SYM-AM-26-151

Excerpt from the Proceedings

of the

Twenty-Third Annual Acquisition Research Symposium and Innovation Summit

Volume III

"Accelerating Warfighting Capabilities"

Neuro-Secure Manned-Unmanned Teaming: A Reference Architecture for Cognitive-Adaptive Warfighting Capability

Published: April 30, 2026

The research presented in this report was supported by the Acquisition Research Program, Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, please contact:

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
E: arp@nps.edu
www.acquisitionresearch.net

Copies of Symposium Proceedings and Presentations; and Acquisition Sponsored Faculty and Student Research Reports and Posters may be printed from the **NPS Defense Acquisition & Innovation Repository** at **https://dair.nps.edu/**.

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF ACQUISITION, FINANCE, AND MANPOWER
NAVAL POSTGRADUATE SCHOOL

Neuro-Secure Manned-Unmanned Teaming: A Reference Architecture for Cognitive-Adaptive Warfighting Capability

Laura Samso Pericon—is Founder of Synarea Insights and a professional focused on emerging defense technologies, autonomy, cyber resilience, technology transition, and human-machine teaming. Her work spans cyber strategy, operational readiness, acquisition pathways, emerging capability assessment, and the secure integration of advanced technologies into mission-relevant environments. She examines how autonomy, cognitive systems, cybersecurity, and governance intersect in future defense architectures. Her current research explores Neuro-Secure Manned-Unmanned Teaming as a reference architecture for advancing cognitive-adaptive warfighter capability while preserving human authority, cyber resilience, and responsible transition. [laura@laurasamso.com]

Abstract

Modern military operations are reaching levels of cognitive complexity that increasingly exceed the capacity of traditional human-machine interfaces. While non-invasive brain-computer interfaces and neuro-adaptive systems demonstrate technical feasibility, a critical transition gap persists between controlled demonstrations and sustained warfighter capability. This paper contributes a Neuro-Secure Manned-Unmanned Teaming (MUM-T) Reference Architecture, a transition-oriented model integrating cognitive-state sensing, trust-adaptive autonomy, neural-signal and human-machine-interface cybersecurity, neurocognitive-integrity safeguards, and modular software integration. Its objective is Cognitive Overmatch: the ability of human-machine teams to maintain decision quality, cognitive tempo, workload control, and mission effectiveness under contested, high-tempo conditions. The paper argues that current limitations are architectural rather than purely technical. It proposes a layered design and a phased roadmap spanning passive neuroadaptive monitoring, bounded adaptive autonomy, and future secure neuro-interaction. The contribution is a reference architecture and readiness pathway that defines what must be engineered, validated, secured, and governed for neuro-adaptive MUM-T to mature into reliable and scalable warfighter capability.

Keywords: Neuro-Secure MUM-T; Cognitive Overmatch; cognitive-state sensing; trust-adaptive autonomy; neural-signal cybersecurity; neurocognitive integrity; Technology Transition and Readiness

Introduction and Contribution

Human-machine teaming is transitioning from platform control toward supervisory control of multiple autonomous systems, particularly in Manned-Unmanned Teaming (MUM-T) environments. While autonomous platforms are advancing rapidly, the human-machine interface (HMI) is emerging as a limiting factor in mission performance. DARPA's Air Combat Evolution and NATO human-autonomy teaming research demonstrate the shift toward humans acting as mission commanders over collaborative autonomous systems rather than as single-platform operators (Defense Advanced Research Projects Agency [DARPA], n.d.; NATO Science and Technology Organization [NATO STO], 2020).

This creates a near-term operational challenge: platform autonomy is scaling faster than human cognitive capacity to manage it. Without improved cognitive support, operators risk overload, degraded decision quality, automation surprise, and inappropriate reliance. The transition from demonstration to operational capability is therefore an immediate Technology Transition and Readiness problem rather than a distant research question.

The central contribution of this paper is the Neuro-Secure MUM-T Reference Architecture. It integrates cognitive sensing, HMI design, adaptive autonomy, cybersecurity, and governance into a unified mission system. The novelty is not any single component, but their integration into a closed-loop, confidence-bounded, and security-governed decision system.

The architecture is designed to support Cognitive Overmatch, defined here as preserving decision quality, cognitive tempo, workload control, and trust calibration under contested conditions. Cognitive Overmatch is achieved only when improvements in those factors are measurable under operationally realistic conditions. The architecture is a transition-oriented reference model that defines what must be architected, secured, tested, and governed before neuro-adaptive MUM-T can mature into sustained warfighter capability.

State of the Art and Transition Gap

Brain-computer interfaces and cognitive-state sensing. Electroencephalography (EEG)-based and other non-invasive BCI systems can estimate workload, attention, intent indicators, or fatigue in controlled environments. Reviews identify typical BCI pipelines of acquisition, preprocessing, feature extraction, classification, and feedback, while also emphasizing calibration burden, signal variability, and artifact sensitivity (Abiri et al., 2019; Lotte et al., 2018; Nicolas-Alonso & Gomez-Gil, 2012; Wolpaw et al., 2002). Passive BCI work is especially relevant because it treats neural data as operator-state evidence rather than direct command (Zander & Kothe, 2011).

Human-autonomy teaming and MUM-T. Official and institutional MUM-T and human-autonomy teaming initiatives, including DARPA Air Combat Evolution and NATO human-autonomy teaming work, demonstrate platform-side momentum, but human supervisory burden remains a key constraint (DARPA, n.d.; NATO STO, 2020). Peer-reviewed multirobot and aviation HMI studies highlight workload, situation awareness, supervisory control, and trust challenges in multi-asset teaming (Chen & Barnes, 2014; Lim et al., 2018; Taylor et al., 2017).

Neural and HMI cybersecurity. BCI security literature shows that neural data can be a side channel and that BCI models can be exposed to spoofing, replay, fake P300, adversarial, and backdoor risks (Martinovic et al., 2012; Meng et al., 2023; Mezzina et al., 2021). These risks extend beyond data confidentiality into operator-state integrity and mission decision loops.

The transition gap is architectural: cognitive sensing is not yet operationally robust; trust-adaptive autonomy is not safely bounded; neural/HMI pathways are not secured as mission systems; and no unified architecture links sensing, trust, autonomy, and mission execution.

Proposed Neuro-Secure MUM-T Reference Architecture

The proposed architecture is a layered, transition-oriented architecture that integrates cognitive sensing, decision-support HMI, adaptive autonomy, and cybersecurity into a unified MUM-T mission system. It treats the human operator, HMI, neural-signal pathway, autonomy logic, unmanned-system tasking chain, and cyber controls as one cyber-physical mission system.

In this paper, Manned-Unmanned Teaming refers to a mission configuration in which a human operator or crewed platform supervises, coordinates, or collaborates with one or more unmanned systems through autonomy services, mission software and HMIs. The proposed architecture does not attempt to replace existing MUM-T command structures. Instead, it adds a neuro-secure decision-support layer that helps manage operator workload, trust calibration, interface adaptation, and cyber-cognitive resilience while preserving human authority over mission-relevant action.

Layer	Function	Core Requirement
Mission context	Threat, mission phase, communications, platform state	Context-aware interpretation
HMI/decision support	Alerts, recommendations, controls	Transparency and low cognitive load
Multi-modal sensing	EEG, gaze, physiology, behavior	No single-point reliance
Signal quality	Artifact filtering and validation	Confidence gating
Cognitive-state estimation	Workload, attention, fatigue, stress	Probabilistic and explainable
Trust calibration	Reliance, risk, autonomy confidence	Context and performance awareness
Bounded adaptive autonomy	Task support and interface adaptation	Reversible and auditable
MUM-T execution	Unmanned-system coordination	Authority validation
Neural/HMI cybersecurity	Data, model, and interface protection	Authentication and anomaly detection
Neurocognitive integrity	Operator-state protection	Manipulation detection
Data governance	Access, retention, provenance	Minimization and counterintelligence control
Modular Open Systems Approach (MOSA) / software integration	Replaceable components	Interoperability and upgradeability
Test and evaluation	Mission and resilience validation	Operational metrics

Data flow. Mission context and multi-modal sensing feed signal validation; validated signals feed cognitive-state estimation; estimates are combined with trust calibration and mission risk; bounded autonomy then supports MUM-T execution; feedback returns to test, evaluation, and continuous improvement. Cybersecurity, governance, and neurocognitive-integrity controls operate across all layers.

The architecture must demonstrate value against traditional HMI and non-neural workload models, including gaze-based and behavior-based systems. If neuro-adaptive integration does not produce measurable improvement over these baselines, it should remain limited to research, training, or monitoring applications.

Operational Scenario and Cyber-Cognitive Risk

Consider a pilot or mission operator supervising multiple unmanned systems in a degraded communications and contested electromagnetic environment. The operator must

interpret sensor feeds, autonomy recommendations, changing threats, and mission constraints under time pressure. A conventional HMI may increase information density precisely when the operator has reduced cognitive capacity, increasing the risk of missed cues or automation surprise.

Under the proposed architecture, multi-modal sensing estimates workload and vigilance; signal validation and cross-modal verification check whether neural or physiological indicators align with gaze, behavior, explicit input, mission context, and system telemetry; trust calibration adjusts support rather than authority; and bounded autonomy simplifies information presentation or recommends task reallocation without bypassing human command.

This paper uses Cognitive Denial of Service (C-DoS) as a proposed analytic term for adversarial action that degrades mission performance by overwhelming or manipulating the operator-state loop rather than directly attacking the unmanned platform. Adversarial Operator-State Manipulation refers to corrupting cognitive, physiological, behavioral, or trust-related indicators that feed adaptive autonomy. This reframes cybersecurity from protecting systems to protecting the human-machine decision loop as a mission-critical asset.

Mitigation requires signal authentication, anomaly detection, model-integrity checks, cross-modal verification, static resilience modes that revert to essential displays, and operator override. Future bidirectional or stimulation-capable neurotechnology should remain behind stronger cyber, safety, consent, and policy gates because passive EEG does not inject signals, while stimulation-capable systems introduce materially different risks (Pugh et al., 2018). The strategic concern is not that neural signals directly make decisions, but that manipulated neural, physiological, or operator-state inputs could bias the decision-support environment by altering cognitive-state estimation, trust calibration, interface behavior, and autonomy recommendations. In a MUM-T context, this creates a cascade risk: altered operator-state evidence can affect the cognitive-state estimator, which can affect trust calibration, which can affect adaptive autonomy, which can influence mission execution.

Transition Roadmap and Readiness Framework

Phase	Purpose	Risk	Gate
Phase 1: Passive neuroadaptive monitoring	Monitor workload, fatigue, vigilance, and cognitive burden	Fragile signals, privacy, false positives	Reliable estimates under movement, fatigue, stress, and noise
Phase 2: Bounded trust-adaptive autonomy	Adapt information, alerts, task support, and decision aids	Overtrust, undertrust, false adaptation	Improved performance without unsafe reliance or loss of authority
Phase 3: Secure neuro-interaction	Explore future intentional or bidirectional pathways	Neurocognitive integrity and cyber-physical risk	Cyber-resilient operation, fail-safe fallback, and operational benefit

Six readiness gates structure transition: laboratory feasibility, multi-modal robustness, trust-adaptive safety, cyber and neurocognitive resilience, operationally realistic MUM-T validation, and transition decision. Gate evidence should include cognitive-state validity, false-adaptation rate, trust calibration, workload, situation awareness, anomaly detection, fallback success, operator override quality, interoperability, sustainment burden, and upgradeability.

Cognitive Overmatch is not an aspirational label; it is a testable objective. It is achieved only if the architecture produces measurable improvements in decision tempo, workload control, trust calibration, cyber resilience, and mission performance under contested conditions.

Human Authority, Failure-Safe Design, and Governance

The system is a decision-support layer, not a decision-replacement layer. Cognitive-state data should never directly authorize lethal or safety-critical action. Instead, it should support bounded interface adaptation, advisory autonomy, workload management, task allocation, and recovery cues unless separately validated and authorized under policy.

Failure-safe design requires red-line conditions for suspending neuro-adaptive adjustment: manual override, signal-quality failure, conflicting sensor inputs, failed authentication or provenance, suspicious model behavior, HMI anomaly, or safety-critical mission phase. In those cases, the system should degrade gracefully, preserve essential data, log the event, and return control through explicit operator confirmation rather than abrupt disconnection.

Data governance is also a counterintelligence requirement. Neurophysiological and HMI logs could reveal fatigue cycles, stress triggers, workload vulnerabilities, training exposure, or readiness patterns. Mitigation requires minimization, access control, retention limits, audit logs, provenance protection, restrictions on personnel-use decisions, and separation of raw neural data from operational sharing where feasible (Ienca & Haselager, 2016; Martinovic et al., 2012).

Acquisition and Test Implications

Neuro-adaptive MUM-T should not be acquired as a monolithic brain-controlled platform. It should be matured as a modular, software-intensive, human-centered capability composed of replaceable sensors, signal-processing pipelines, cognitive-state models, HMI components, autonomy services, cyber controls, and test harnesses. This aligns with the Modular Open Systems Approach (MOSA) and software acquisition guidance, as well as defense acquisition priorities that emphasize modularity, software-centric development, speed of iteration, cyber resilience, and broader industrial-base participation (Defense Acquisition University, n.d.-a, n.d.-b; Department of Defense, 2020).

Operationally realistic test and evaluation should compare conventional HMI, non-neural workload-support baselines, and the full Neuro-Secure architecture. It should measure mission performance, workload reduction, false-adaptation rate, override behavior, situation awareness, cyber resilience, fallback success, and sustainment. The architecture should advance only when the evidence demonstrates measurable marginal value over simpler approaches.

Conclusion

This paper contributes a Neuro-Secure MUM-T Reference Architecture that integrates cognitive sensing, trust-adaptive autonomy, neural/HMI cybersecurity, neurocognitive integrity, data governance, modular integration, and operational test and evaluation into a unified transition pathway. Its purpose is not technological novelty for its own sake, but Cognitive Overmatch: preserving human-machine decision advantage under contested conditions. In this framing, neuro-adaptive inputs serve as a bounded decision-support layer for MUM-T operations, not as independent mission authority or direct replacement for human judgment.

The architecture provides a credible pathway from demonstration toward sustained warfighter capability by specifying what must be architected, validated, secured, governed, and acquired. It also preserves an evidence boundary: public research supports feasibility and the

urgency of human-autonomy teaming, while operational transition requires further validation under realistic, adversarial, and sustainment conditions.

References

Abiri, R., Borhani, S., Sellers, E. W., Jiang, Y., & Zhao, X. (2019). A comprehensive review of EEG-based brain-computer interface paradigms. *Journal of Neural Engineering*, *16*(1), 011001. https://doi.org/10.1088/1741-2552/aaf12e

Chen, J. Y. C., & Barnes, M. J. (2014). Human-agent teaming for multirobot control: A review of human factors issues. *IEEE Transactions on Human-Machine Systems*, *44*(1), 13–29. https://doi.org/10.1109/THMS.2013.2293535

Defense Acquisition University. (n.d.-a). *Modular Open Systems Approach (MOSA)*. https://www.dau.edu/cop/mosa

Defense Acquisition University. (n.d.-b). *Software Acquisition Pathway*. https://aaf.dau.edu/aaf/software/

Defense Advanced Research Projects Agency. (n.d.). *Air Combat Evolution (ACE)*. https://www.darpa.mil/research/programs/air-combat-evolution

Department of Defense. (2020). *Operation of the Software Acquisition Pathway* (DoD Instruction 5000.87). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF

Ienca, M., & Haselager, P. (2016). Hacking the brain: Brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*(2), 117–129. https://doi.org/10.1007/s10676-016-9398-9

Lim, Y., Gardi, A., Sabatini, R., Ramasamy, S., Kistan, T., Ezer, N., Vince, J., & Bolia, R. (2018). Avionics human-machine interfaces and interactions for manned and unmanned aircraft. *Progress in Aerospace Sciences*, *102*, 1–46. https://doi.org/10.1016/j.paerosci.2018.05.002

Lotte, F., Bougrain, L., Cichocki, A., Clerc, M., Congedo, M., Rakotomamonjy, A., & Yger, F. (2018). A review of classification algorithms for EEG-based brain-computer interfaces: A 10 year update. *Journal of Neural Engineering*, *15*(3), 031005. https://doi.org/10.1088/1741-2552/aab2f2

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the 21st USENIX Security Symposium* (pp. 143–158). USENIX Association. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic

Meng, L., Jiang, X., Huang, J., Zeng, Z., Yu, S., Jung, T.-P., Lin, C.-T., Chavarriaga, R., & Wu, D. (2023). EEG-based brain-computer interfaces are vulnerable to backdoor attacks. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *31*, 2224–2234. https://doi.org/10.1109/TNSRE.2023.3273598

Mezzina, G., Annese, V. F., & De Venuto, D. (2021). A cybersecure P300-based brain-to-computer interface against noise-based and fake P300 cyberattacks. *Sensors*, *21*(24), 8280. https://doi.org/10.3390/s21248280

NATO Science and Technology Organization. (2020). *Human-autonomy teaming: Supporting dynamically adjustable collaboration* (STO-TR-HFM-247). https://doi.org/10.14339/STO-TR-HFM-247

Nicolas-Alonso, L. F., & Gomez-Gil, J. (2012). Brain computer interfaces, a review. *Sensors*, *12*(2), 1211–1279. https://doi.org/10.3390/s120201211

Pugh, J., Pycroft, L., Sandberg, A., Aziz, T., & Savulescu, J. (2018). Brainjacking in deep brain stimulation and autonomy. *Ethics and Information Technology*, *20*, 219–232. https://doi.org/10.1007/s10676-018-9466-4

Taylor, G. S., Alicia, T. J., Turpin, T., & Surana, A. (2017). Controlling multiple unmanned aircraft from a manned helicopter: The need for advanced autonomy and refined pilot-vehicle interface. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 66–70. https://doi.org/10.1177/1541931213601485

Wolpaw, J. R., Birbaumer, N., McFarland, D. J., Pfurtscheller, G., & Vaughan, T. M. (2002). Brain-computer interfaces for communication and control. *Clinical Neurophysiology*, *113*(6), 767–791. https://doi.org/10.1016/S1388-2457(02)00057-3

Zander, T. O., & Kothe, C. A. (2011). Towards passive brain-computer interfaces: Applying brain-computer interface technology to human-machine systems in general. *Journal of Neural Engineering*, *8*(2), 025005. https://doi.org/10.1088/1741-2560/8/2/025005


Acquisition Research Program
Department of Acquisition, Finance, and Manpower
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net