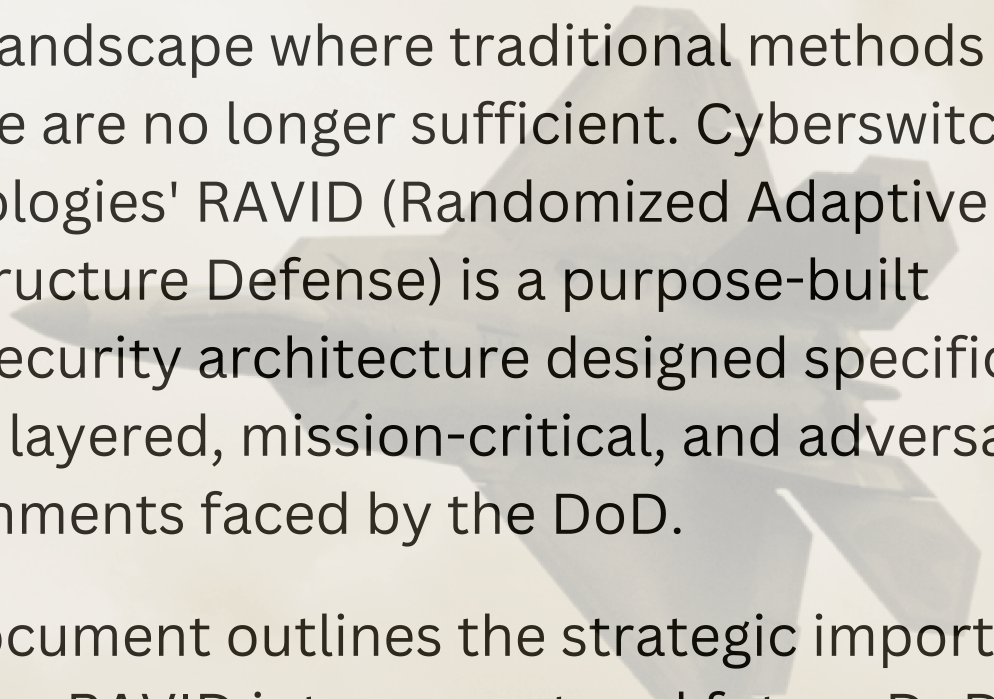
CYBERSWITCH TECHNOLOGIES

RAVID AND THE FUTURE OF DEFENSE-GRADE CYBERSECURITY

www.cyberswitchtech.com

Executive Summary



The Department of Defense (DoD) operates under a cyber landscape where traditional methods of network defense are no longer sufficient. Cyberswitch Technologies' RAVID (Randomized Adaptive Virtual Infrastructure Defense) is a purpose-built cybersecurity architecture designed specifically for the kind of layered, mission-critical, and adversary-rich environments faced by the DoD.

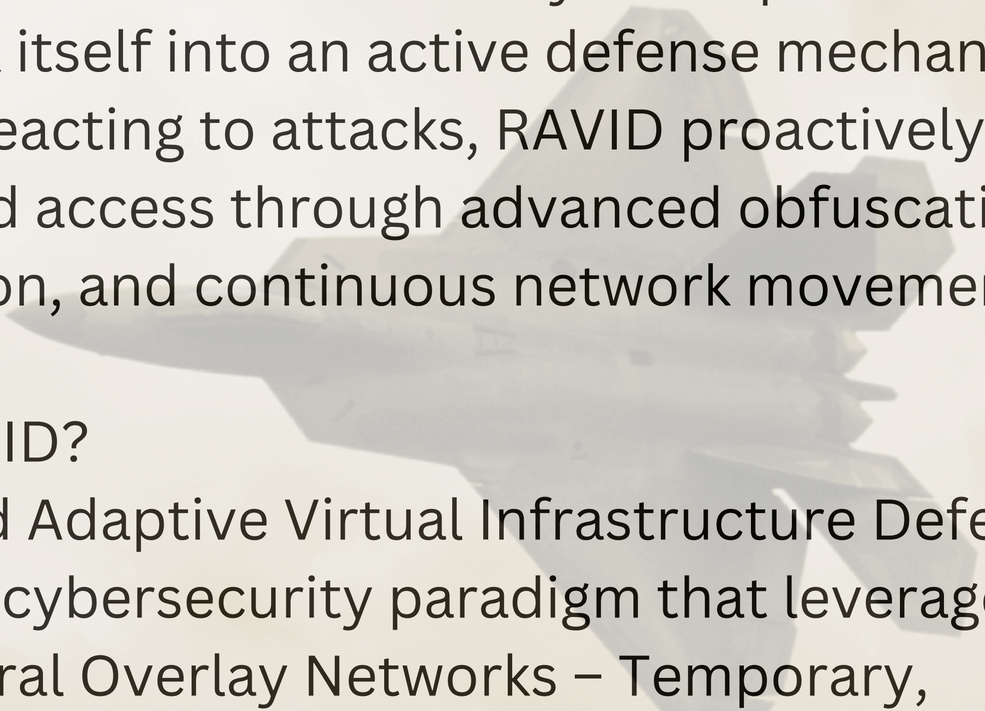
This document outlines the strategic importance of adopting RAVID into current and future DoD cybersecurity frameworks, complementing the Zero Trust model and aligning with DISA’s mission to safeguard defense networks.

Introduction: The Cyber War Has Evolved

Traditional perimeter defenses, VPNs, and static network architectures are fundamentally flawed in modern information warfare. Despite investments in next-gen firewalls, SIEMs, and endpoint detection systems, the adversary still gains access through predictable infrastructure and static trust models. The result? Breaches continue across DoD and DIB partners.

It's time for an evolution.

RAVID introduces a revolutionary concept: transform the network itself into an active defense mechanism. Instead of reacting to attacks, RAVID proactively denies visibility and access through advanced obfuscation, segmentation, and continuous network movement.

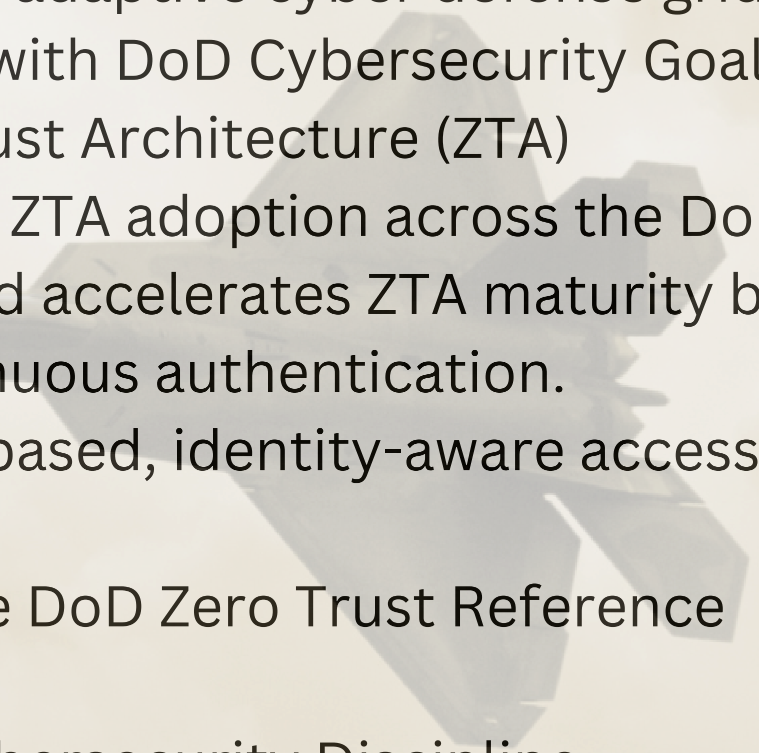


What is RAVID?

Randomized Adaptive Virtual Infrastructure Defense (RAVID) is a cybersecurity paradigm that leverages:

- Ephemeral Overlay Networks – Temporary, constantly rotating network paths that prevent attackers from discovering, profiling, or targeting infrastructure.
- Zero Trust Access Controls – Enforces identity- and behavior-based access validation at every layer, never trusting by default.
- Behavioral AI Monitoring – Continuously assesses user, device, and network behavior to detect anomalies in real time.
- Micro and Macro Segmentation – Isolates critical assets and compartments systems to prevent lateral movement post-compromise.

Together, these technologies reduce attack surfaces by up to 95%, turning static infrastructure into a dynamic, invisible, and highly adaptive cyber defense grid.



RAVID's Alignment with DoD Cybersecurity Goals

1. Supports Zero Trust Architecture (ZTA)

DISA has mandated ZTA adoption across the DoD. RAVID enhances and accelerates ZTA maturity by:

- Enforcing continuous authentication.
- Utilizing policy-based, identity-aware access to assets.
- Aligning with the DoD Zero Trust Reference Architecture.

2. Complements Cybersecurity Discipline Implementation Plan

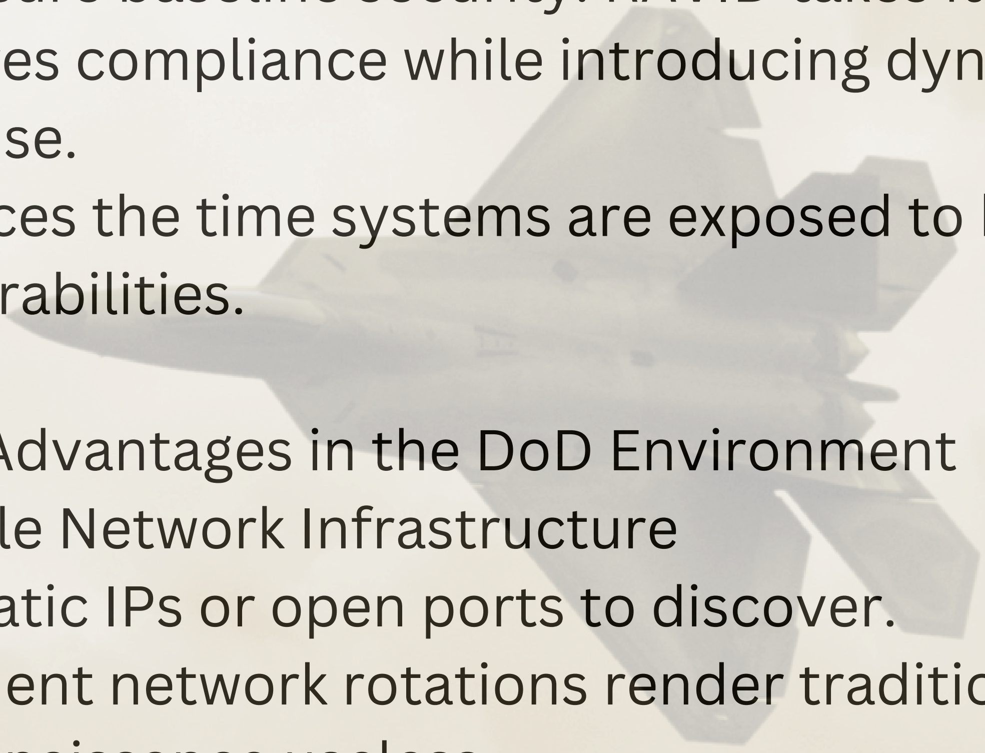
RAVID operationalizes key pillars of the Cybersecurity Discipline Implementation Plan:

- Hardened Infrastructure: Randomized and adaptive networks.
- Continuous Monitoring: Behavioral and AI-powered surveillance.
- Incident Response: Real-time detection and network-level mitigation.

3. Surpasses Static Security Technical Implementation Guides (STIGs)

STIGs ensure baseline security. RAVID takes it further:

- Ensures compliance while introducing dynamic defense.
- Reduces the time systems are exposed to known vulnerabilities.



Tactical Advantages in the DoD Environment

A. Invisible Network Infrastructure

- No static IPs or open ports to discover.
- Frequent network rotations render traditional reconnaissance useless.
- Attackers are forced to target what they cannot see—resulting in higher failure rates.

B. Resilience for Operational Technology (OT) and Weapon Systems

- Works with legacy and classified systems.
- Introduces obfuscation without latency burdens.
- Compatible with SCADA and ICS platforms.

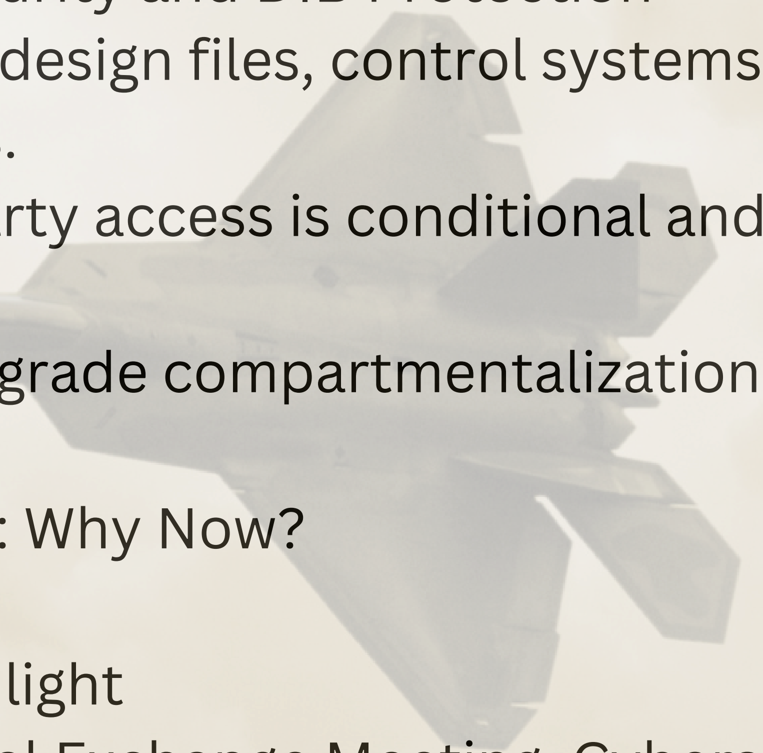
C. Secure Multi-Domain Operations (MDO)

- Enables secure data transmission across joint, coalition, and allied environments.
- Adapts network overlays based on the domain and threat posture.

- Provides secure overlays in contested and degraded environments.

D. Supply Chain Security and DIB Protection

- Limits access to design files, control systems, and sensitive comms.
- Ensures third-party access is conditional and monitored.
- Supports TSSCI-grade compartmentalization.



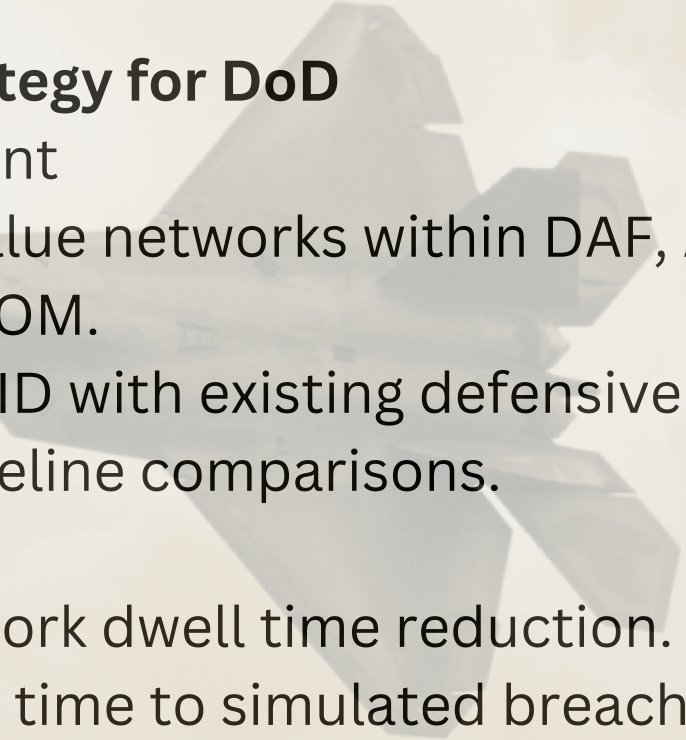
Case for Integration: Why Now?

DISA TEM 2025 Highlight

At the DISA Technical Exchange Meeting, Cyberswitch Technologies demonstrated how RAVID prevents DDoS, ransomware, and data exfiltration attacks before they occur by eliminating traditional vectors of entry. The concept of moving target defense was repeatedly emphasized as the next phase of cyber operations. RAVID embodies this doctrine.

Reinforcing JADC2 and ABMS

Joint All-Domain Command and Control (JADC2) and the Air Force’s Advanced Battle Management System (ABMS) demand secure, fast, and trusted connectivity. RAVID overlays provide secure interconnects between assets, commands, and allies without increasing attack surfaces.

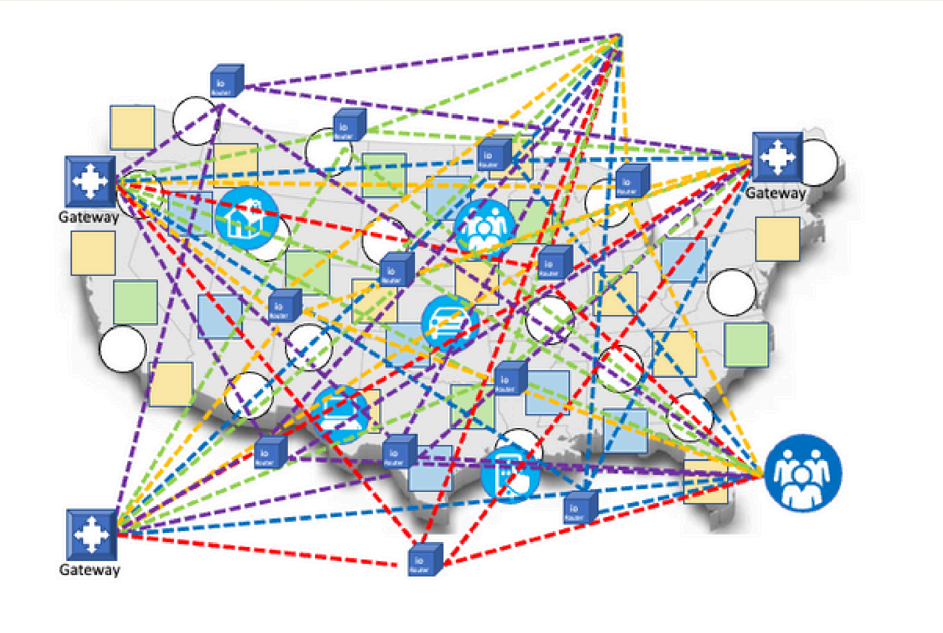


Deployment Strategy for DoD

1. Pilot Deployment
    - Select high-value networks within DAF, Army Cyber, or USCYBERCOM.
    - Integrate RAVID with existing defensive systems and begin baseline comparisons.
2. Evaluation
    - Measure network dwell time reduction.
    - Test response time to simulated breach events.
    - Validate Zero Trust maturity improvement.
3. Widespread Adoption
    - Utilize RAVID across combatant commands and DIB nodes.
    - Standardize ephemeral overlay usage.
    - Train cyber teams on dynamic defense operations.

Closing Message to DoD Stakeholders

This is not another tool. RAVID is a shift in doctrine. The same tactics that protect critical assets in the intelligence community can and must be applied across the defense landscape. Cyberswitch Technologies has made TSSCI-level security available to all echelons of DoD operations—without disrupting workflows or needing a rip-and-replace approach. With RAVID, the adversary never sees you coming—and that's the point.



CYBERSWITCH TECHNOLOGIES

CYBERSECURITY

Cybersecurity is complicated, ever-evolving, and 24/7.

The greatest business value is with an expert partner who can assess your current risks, secure your data and networks, and help you plan for the future.

Our team is comprised of industry experts with successful client implementations in Professional Sports, Entertainment, Media, Commercial, Federal, Civilian and Public Sector.

CONTACT INFORMATION

Marcus Crockett, CEO

Cyberswitch Technologies

☎ 678.235.9076

✉ ceo@cyberswitchtech.com