



THE HUMAN ELEMENT OF AUTONOMY

Why Human-Machine Readiness
Will Determine the Future of
Military Advantage



THE HUMAN ELEMENT OF AUTONOMY

“The future battlefield will not be won by the organization that fields autonomous systems first. It will be won by the organization that learns how to integrate human judgement and machine-enabled capability faster than its competitors.”

Executive Summary

Autonomous systems are moving quickly from experimentation to operational relevance. Across maritime, air, land, cyber, and space domains, defense organizations are investing in unmanned platforms, artificial intelligence, sensor fusion, machine-speed decision support, and distributed autonomous operations. The promise is compelling: greater endurance, reduced risk to personnel, faster decision cycles, wider operational reach, and more scalable force structures.

Yet the most important determinant of success may not be the technology's maturity. It will be the readiness of the people and organizations expected to employ it. Autonomy does not remove the human element from military operations. It changes where human decision is required, how it is exercised, and what kinds of expertise are needed to translate machine-enabled capability into operational advantage.

The prevailing conversation around autonomy tends to emphasize platforms, algorithms, payloads, and production scale. Those are necessary conversations, but they are incomplete. A force can acquire autonomous systems and still remain unprepared to use them well. Operators must understand autonomous behaviors. Maintainers must be ready for software-defined sustainment. Staff must know how to interpret machine-generated recommendations. Commanders must learn to lead organizations in which human and machine cognition interact continuously.

This paper argues that Human-Machine Readiness should become a strategic priority equal to platform performance, cybersecurity, reliability, and mission effectiveness. The concept is straightforward: future readiness will depend not only on whether systems are available, but on whether people can employ, supervise, sustain, and trust them under realistic operational conditions.

Several implications follow. First, workforce development cannot wait until fielding. It must begin during system development and mature alongside software, mission

concepts, and operational employment models. Second, trust must be built through experience, not briefings. Personnel need repeated exposure to routine operations, degraded conditions, edge cases, and system failures before those situations arise in the field. Third, readiness must evolve at the pace of software. Autonomous systems will not remain static, and neither can the workforce behind them.

Digital twins, operationally representative simulations, virtual maintenance environments, and human-machine interfaces that mirror operational workflows are not simply training enhancements. Used properly, they become a readiness infrastructure. They allow organizations to prepare personnel before hardware is widely available, expose teams to rare and high-risk scenarios, support software-driven updates, and continuously measure proficiency.

The central thesis is simple: every major military revolution has rewarded organizations that adapted faster than their competitors. The autonomy revolution will be no different. The decisive advantage will belong not to the force that fields autonomous systems first, but to the force that learns how to integrate human decision-making and machine-enabled capability fastest.

Autonomy Is an Adaptation Challenge

Every major military revolution has been, at its core, a human adaptation challenge. The tank did not transform warfare merely because it was mechanically superior to the horse. It transformed warfare because organizations learned how to employ armored formations differently from infantry formations. Aircraft did not change war simply because they could fly. They changed war because militaries developed new concepts for reconnaissance, air superiority, close air support, strategic attack, and command and control. Precision-guided weapons did not create an advantage solely through accuracy. They became decisive when forces adapted intelligence collection, targeting processes, doctrine, and operational planning around that accuracy.

Autonomy belongs in that same historical category.



It is not simply a new class of platform or a new layer of software. It is a change in the relationship between people, information, and machines. Historically, military technologies functioned primarily as tools. People remained responsible for sensing, analyzing, deciding, and acting. Machines extended human capability but left the essential decision cycle firmly in human hands.

Autonomous systems alter that model. Increasingly, machines participate directly in sensing, analysis, prioritization, recommendation, navigation, and execution. They can continuously monitor large environments, detect patterns across data streams, classify anomalies, recommend courses of action, and execute predefined behaviors with limited human intervention. This creates tremendous military opportunity but also a different kind of organizational problem.

The challenge is no longer only to field autonomous systems. It is to create formations capable of using them under pressure, at scale, and in contested environments. A maritime force operating unmanned surface vessels, an air component integrating Collaborative Combat Aircraft, or a logistics organization experimenting with autonomous resupply will all confront the same basic issue: technology performance matters, but organizational adaptation determines operational value.

This distinction is not academic. The Department of Defense's Replicator initiative demonstrates a clear push toward fielding large numbers of autonomous systems across domains.¹ The Air Force's Collaborative Combat Aircraft program is explicitly built around human-machine teaming, not isolated unmanned platforms. DARPA's Sea Hunter demonstrated the technical viability of an unmanned ocean-going vessel, but its long-term relevance depends on how such systems are supervised, sustained, trusted, and integrated into fleet operations.

The autonomy revolution, then, is not fundamentally about machines. It is about adapting military organizations to operate with machines that can sense, decide, and act in increasingly sophisticated ways. That adaptation will require new competencies, new readiness models, and a more serious approach to workforce preparation than most programs have historically required.

The Human-Machine Battlespace

Future warfare will increasingly occur within a human-machine battlespace: an operational environment in which people and autonomous systems constantly interact to generate combat power. This is more than a change in equipment. It is a shift in how military organizations perceive, decide, coordinate, and act.

For generations, combat power was organized around human decision processes supported by machines. Commanders and staffs gathered information, made assessments, selected courses of action, and directed forces. Platforms extended reach, mobility, lethality, and persistence, but they generally did not participate in the decision process. Autonomy changes that relationship. Machines are increasingly capable of generating information, ranking options, managing tasks, and recommending action. In some mission areas, they can act before a human could reasonably process the same volume of information.

This creates both opportunity and risk. Machine speed can improve responsiveness, compress kill chains, and diminish cognitive burden. It can also overwhelm commanders and staffs with recommendations, alerts, confidence scores, and autonomous status reports. A future operations center may not suffer from a lack of information. It may struggle to determine which information matters, which recommendations warrant action, and which systems call for human

1. Klare, M. T. (2023). Pentagon Plans Mass Autonomous Weapons Deployment. *Arms Control Today*, 53(8), 36–37.

intervention.

The point is not that machines are replacing judgment. War remains a human activity shaped by uncertainty, deception, politics, fear, culture, ethics, and intent. Machines can process information, but they do not understand strategy. They can identify patterns but do not understand the political consequences. They can recommend actions, but they do not establish national objectives. As autonomous systems assume more of the sensing and processing burden, the human decisions that remain become more important, not less.

The best organizations will therefore view autonomy as augmentation rather than replacement. Machines bring persistence, scale, speed, precision, and consistency. Humans bring context, creativity, ethical judgment, adaptability, and intent recognition. The operational advantage comes from deliberately combining these strengths.

This has direct implications for readiness. Human-machine integration can no longer be treated as a narrow technical specialty. Mission command, intelligence, fires, maneuver, protection, and sustainment are all being shaped by autonomous and AI-enabled systems. The ability to understand and collaborate with those systems is becoming a warfighting competency in its own right.

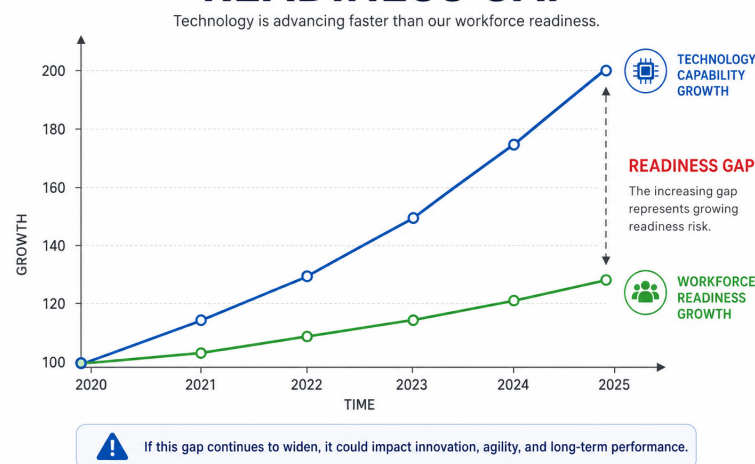
The Human Readiness Gap

Defense organizations are advancing autonomy faster than they are preparing the workforce that must employ it. That divergence is creating a Human Readiness Gap: the distance between what autonomous systems can technically do and what organizations are prepared to do with them operationally.

The Defense Acquisition Enterprise is highly practiced at measuring technical progress. Programs can evaluate platform reliability, software maturity, mission effectiveness, cybersecurity compliance, sensor performance, and production readiness. These metrics are necessary. They also create a bias toward what can be measured easily. Workforce readiness is more difficult to quantify, so it often receives less disciplined attention.

How should a program measure an operator's ability to supervise multiple autonomous systems simultaneously? How should a commander evaluate the reliability of machine-generated recommendations under pressure? How does a maintenance organization know whether its personnel can diagnose software-defined failures they have never seen before? How does a staff develop confidence in AI-enabled planning tools without becoming dependent on them? These questions are central to operational readiness, but they are not yet treated with the same rigor as platform performance.

READINESS GAP



The result is a dangerous mismatch. Technology evolves continuously; workforce development often remains episodic.² Software moves at one pace; institutional training pipelines move at another. Autonomous systems may change through updates, new autonomy behaviors, revised interfaces, or new mission applications, while personnel remain trained on a prior baseline.

Trust is where this gap becomes most visible. Too little trust leads personnel to intervene unnecessarily, ignore valid recommendations, and underuse capability. Too much trust leads to complacency and missed anomalies. The objective is calibrated trust: confidence that reflects actual system performance, known limitations, operating context, and mission risk. Calibrated trust cannot be created by policy or presentation. It comes from repeated experience with systems operating under realistic conditions.

The same gap affects maintainers and logisticians. A platform may be mechanically sound but operationally degraded due to software configuration, sensor fusion conflicts, data synchronization issues, communication latency, or cyber-related constraints. The maintainer of the future must be able to diagnose behavior as well as hardware. That is a different form of readiness than traditional mechanical troubleshooting.

The Human Readiness Gap should concern program managers, commanders, and industry executives alike. Sophisticated technology without corresponding human understanding can create brittle operational concepts. The force may possess capability, but lacks the confidence, judgment, and sustainment depth required to employ it at scale.

Human-Machine Combat Thinking

Closing the Human Readiness Gap calls for more than new training material. It requires a new way of thinking about military operations. Future personnel must learn to evaluate missions through both human and machine lenses. This can be described as Human-Machine

Combat Thinking.

Traditional military education teaches professionals to assess terrain, enemy capabilities, friendly capabilities, logistics, command relationships, risk, timing, and intent. These skills continue to be essential. Autonomy adds one more layer. Leaders and staff must also ask how machines are sensing the environment, what assumptions are embedded in recommendations, how confidence is being communicated, and how adversaries might manipulate machine-generated outputs.

Human-Machine Combat Thinking changes the questions personnel ask. What can the system detect that humans may miss? What can humans understand that the system may misclassify? How reliable is the data used to generate the recommendation? What happens if communications degrade? Is the system behaving unexpectedly, or is it behaving correctly in a way personnel do not yet understand? When is intervention necessary, and when does intervention reduce mission effectiveness?

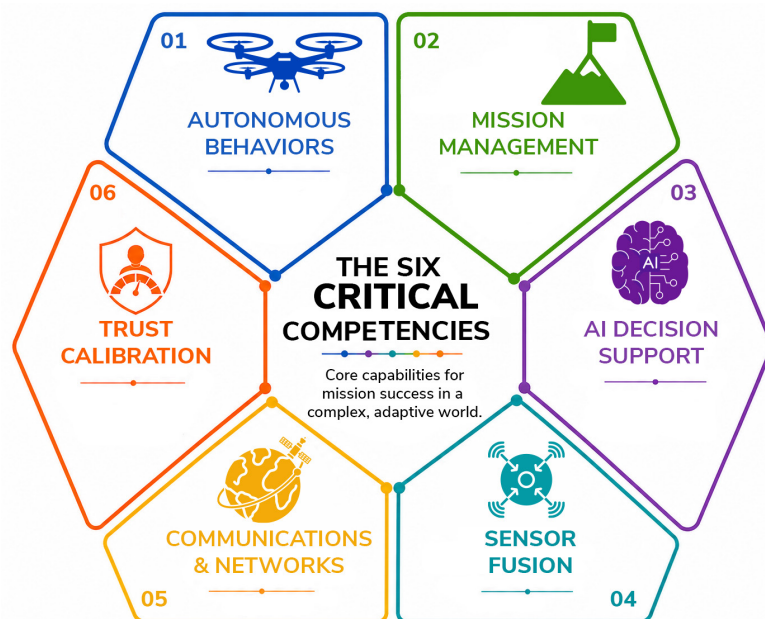
These questions should become as routine as intelligence preparation, fires planning, and logistics estimates. They should not be reserved for engineers, software developers, or AI specialists. Operators need this mindset. Maintainers need it. Analysts need it. Staff officers need it. Commanders need it.

Consider a maritime task group receiving a machine-generated warning from an autonomous sensor network. The system identifies a pattern of vessel behavior as suspicious and recommends repositioning assets. A traditional review might focus on the recommendation itself. A human-machine review asks deeper questions: What data supports the assessment? What confidence level is being reported? Could environmental conditions, spoofing, or adversary deception be influencing the result? What information is missing? What risk is created by acting, and what risk is created by waiting?

In this model, the machine contributes speed, persistence, and analysis. The human contributes context, skepticism, judgment, and intent. The decision is stronger because it reflects both.

The Autonomous Workforce Competency Framework

If Human-Machine Readiness is to become more than a slogan, organizations need a functional framework for workforce development. Six competencies consistently emerge across autonomous operations regardless of domain or platform: understanding autonomous behaviors, mission management and supervision, AI-assisted decision-making, sensor fusion interpretation, communications and network management, and trust



calibration.

First, personnel must understand autonomous behaviors. Traditional systems usually respond directly to human inputs. Autonomous systems respond to mission objectives, environmental conditions, programmed logic, confidence thresholds, and operational constraints. Personnel must understand state changes, decision pathways, contingency responses, recovery modes, and escalation criteria. Without that understanding, a system may appear unpredictable even when it is operating properly.

Second, personnel must master mission management and supervision. Autonomy shifts the operator's role from direct control to outcome management. Future mission supervisors will define objectives, set boundaries, monitor execution, manage exceptions, and decide when to intervene. This is particularly important when one person or team supervises multiple autonomous assets across a distributed mission environment.

Third, personnel must learn to make AI-assisted decisions. Machine-generated recommendations will increasingly influence intelligence analysis, route planning, logistics, targeting, risk assessment, and sustainment decisions. Effective personnel must understand confidence levels, data quality, assumptions, uncertainty, and override criteria. The objective is neither blind acceptance nor reflexive skepticism. It is an informed evaluation.

Fourth, personnel must interpret sensor fusion. Autonomous systems usually combine radar, electro-optical, infrared, acoustic, navigation, intelligence, and network data into a fused operational picture. That picture can improve awareness, but it can also obscure uncertainty. Personnel must understand what the system knows, what it does not know, and where environmental

influences or adversary actions may distort interpretation.

Fifth, personnel must understand communications and network management. Autonomous systems rarely operate alone. They rely on data links, mesh networks, satellite communications, edge computing, cloud-enabled mission systems, and cyber-secure architectures. Personnel need to understand how information moves, what happens when networks degrade, and how autonomous behaviors change when connectivity is limited or contested.

Finally, personnel must develop calibrated trust. Trust is not a soft skill. It is an operational variable. Under-trust reduces capability. Over-trust increases risk. Calibrated trust develops through exposure, practice, and an honest understanding of the system's strengths and limitations.

These competencies should be treated as force development objectives, not simply training tasks. They are the foundation for operational effectiveness in a human-machine battlespace.

specialties. It will reshape many existing ones. Operators, maintainers, analysts, logisticians, staff officers, and commanders will all experience changes in responsibility as autonomous systems become more deeply integrated into operations.

The operator becomes a mission manager. Rather than controlling every movement of a platform, the operator establishes objectives, defines constraints, supervises execution, and manages exceptions. The value shifts from manual control to judgment, prioritization, and orchestration. This is a major change in mindset. It requires personnel who are comfortable managing outcomes rather than inputs.

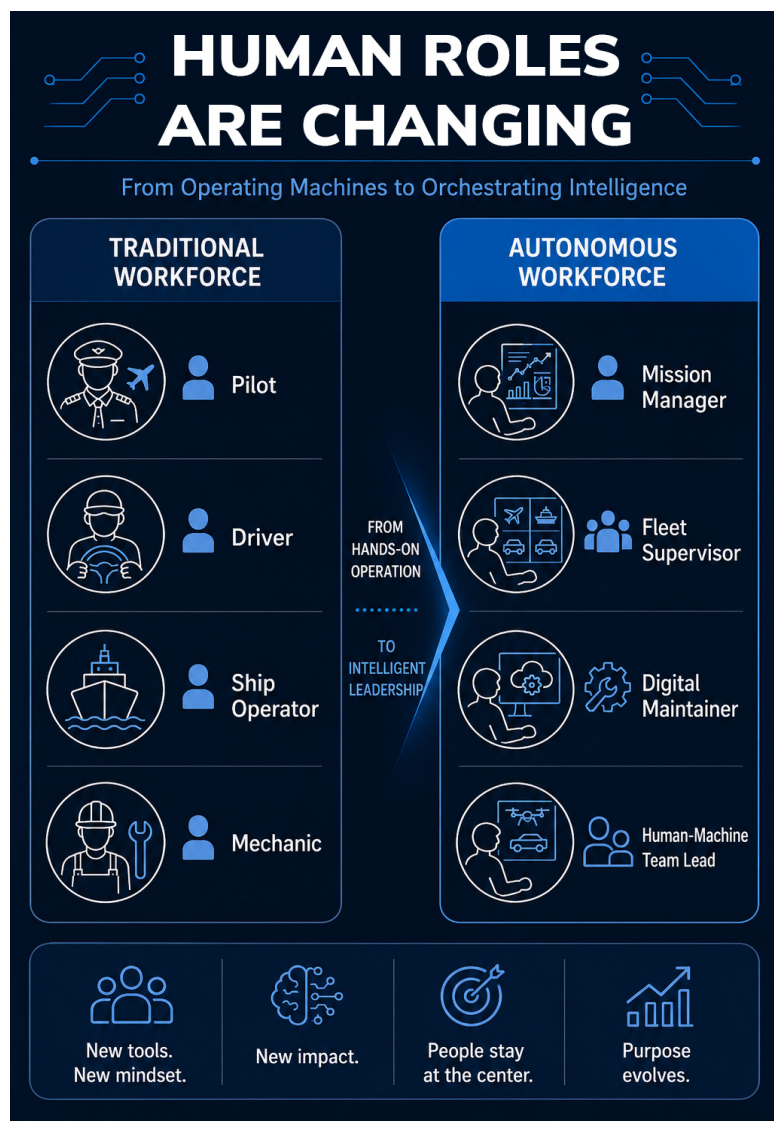
The maintainer becomes a digital sustainment specialist. Mechanical and electrical expertise continue to be essential, but autonomous systems add autonomy engines, mission software, sensor fusion frameworks, embedded computing, cybersecurity controls, and data management. Failures may emerge from software interactions, degraded communications, corrupted data, or configuration errors. The maintainer must troubleshoot the behavior of an integrated system, not merely the condition of a component.

The intelligence analyst becomes a human-machine interpreter. AI-enabled tools can process large volumes of ISR and operational data, but analysts must validate outputs, understand uncertainty, recognize deception, and translate machine-generated insights pertaining to operational relevance. Machines can identify patterns. Humans decide what those patterns mean.

The staff officer becomes a human-machine integrator. Staff sits between information and decision. As AI-enabled planning, predictive analytics, and autonomous collection systems become more common, staff must learn to incorporate machine-generated recommendations into planning without surrendering judgment. The challenge will not be receiving information. It will be determining how to use it well.

The commander becomes a leader of human-machine teams. Command remains a human responsibility, but the environment in which it operates is changing. Leaders will increasingly oversee organizations characterized by continuous information flow, machine-speed analytics, distributed autonomous operations, and autonomous sustainment networks. Commanders must create cultures that embrace innovation while retaining critical thinking and accountability.

These shifts will blur the line between technical and operational expertise. Operators will require systems understanding. Maintainers will require analytical skills. Staff will require familiarity with AI-enabled decision



The Workforce Transformation Ahead

Autonomy will not create only a handful of new

specialties. It will reshape many existing ones. Operators, decision support. Leaders will require fluency in human-machine interaction. The future force must be both operationally proficient and digitally fluent.

Contested Logistics and Autonomous Sustainment

For all the attention paid to autonomy, navigation, AI, and human-machine teaming, the long-term success of autonomous operations may depend on a less visible factor: sustainment. A force that cannot maintain, repair, update, and supply autonomous systems under pressure will not convert autonomy into a durable advantage.

Sustainment is already a strategic challenge in contested environments. Future adversaries will seek to disrupt transportation networks, communications links, supply chains, maintenance facilities, fuel distribution, and data infrastructure. Autonomous systems may reduce some risks, but they also introduce new dependencies. Software, networks, sensors, cybersecurity, and data quality become central to readiness.

This changes the meaning of mission capable. A platform may be mechanically ready but operationally degraded because its software baseline is outdated, its sensor fusion model is producing conflicts, or its communications architecture is unstable. Traditional readiness measures remain necessary, but they are no longer sufficient. Autonomous operations require both digital and mechanical readiness.

Predictive maintenance illustrates both the opportunity and the workforce challenge. AI-enabled systems can identify trends, forecast failures, and refine maintenance actions before operational impact occurs. This can improve availability and reduce lifecycle costs, but it also requires maintainers to interpret machine-generated assessments. They must understand confidence, data quality, predictive uncertainty, and operational priority. The maintainer becomes part of the predictive maintenance architecture.

Autonomous logistics raises similar issues. Unmanned resupply vehicles, unmanned cargo aircraft, autonomous maritime logistics platforms, AI-enabled inventory management, and dynamic route optimization can increase resilience. They also require logisticians who understand both physical supply chains and the digital systems that enable autonomous movement, routing, and prioritization.

The sustainment problem becomes even more complex as software evolves. Autonomous systems do not exist as static platforms. Updates may introduce new behaviors, interfaces, mission workflows, and diagnostic requirements.³ A workforce trained on one software baseline may face a different operational reality months

later. Sustaining autonomous capability, therefore, means sustaining organizational understanding.

This is where digital readiness infrastructure becomes important. Digital twins, simulation environments, and virtual maintenance systems enable organizations to expose personnel to changing configurations, rare failure modes, complex troubleshooting scenarios, and operationally relevant maintenance tasks before they occur in the field. The point is not to replace physical maintenance experience. It is to expand, accelerate, and make it repeatable.

Sea Hunter: The Readiness Lesson Behind the Technology

Sea Hunter remains one of the clearest examples of why technology readiness and operational readiness are not the same thing. Developed under DARPA's Anti-Submarine Warfare Continuous Trail Unmanned Vessel program, Sea Hunter demonstrated the viability of an unmanned ocean-going vessel and later transitioned to the Office of Naval Research for continued development as a medium displacement unmanned surface vessel.

The technical achievement was significant. Sea Hunter demonstrated that an unmanned surface vessel could operate for extended periods, navigate maritime environments, and serve as a foundation for future unmanned maritime concepts. These results mattered because a Navy operating over extensive areas, facing persistent surveillance demands, and increasingly interested in distributed maritime operations needed them.

Yet Sea Hunter's deeper lesson is organizational. Beyond proving that an unmanned vessel can operate, it shows that autonomous vessels are not simply ships without crews. They require new approaches to supervision, maintenance, command relationships, communications, mission planning, fleet integration, and operational trust. The absence of a crew on board does not eliminate human responsibility. It relocates it.

Operators must understand autonomous navigation decisions and intervention criteria. Maintainers must be prepared for software-driven diagnostics, sensor dependencies, communications issues, and autonomy-related sustainment. Commanders must determine how unmanned vessels fit into fleet tactics, rules of engagement, risk decisions, and distributed operations. Staff must understand what information the vessel provides, how reliable it is, and how to incorporate that information into planning.

Sea Hunter illustrates a broader point applicable to every domain: the successful demonstration of autonomy is not the same as institutional readiness for autonomy.

3. Sinan, M., Shahin, M., & Gondal, I. (2025). Integrating security controls in DevSecOps: Challenges, solutions, and future research directions. *Journal of Software: Evolution and Process*, 37(6), e70029.

WHAT AUTONOMOUS PLATFORM DEVELOPERS CAN LEARN FROM SEA HUNTER

SEA HUNTER (USV-1)

The U.S. Navy's pioneering unmanned surface vessel that completed the first autonomous transoceanic voyage in 2016.



1. START WITH A CLEAR MISSION

Sea Hunter was built for a specific mission—persistent, long-endurance operations. Define the mission first; design to enable it.



2. ITERATE RELENTLESSLY

Sea Hunter evolved through rapid prototyping and at-sea experimentation. Build, test, learn, and iterate—fast.



3. DESIGN FOR MODULARITY

Modular payloads and open architecture enable flexibility, upgrades, and mission adaptability over time.



4. BUILD IN RESILIENCE

Sea Hunter operated in harsh conditions autonomously. Robust autonomy, fault tolerance, and redundancy are essential.



5. PEOPLE + AUTONOMY = MULTIPLIER

Sea Hunter doesn't replace the warfighter—it extends their reach. Design systems that augment human decision-making.



SEA HUNTER PROVES WHAT'S POSSIBLE.
THE LESSONS GUIDE WHAT'S NEXT.



MISSION
FIRST



ITERATE
CONTINUOUSLY



STAY
MODULAR



ENGINEER
RESILIENCE



EMPOWER
HUMANS

That distinction matters because a prototype can prove that a machine works. It cannot, by itself, prove that an organization is ready to employ that machine at scale, in contested conditions, across a lifecycle measured in years.⁴

The lesson for defense leaders and autonomous platform developers is direct. Build workforce readiness alongside technical maturity. If organizations wait until platforms arrive to build the workforce, trust, interfaces, sustainment concepts, and readiness measures required to employ them, operational adoption will fall short of technological promise.

Building Human-Machine Readiness

If Human-Machine Readiness is a strategic capability, then it requires infrastructure. The force cannot rely solely on classroom instruction, physical asset access, or episodic qualification events because those approaches do not support the depth of readiness this capability demands. It needs environments that allow personnel to develop understanding, experience, trust, and adaptability before operational consequences exist, making the investment in such infrastructure necessary. Build those environments now to support readiness as a strategic capability.

Digital twins are central to this shift. Although often discussed in engineering or test contexts, their readiness value is substantial. A digital twin can provide a living representation of an operational system that evolves with the platform. Use them to let operators explore mission workflows, maintainers practice procedures, staff rehearse concepts of operation, and leaders evaluate command relationships and decision points before hardware is widely available.

This effectively shifts readiness left. Instead of waiting for fielding, organizations can begin preparing personnel during development. Make that preparation deliberate so the workforce already has a foundation of familiarity and understanding by the time platforms arrive. This is particularly valuable for autonomous programs in which physical systems are scarce, expensive, geographically dispersed, or still undergoing test and evaluation.

Operationally representative interfaces are equally important. The interface is where autonomy becomes visible to humans. It is where personnel see system status, confidence indicators, alerts, recommendations, health information,

4. Wirtz, J. J. (2023). Designing Maritime Campaigns with Unmanned Systems: Overcoming the Innovation Paradox. Center for International Maritime Security.

and mission progress. If the interface obscures autonomous behavior, trust suffers. If the training interface differs significantly from the operational interface, proficiency suffers. Therefore, design readiness environments to mirror operational workflows as closely as possible.

Simulation and immersive environments provide the experience needed to build judgment. Personnel must encounter degraded communications, sensor conflicts, software anomalies, unexpected autonomous behaviors, and decision-support uncertainty. Because these scenarios may be rare, expensive, or unsafe to reproduce with operational assets, make them repeatable in digital environments.

Virtual maintenance environments expand the same logic into sustainment. They allow maintainers to learn procedures, diagnose faults, experience uncommon failures, and prepare for evolving software-defined systems without waiting for access to operational hardware. For autonomous fleets, where availability and sustainment depth will determine operational value, this capability is not a luxury. Treat it as a readiness requirement and invest accordingly.

The larger point is that readiness must evolve at the speed of software. Autonomous systems will change. Interfaces will change. Mission behaviors will change. Threat environments will change. Build a readiness ecosystem that can update, measure proficiency, identify gaps, and support continuous learning. The organizations that build this capability will adapt faster than those that rely on legacy training timelines.

Building Human-Machine Readiness

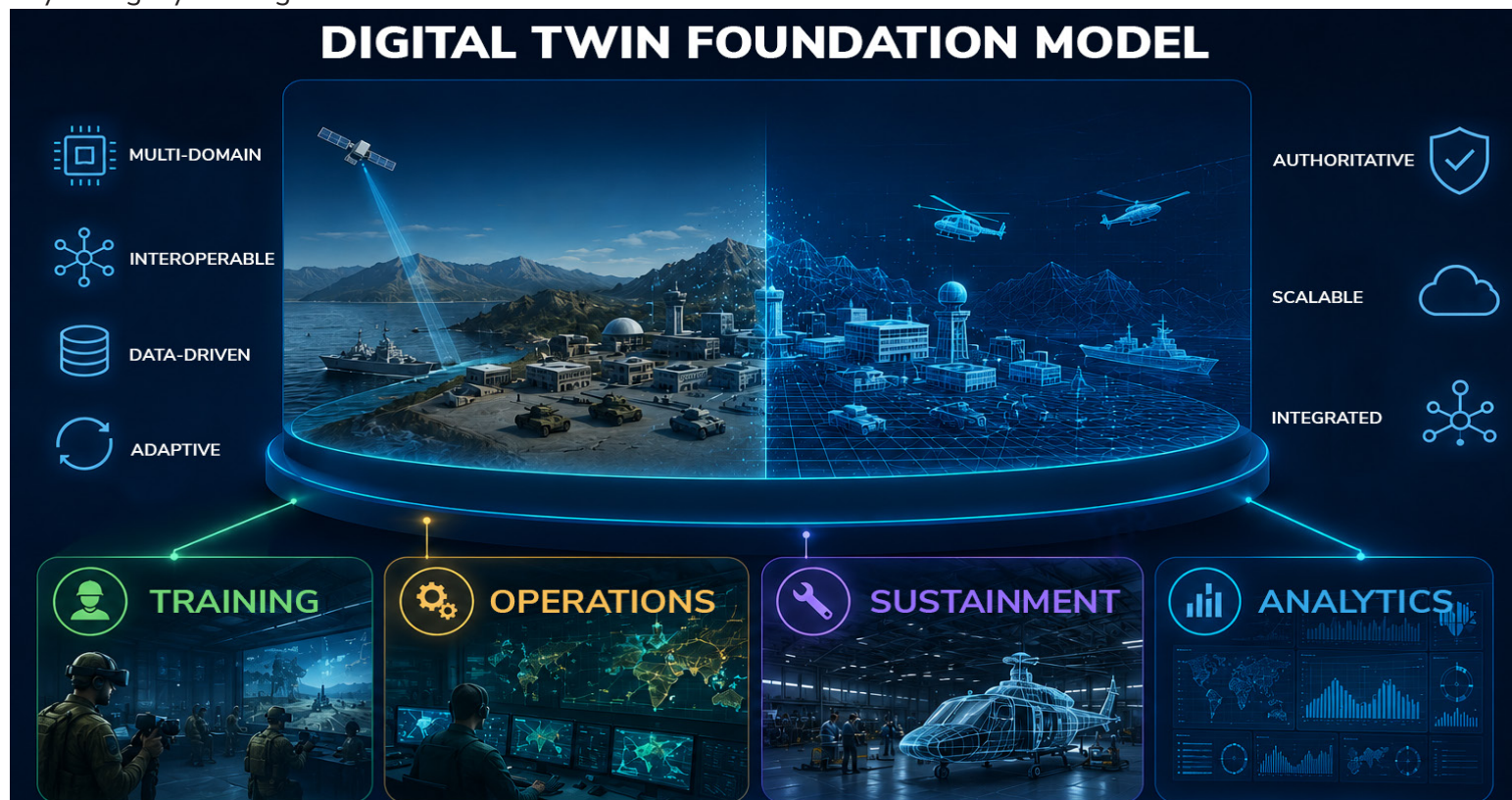
Leaders need a way to assess whether their organizations are progressing from technology adoption to operational integration. A Human-Machine Readiness Maturity Model provides that structure.⁵ It is not intended to create another compliance exercise. Instead, it helps leaders identify where workforce readiness is strong, where gaps remain, and where investment should be prioritized.

Level One is Platform Familiarization. Personnel understand basic terminology, mission roles, architecture, and system purpose. This stage is necessary, but it is awareness. Personnel may know what a system does without understanding how it behaves.

Level Two is Operational Understanding. Operators understand standard workflows and routine system behavior. Maintainers understand basic procedures and diagnostics. Staff understands likely mission applications. The organization can use the system in expected conditions, but it remains vulnerable in complex or degraded conditions.

Level Three is Autonomous Mission Management. Personnel supervise autonomous operations rather than simply operating systems. They monitor behaviors, manage exceptions, adjust mission parameters, interpret alerts, and exercise oversight. Maintainers diagnose software-defined behavior. Staff incorporates machine-generated insights into planning. Competence shifts from procedure to supervision.

DIGITAL TWIN FOUNDATION MODEL



5. Ladu, L., Koch, C., Ashari, P. A., Blind, K., & Castka, P. (2024). Technology adoption and digital maturity in the conformity assessment industry: Empirical evidence from an international study. *Technology in Society*, 77, 102564.

Level Four is Human-Machine Teaming. The organization collaborates with autonomous systems as part of normal operations. Personnel are proficient in AI-assisted decision-making, sensor fusion interpretation, multi-system supervision, trust calibration, and distributed autonomous operations. Commanders use machine-speed analysis while maintaining human judgment.

Level Five is Autonomous Force Readiness. Human-Machine Readiness is institutionalized. Digital twins, simulation, virtual maintenance environments, operational interfaces, readiness measurement, and continuous learning function as a cohesive ecosystem. The organization adapts quickly to new software, threats, and mission requirements.

The maturity model matters because fielding is not the same as readiness. Training is not automatically readiness. Qualification is not necessarily readiness. Readiness exists when personnel can employ, supervise, sustain, and trust autonomous systems under realistic operational conditions.



Strategic Recommendations for Defense Leaders

The defense community does not face a technology challenge alone. It faces an adaptation challenge. Autonomous systems will continue to mature; the question is whether organizations can adapt doctrine, workforce development, sustainment, and leadership fast enough to realize their potential.

First, treat human readiness as a program requirement. Build workforce competencies, trust objectives, sustainment readiness, human-machine interface requirements, and readiness assessment into program design early. Link them to program outcomes, and do not add them after fielding.

Second, begin workforce development before platform delivery. Use digital environments to prepare operators, maintainers, staff, and leaders before physical systems are widely available. Reduce the lag between fielding and operational readiness.

Third, build trust through experience. Give personnel repeated exposure to autonomous behavior, machine-generated recommendations, degraded operations, and failure scenarios. Do not rely on briefings alone. Build trust through experience.

Fourth, invest in readiness infrastructure. Treat digital twins, simulation, virtual maintenance environments, and operationally representative interfaces as core enablers of autonomous readiness. Use them to improve proficiency at scale.

Fifth, measure Human-Machine Readiness. Evaluate autonomous behavior understanding, mission supervision proficiency, AI-assisted decision-making, trust calibration, digital sustainment skills, and adaptability to software evolution. Measure what you want sustained attention on.

Sixth, train for failure, not just success. Prepare personnel for degraded conditions by planning for disrupted networks, sensors, data, and communications that autonomous operations depend on. Do not train only for the ideal ones.

Finally, develop human-machine leaders. Ensure commanders and senior leaders understand how to lead organizations in which human and machine cognition interact continuously. Address culture, judgment, accountability, and adaptation as core requirements.

Building Readiness at Scale: Why Commercial-Off-the-Shelf Solutions Matter

Every major defense modernization effort faces the same core constraint: time.

Autonomous capabilities are evolving faster than traditional acquisition, training, and workforce development processes were designed to support. New mission software, artificial intelligence models, autonomy engines, and human-machine interfaces are being updated on timelines measured in weeks or months rather than years. At the same time, military organizations must prepare increasingly diverse workforces to operate, supervise, maintain, and sustain these systems across multiple domains.

The challenge is not simply developing effective readiness solutions. It is developing them quickly enough to keep pace with technological change.

Historically, many defense training programs have relied heavily on custom-developed instructional systems that were designed around a single platform or program of record. While these bespoke solutions commonly satisfy immediate program requirements, they can be expensive to develop, difficult to maintain, and challenging to update as software-defined capabilities evolve. By the time a fully customized training system reaches maturity, the operational platform it supports may already have undergone significant changes.

Autonomous systems demand a different approach.

Rather than treating readiness as a one-time deliverable, organizations should adopt it as a continuously evolving capability supported by modular, interoperable, and commercially proven technologies.

Commercial-off-the-shelf (COTS) software provides an important foundation for this transformation.

Mature COTS platforms deliver capabilities that have already been developed, tested, and refined across multiple defense and industrial applications. Instead of investing years building common infrastructure from the ground up, programs can focus their resources on mission-specific content, operational workflows, and platform-unique behaviors. This approach lowers technical risk, accelerates deployment, and shortens the time required to deliver meaningful readiness capabilities to the field.

Equally important, COTS-based architectures are inherently more adaptable to software-defined systems.

As autonomous platforms evolve through new software releases, updated mission logic, or expanded operational

capabilities, the supporting readiness ecosystem must evolve as well. Modern COTS platforms are designed for iterative development, enabling organizations to update instructional content, simulation environments, digital twins, operational interfaces, and maintenance procedures without rebuilding the underlying framework. This continuous update model more closely aligns with the software development practices already common in autonomous systems engineering.

Because they are designed for broad applicability, commercial platforms generally support multiple programs, services, and mission areas using a common technology foundation. This creates opportunities for standardization across organizations while reducing lifecycle costs and simplifying long-term sustainment. Operators transitioning between autonomous platforms encounter familiar interaction models. Maintainers leverage common diagnostic workflows. Program offices benefit from reusable capabilities instead of isolated point solutions.

Perhaps most importantly, COTS solutions enable readiness to begin long before operational systems are widely available.

Through integrating digital twins, operationally representative human-machine interfaces, immersive simulation, and virtual maintenance environments within a common architecture, organizations can prepare operators, maintainers, mission supervisors, and support personnel while platforms are still under development. Workforce readiness no longer waits for hardware delivery. It progresses alongside engineering, testing, and operational unification.

This approach fundamentally changes the relationship between technology development and force development.

Rather than viewing readiness as the final phase of acquisition, organizations can generate operational proficiency throughout the program lifecycle, reducing risk during fielding while accelerating the transition from initial capability to sustained operational employment.

The benefits are particularly significant for autonomous programs, where software evolution is continuous and operational concepts continue to mature after deployment. A modern COTS-based readiness ecosystem allows organizations to incorporate new mission capabilities, updated autonomy behaviors, revised operating procedures, and emerging threats into training and sustainment environments at the same pace they are introduced into operational systems.

This represents more than an acquisition strategy.

It represents a new philosophy of readiness.

The objective is not simply to build training systems more efficiently.

The objective is to create a persistent readiness ecosystem that develops alongside autonomous capability across its lifecycle.

As military organizations continue their transition toward autonomous operations, commercially proven readiness technologies will increasingly become strategic enablers rather than supporting tools. They provide the scalable digital foundation needed to prepare the workforce behind autonomous systems while allowing government and industry to focus their resources on mission capability rather than rebuilding common infrastructure.

Ultimately, organizations that combine commercial innovation alongside mission-specific expertise will be best positioned to deliver Human-Machine Readiness at the speed the autonomous era requires.

Conclusion:

The Organizations That Learn Fastest Will Win

Every major military revolution creates a gap between those who possess new technology and those who understand how to use it well. The winners are rarely determined solely by technology. They are determined by adaptation.

The autonomous era will follow the same pattern. Autonomous systems will provide greater endurance, broader reach, faster decision cycles, improved situational

awareness, and new forms of operational scale. Those advantages are real, but they are not automatic. They become meaningful only when organizations develop the people, processes, sustainment models, interfaces, and readiness ecosystems needed to employ them effectively and turn them into operational advantage.

Human-Machine Readiness is therefore not a training issue in the narrow sense. It is a force development issue. It influences acquisition, doctrine, sustainment, command and control, leadership, operational planning, and mission assurance. It determines whether autonomous systems remain promising technologies or become trusted elements of combat power and operational effectiveness.

The decisive advantage will not belong to the organization that fields autonomous systems first. It will belong to the organization that learns how to integrate human judgment and machine-enabled capability faster than its competitors and convert that integration into better outcomes.

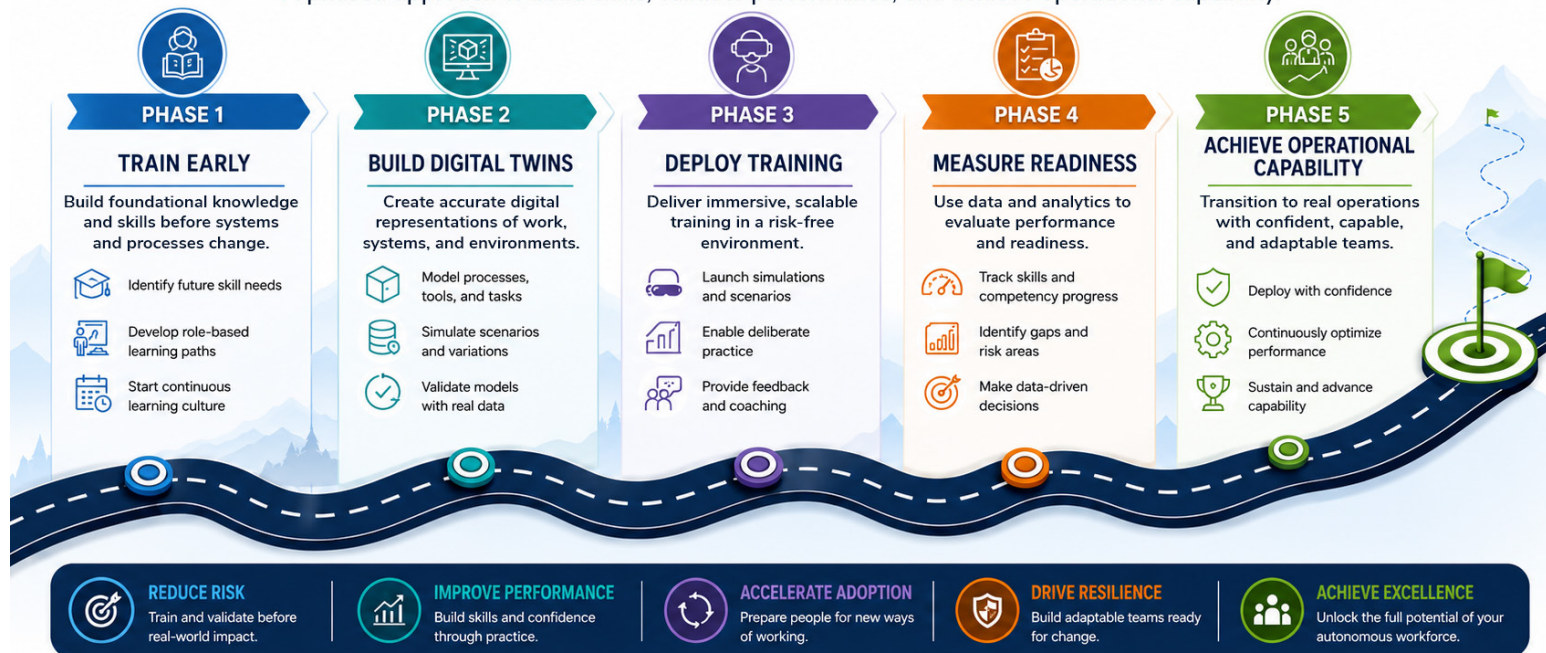
Autonomy will change the battlefield.

Human-Machine Readiness will decide who benefits from that change.

To secure that advantage, develop Human-Machine Readiness now.

ROADMAP TO AUTONOMOUS WORKFORCE READINESS

A phased approach to build skills, validate performance, and achieve operational capability.



**PREPARE TODAY.
PROTECT TOMORROW.
LEAD BEYOND.**

ABOUT THE AUTHORS



DAWN HAULTER

Director of Business Development & Marketing at The DiSTI Corporation. Dawn is a specialist in driving strategic growth across defense, aerospace, automotive, and space markets through advanced modeling and simulation solutions. Focused on connecting mission-critical challenges with immersive training, digital twin technologies, and safety-critical HMI platforms that accelerate readiness and reduce risk.



TOM DOW

Senior Instructional Systems Designer at The DiSTI Corporation. Tom is a retired U.S. Army Command Sergeant Major with nearly three decades of distinguished military service, including four combat deployments with the 82nd Airborne Division and 101st Airborne Division. As a Senior Enlisted Advisor for the U.S. Army PEO STRI, he helped advance training and readiness capabilities across the force.