

Human–Machine Collaboration in Military Operations: Challenges for Future Defense Systems

Henrik Solvang-Okafor

Department of Human Factors and Defense Systems Engineering Nordic Institute for Strategic Technology, Oslo, Norway

Article History

Received June, 09th , 2026

Accepted June, 10th , 2026

Published June, 11th, 2026



© 2026 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license

<https://creativecommons.org/licenses/by/4.0>

Abstract

The integration of autonomous and semi-autonomous technologies into armed forces is transforming how military operations are planned, commanded, and executed. Human–machine collaboration, often described as human–machine teaming, promises faster decisions, wider situational coverage, and reduced exposure of personnel to danger, yet it also introduces demanding technical, cognitive, ethical, and organizational challenges. This article examines those challenges through an integrative conceptual review of the human factors, automation, and defense studies literature. It analyzes the conceptual foundations of teaming, the allocation of autonomy within command structures, trust calibration, situation awareness and workload, interface design, ethical and legal accountability, cyber resilience, training and doctrine, and interoperability. A conceptual graph compares the operational criticality of each challenge with the estimated maturity of current solutions, revealing that accountability, trust, and cyber resilience are the areas where need most exceeds readiness. The article argues that future defense systems should be designed around meaningful human control, transparent machine reasoning, adaptive training, and shared international standards, so that human judgment and machine speed reinforce rather than undermine one another.

Keywords: human–machine teaming, military autonomy, trust in automation, meaningful human control, defense systems

INTRODUCTION

Armed forces around the world are investing heavily in unmanned vehicles, decision-support algorithms, intelligent sensors, and networked command systems. Early military automation largely replaced physical labor or extended human senses, as in autopilots, radar tracking, and remotely piloted aircraft. Contemporary systems go further: they interpret data, propose courses of action, prioritize targets, and in some cases act with limited human intervention. As a

result, the central question is no longer whether machines will participate in military operations, but how people and machines should share cognition, authority, and responsibility in environments characterized by uncertainty, time pressure, and lethal consequences. The idea of human-machine collaboration reflects a shift in perspective from using tools to working with partners. In a teaming relationship, the machine contributes capabilities such as rapid computation, persistent attention, and pattern recognition at scale, while the human contributes contextual understanding, moral reasoning, adaptability to novel circumstances, and legitimate accountability. The promise of this complementarity is considerable. However, decades of research on automation show that poorly designed collaboration can produce complacency, mode confusion, loss of skill, and catastrophic misuse (Parasuraman & Riley, 1997; Bainbridge, 1983). In military settings these problems are amplified by adversaries who actively seek to deceive, disrupt, and exploit both the machine and its human supervisor. Policy debate has also intensified. Analysts such as Scharre (2018) and Horowitz (2019) have shown that autonomy can shorten decision cycles and alter strategic stability, while ethicists such as Sparrow (2007) question whether responsibility can be meaningfully assigned when machines select and engage targets. National and institutional documents, including the United States Department of Defense Directive on autonomy in weapon systems (2023) and the Defense Science Board (2016) study on autonomy, emphasize appropriate levels of human judgment but leave much of the engineering and organizational detail unresolved. This article contributes an integrated view of the principal challenges confronting human-machine collaboration in future defense systems. Using a conceptual review approach, it synthesizes insights from human factors engineering, cognitive science, military studies, law, and ethics. The analysis proceeds through a sequence of thematic sections covering conceptual foundations, autonomy and command, trust, situation awareness, interface design, accountability, cyber resilience, training and doctrine, and interoperability. A summary then consolidates the main findings and implications for designers, commanders, and policymakers.

Conceptual Foundations of Human-Machine Teaming:

Human-machine collaboration in the military domain refers to the coordinated pursuit of mission goals by human personnel and intelligent systems that share information, divide tasks, and adjust to one another over time. It differs from simple automation in that the machine is not a passive instrument executing fixed commands; it exhibits a degree of initiative, interprets context, and communicates its own state and intentions. Sheridan (1992) described this relationship through the concept of supervisory control, in which a human operator intermittently programs, monitors, and intervenes in a system that otherwise acts on its own. This model remains a valuable foundation, although modern machine learning systems extend it by adapting their behavior in ways that even their designers may not fully anticipate. Effective teaming depends on properties that human teams take for granted: shared goals, mutual predictability, common ground, and the ability to direct one another's attention. When a machine partner lacks a workable model of what the human intends, or the human lacks a model of how the machine reasons, coordination breaks down quickly. Military operations add further complexity because teams are distributed across domains, including land, sea, air, space, and cyberspace, and because the composition of a team may change as units rotate, communications degrade, or new platforms join the formation. Human-machine collaboration therefore has to be understood as a property of an entire socio-technical system rather than of a single interface or algorithm. A further conceptual challenge concerns the vocabulary itself. Terms such as autonomy, automation, and artificial intelligence are used inconsistently across services, nations, and disciplines, which hampers requirement setting, testing, and international dialogue. Clarifying whether a system is automatic, adaptive, or genuinely autonomous in specific functions such as navigation, target recognition, or engagement is essential, because the appropriate safeguards differ markedly. A functional rather than platform-based description of autonomy, in which each task is examined separately for its degree of machine independence, offers a more precise basis for design and governance.

Levels of Autonomy and Command Structures:

A central design decision in any collaborative military system is how much authority to delegate to the machine and under what conditions. Parasuraman, Sheridan, and Wickens (2000) proposed that automation can be applied differently across stages of information acquisition, information analysis, decision selection, and action implementation, with the level of automation varying at each stage. This framework shows that autonomy is not a single dial but a set of choices. A surveillance drone may operate with high autonomy in navigation and sensor management while remaining under tight human control for weapon release. Defining these boundaries explicitly is a prerequisite for safe and lawful operations. Command structures must also adapt. Traditional military hierarchies assume that humans issue orders and other humans interpret them with judgment and initiative, often described as mission command. Introducing machine agents that act at speeds beyond human reaction challenges this model, because the commander may be unable to intervene in real time. Two broad models are commonly discussed: humans in the loop, who approve each critical action; humans on the loop, who supervise and can veto; and humans out of the loop, where the system acts independently once activated. Each model suits different circumstances, and the choice reflects a trade-off between speed, risk, and control. Horowitz (2019) cautions that competitive pressure to accelerate decision cycles may push

states toward weaker human oversight than they would otherwise prefer. Dynamic allocation of authority represents a promising direction. Rather than fixing the level of autonomy in advance, future systems may adjust it according to mission phase, communication availability, threat level, and operator state. Such adaptive allocation, however, raises its own difficulties: operators must understand when and why authority shifts, and the transitions themselves can create confusion if poorly signaled. Command doctrine therefore needs to specify not only who is responsible at any moment but also how responsibility is handed back and forth between people and machines under stress.

Trust Calibration and Reliance on Automation:

Trust is the willingness to rely on a system when outcomes are uncertain, and it is among the most studied variables in human–automation interaction. Lee and See (2004) argued that the goal is not maximal trust but appropriate reliance, in which the operator's confidence matches the actual capability of the system. Overtrust leads to complacency and the acceptance of erroneous recommendations, while undertrust leads to disuse of valuable capabilities. Parasuraman and Riley (1997) documented numerous cases in which both patterns produced serious accidents, and military history contains similar episodes involving automated air defense and identification systems. In defense contexts, trust calibration is complicated by the opacity of modern machine learning. Deep neural networks may perform impressively in testing yet fail unpredictably when conditions differ from their training data, for example under camouflage, electronic deception, or unfamiliar terrain. Operators cannot easily judge the boundaries of such systems from experience alone. Trust is further shaped by organizational culture, previous exposure to the technology, and the stakes of the decision at hand. A commander who has seen a system perform reliably in exercises may extend more confidence than is justified in combat, where the operating envelope is far less forgiving. Supporting calibrated trust requires systems that communicate their uncertainty, limitations, and reasoning in forms that operators can quickly interpret. Confidence indicators, explanations of key factors, and clear signaling of out-of-envelope conditions can help, provided they are validated with realistic users. Trust also develops over time through repeated, transparent interaction, which argues for early and continuous involvement of operators in design and testing rather than late-stage familiarization. Importantly, trust must be bidirectional in the sense that machines should be designed to recognize human limits, such as fatigue or overload, and adjust their behavior accordingly.

Situation Awareness and Cognitive Workload:

Situation awareness, defined by Endsley (1995) as the perception of elements in the environment, the comprehension of their meaning, and the projection of their future status, is fundamental to sound military decision making. Intelligent systems can substantially enhance each of these levels by fusing data from many sensors and presenting a coherent picture. At the same time, automation can undermine awareness when operators become passive monitors who are out of the loop. Bainbridge (1983) described this as one of the ironies of automation: the more reliable the system, the less practice the human has, and the less prepared that person is to take over when the system fails. Cognitive workload presents a related tension. Automation is often introduced to reduce workload, but it may merely change its nature, replacing manual tasks with demanding supervisory tasks such as verifying outputs, managing multiple platforms, and reconciling conflicting information. A single operator controlling several unmanned vehicles may experience long periods of low activity punctuated by sudden spikes of intense demand. Both extremes degrade performance, the former through vigilance decrements and the latter through overload. Future systems must therefore be designed with an understanding of workload dynamics over entire missions rather than average values. Information overload is an equally serious concern at the command level. Networked sensors and analytic tools can generate more data than staff can digest, and algorithmic prioritization may inadvertently hide relevant details. Designers should support shared situation awareness across the team, including the machine components, so that all members hold compatible understandings of the operational picture. Techniques such as adaptive displays, attention cueing, and structured handover briefings can help preserve awareness during transitions between human and machine control.

Interface Design and Operator–Machine Communication:

The interface is where collaboration becomes tangible, and its design strongly influences whether teaming succeeds. Military interfaces must function under noise, vibration, stress, protective equipment, and limited bandwidth, which constrains the use of complex graphical displays and fine manual input. Operators need to see what the system is doing, why it is doing it, and what it will do next. Opaque automation that acts without explanation produces surprise and mode confusion, whereas transparent designs allow the human to anticipate behavior and intervene appropriately. Communication in an effective team is bidirectional and multimodal. Emerging approaches include natural language dialogue, gesture and gaze control, augmented reality displays, and even neural or physiological sensing to estimate operator state. These technologies offer the possibility of more fluid exchange, but they also present risks, including misrecognition of commands, increased cognitive demands, and new vulnerabilities to interference. Interfaces should support graceful degradation so that operators can continue to function when communications are disrupted or when advanced modalities fail. Another design challenge is supporting the control of many machines by few people, a requirement that arises from the growth of swarming and multi-vehicle concepts. Controlling individual

platforms one at a time is not feasible at scale, so operators must instead direct groups through high-level intent, with the machines coordinating among themselves. This calls for abstractions that let people specify objectives and constraints rather than detailed actions, together with mechanisms for monitoring group behavior and intervening selectively. Evaluating such interfaces demands realistic, high-fidelity experimentation with trained military users rather than laboratory tasks with student participants.

Ethical, Legal, and Accountability Challenges:

Ethical and legal questions form perhaps the most contested dimension of military human-machine collaboration. International humanitarian law requires that attacks distinguish between combatants and civilians, be proportionate, and take feasible precautions to minimize harm. Commanders and operators bear responsibility for compliance. When machines contribute to target identification or engagement, it becomes difficult to determine who is accountable if an error occurs. Sparrow (2007) argued that this may create a responsibility gap in which neither the programmer, the commander, nor the machine can be justly held liable. Others contend that existing doctrines of command responsibility can accommodate such systems provided humans retain meaningful control. The notion of meaningful human control has become central to international discussions, yet its practical content remains debated. At minimum it suggests that humans should have sufficient information, time, and capacity to make informed judgments, and that their decisions should genuinely determine outcomes rather than serve as a mere formality. Cummings (2017) has warned that in time-critical scenarios, operators may be reduced to rubber-stamping machine recommendations, a pattern sometimes called automation bias, which satisfies procedural requirements without delivering true oversight. Genuine control therefore depends on design, training, and tempo, not merely on the presence of a human in the process. Beyond legal compliance, moral concerns include the dignity of those affected by automated force, the risk of lowering barriers to the use of force, and the psychological burden on operators who participate in machine-mediated killing at a distance. Policy frameworks such as the United States Department of Defense Directive 3000.09 (2023) call for appropriate levels of human judgment and rigorous testing, but compliance verification remains difficult across diverse systems. Continued international dialogue, supported by transparent national review procedures and technical standards, will be necessary to build shared expectations and reduce the danger of destabilizing misunderstandings.

Cybersecurity, Adversarial Threats, and System Resilience:

Collaborative military systems depend on data, software, and communications that adversaries will attempt to compromise. Cyber intrusions can corrupt sensor feeds, alter algorithms, or sever links between humans and machines, with potentially severe operational consequences. Machine learning introduces additional attack surfaces, including adversarial examples that cause misclassification with subtle manipulations, data poisoning during training, and model extraction through repeated querying. Because human operators rely on the machine's outputs to understand the battlefield, deception of the system effectively becomes deception of the commander. Resilience therefore has to be a design principle rather than an afterthought. Systems should be capable of detecting anomalies, degrading gracefully, and returning control to humans when their integrity is in doubt. Redundancy, diversity of sensing, authentication of data sources, and secure update mechanisms contribute to robustness. Equally important, operators must be trained to recognize signs of compromise and to maintain the ability to operate with reduced automation. The Defense Science Board (2016) highlighted that the benefits of autonomy are accompanied by new vulnerabilities, and that testing must therefore include adversarial conditions as a matter of course. Electronic warfare adds a further dimension. Contested electromagnetic environments may deny the bandwidth necessary for continuous remote supervision, forcing systems to operate with greater independence than planned. This compels designers to consider carefully what behaviors are acceptable when communications are lost, and to specify safe defaults. Human-machine collaboration in such circumstances relies on pre-delegated intent, clear rules of engagement encoded in system behavior, and robust mechanisms for reestablishing contact and reasserting human authority as soon as conditions permit.

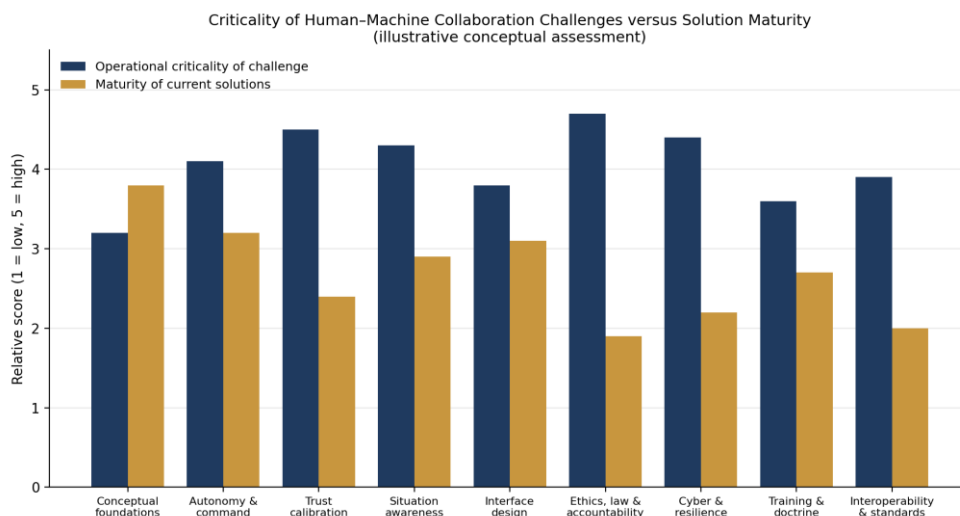
Training, Doctrine, and Organizational Adaptation:

Technology alone cannot deliver effective teaming; personnel must be prepared to work with intelligent systems, and organizations must adjust doctrine, structure, and culture accordingly. Training should extend beyond operating procedures to include an understanding of how the machine works, where it is likely to fail, and how to detect and counteract automation bias. Simulation and live-virtual-constructive exercises can expose personnel to rare failure modes safely, enabling them to practice intervention and recovery. Training must also address skill retention, since heavy reliance on automation can erode the manual and cognitive abilities needed when systems fail. Doctrine needs to evolve in step. Concepts of operations should specify how autonomous elements are integrated into plans, how authority is delegated, and how responsibilities are divided between operators, commanders, and technical support staff. New roles are emerging, such as algorithm supervisors, data curators, and autonomy test specialists, and career paths and professional military education must recognize them. Leaders at all levels need sufficient technical literacy to ask pertinent questions about system limits, while technical specialists need an appreciation of operational and ethical contexts. Organizational culture is a subtle but decisive factor. Resistance to adoption can arise from distrust, fear of

obsolescence, or previous negative experiences, while uncritical enthusiasm can lead to overreliance. Fostering a culture of informed, critical engagement, in which personnel feel empowered to question and override machine outputs, supports safer collaboration. Iterative experimentation, with feedback loops between operators and developers, allows doctrine and technology to co-evolve and shortens the distance between laboratory concepts and field realities.

Interoperability, Standards, and Future Research Directions:

Modern operations are conducted by coalitions, and human-machine systems must therefore function across national boundaries, services, and generations of equipment. Differences in data formats, communication protocols, autonomy levels, and rules of engagement can impede collaboration among allies. Common technical standards, shared testing methodologies, and agreed definitions would ease integration and enhance mutual trust. Alliances such as NATO have begun to articulate principles for responsible use of artificial intelligence, and further work is required to translate such principles into verifiable engineering practice. Several research directions merit sustained attention. Methods for verification and validation of learning-enabled systems remain immature, particularly for guaranteeing behavior in unfamiliar circumstances. Explainable and transparent artificial intelligence tailored to operational users, rather than to data scientists, is needed to support calibrated trust. Models of team cognition that treat machines as genuine teammates, including mutual theory of mind and shared mental models, could guide design. Finally, empirical studies of how automation affects decision quality, stress, and moral experience in realistic military contexts are scarce and should be expanded. Looking ahead, the strategic environment will place competing demands on defense organizations: the need for speed and scale, the imperative to preserve human judgment, and the obligation to uphold legal and ethical commitments. Navigating these demands will require collaboration among engineers, military professionals, legal experts, ethicists, and policymakers. Investment in interdisciplinary research, transparent governance, and international confidence-building can help ensure that future systems enhance security without eroding accountability or stability.



Summary:

Human-machine collaboration will be a defining feature of future military operations, offering gains in speed, awareness, and force protection while raising complex challenges. The analysis shows that these challenges are interdependent: unclear conceptual foundations impede the allocation of autonomy; poorly calibrated trust undermines situation awareness; weak interfaces obscure machine reasoning; and inadequate training and doctrine leave personnel unprepared to exercise genuine control. Ethical, legal, and cyber dimensions cut across all of these, because both accountability and resilience depend on how people and machines are designed to work together. The conceptual graph presented in this article suggests that the challenges of accountability, trust calibration, cyber resilience, and interoperability are those where operational criticality most exceeds the maturity of existing solutions, and these should therefore receive priority in research and acquisition. For designers, the implications include building transparent systems that communicate uncertainty, supporting adaptive allocation of authority, and testing under adversarial conditions. For commanders and educators, they include cultivating critical engagement with machine outputs and sustaining human skills. For policymakers, they include advancing shared standards and meaningful human control as practical, verifiable requirements. If pursued together, these measures can enable human judgment and machine capability to reinforce each other in the service of lawful and effective defense.

References:

- Bainbridge, L. (1983). Ironies of automation. *Automatica*, 19(6), 775–779.
- Cummings, M. L. (2017). Artificial intelligence and the future of warfare. Chatham House, The Royal Institute of International Affairs.
- Defense Science Board. (2016). Summer study on autonomy. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64.
- Horowitz, M. C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. *Journal of Strategic Studies*, 42(6), 764–788.
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 50–80.
- Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230–253.
- Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 30(3), 286–297.
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- Sheridan, T. B. (1992). *Telerobotics, automation, and human supervisory control*. MIT Press.
- Sparrow, R. (2007). Killer robots. *Journal of Applied Philosophy*, 24(1), 62–77.
- U.S. Department of Defense. (2023). Directive 3000.09: Autonomy in weapon systems. Office of the Under Secretary of Defense for Policy.