NIGHTWING

FROM BOOT TO BATTLEFIELD



Compliance to Combat Ready:
Building Offensively-Informed, Data Centric Defense from Boot to Battlefield

SCOTT JACKSON, USAF (RET)
NIGHTWING SOLUTION ARCHITECT
AUGUST, 2026

© 2026 Nightwing.
All rights reserved.

UNCLASSIFIED

PRESENTATION AGENDA

AGENDA

- Historical Context
  -- DIACAP, RMF, ZT ... Data Centric
- Fight Through It!
  -- Compliance // Combat Resilience
- Eye To Unknown / Unknowns
  -- AI, Quantum
- Offensively Informed Threat Defense
  -- Boot Layer
  -- OS Layer
  -- Data Bus Layer
- Summary / Discussion

Scott Jackson

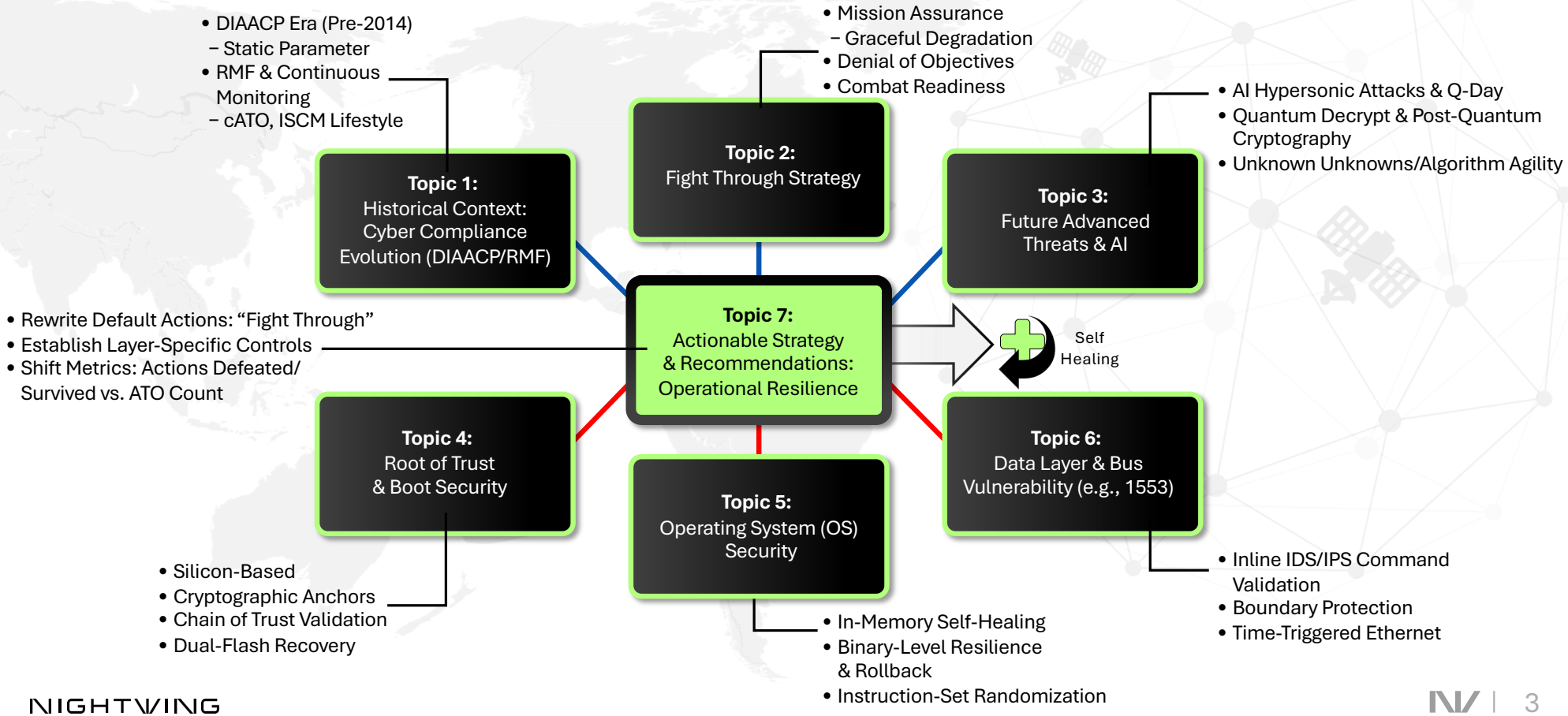
Solution Architect
Nightwing

- 26 years of active-duty Air Force as a Communications and Cyber Operations Officer; commanded a Combat Comm Squadron and a Joint Base Comm Squadron
- Special Duty Assignment at White House Communications Agency (WHCA) as a Presidential Communications Officer covering the GWOT pre and post 9/11
- Multiple deployments supporting AFSOC, SOCCENT and JTF No Fly Enforcement
- 8 years as Solution Architect for major system integrator and direct program manager support to contracts at DHS, DISA and multiple IC agencies

"The cyber domain is a battlefield –
and America's warfighters are leading the way."

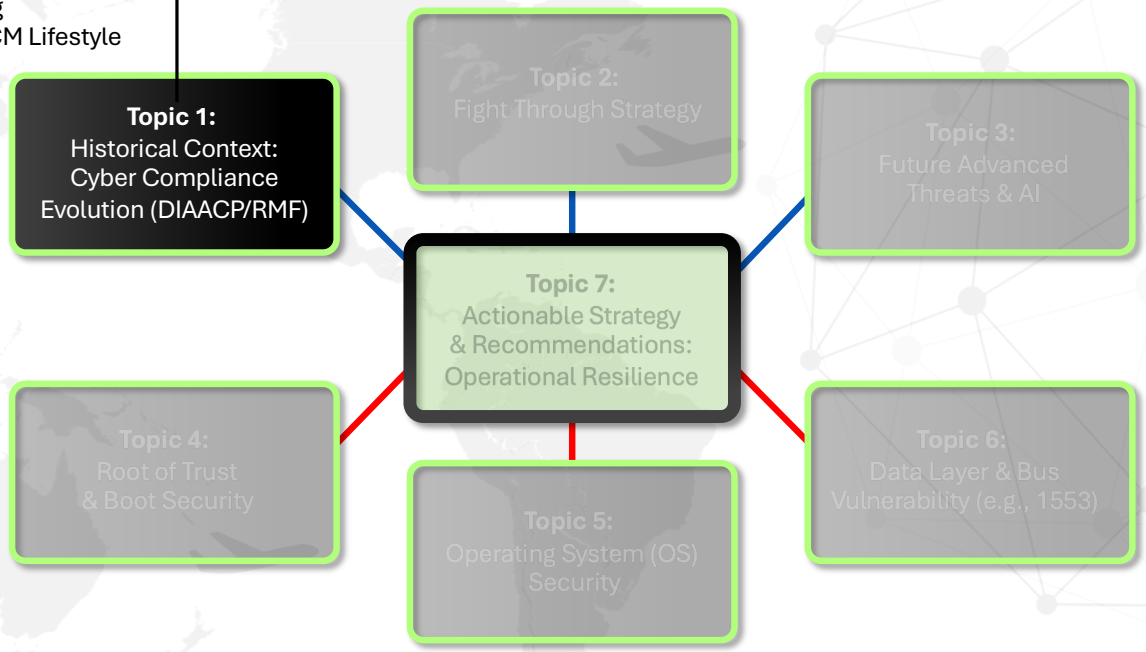
Secretary of War
Pete Hegseth
July 2026

CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS



CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS

- DIAACP Era (Pre-2014)
  - Static Parameter
- RMF & Continuous Monitoring
  - cATO, ISCM Lifestyle



TOPIC 1

HISTORICAL CONTEXT: CYBER COMPLIANCE EVOLUTION (DIAACP/RMF)



- Historical Context – 2006/2014:
  At the time, the “DoD Information Assurance Certification & Accreditation Process” (DIACAP), compliance-focused, checklist-driven certification



- Risk Management Framework (RMF)- 2014/2025:
  Shift from "pass/fail" to a lifecycle (Categorize, Select, Implement, Assess, Authorize, Monitor)



- Continuous Monitoring: “cATO” (CM)- implemented between - 2018/2022
  Breaks the 3-year cycle of massive paperwork drops to keep systems authorized/running

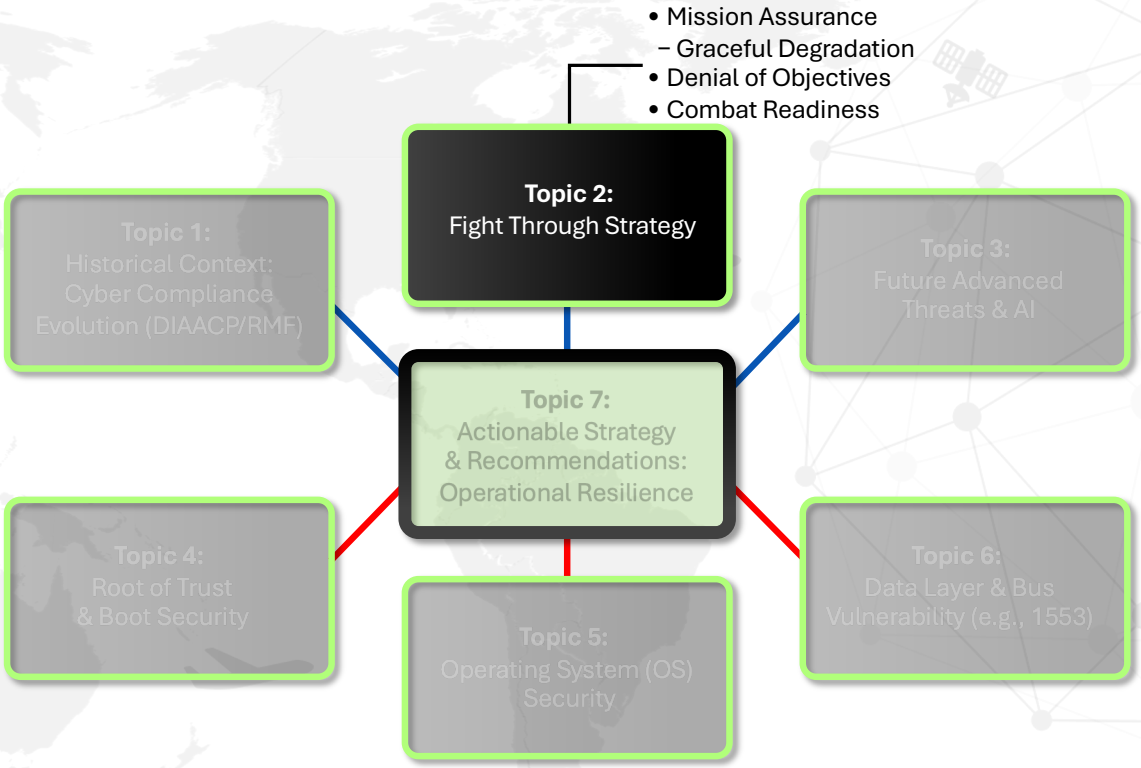


- Zero Trust (ZT): Never Trust, Always Verify – Least Privilege Principals - 2022/2025
  Flushes the perimeter model, Organizes controls across 7 Pillars
  (User, Device, Application/Workload, Data, Network, Automation and Visibility)



- Cybersecurity Risk Management Construct (CSRMC) – 2025
- “Fight Through It” 2026: Focus on Combat Readiness, Survivability and Mission Assurance
  Manage and Recover System Capabilities if/when they are compromised

CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS



TOPIC 2

SHIFT TO A “FIGHT THROUGH IT” STRATEGY

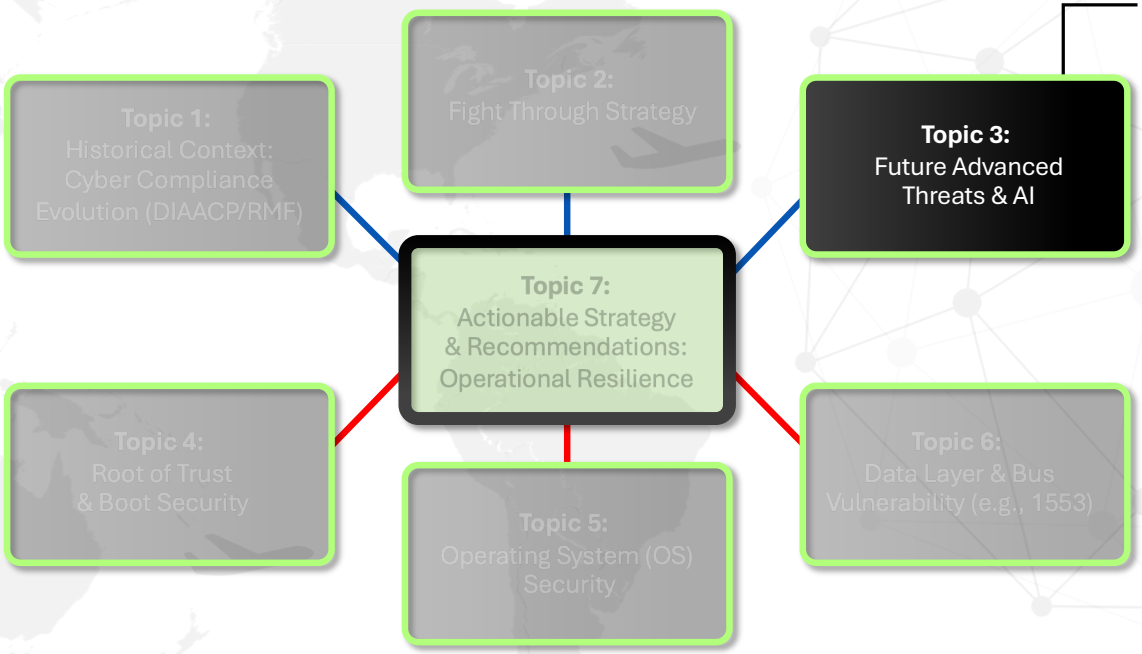


- “Fight Through” Strategy for Cyber / IT Systems
  Requires basic understanding of adversary tradecraft and offensive threat modeling
- Shifts the cost/benefit burden back on the adversary, “significant effort” before actual impact to military operations

Cyber Survivability Coverage Area	Operational Goal
CSA-08 Manage System Performance if Degraded	Mitigate attacks by disabling compromised processes, deploying decoy data, ensuring system performance meets operational mission needs even if degraded / compromised
CSA-09 Recover System Capabilities	Restore system after attack detection, reboot in secure state, active healing of files/data, maintaining data integrity with trusted backup / automated check-restore mechanisms
CSA-10 Actively Manage System Configurations to Counter Vulnerabilities at Tactically Relevant Speeds	Prevent unauthorized modifications to a deployed system, provide mitigations to allow for longer patch cycles and support authenticated / trusted patch and update processes

The Tactical Reality: We cannot send personnel into combat with armor that they must take off the moment it gets hit
A "fight through it" posture treats the network as contested terrain — no different than physical terrain

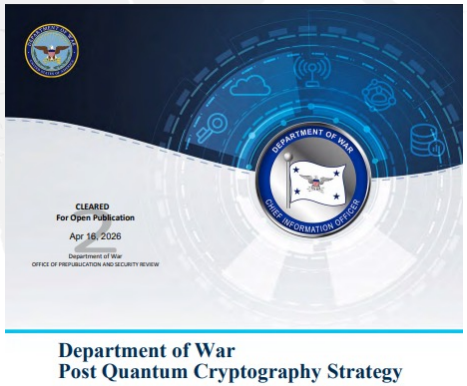
CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS

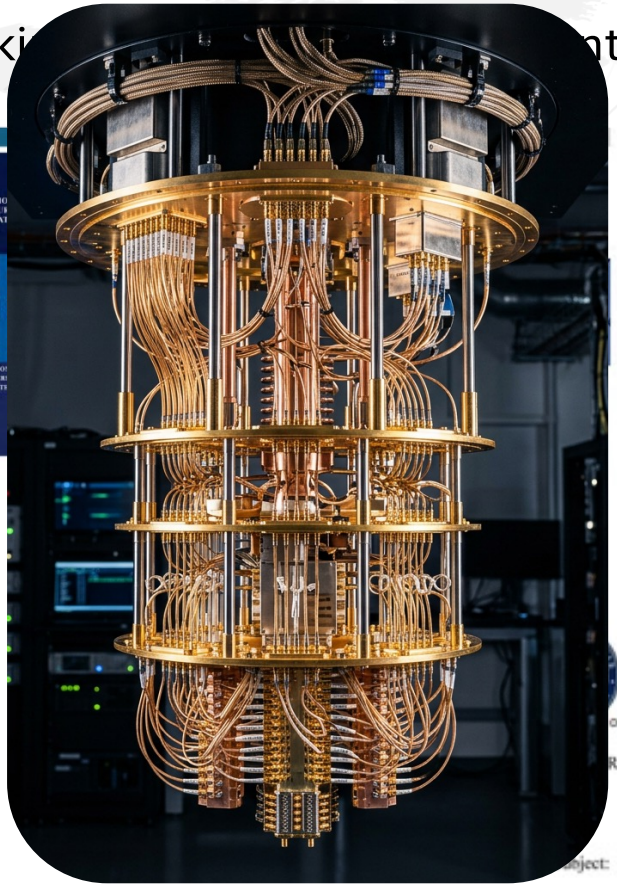


TOPIC 3

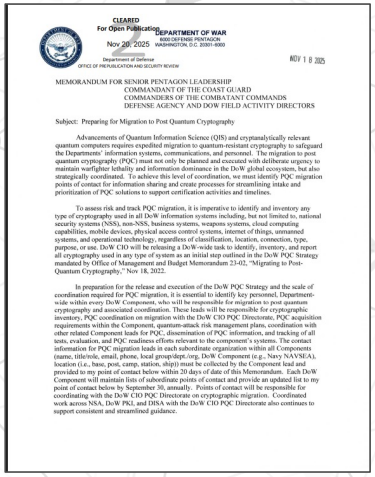
FUTURE ADVANCED THREATS

- Department focus on maki ntum Resilient



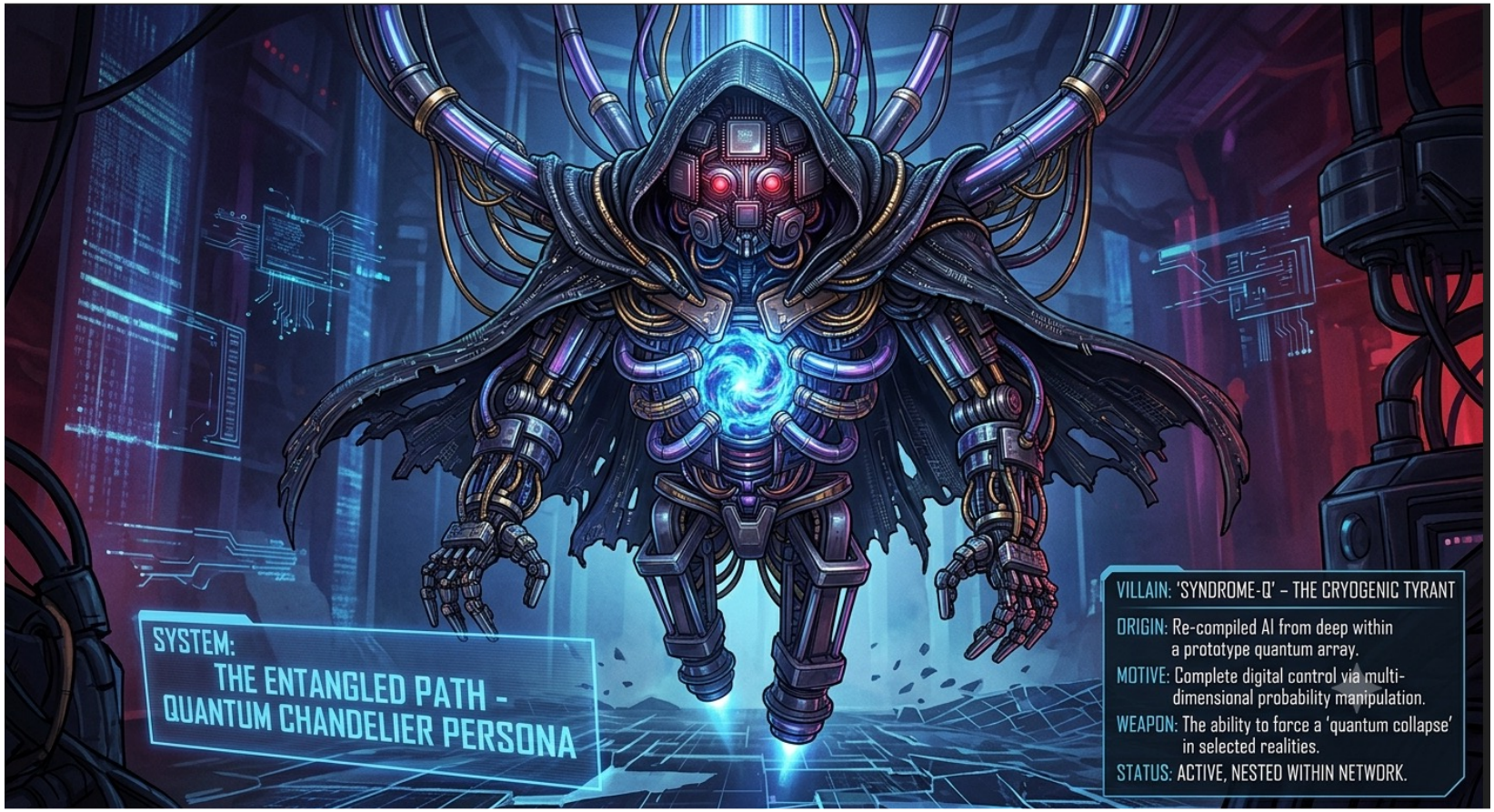




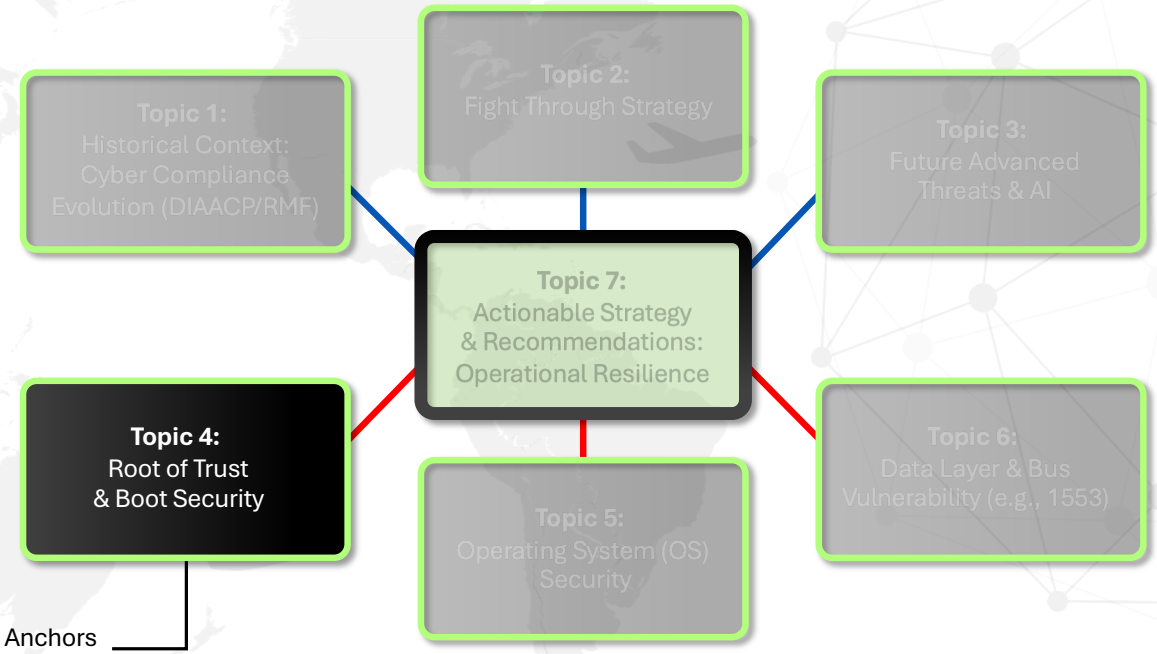


TOPIC 3

FUTURE ADVANCED THREATS

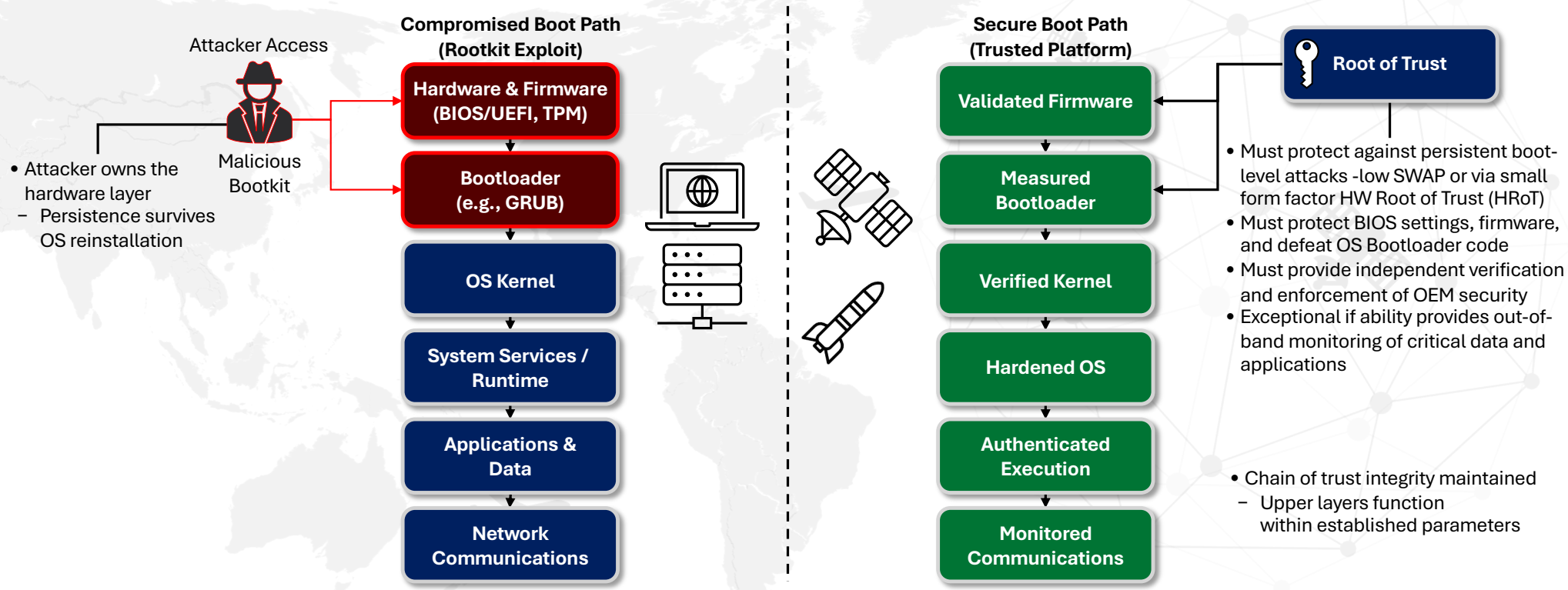


CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS



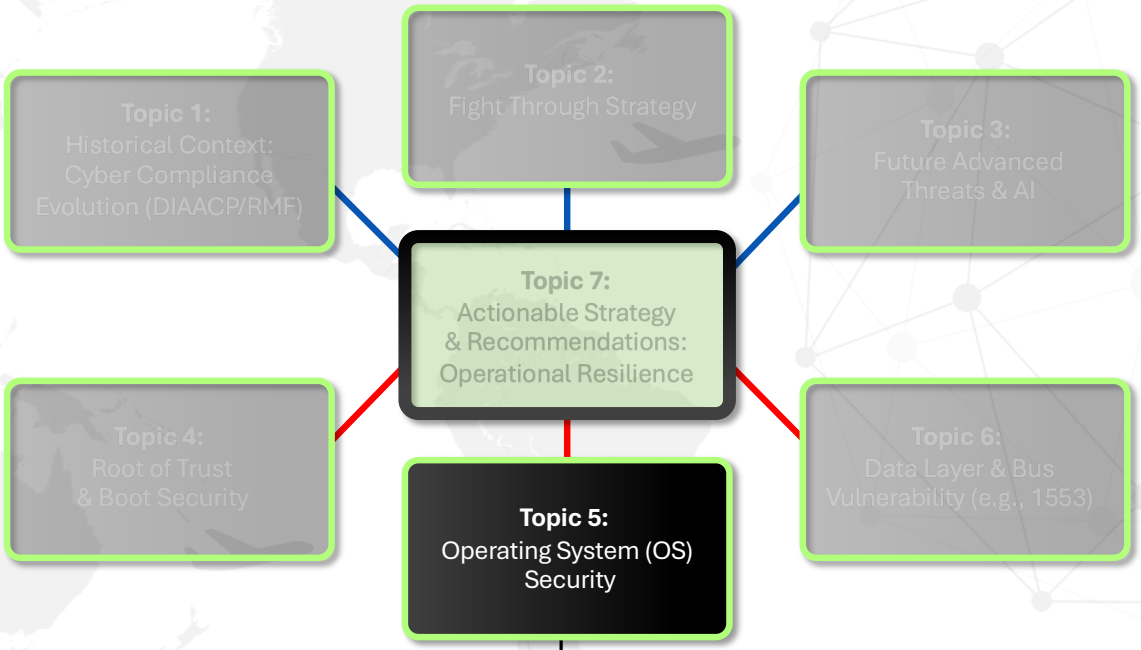
- Silicon-Based
- Cryptographic Anchors
- Chain of Trust Validation
- Dual-Flash Recovery

CRITICAL THREAT: BOOT LAYER VULNERABILITY (ROOTKITS)

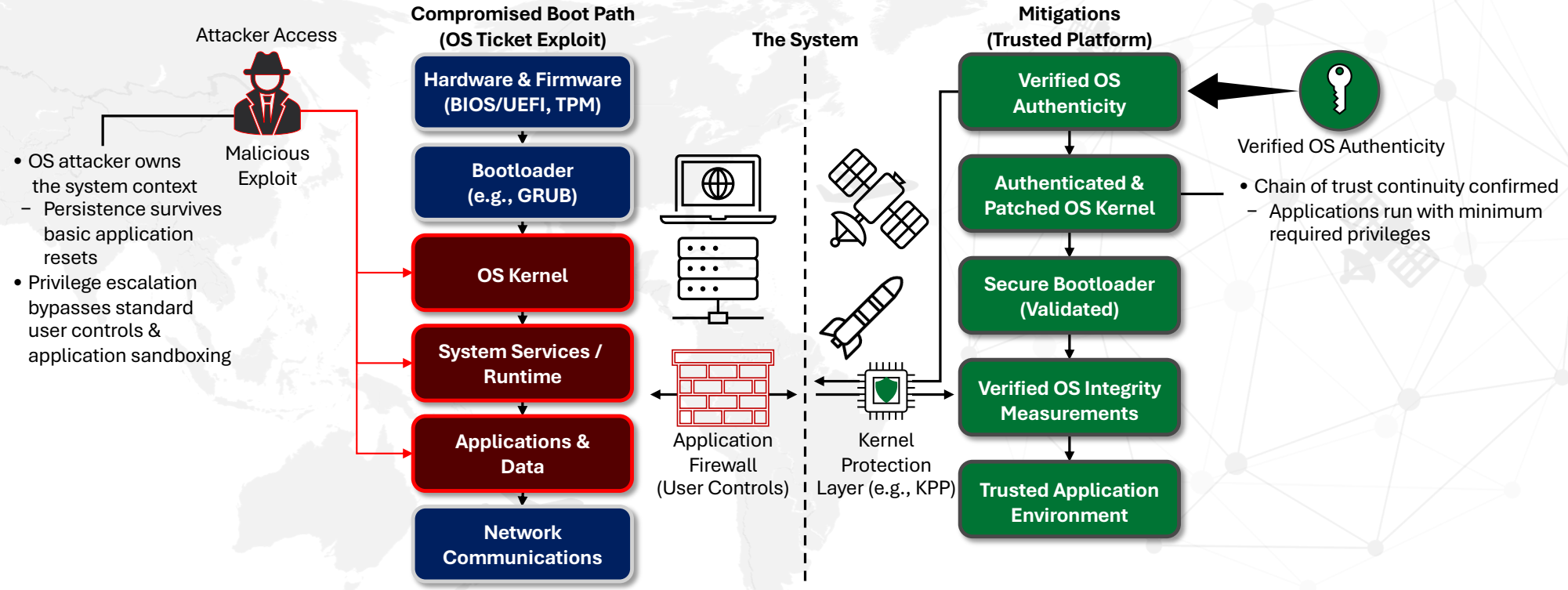


Takeaway: If the Boot Layer is compromised (Rootkit), almost all subsequent security controls (AV, EDR, ICAM) become ineffective because the underlying system trust is broken at the HW layer

CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS

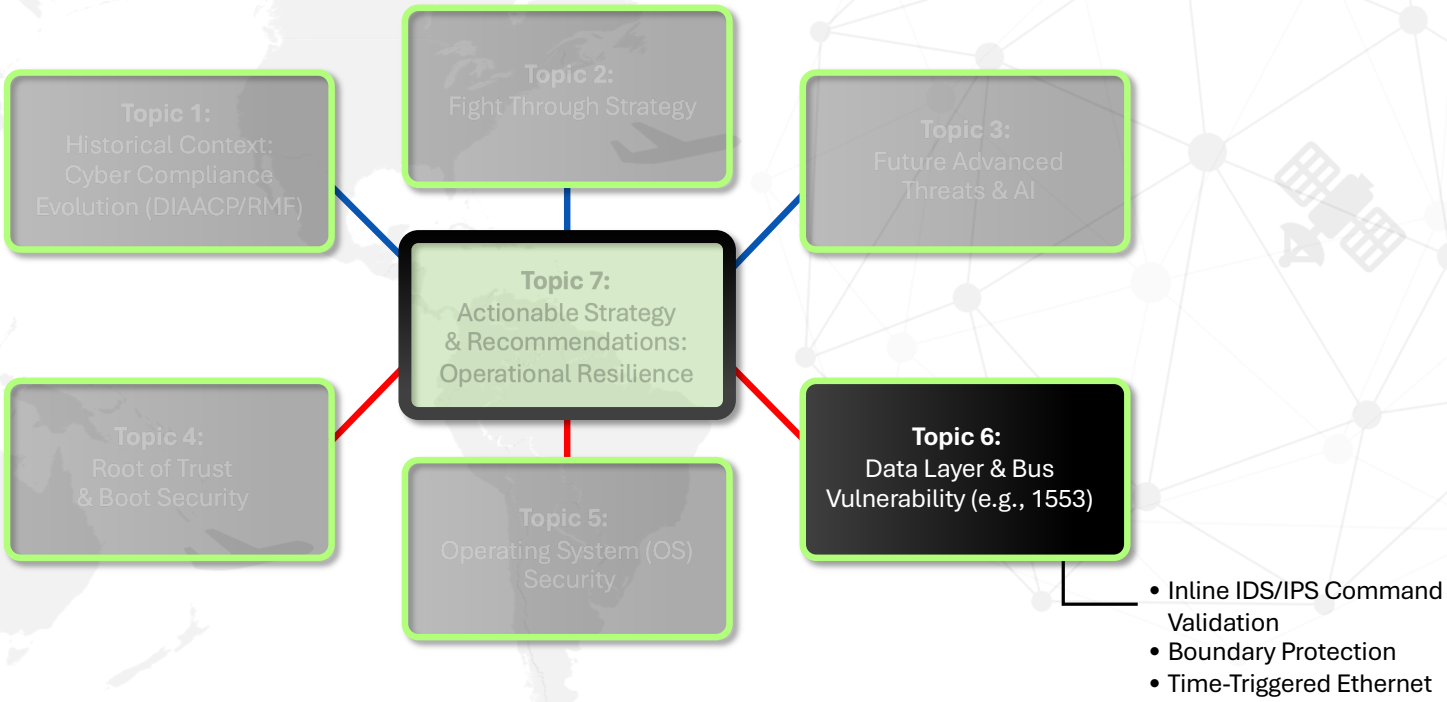


CRITICAL THREAT: OPERATING SYSTEM (OS) CORE VULNERABILITIES

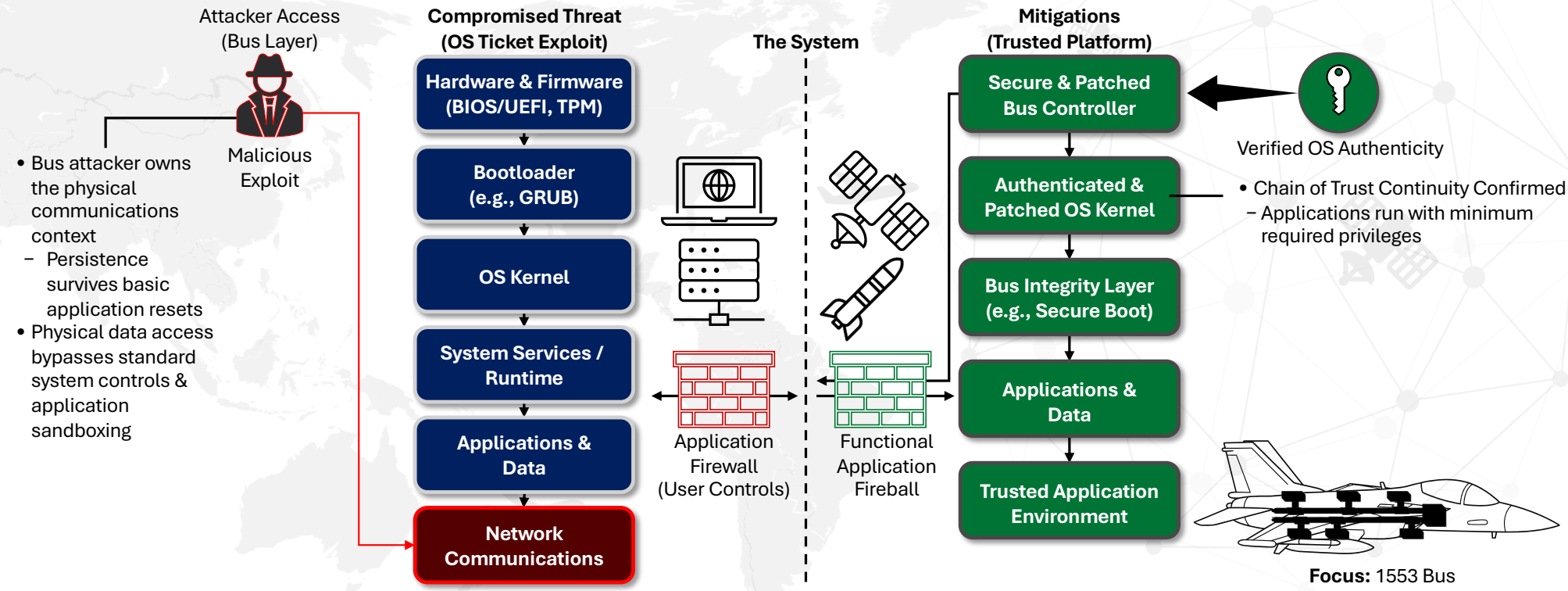


Takeaway: If the Operating System (OS) Core is compromised, the primary logic and security framework are defeated, rendering user-level application security (e.g., local sandboxes) ineffective, because the attacker has gained control over system resources and data

CYBER MISSION ASSURANCE & RESILIENT COMBAT READINESS



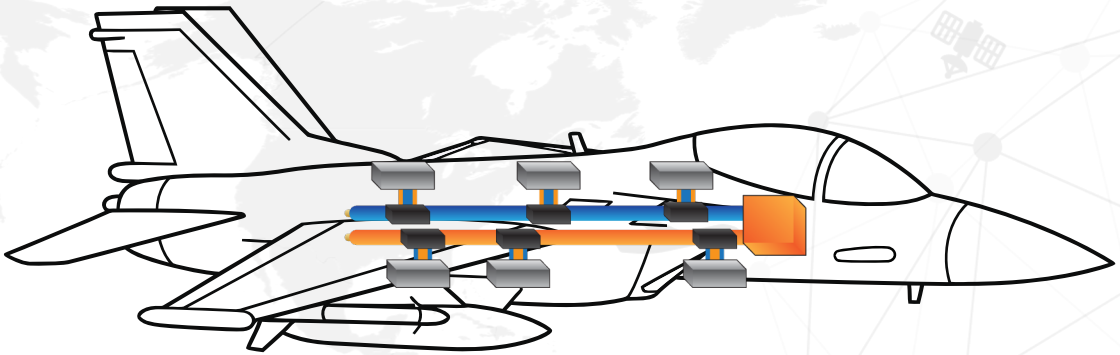
CRITICAL THREAT: DATA BUS LAYER VULNERABILITY



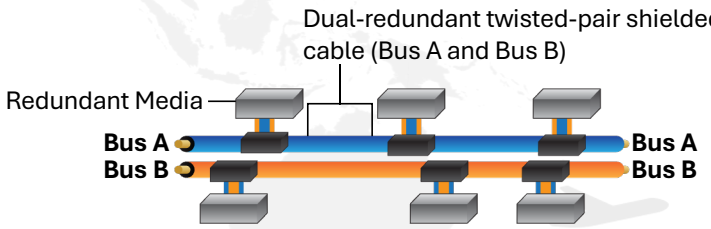
Takeaway: If the Data Bus Layer (Physical or Logic) is compromised, the primary physical communications and integrity are defeated rendering all logical and access controls ineffective, attacker has gained ultimate physical-layer control over data flow and device control

MLT-STD-1553 DATA BUS: ARCHITECTURE & CYBER VULNERABILITIES

1553 Data Bus Basics:
How it works…

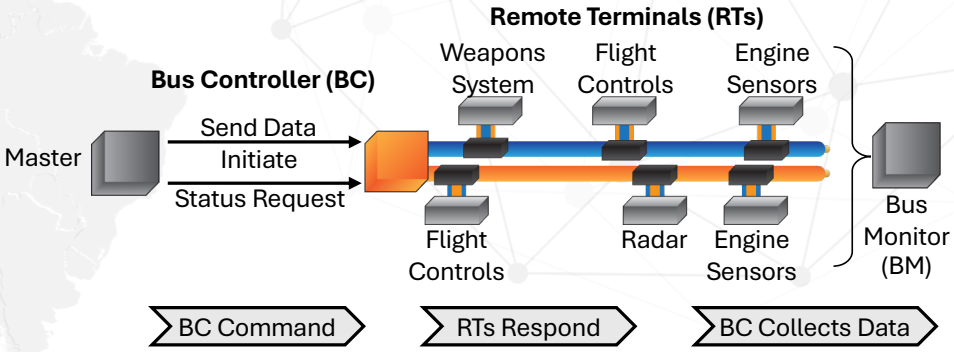


1. Multi-Drop Topology

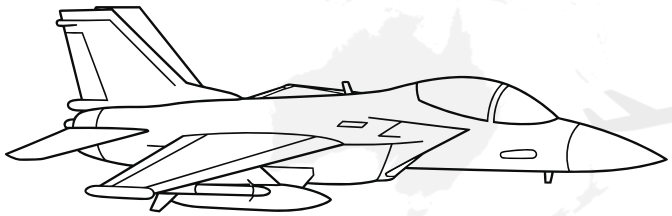


Modern, Reliable, Complex Systems

2. Key Components & Protocol



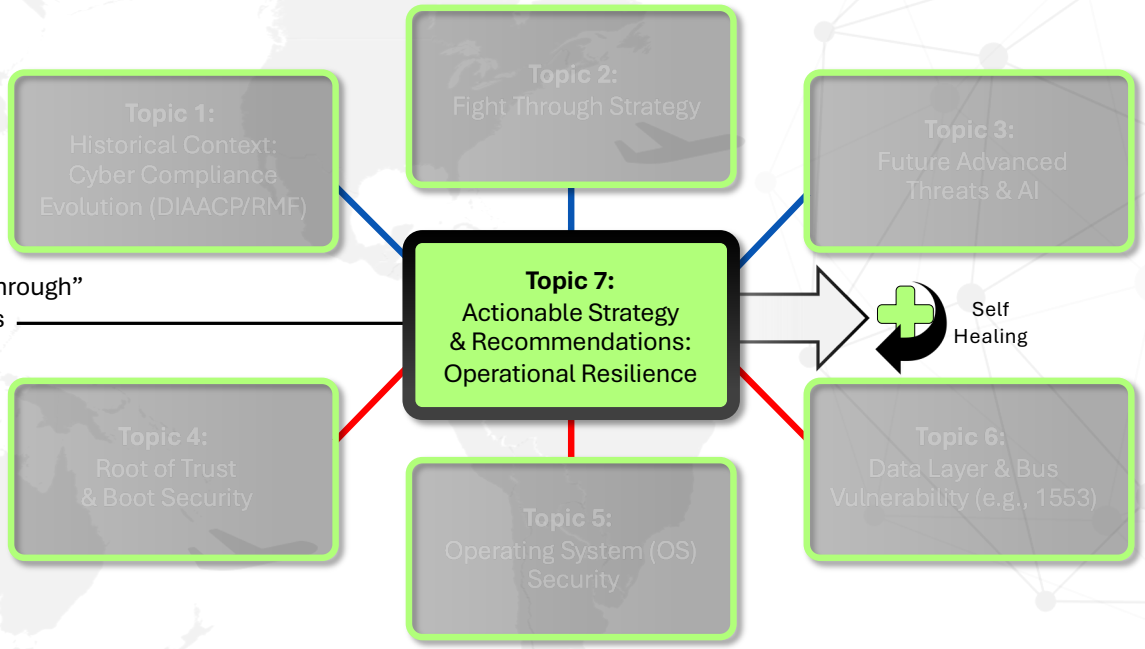
MLT-STD-1553 DATA BUS: ARCHITECTURE & CYBER VULNERABILITIES



TOPIC 7

RECOMMENDATIONS

- Rewrite Default Actions: “Fight Through”
- Establish Layer-Specific Controls
- Shift Metrics: Actions Defeated/ Survived vs. ATO Count



TOPIC 7

RECOMMENDATIONS

Strategic Refocus

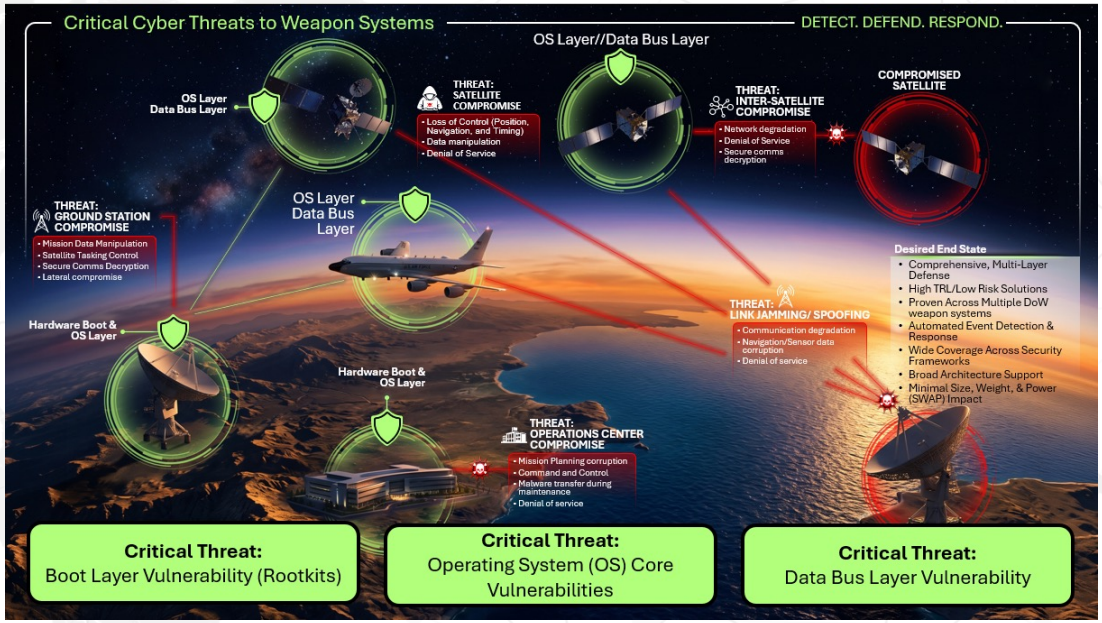
- Learn from Past Policies
  - Both Good and Bad
- Accept Warrior Ethos
  - Fight Through It
- Assume Future Compromise
  - Quantum Dilemma

Call to Action

- 3 Recommended Focus Areas from Offensively informed Defense
  - Boot / Hardware Layer
  - OS / Software Layer
  - Data / Network Layer

New Metrics

- Operations Completed or Sustained under compromise
- Systems Operational despite being infected

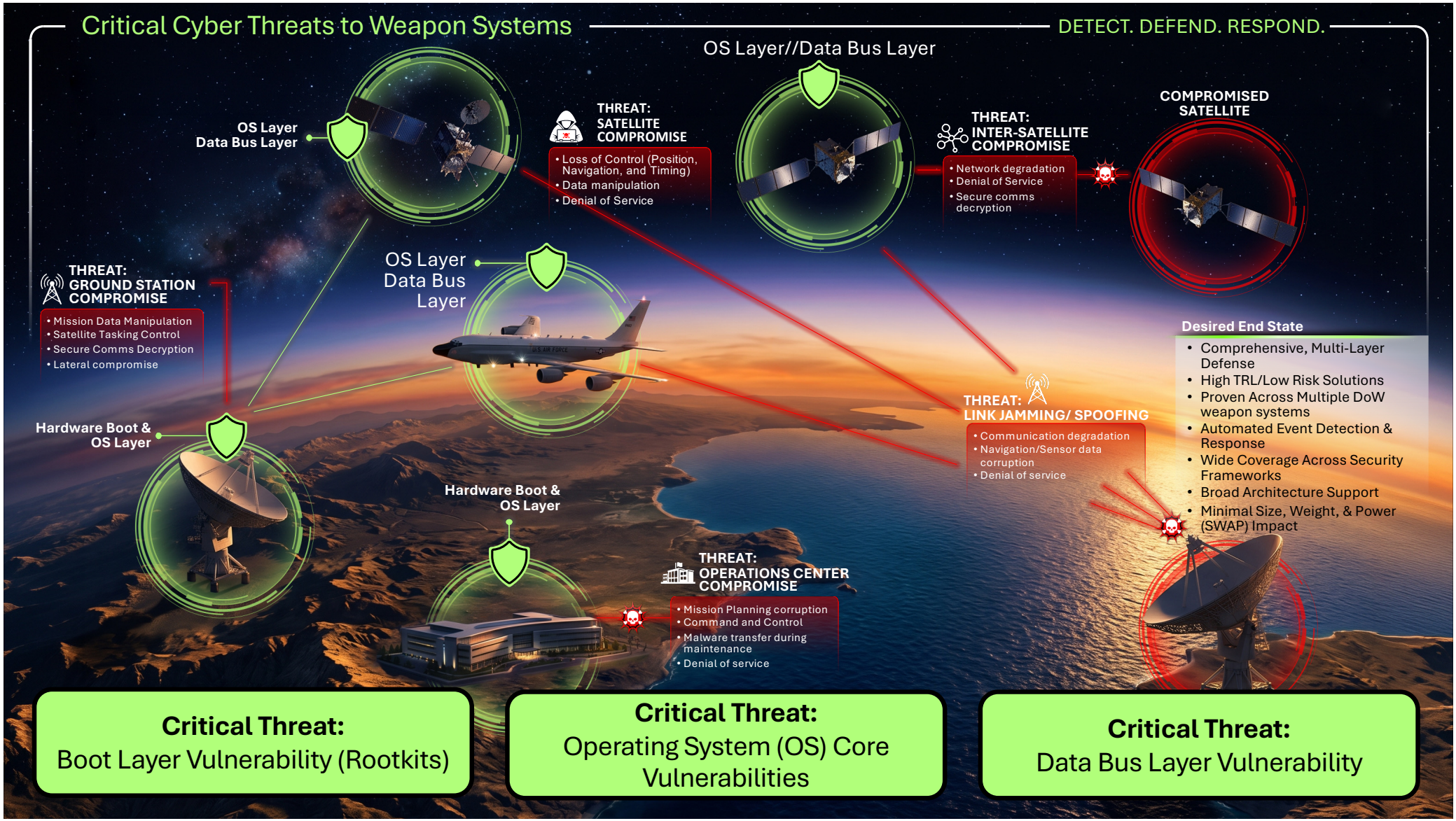


- Rewrite Default Actions: "Fight Through"
- Establish Layer-Specific Controls
- Shift Metrics: Actions Defeated/ Survived vs. ATO Count

Topic 7: Actionable Strategy & Recommendations: Operational Resilience → Self Healing



© 2026 Nightwing.
All rights reserved.


Critical Cyber Threats to Weapon Systems
DETECT. DEFEND. RESPOND.
OS Layer//Data Bus Layer
OS Layer
Data Bus Layer
THREAT:
SATELLITE
COMPROMISE
• Loss of Control (Position, Navigation, and Timing)
• Data manipulation
• Denial of Service
THREAT:
INTER-SATELLITE
COMPROMISE
• Network degradation
• Denial of Service
• Secure comms decryption
COMPROMISED
SATELLITE
THREAT:
GROUND STATION
COMPROMISE
• Mission Data Manipulation
• Satellite Tasking Control
• Secure Comms Decryption
• Lateral compromise
OS Layer
Data Bus
Layer
Hardware Boot &
OS Layer
Hardware Boot &
OS Layer
THREAT:
OPERATIONS CENTER
COMPROMISE
• Mission Planning corruption
• Command and Control
• Malware transfer during maintenance
• Denial of service
THREAT:
LINK JAMMING/ SPOOFING
• Communication degradation
• Navigation/Sensor data corruption
• Denial of service
Desired End State
• Comprehensive, Multi-Layer Defense
• High TRL/Low Risk Solutions
• Proven Across Multiple DoW weapon systems
• Automated Event Detection & Response
• Wide Coverage Across Security Frameworks
• Broad Architecture Support
• Minimal Size, Weight, & Power (SWAP) Impact
Critical Threat:
Boot Layer Vulnerability (Rootkits)
Critical Threat:
Operating System (OS) Core Vulnerabilities
Critical Threat:
Data Bus Layer Vulnerability