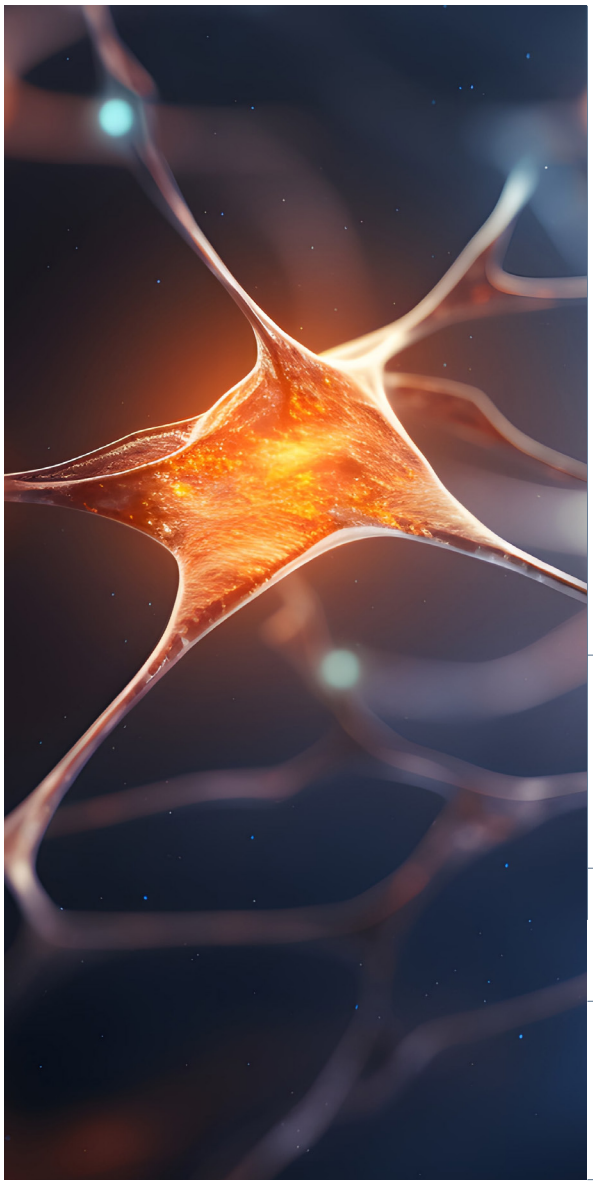
IST-HFM-ET-132 (Planned)
Understanding Hostile States' Internal Information Environment and Control

IST-HFM-ET-132 (Submitted)
Cognitive Warfare: Weapons, Methods & Securing Cognitive Assets

HFM-428-RWS (Submitted)
Technology Enablers for Cognitive Warfare: Operator and Technical Perspectives

Figure 4. Since 2019, STO has 20 initiated Cognitive Warfare activities, including activities as outcomes of the STB CPoW Research Strategic Challenge Cognitive Warfare 2022. Six of the STO activities are Public Release (green border), fourteen are NATO UNCLASSIFIED or above (blue and red borders). Colour shadings represent status of activities as of 20 April 2025: White; submitted for STB approval. Grey; planned. Light Blue; ongoing. Blue; completed. The HFM-ST-356, HFM-361 RSY, HFM-377 and SAS-161 reports are publicly available on the NATO STO website.20

[20] Science & Technology Organizing (STO), STO Scientific Publications, available at www.sto.nato.int/publications/.



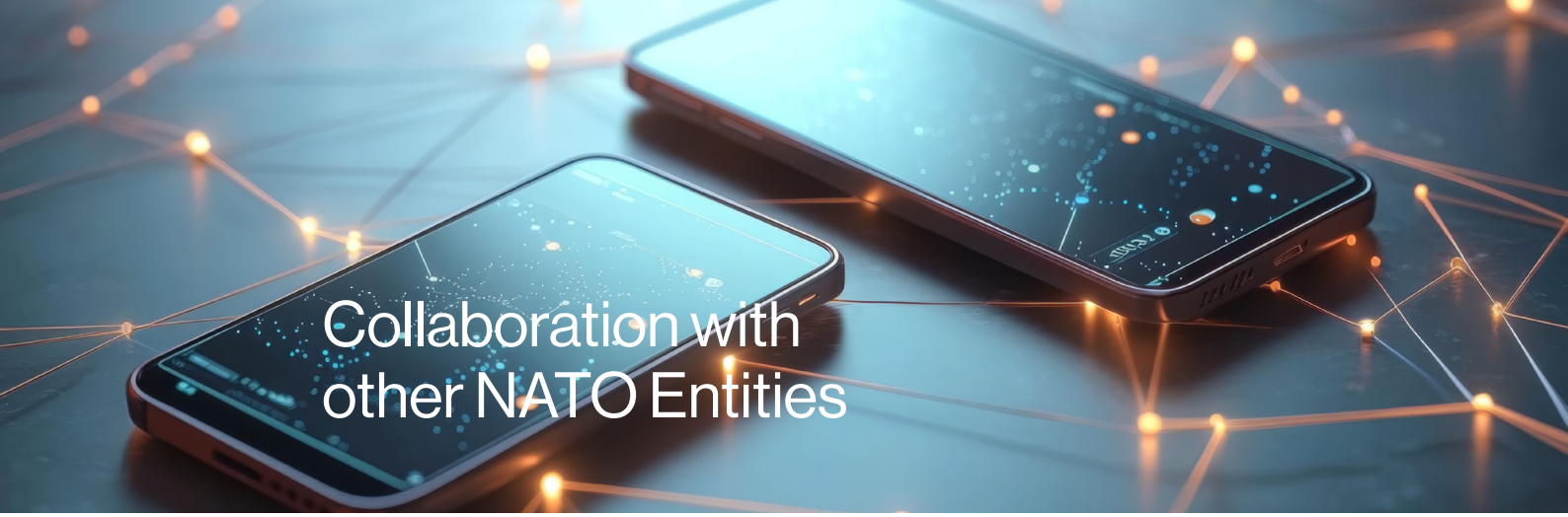
STO's work has led to the establishment of a broad network and Community of Interest on Cognitive Warfare. This community meets frequently, both virtually and in-person, through STO meetings to discuss and identify research needs, further strengthening NATO Allies' ability to counter Cognitive Warfare. This clearly demonstrates how the STO community enhances and empowers knowledge and S&T through collaboration on common challenges and needs. The Proceedings from RSY 361 and 377 are publicly available on the NATO STO website.

In summary, the STO's work and activities have highlighted three major functions of Cognitive Warfare, illustrating the goals where S&T, methods, and the development of emerging capabilities need attention to further increase knowledge and understanding to maintain and defend our democratic values:

Degrade capabilities of adversaries: Reduce their ability to influence and change behaviour, thereby ensuring Allied decision-making ability and Cognitive Superiority

Improve human and technological cognition: Enhance cognitive capabilities above the current baseline.

Withstand and recover performance (resilience): Retain and recover performance in the face of cognitive threats.



Collaboration with other NATO Entities

The results from HFM-ST-356 provided valuable inputs to NATO ACT and the development of the NATO Cognitive Warfare Concept.[21] This concept was developed in collaboration with a large Community of Interest across the Alliance, particularly with the HFM-ST-356 team. The concept was tasked by the Military Committee (MC) as part of the Warfare Development Agenda (WDA) to enhance NATO's knowledge of emerging threats in the cognitive dimension.

HFM-ST-356 also provided inputs and supported the NATO Industrial Advisory Group (NIAG) in its study (SG-278) on "Cognitive Augmentation for Military Applications" to assess the modernization of human cognition augmentation. This NIAG study addressed various training tools, methods, technologies, risks, ethical, moral, and legal considerations, shedding light on how to strengthen the rapid evolution of human integration with technological advancements.

In April 2023, NATO's STO and Public Diplomacy Division (PDD) held a workshop on disinformation at NATO Headquarters to build a common understanding of the issues and concerns. The event brought together representatives from government, industry, and academia with NATO officials to examine disinformation and hostile information activities. Participants from the 2022 Cognitive Warfare workshop in Norway also attended to discuss the connections between the information environment and cognitive aspects.

[21] NATO ACT Cognitive Warfare Concept, Exploratory Work 2023.

Conclusion

Cognitive Warfare seeks *"to exploit facets of cognition to disrupt, undermine, influence, or modify human decision-making by altering human behaviour and cognition through any means and technological advances."*[22] It uses military and non-military tactics, targeting both military operators and civilian populations across the crisis spectrum.

Cognitive Warfare seeks "to exploit facets of cognition to disrupt, undermine, influence, or modify human decision-making by altering human behaviour and cognition through any means and technological advances". It uses military and non-military tactics, targeting both military operators and civilian populations across the crisis spectrum.
Some experts argue that NATO Allies and Partners are already in an era of continuous warfare, with foreign interference staying below the threshold of armed conflict but still significantly impacting human behaviour. In addition, emerging technologies will develop over the next decades that can also affect human cognition, requiring the Alliance to continue monitoring and evaluating these to assess the opportunities and challenges for the Alliance's future Cognitive Superiority capabilities.

Allies and NATO need the appropriate means to detect and analyse Cognitive Warfare attacks, while developing mitigation strategies that increase our resilience to such warfare. Given that Cognitive Warfare poses significant challenges to military and civilians alike, we must pursue a whole-of-government approach to collaborative research, policy-making, strategy development, and resilience planning across responsible ministries involved in defence and security.

The STO supports NATO through developing Cognitive Warfare capabilities and strengthening NATO's knowledge of the cognitive dimension. This includes shaping this dimension to better counter threats in the cognitive battlespace and achieve Cognitive Superiority. STO's research-based knowledge on Cognitive Warfare also offers advice to NATO's military and political leadership on policy development within this area. The STO's work has identified three major functions of Cognitive Warfare where S&T and the development of emerging capabilities need attention to further increase knowledge and understanding to mitigate and respond to Cognitive Warfare: i) to degrade the capabilities of adversaries to ensure Allied decision-making ability and cognitive superiority, ii) to improve human and technological cognition above the current baseline, and iii) to withstand and recover performance, strengthening NATO's resilience to cognitive threats.

S&T is needed to understand how technology can influence human decision-making at individual, organisational and societal levels, how human behaviour can be altered to align with adversaries' objectives, and how to defend and secure the cognitive battlespace.

In 2022, the NATO STB recognised Cognitive Warfare as a strategic research challenge and since then (as of April 2025) 20 STO activities related to Cognitive Warfare have been established, involving 26 NATO Allies and Partners, and five associated NATO organisations. STO's interdisciplinary approach and collaboration with stakeholders has improved NATO's understanding and response to Cognitive Warfare. The STO has also established a broad Cognitive Warfare Community of Interest to improve NATO's understanding of the cognitive dimension for future warfare capabilities, and to achieve cognitive superiority in future conflicts and over NATO's adversaries. As the future of warfare increasingly focusses on Multi-Domain Operations, there is no doubt that Cognitive Warfare will remain a key research theme for ongoing and future work within the STO to support NATO's core mission.

[22] See Note 16.

List of Acronyms

ACT – Allied Command Transformation

AI – Artificial Intelligence

CAOC - Combined Air Operations Centre

C-IED CoE - Counter-Improvised Explosive Devices Centre of Excellence

CoE – Centre of Excellence

COVID-19 – Coronavirus

CPoW – Collaborative Program of Work

CSRR – Chief Scientist Research Report. Plural, CSRRs.

EDT – Emerging Disruptive Technology. Plural EDTs.

FFI – Norwegian Defence Research Establishment.

HFM – Human Factors and Medicine

HUMINT – Human Intelligence

IE – Information Environment.

InfoOps – Information Operations

JALLC - Joint Analysis and Lessons Learned Centre.

MC – Military Committee

MDO – Multi-Domain Operations

NIAG – NATO Industrial Advisory Group

NWCC – NATO Warfighting Capstone Concept

OODA – Observe, Orient, Decide, and Act

OSC – NATO Office of Strategic Communications.

OSINT – Open-Source Intelligence

PDD – Public Diplomacy Division

PsyOps – Psychological Operations

SOCMINT – Social Media Intelligence

STB – Science & Technology Board

STC – Science & Technical Committee. Plural, STCs.

STO – Science & Technology Organization

STRATCOM CoE – Strategic Communications Centre of Excellence.

S&T – Science & Technology

TNO – Organisation for Applied Scientific Research in the Netherlands

WDA – Warfare Development Agenda

WDI – Warfare Development Imperative. Plural, WDIs.

Contributors

Dr. Janet Blatny

Acknowledgements

This publication would not have been possible without the valuable research inputs and the dedication of all contributions from the members of the NATO STO network of experts, especially those participating in the 20 NATO STO Cognitive Warfare activities mentioned in this report. The contributions of many individuals and bodies are gratefully acknowledged.

Contact Details

Office of the Chief Scientist (OCS)
Address: NATO STO-OCS, NATO HQ -Blvd. Léopold III, B – 1110 Brussels – Belgium
Email: mbx.sto@hq.nato.int

List of Links

LinkedIn: NATO Science & Technology Organization (STO)

YouTube: NATO Science & Technology Organization (STO)

Website

Science & Technology Organization (STO)

The Chief Scientist Research Reports (CSRRs) provide NATO's senior political and military leadership with clear, evidence-based insight into science & technology developments.

The Alliance's resilience stems from a combination of civil preparedness and military capacity. The STO activities that are aligned with the Seven Baseline Requirements for resilience build our collective understanding of the concept of resilience. This CSRR serves as a guide for shaping both future research programmes and activities, as well as building partnerships between the research and resilience expert communities.

STO - NATO Science & Technological Organization
NATO Headquarters, Boulevard Léopold III, 1110 Brussels, Belgium