

Securing Autonomous Operations

A Practical Framework for Trusted Information in Autonomous Defense Missions

Autonomous capability adoption is accelerating globally, with rapid reforms and investment across the United States, United Kingdom, and wider Five Eyes community. New policy, funding, and acquisitions are driving the rapid delivery of uncrewed platforms, autonomous Intelligence, Surveillance and Reconnaissance (ISR), AI enabled decision support, and joint Command and control (C2) systems. These systems promise faster decisions, expanded reach, and reduced risk to personnel.

Modern missions increasingly rely on autonomous systems to operate across services, allies, classifications, and domains. Operational tempo continues to rise, and decisions that once took minutes or hours now need to be made in just seconds. Coalition environments add complexity, and connected platforms expand exposure increasing operational risk and vulnerability to disruption or compromise. Mission leaders must navigate this shift while maintaining safety, alignment, and mission confidence.

Trusted information infrastructure is now essential for delivering autonomous capability at mission speed.

The Mission Reality

Autonomous missions operate in a data environment that span:

- Classified and unclassified environments
- Across land, sea, air, space, and cyber
- Coalition and partner ecosystems
- Platforms, operators, and AI systems
- Distributed teams operating across geographies and time zones

Modern operations demand speed and trust. Decisions happen in seconds. Teams depend on current, validated information to act confidently. Without assurance, every connection becomes a risk.



Why Securing Autonomous Systems Matters Now

Introduction

Autonomous systems depend on mission data that must be current, validated, and available when required. When information is delayed, incomplete, or unverifiable, autonomous behavior becomes unpredictable, and operators lose confidence in system outputs.

Uncrewed platforms, autonomous ISR, edge AI, and joint C2 systems all rely on information that moves across domains, classifications, and partners. Legacy movement controls, inconsistent validation, and fragmented data flows create friction that slows autonomous operations and increases risk. Mission leaders need trusted information that helps support safe, confident, and effective autonomous behavior across environments.

As autonomous systems become central to defense operations, securing their information flows is critical. Failure to do so exposes missions to disruption, data compromise, and loss of operational confidence.

This guide gives mission leaders a clear framework to:

- **Navigate** the complexity of autonomous operations across land, sea, air, space, and cyber
- **Identify** gaps that limit confidence in data
- **Enhance** the reliability of AI and autonomous systems by securing the data that drives their decisions
- **Identify** friction points in information flow that slow decision-making and erode mission confidence

Building trusted information infrastructure is the first step toward operational advantage. Mission speed and confidence start with securing your data.

The Mission Tempo Challenge in Autonomous Operations	04
The Autonomous Mission Reality	05
Autonomous Trust Framework	06
Protecting Mission Data Through Hardware-Level Separation	07
Trusted Information Sharing Across Domains	08
Real-Time Access to Validated Mission Data	09
Enabling Rapid Integration of Autonomous Systems	10
Reducing Insider Risk in Autonomous System Environments	11
What Trusted Information Looks Like in Practice	12
Executive Trusted Data Checklist	12
Partnering to Protect the Autonomous Mission	13
From Framework to Action	13

The Mission Tempo Challenge in Autonomous Operations

Mission leaders must enable autonomous systems to operate at the speed required for modern operations. However, while the systems move fast, the information behind them often doesn't.

Mission data may arrive late, incomplete, or without validation. Delayed or unverifiable information undermines autonomous operations because it leads to unpredictable system behavior and erodes operator confidence, ultimately creating a tempo mismatch that introduces operational risk long before an adversary is involved.

The Risk of Not Securing These Operations is Significant

- Misclassification of targets
- Navigation into threat zones
- Failure to execute critical tasks
- Loss of operator confidence
- Manual workarounds slowing mission tempo
- Undermined coalition operations



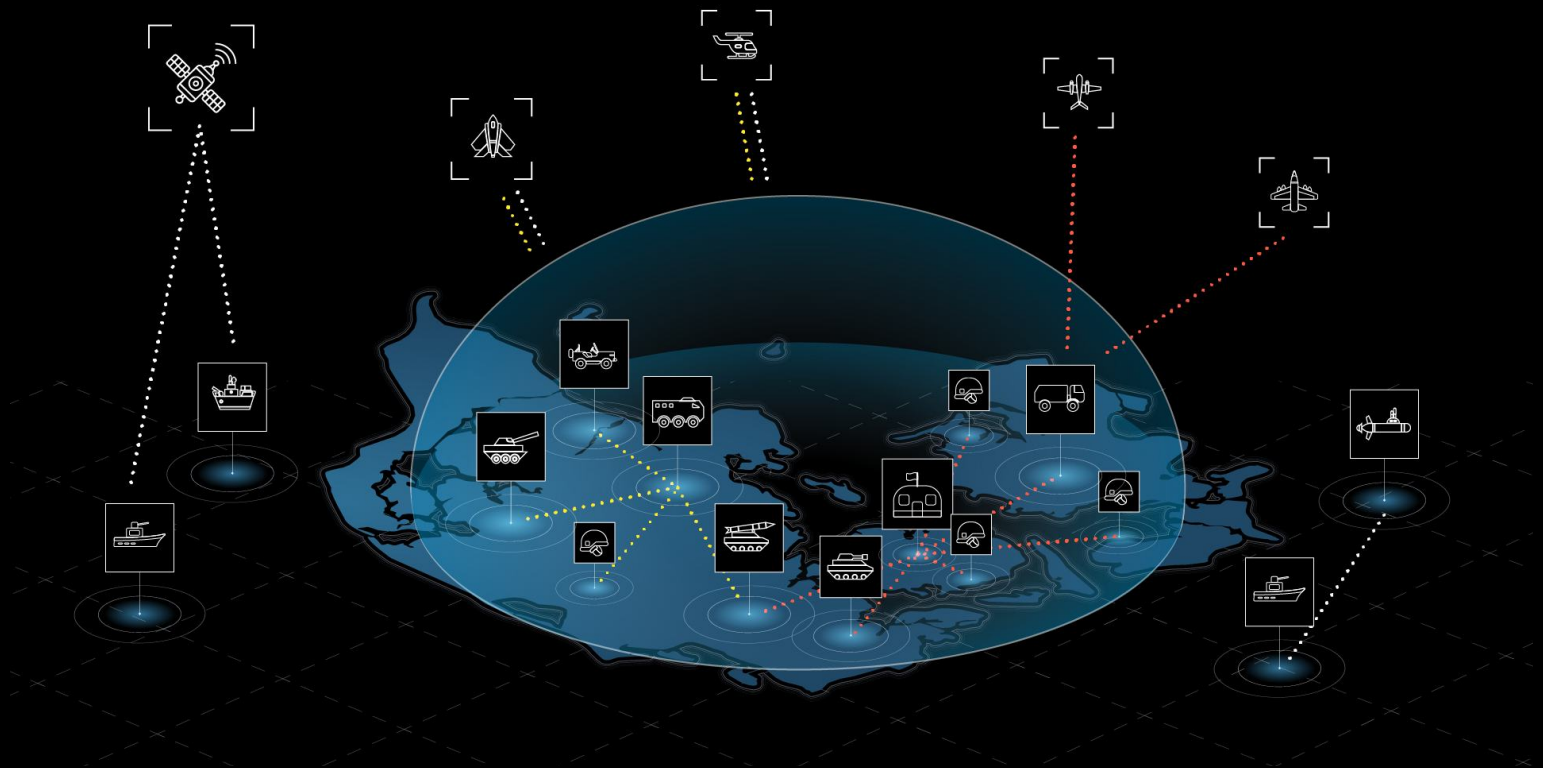
The Autonomous Mission Reality

Autonomous missions will fail without secure, timely data. Investments in unmanned systems are futile if information flows are not protected. Mission leaders operate in environments where autonomous systems must make continuous decisions based on dynamic, multi-domain information.

Autonomous missions depend on telemetry, ISR payloads, sensor data, and mission context that arrive at high volume and high speed. AI systems analyze and interpret this information, while operators and coalition partners rely on it to make decisions.

Information rarely arrives in a predictable way. It moves across domains, classifications, and networks with different validation requirements and trust levels. Autonomous systems must act even when the information picture is incomplete or changing.

Defense organizations must field autonomous capability quickly, integrate modern Commercial Off-The-Shelf (COTS) technologies, and operate across coalition networks not originally designed for autonomous systems. Connected platforms expand exposure, and legacy infrastructure struggles to support the tempo required for autonomous operations.



Autonomous Trust Framework

Core Pillars of Autonomous Trust

Autonomous missions rely on trusted information that help protect mission critical data, move it safely across domains, and keep it aligned with fast-changing operational conditions.

These pillars work together to support reliable autonomous systems, strengthen mission confidence, and help maintain tempo across complex environments.

1. DATA PROTECTION

Secure mission data, keeping information locked down in tough environments

2. TRUSTED SHARING

Breaks silos to deliver a unified picture, connecting partners instantly

3. REAL-TIME DATA

Data that remains trustworthy across its entire lifecycle

4. RAPID INTEGRATION

Deploying new technology fast, ensuring platforms are working together to keep mission tempo high

5. INSIDER RISK

Catch risky behavior early and protect sensitive data, tightening controls everywhere

1.

Protecting Mission Data Through Hardware-Level Separation

The Operational Challenge

Autonomous systems are often deployed in environments where adversaries actively search for vulnerabilities. Software-only defenses are frequently targeted, and even a minor flaw can be exploited to access mission-critical data.

This risk is real and immediate. Compromised data can result in loss of operational control, breakdown of coalition trust, and mission failure. The challenge is ensuring mission data remains secure, even if software defenses are breached.

What Changes With Hardware-Level Separation

Mission data moves safely and consistently across domains, classifications, and partner networks. Autonomous systems receive the information they need without delay, helping maintain alignment across joint and coalition operations.

Why It Matters

Autonomous platforms rely on shared situational awareness. When partners operate from different versions of the truth, autonomous behavior becomes misaligned and mission confidence erodes. Trusted sharing helps maintain coherence across mission environments.

How It Works

Trusted sharing applies consistent movement and validation controls across domains, enabling mission data to flow safely between networks. These protections help maintain data integrity, reduce friction, and support autonomous systems operating in multi-domain and coalition environments.

Example Scenario

An autonomous ISR platform processes sensor data and feeds it into onboard AI models. Modern adversaries increasingly target software-based security appliances, attempting to manipulate inputs or bypass defenses.

When protection relies solely on complex software stacks, a single exploited weakness can expose mission-critical data and disrupt autonomous operations.



2.

Trusted Information Sharing Across Domains

The Operational Challenge

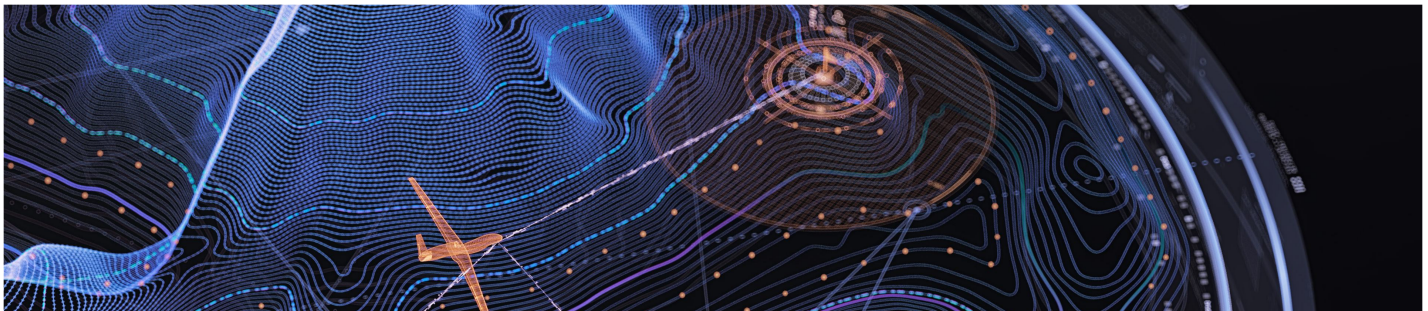
Autonomous systems and mission leaders must operate across a landscape that includes multiple domains, security classifications, and coalition partners. In reality, information can often be fragmented, delayed, or restricted as it moves between these domains. This can lead to inconsistent operational pictures, misaligned decisions, and gaps in situational awareness. When partners and systems rely on different versions of the truth, autonomous behavior becomes unpredictable, and mission confidence suffers. The challenge is to ensure that information flows securely and consistently, so every participant operates from a shared, accurate understanding.

What Changes With Trusted Information Sharing

Mission data moves safely and consistently across domains, classifications, and partner networks. Autonomous systems and mission leaders receive the information they need without delay, helping maintain alignment and coherence across joint and coalition operations.

Why It Matters

Shared situational awareness is essential for autonomous platforms and mission leaders. When partners operate from different versions of the truth, autonomous behavior becomes misaligned, and mission confidence erodes. Trusted information sharing helps maintain coherence across mission environments and supports effective decision-making.



How It Works

Trusted information sharing applies consistent movement and validation controls across domains. These protections ensure that mission data flows securely between networks, maintains integrity, reduces friction, and supports autonomous systems operating in multi-domain and coalition environments.

Example Scenario

A coalition operation involves autonomous air, ground, and maritime platforms from several nations. Each platform collects and processes mission data, but differences in classification, network protocols, and sharing policies prevent seamless exchange. As a result, some partners operate with outdated or incomplete information, leading to conflicting actions and reduced mission effectiveness.



3.

Real-Time Access to Validated Mission Data

The Operational Challenge

Autonomous platforms must make decisions at machine speed, but mission data can risk being delayed, incomplete, or inconsistent. These gaps can cause AI systems to misclassify targets, generate unreliable recommendations, and force operators to intervene.

The result is slower operational tempo and diminished capability. Ensuring every decision is based on the most current and trustworthy data, especially when the stakes are high can be challenging.

What Changes With Real-Time Data

Mission data is continuously updated, validated, and aligned with current conditions. Autonomous systems receive timely, trustworthy information that supports accurate assessments and reduces the need for operator correction.

Why It Matters

Autonomous systems operate at machine speed. When data lags, decisions become increasingly risky. Real-time validated data helps maintain tempo, accuracy, and mission confidence.

Example Scenario

An autonomous air platform uses edge AI to classify objects and recommend actions. If mission data is even slightly out of date, the AI system may misclassify targets or produce unreliable recommendations. Operators intervene more often, slowing operational tempo and reducing capability value.

How It Works

Real-time data movement validates and updates mission information as it flows across platforms, edge nodes, and tactical networks. These protections help remove corrupted inputs, maintain consistency, and support autonomous systems acting during time-sensitive operations.

4.

Enabling Rapid Integration of Autonomous Systems

The Operational Challenge

Defense organizations need to adopt new technologies quickly to maintain operational advantage. Legacy systems and custom architectures create bottlenecks, making integration slow and costly.

This delay can result in missed opportunities, reduced agility, and increased friction across programs.

The challenge is to enable rapid adoption of modern capabilities without waiting for lengthy engineering cycles.

What Changes With Rapid Integration

Trusted information infrastructure helps integrate modern COTS technologies quickly and safely. New sensors, platforms, and AI systems can be fielded without waiting for long custom builds or complex re-engineering

Why It Matters

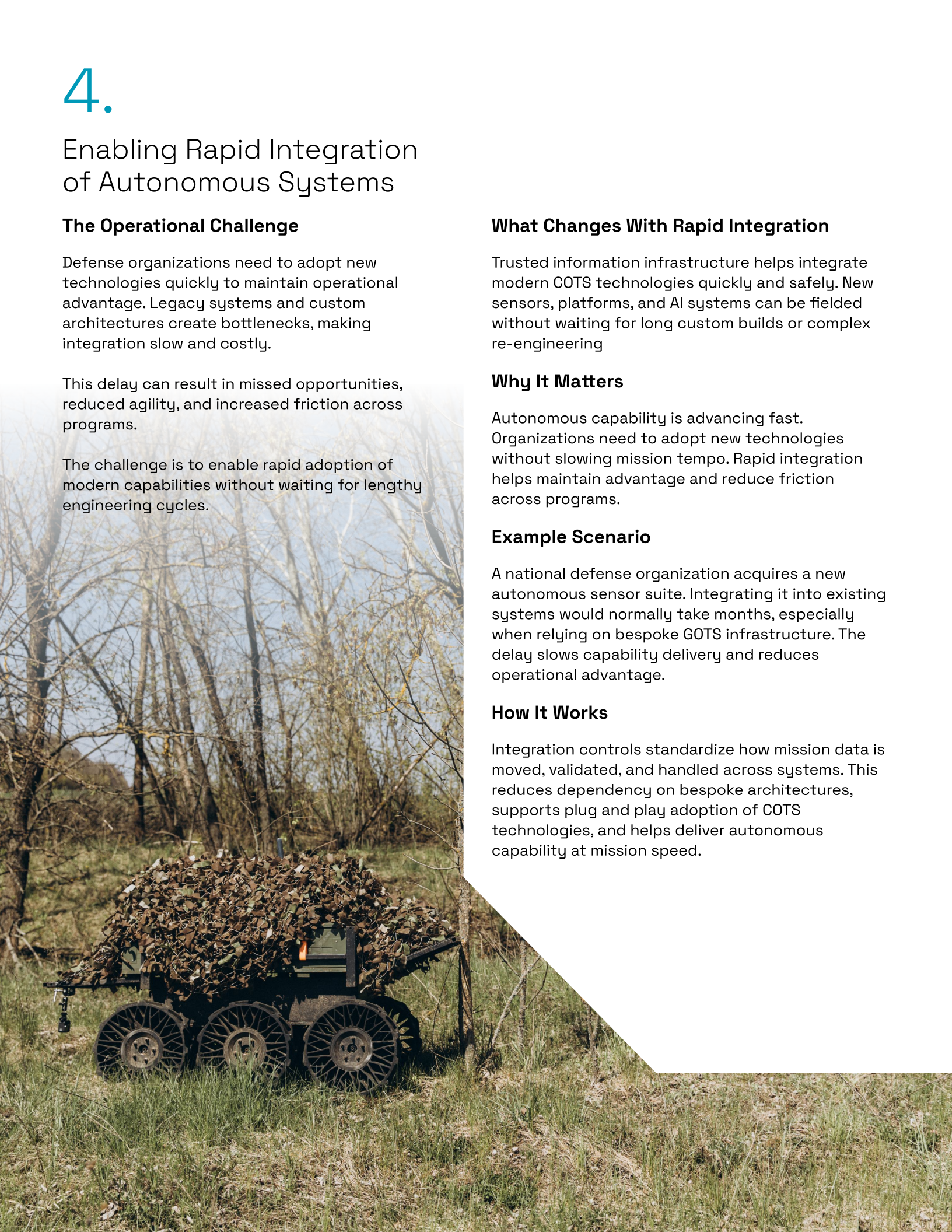
Autonomous capability is advancing fast. Organizations need to adopt new technologies without slowing mission tempo. Rapid integration helps maintain advantage and reduce friction across programs.

Example Scenario

A national defense organization acquires a new autonomous sensor suite. Integrating it into existing systems would normally take months, especially when relying on bespoke GOTS infrastructure. The delay slows capability delivery and reduces operational advantage.

How It Works

Integration controls standardize how mission data is moved, validated, and handled across systems. This reduces dependency on bespoke architectures, supports plug and play adoption of COTS technologies, and helps deliver autonomous capability at mission speed.



5.

Reducing Insider Risk in Autonomous System Environments

The Operational Challenge

Sensitive mission data is vulnerable to insider threats, whether accidental or intentional. Privileged access can be misused, and subtle behavioral anomalies can often go undetected until damage is done.

A single insider action can compromise data integrity, disrupt operations, or expose critical information.

What Changes With Insider Risk Protections

Trusted information infrastructure helps integrate modern COTS technologies quickly and safely. New sensors, platforms, and AI systems can be fielded without waiting for long custom builds or complex re engineering

Why It Matters

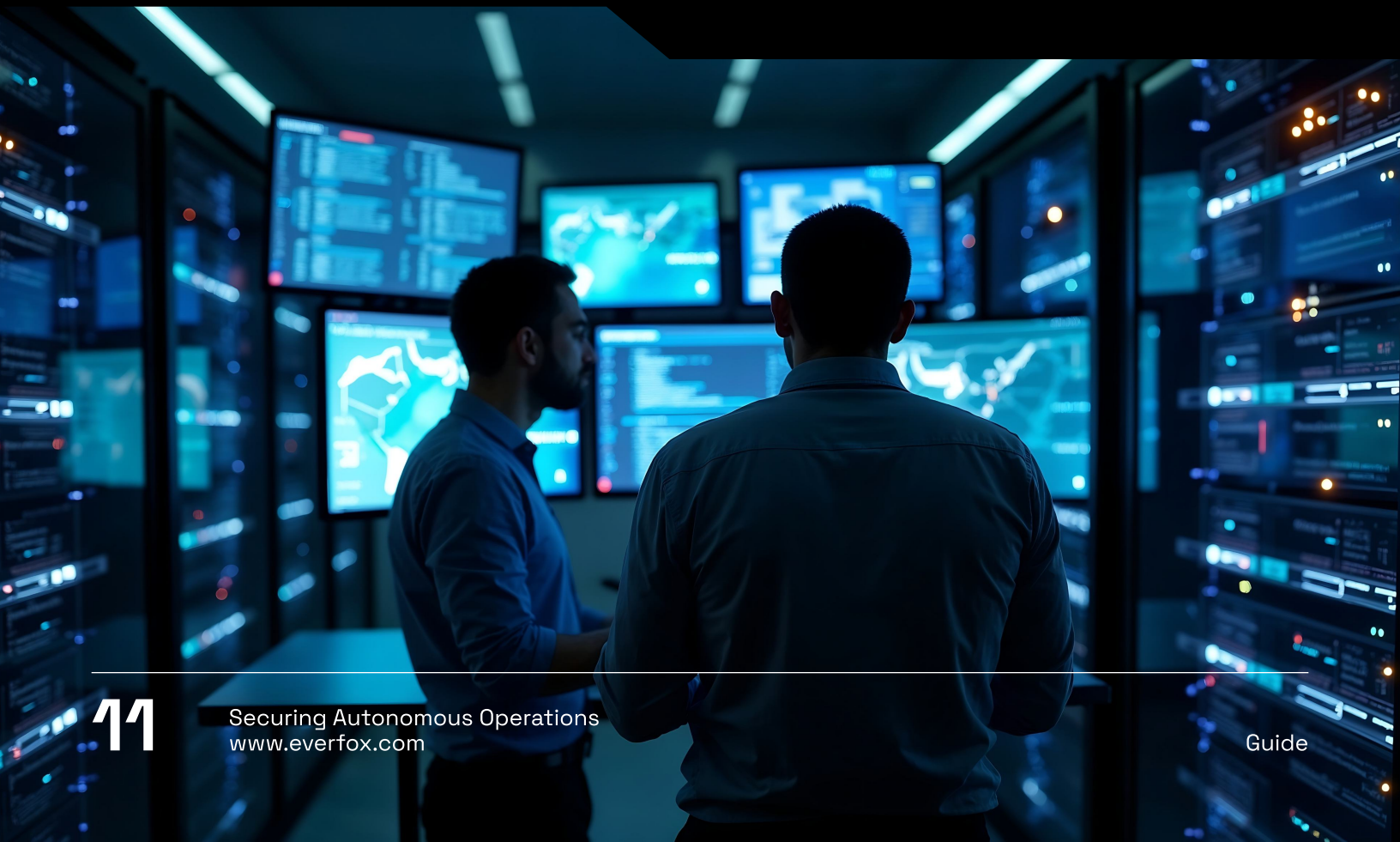
Autonomous systems rely on sensitive mission data. Insider activity can compromise integrity, disrupt operations, or expose critical information. Reducing insider risk helps maintain mission assurance.

Example Scenario

An operator with elevated privileges accesses mission data used by an autonomous ground system. Unusual behavior goes unnoticed, creating a hidden vulnerability that could disrupt autonomous operations or expose sensitive information.

How It Works

Insider risk protections monitor privileged access, analyze behavioral patterns, and apply controls that restrict suspicious activity. These safeguards operate across autonomous platforms and mission systems without slowing operational tempo.



What Trusted Information Looks Like in Practice

Trusted information architectures produce clear operational advantages:

- Information moves quickly and securely across domains, classifications, and partner networks
- Consistent controls ensure data integrity and reliability, regardless of where or how it is accessed
- Autonomous platforms and mission leaders operate with a unified, accurate operational picture
- Dependence on manual processes and workarounds is reduced, enabling faster, more confident decision-making

When trust is built into every stage of the data pipeline, autonomous systems and mission leaders receive timely information that supports situational awareness and decision dominance.

This foundation helps teams act with speed and confidence, adapting to emerging threats and operational demands.



53%

organizations in government, defense and critical services still rely on **manual data transfer**, including paper, to move sensitive information.¹

Executive Trusted Data Checklist

This checklist helps leaders evaluate how effectively their organization enables secure and consistent information sharing for autonomous and coalition operations. It translates complex technical and operational requirements into clear points for leadership discussions.

Use the checklist to evaluate

MISSION TEMPO & TIME TO DECISION

- ☐ Have you mapped mission-critical information flows across autonomous platforms?
- ☐ Are you Identifying latency and validation bottlenecks?
- ☐ Are high-consequence mission decisions prioritized?

CAPABILITY ADOPTION & INTEGRATION

- ☐ Are autonomy programs aligned with rapid acquisition mandates?
- ☐ Is the adoption of modern COTS technologies prioritized?
- ☐ Are classification, validation, and movement controls modernized?

COALITION & OPERATIONAL

- ☐ Is consistent information maintained across domains, classifications, and partners?
- ☐ Are insider risk signals monitored across systems and operators?
- ☐ Is accountability for data protection reinforced at the leadership level?

Partnering to Protect the Autonomous Mission

From Framework to Action

Trusted information infrastructure supports autonomous capability at mission speed. It helps maintain validated mission data, strengthens coalition interoperability, and accelerates capability adoption.

Organizations can begin by examining:

- How autonomous workflows operate across environments
- Where information friction introduces delays or risk
- Whether identity and privilege models reflect autonomous mission roles
- How insider risk signals are monitored across systems
- Whether architecture can sustain autonomous operations during disruption

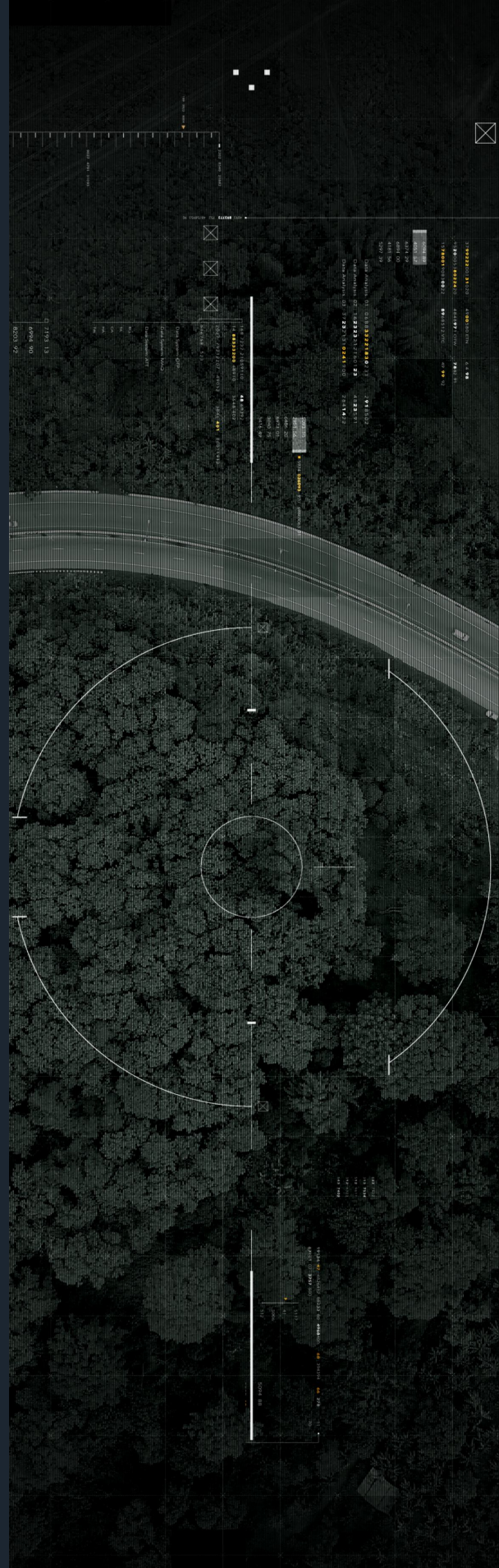
Autonomous systems are transforming defense operations. Trusted information helps enable their success.

Everfox provides the trusted information platform relied on by autonomous and coalition missions. Our solutions support real-time, Cross Domain movement of mission data so commanders, operators, and autonomous systems act with confidence at mission speed. Everfox strengthens mission assurance across modern autonomous and coalition operations.

If you are ready to advance your mission's security and operational effectiveness, take the next step. Schedule a consultation with Everfox to review your current capabilities, identify areas for improvement, and explore solutions designed for secure Cross Domain operations.

Empower your teams to operate securely and confidently wherever the mission takes them. Mission-ready security architectures are within reach.

Let's partner to protect your autonomous mission.





About Everfox

Everfox secures the data, networks, and people that protect national security and global defense, empowering agencies to operate confidently in high-consequence environments, all while realizing efficiencies in cost, capabilities and productivity.

Built for mission-critical operations, Everfox empowers governments, allies, and enterprises to collaborate securely, operate confidently, and act at mission speed.

Unlike traditional cybersecurity vendors, we don't just defend systems, we defend missions. Our purpose is clear, protect the data that protects the people that protect us.

Sources

¹ CYBER360 Report, 2026, Defending the Digital Battlespace, <https://info.everfox.com/cyber360-defending-the-digital-battlespace>

Learn More

www.everfox.com

© Everfox 2026