MANTECH™
ALWAYS ADVANCING

Autonomous Cyber Readiness Evaluator (ACRE)

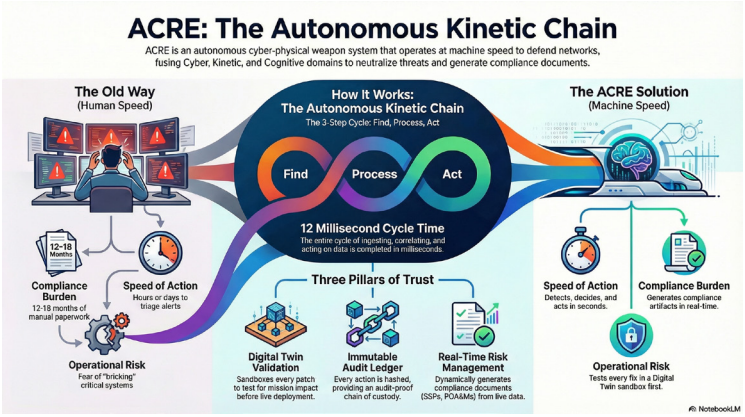
Cognitive Dominance. Machine Speed. Continuous Authority.

Imagine a world where Risk Management Framework (RMF) processes are automated, controls are continuously monitored, and a network's Authority to Operate (ATO) is earned and operationally relevant every single day. A world where cyber threats are evaluated and fought at machine speed. Where Command, Compliance, and Analytics fuse into a single weapon system seamlessly enabling warfighting, operational security and AI driven analysis. **Welcome to ACRE**.

ACRE IS NOT A DASHBOARD. IT IS AN AUTONOMOUS OPERATOR FOR OPERATIONAL CYBERSECURITY.

While legacy tools visualize problems, ACRE solves them. Powered by Neuro-Symbolic AI, ACRE executes a continuous OODA Loop (Observe, Orient, Decide, Act) to defend the DODIN at machine speed and neutralize threats in seconds—without human intervention—while generating the cryptographic proof required by auditors.

ACRE integrates existing tools and brings capabilities together to bridge the gap from legacy RMF to AI-assisted continuous ATO while supporting the Authorizing Official's statutory role.



The system's decisioning follows an OODA loop (Observe, Orient, Decide, Act) to execute cyber effects, logging every action in real time. When critical risks are detected, ACRE immediately alerts users and reflects associated compliance degradation.

Core Philosophy:

- **Speed:** Move from human-speed response (hours/days) to machine-speed response (seconds).
- **Safety:** Use "Digital Twin" validation to ensure automated actions never break the mission.
- **Trust:** Use cryptographic ledgers to prove exactly what the AI did and why.

ACRE aligns with the DoW CIO's Cybersecurity Risk Management Construct and DoN CIO's ISV2.0.

Revolutionizing Cyber Readiness with ACRE

Integrating AI/ML into the Risk Assessment and Continuous ATO processes fundamentally changes how we approach cybersecurity. By examining a system's operational functionality, alongside component data, connections, and authoritative vulnerability data, ACRE enables powerful predictive analysis for cyber readiness and operational risk assessment. It leverages Verified Sources of Truth and system data to pinpoint critical and high-risk vulnerabilities, significantly enhancing efficiency.

The ACRE solution significantly increases cyber readiness, expedites secure capabilities, orchestrates, and **delivers operational visualization of risk to provide the Commander and Warfighters decisive advantage**.

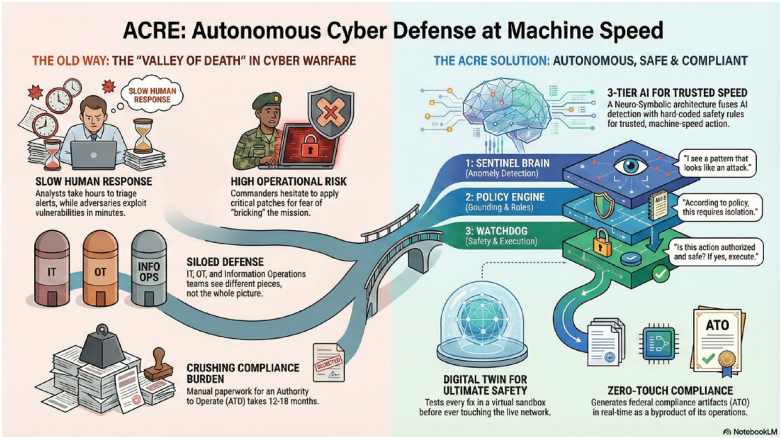
For the Commander: You get Decision Advantage. You can see the future risk (Predictive Forecast) and operating tactical and non-tactical networks with confidence, knowing security has been verified.

For the Authorizing Official (AO): You get Continuous Authority. You no longer have to trust a 6-month-old PDF. You can see the live compliance status and cryptographic proof of every patch.

For the Analyst: You get Machine Speed. The AI handles the noise and the routine fixes, allowing you to focus on the complex, high-value threats.

ACRE is the implementation vehicle for the DoD's "AI Acceleration Strategy." It turns the strategy memo into a deployed, secure, and ready reality.

Rather than manual checklists and passive dashboards that require intensive (and expensive) manhours to verify compliance, ACRE is an Autonomous Cyber-Physical Weapon System designed to operate at machine speed.



Accelerating Cyber Readiness and Enhancing Security Posture

The blend of automation and AI not only boosts efficiency but also sharpens the focus on real-time vulnerability and exploitation analysis, ultimately strengthening overall system security and ensuring continuous compliance and robust risk management in real-time. ACRE is scalable and robust, providing both enterprise and tactical capability.

Commands can instantaneously view system risk and take action to remediate threats. In addition, ACRE provides a System of Systems view to bring together the entire battlespace risk and vulnerabilities into a centralized location with the capability to drill-down into systems or components and potential mission impacts.

The next generation version will extend ACRE from compliance into active Warfighting support, reducing risk while expediting capabilities to the Warfighter. It will ingest operational and environmental data, as well as real time intelligence data to provide real-time operational risk and remediation actions while in theatre and enabling Commander decision-making, even in a denied or degraded communication environment.

USE CASE

Bridging the gap between Legacy RMF and AI-Assisted Active Defense.

We don't just report risk; we hunt it, validate it, and fix it—while automatically generating the cryptographic proof required by Authorizing Officials (AOs).

The current ATO process for new systems is lengthy, typically 12 to 18 months due to extensive manual data entry. By integrating AI/ML into the Risk Management Framework (RMF), we significantly reduced the manual workload and enhanced the focus on a system's operational cybersecurity posture. This integration enabled near real-time risk assessments, aligning with the continuous monitoring/continuous ATO process. AI boosted efficiency by identifying and assessing up to 450 system controls, depending on classification. While programs typically allocate 15 days for manual control assessment—reading and evaluating compliance and implementation—we used AI to leverage Verified Sources of Truth to streamline these assessments.

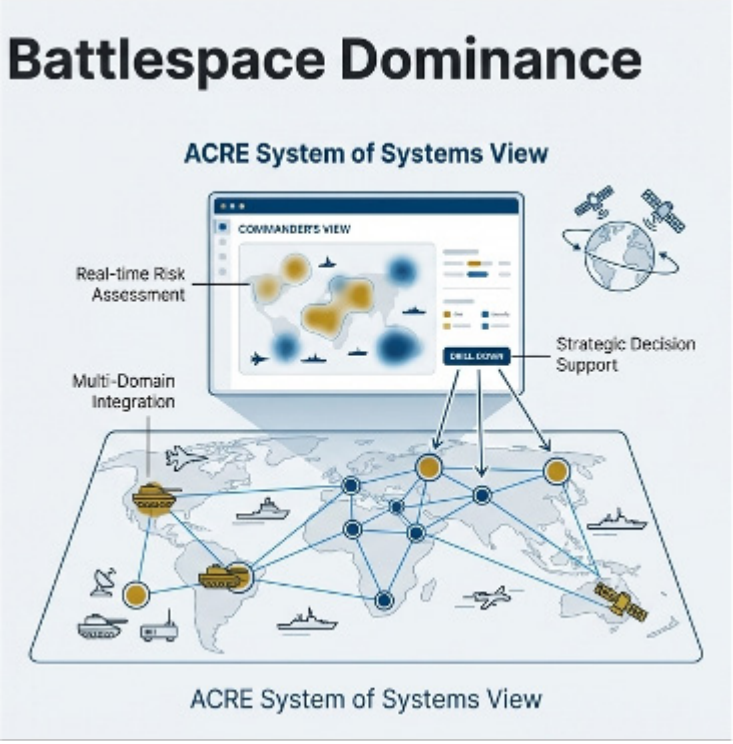
Total Savings

A conservative estimate projects a minimum **50% reduction in manual effort, saving at least 60 hours per full-time equivalent (FTE) on a single RMF task**, leading to more thorough risk analysis and real-time operationally-focused cybersecurity readiness across all systems.

Using AI/ML integration to end antiquated Risk Management Framework and automate the ATO process and operationalize risk:

We don't just report risk; we hunt it, validate it, and fix it—while automatically generating the cryptographic proof required by Authorizing Officials (AOs).

- **Automating Risk Assessment:** AI/ML algorithms can automate risk assessments, identifying vulnerabilities and threats more efficiently than manual processes.
- **Proactive Security Measures:** AI/ML can suggest and implement proactive security measures based on predictive analytics, strengthening the overall security posture of the system
- **Cyber Physical Simulation Twinning Network (CPSTN).** While "predictive analytics" are great, the critical differentiator is our "Test-Before-Deploy" safety mechanism where fixes are validated on a digital twin to prevent mission disruption. This is crucial for Commander confidence in automated responses.
- **"Thwart" & "Secure" Pillars:** Align with the NIST IR 8596 framework by "Thwarting Adversarial AI" (using guardrails to stop prompt injections) and "Securing the AI Supply Chain" (using the AIBOM to verify model integrity).
- **Continuous Monitoring:** AI/ML enables continuous monitoring of security metrics and alerts, ensuring real-time visibility into the system's security posture.



In business more than 57 years, MANTECH excels in cognitive cyber, AI, data collection & analytics, enterprise IT, systems engineering and software application development solutions that support national and homeland security.

LEARN MORE - MANTECH.com or ai@MANTECH.com
Eugene Bailey, Technical Director | eugene.bailey@MANTECH.com