



Countering Cognitive Warfare with Advanced Distributed Learning

This info paper was developed by the PfPC ADL Working Group with the support of the Moldova Military Academy to inform next-generation Education, Training, Exercises, and Evaluation among security partners.

This info paper is intended to give military and civilian leaders involved with training and education (e.g., commandants, deans, department directors, faculty, and staff) a quick and pragmatic overview of how Advanced Distributed Learning (ADL) can be used to develop capabilities to counter cognitive warfare. It is a 15-minute read.

What is cognitive warfare, and how can ADL contribute to countering it?

Cognitive warfare aims to undermine rationality by manipulating emotions and subconscious reactions. It employs subversive psychological and information operations to target groups and individuals, leveraging rapid advancement in new technologies such as artificial intelligence (AI) and exploiting increased global interconnectedness through social media. Technological development is a key driver of cognitive warfare, enabling actors to rapidly modify their malign influence and utilize their targets' specific vulnerabilities. Given its potential for profound and far-reaching effects, some have proposed designating cognition as a new battlespace or domain of warfare.¹ NATO defines cognitive warfare as “activities conducted in synchronization with other instruments of power, to affect attitudes and behaviors by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage,”² with a goal to “exploit facets of cognition to disrupt, undermine, influence, or modify human decisions.”³

A small number of actors currently represent a cognitive warfare threat, but their attacks are aimed at many states, including NATO members and partners. Cognitive warfare is a challenge for allies and partners as a community, with potential implications for international stability,⁴ and an effective response requires a partnerships approach with an operational framework. Training and education should be deployed both to build resilience across allies and partners, and to counter specific cognitive threats as they arise. A structured, responsive, agile, and cost-effective education and training response by NATO Allies and Partners requires (1) developing instructional content

¹ Bernard Claverie, François Du Cluzel. “Cognitive Warfare”: The Advent of the Concept of “Cognitics” in the Field of Warfare. Bernard Claverie; Baptiste Prébot; Norbou Buchler; François du Cluzel. Cognitive Warfare: The Future of Cognitive Dominance, NATO Collaboration Support Office, pp.2, 1-7, 2022, 978-92-837-2392-9. <https://hal.science/hal-03635889/document>

² NATO Allied Command Transformation: Cognitive Warfare. <https://www.act.nato.int/activities/cognitive-warfare/>

³ NATO Science & Technology Organization Technical Report TR-HFM-ET-356: Mitigating and Responding to Cognitive Warfare.

⁴ Jean-Marc Rickli, Federico Mantellassi, and Gwyn Glasser. Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century. GCSP Policy Brief No. 9. August 2023. <https://www.gcsp.ch/publications/peace-mind-cognitive-warfare-and-governance-subversion-21st-century>

based on shared interoperability standards, (2) sharing education and training content, and (3) building a community of practice.

Advanced Distributed Learning (ADL) provides a model for developing and delivering modular, accessible, and personalized training that is cost-effective, agile and sharable. In addition, there are many lessons for the NATO community to learn from allied and partner nations that have been targets of intense cognitive warfare and utilized that experience to become leading innovators in cognitive operations response. Their expertise, including the effective use of ADL, is a valuable resource to be shared among allies and partners when developing a coordinated operational framework for combatting cognitive threats.

How are nations and organizations responding to cognitive threats?

Different actors have responded to the cognitive warfare threat in various ways: Ukraine is actively engaging Russian cognitive operations as part of its national defense; Finland has long built societal resilience through comprehensive education; NATO organizations have conducted conceptual development on cognitive warfare; and the European Union supports and enables actors through information and resources. Each of these examples provides insights into developing a partnerships approach to support training and education initiatives.

Ukraine embraces the right to publicly debate a wide range of issues on which consensus is difficult to achieve, such as military mobilization, ideological differences, and the status of minorities. This commitment to freedom of conscience and expression is an integral part of Ukraine's democratic political system, but Russia uses it to achieve cognitive effects. Russia targets and exacerbates disputes in Ukraine by amplifying polarized points of view and fueling emotional reactions to divisive questions (e.g., What is the acceptable price of resistance? Who could be mobilized? Who is making money off the war?). Russia's cognitive warfare erodes the notion of truth in Ukraine, undermining authoritative sources of information, generating public and political confusion, and delaying decision making. It distracts and disillusiones the Ukrainian people and demobilizes support for the war effort. Simultaneously resisting Russia's cognitive and kinetic warfare, Ukraine's countermeasures largely have focused on isolating the public from Russian informational influence: It has banned all Russian communication channels and is developing the capability to dampen informational, financial, and individual means of malign influencing.

Finland has built resilience against cognitive warfare as part of its comprehensive whole-of-society approach to security, governed by the Security Strategy for Society and encompassing governmental actors at all levels, non-governmental organizations, and the private sector.⁵ The approach includes a variety of actions specifically addressing cognitive warfare. At all levels of education, beginning with early childhood, Finland integrates the teaching of practical skills to

⁵ The Security Committee (of Finland). <https://turvallisuuoskomitea.fi/en/frontpage/>

identify disinformation.⁶ Universities and other educational institutions provide specific courses on countering influencing operations, a majority of which are open to the public. A key to the success of the Finnish approach is the wide availability of both in-person and online training and educational materials. In addition to education, Finland’s strategy focuses on clear communication about identified threats, with strong cooperation among all relevant actors on sharing information and best practices for countering cognitive warfare actions.

The European Union focuses its cognitive warfare response on strengthening capabilities and information sharing. As part of its Strategic Compass for Security and Defense, the EU has developed a Foreign Information Manipulation and Interference (FIMI) toolbox, a catalogue of tools member states can utilize in their efforts to counter cognitive operations, including situational awareness, resilience building, disruption and regulatory responses, and diplomatic responses. In addition, the European External Action Service (EEAS) produces an annual public report of key FIMI incidents targeting the EU and its allies, providing information to all responders. The EU also funds entities and projects to develop education and training programs and support communities of practice.⁷

NATO has driven the conceptual understanding of cognitive warfare, with NATO Allied Command Transformation (ACT) taking the lead through workshops and publications. The Alliance’s effort includes a NATO Science & Technology Organization (STO) exploratory team, which published a large multi-author study on cognitive warfare in March 2023. “Mitigating and Responding to Cognitive Warfare” highlights the lack of instructional programs to combat cognitive operations and the need to utilize virtual environments for future education and training.

Existing NATO and EU accords on information sharing, education, and training create a foundation for enhanced cooperation on cognitive warfare. In a January 2023 declaration, NATO and the EU renewed their longstanding strategic partnership and called for expanding and deepening their joint efforts on several key topics, including resilience, emerging and disruptive technologies, and FIMI. The support framework for a structured approach to collaboration on cognitive warfare education and training is already in place: NATO and the EU share many member states, and their education and training topics and audiences are largely complementary, including partner nation contributions.

What is the role of education and training in cognitive warfare?

Confronting cognitive warfare requires all echelons, from leaders to enlisted and civilian entities, to develop competencies and support through coherent training and education across diverse civilian and military organizations. A structured ADL program provides agile, resilient education

⁶ John Henley. How Finland starts its fight against fake news in primary schools. The Guardian. January 29, 2020. <https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news>

⁷ For additional information, see https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en, <https://www.disinfo.eu/> & <https://esdc.europa.eu/2024/05/28/cognitive-warfare-in-the-new-international-competition-an-emerging-challenge-for-the-eu-pilot-course/>

and training focused on specific methods to counter cognitive warfare. It can enable a swift and flexible learning-based response; but interoperability and standardization are critical to ADL content development, sharing, and delivery to the widest spectrum of participants.

Cognitive warfare threats are constantly evolving, and competence on counter-influence tools must keep pace, supported by active, engaged education and training. This could take the form of a basic instructional module that is expanded over time by adding micro-learning elements that augment and refine the content. For example, an existing e-learning course on Hybrid Influencing, Disinformation, and Information Manipulation would benefit from integrating perspectives on human cognition. Cooperation and sharing of relevant basic training content with public education entities would support a whole-of-society approach.

Experiential training, including simulations and gamified approaches, supports developing psychological resilience and can be enhanced through ADL-enabled pre-training. In experiential training, the training audience is exposed to cognitive influence tactics in a controlled environment, with the opportunity for reflection and feedback. Joint conduct of experiential training is also an effective way to build a community of practice that participants can utilize after the training.

Education and training programs must include an increased focus on AI skillsets because AI functions as a force multiplier for both conducting and countering cognitive warfare. AI enables hostile actors to conduct influence operations that are simultaneously wider-scale and more precisely targeted at individuals based on behavioral analysis. However, AI-enabled systems also can help counter cognitive operations by detecting hostile actions as well as supporting fact-checking and verifying information. Publicly available and private AI systems are novel and rapidly developing; therefore, training should focus on both the practical use of AI-enabled systems through human-machine teaming, and on abilities to critically evaluate the output of the tools to avoid unintended contamination with disinformation.

Recommendations on training and education for countering cognitive warfare

1. Developing training and education based on shared interoperability standards:

- Conduct a cognitive warfare education and training needs assessment to support curricula development with national training institutions, NATO, and the EU, contributing to a common competency framework that articulates the major components necessary to demonstrate resilience to cognitive warfare. The framework should define different levels of capability (e.g., novice, intermediate, and advanced) so it can be used broadly across different stakeholder groups.
- Develop education and training programs in a coalition approach, aligned with common interoperable technology and policy standards that support sharing and localization of learning content for all personnel to increase their awareness of cognitive warfare and the capacity to counter it. Include key related topics such as critical thinking in a digital age;

countering disinformation; cyber hygiene; cognitive psychology and unconscious biases; and social psychology, influence, and persuasion.

- Use engaging and active forms of learning such as wargames and exercises and include ADL capabilities as supplemental instructions, considering combined effects and both offensive and defensive actions. Account for elements of cognitive warfare such as manipulating emotions, modifying perceptions of reality, and precision spearfishing with AI in existing exercises.
- Ensure that whole-of-society education and training for resilience to cognitive warfare as a critical capability is incorporated in NATO deliberations on threat response thresholds and the use of active measures in the cognitive dimension.
- Fund the development of foundational instruction on AI for all service members to build awareness of the cognitive threat, and provide specific practical training on the use of AI-based counter-influence tools, such as large language models, fact-checking services, and dashboards.

2. Sharing training content:

- Strengthen NATO-EU cooperation on training for resilience to cognitive warfare by leveraging their existing strategic partnership. Organisations with competencies relevant for cognitive warfare that provide existing forums for deeper NATO-EU cooperation include Centres of excellence on Countering Hybrid Threats (Helsinki), Civil-Military Cooperation (Hague), Cooperative Cyber Defence (Tallinn), Crisis Management and Disaster Response (CMDR in Sofia), and Strategic Communication (Rome), as well as the Partnership for Peace Consortium's Irregular Warfare and Hybrid Threats working group. Civilian education entities also have networks relevant for a whole-of-society approach.
- Create an ADL catalogue clearinghouse digital platform to facilitate search and discovery of existing learning content on cognitive resilience for sharing among allies and partners. Any new content should be reviewed for inclusion in NATO's Education and Training Opportunities Catalog (ETOC). The ETOC titles should be visible to partners (when able) and allow for requests of release. Highlight training programs (courses) required to achieve interoperability with NATO's strategic communications and psychological operations structures.
- Consider ways to make instructional content broadly applicable (e.g., to diverse organizations and societal groups, particularly vulnerable groups). Consider different types of interoperability and corresponding standards, including policies, technology (such as courseware formats), concepts (semantic interoperability, such as via the competency framework), and across organizations (such as between military and civilian stakeholders). Usability is also necessary because merely making content available for sharing is insufficient; the friction from discovering, receiving, and incorporating shared content must also be minimized.
- Establish a terms of reference for standardization of content submissions. Guidance should include naming and tagging conventions, to maximize search efficiency. To validate

content, the subject authority (national or organizational) should be identified with contact information for transparency and clarification. Submitted training material may meet partner needs without meeting NATO standards.

3. Building a community of practice:

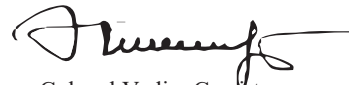
- Support the establishment of communities of practice with NATO and EU partner nations and organizations at different echelons to share experiences centered on required competencies and inform education and training on current adversary capabilities, strategies, and tactics. Leveraging existing networks such as the expert network of the Centre of Excellence for Countering Hybrid Threats provides a basis for this approach. Given the dynamic nature of the cognitive threat, close cooperation between instruction and research is required to maintain relevance and validity of training content and outcomes, and to avoid contamination and malign interference.
- Establish links between communities of practice in partner nations, including civilian and military training and education institutions, to bring in practitioners with experience on cognitive operations to develop education and training and maintain the relevance of instructional content to new forms of cognitive warfare. Collaborate with other groups and organizations, including public higher-education institutions and research institutes, to facilitate the dissemination of this material.



Maj. Gen. (Ret.) Barre R. Seguin
Director
George C. Marshall European Center
For Security Studies, U.S. DoD



Rear Admiral (UH) Placido Torresi
Deputy Chief of Staff
Multi Domain Force Development Headquarters
Supreme Allied Commander Transformation



Colonel Vadim Cemrtan
Rector
Armed Forces Military Academy
Alexandru cel Bun
Ministry of Defense, National Army
Republic of Moldova



Dr. Aaron Presnall
Co-chairman
PfPC ADL Work Group
Jefferson Institute, USA



COL Stephen Banks
Co-chairman
PfPC ADL Work Group
NATO ACT



LtC Michael Nickolaus
Co-chairman
PfPC ADL Work Group
Bundeswehr

Acknowledgements:

This paper was drafted by the Partnership for Peace Consortium (PfPC) Advanced Distributed Learning (ADL) Working Group in conjunction with its meetings in Chişinău in March 2024. The meeting was co-chaired by COL Steven Banks (NATO Allied Command Transformation) and Dr. Aaron Presnall (Jefferson Institute, USA); hosted by Colonel Vadim Cemîrtan, Commandant of the Moldovan Military Academy (MDA); and supported by LT Dionisie Ciubotaru (MDA), and the PfP Consortium Secretariat at the George C. Marshall Center.

The core author group was led by Ville Savoranta (FIN).

Tigran Harutyunyan (AM), Astghik Margaryan (AM), Greta Keremidchieva (BG), Col Dobril Radoslavov (BG), Greta Keremidchieva (BG), Ville Savoranta (FIN), Giorgi Kokhraidze (GE), LTC Giorgi Skirtladze (GE), Éva Kucsmik-Horváth (HU), Aleksandrs Gorbunovs (LV), SGM Sergejs Guzejevs (LV), SGT Madara Šteina (LV), Sergejs Guzejevs (LV), Remi Tremblay (NATO, CA), Sven Bertram (NATO, DEU), Justyna Kowalczyk, (PL), Jerzy Tomasik (NATO,PL), Gigi Roman (NATO, RO), Cem Kumsal (NATO, TR), Dr. Maj Dimitar Bogatinov (NMK), Ljupcho Shosholovski (NMK), Catalin Radu (RO), Emma Nygren (SWE), COL Roman Bakumenko (UA), COL Volodymyr Polevyi (UA), Col Vasyl Osiodlo (UA), Lt Col Olena Rybchuk (UA), LTC Yevhen Sudnikov (UA), Col Maksym Tyshchenko (UA), Dave Hartley (UK), Wg Cdr David Roe (UK), Michael Wadley (UK), and Dr. Sae Schatz (USA).