

Ephemeral Partner Collaboration Environments (EPCE): Tactical zero trust for coalition communications

Secure, agile, and resilient communications for multi-domain operations

Marqus Hutchinson, CTO
Intelligent Waves

Learning objectives

- Understand how Ephemeral Partner Collaboration Environments (EPCE) operationalizes zero trust, a model where every access request is verified continuously
- Learn how EPCE enables secure collaboration across untrusted networks
- Examine real-world examples
- Explore how EPCE supports Agile Combat Employment (ACE)



Why EPCE matters

- Secure coalition communication is a mission-critical challenge in modern operations
- Traditional systems are slow, infrastructure-heavy, or insecure
- EPCE enables fast, zero-footprint, secure collaboration across untrusted networks
- EPCE directly supports Decision Superiority and Joint All-Domain Operations, eliminating comms friction across allied forces
- Designed for software-defined warfare, where agility, identity, and coalition trust boundaries are in constant flux

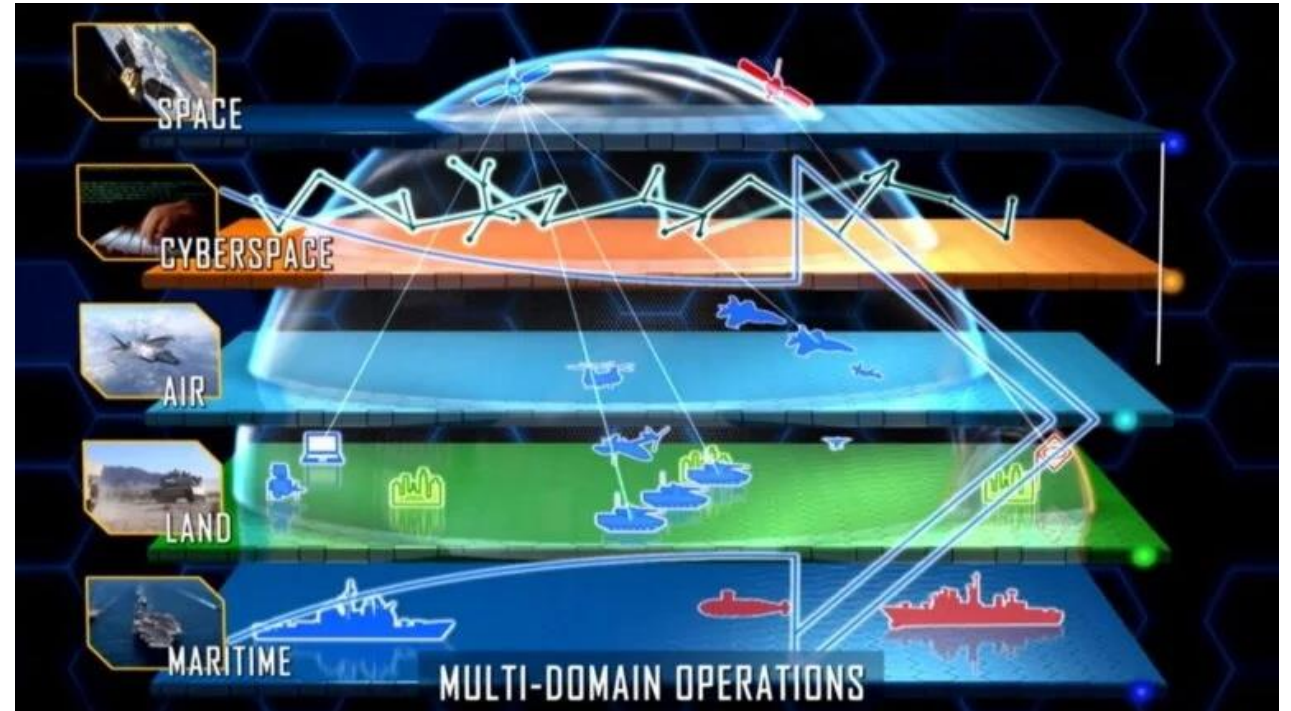


Image source: The Modern Battlespace

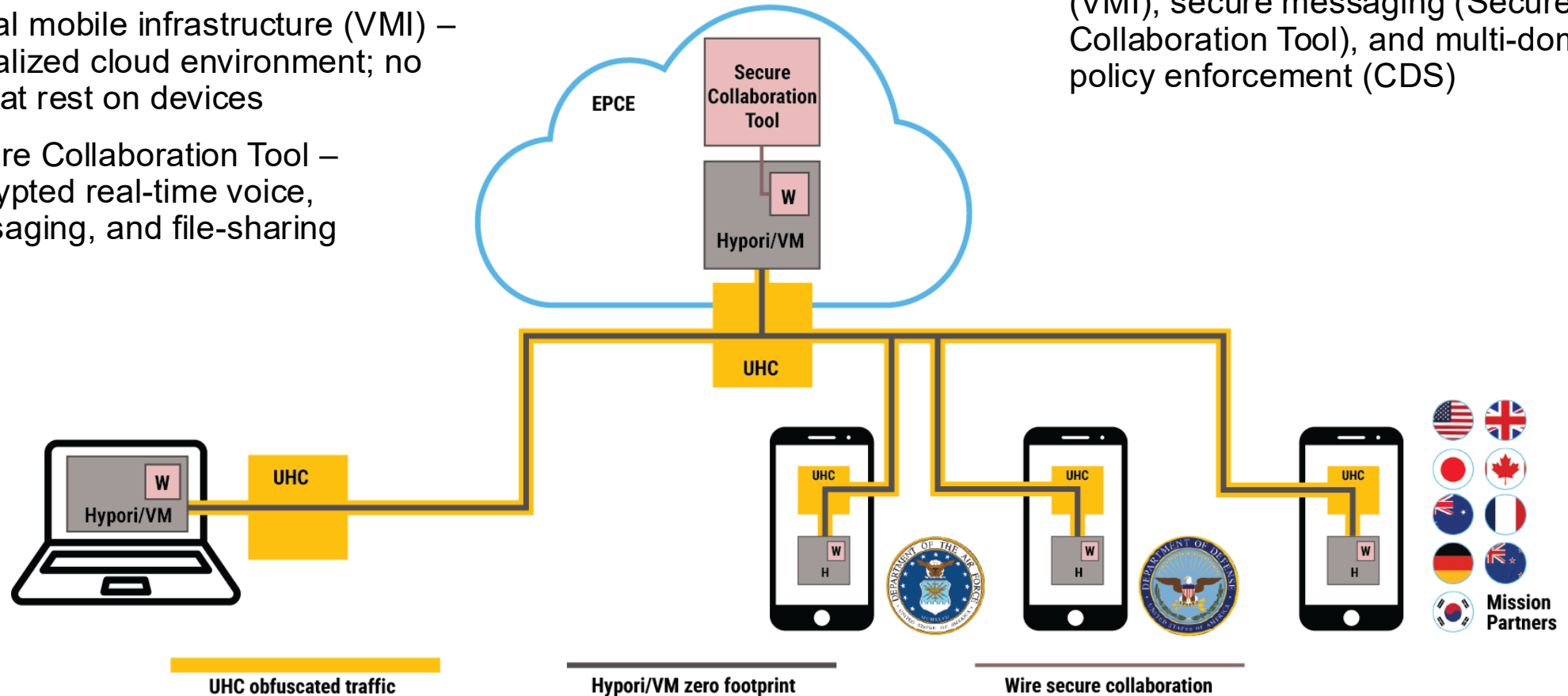
What is EPCE?

- A zero-trust architecture based, rapidly deployable, and temporary collaboration environment
- Zero hardware dependency: EPCE removes the need for relying on the physical security of hardware
- Leaves no data at rest on physical devices
- Fully integrated with Ubiquitous Hidden Core (UHC) and virtual mobile infrastructure
- Built for denied, disrupted, intermittent, and limited (DDIL) environments
- LPI/LPD: EPCE lowers risk of detection and interception by distributing data packets across multiple encrypted paths throughout various geographical regions

EPCE components

- UHC – Obfuscated, multi-path communication across SATCOM, LTE, and ISP networks
- Virtual mobile infrastructure (VMI) – Virtualized cloud environment; no data at rest on devices
- Secure Collaboration Tool – Encrypted real-time voice, messaging, and file-sharing

- Each component aligns with DAF Zero Trust Strategy pillars: Transport obfuscation (UHC), endpoint isolation (VMI), secure messaging (Secure Collaboration Tool), and multi-domain policy enforcement (CDS)



Operationalizing zero trust with EPCE

- Software-defined isolation of sensitive data
- End-to-end encrypted communication between devices
- Real-time access control based on mission needs
- Enables Just-In-Time and Just-Enough Access (JIT/JEA) enforcement across coalition enclaves

EPCE alignment with CJADC2 objectives

CJADC2 Objective	EPCE	Alignment
Enable secure, real-time collaboration across US and coalition forces	UHC (Obfuscated Multi-Path Transport)	Provides resilient, obfuscated data paths over SATCOM, LTE, and terrestrial networks to ensure uninterrupted coalition comms.
Integrate data transport and protection across all domains	UHC + Virtual Mobile Infrastructure (VMI)	Combines multi-path, encrypted transport with virtualized endpoints to meet CJADC2's requirement for secure transport and endpoint security.
Zero trust enforcement from tactical edge to command echelons	VMI	Enforces no data-at-rest, identity-based access, and policy-driven isolation for all users, regardless of device or location.
Support decision advantage in contested environments	UHC + Wire (Secure Collaboration)	Ensures operational tempo by enabling voice, messaging, and file sharing across disaggregated or untrusted networks in DDIL scenarios.
Operate across classified, unclassified, and partner networks	UHC + Wire	Facilitates encrypted, policy-driven communication across network boundaries without requiring shared infrastructure trust chains.

EPCE alignment with MPE objectives

Mission Partner Environment (MPE) mission

Enable rapid, secure, and interoperable information sharing between US forces, allies, and mission partners in support of combined operations across all domains.

MPE vision

A persistent, trusted, and agile coalition environment that supports decision superiority through seamless collaboration — any mission, any partner, anywhere.



EPCE alignment with MPE objectives

Persistent readiness

- Rapid deployment of ephemeral enclaves enables secure collaboration in hours, not days.

Zero trust enforcement

- Identity-based access, no data at rest, and continuous verification meet MPE's zero-trust foundation.

Coalition interoperability

- Seamlessly bridges classified, unclassified, and partner networks — even in DDIL environment environments.

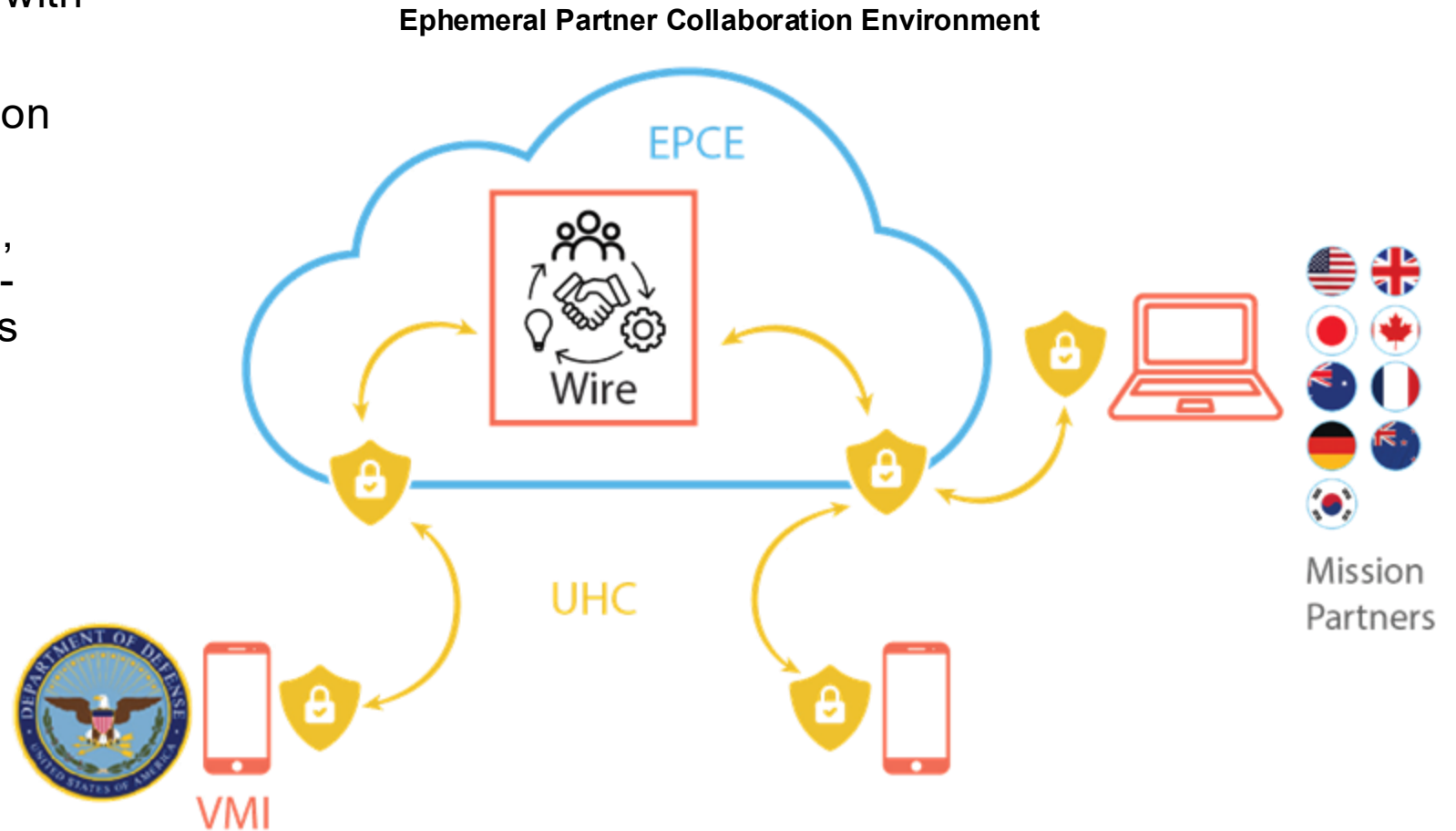
Support to decision advantage

- Reduces communication friction and accelerates operational tempo in multi-domain, partner-enabled missions.



Secure collaboration across untrusted networks

- Obfuscated, multi-path comms with UHC
- Real-time encrypted collaboration using Wire
- Designed to thrive in gray zone, coalition-disaggregated, or non-integrated partner environments



Agility, security, and flexibility

- EPCE is operational within two hours, adaptable to SATCOM, LTE, and terrestrial networks
- Real-time collaboration between US and partner nations, with secure voice and messaging
- A critical enabler of Agile Combat Employment (ACE), supporting rapid deployments and secure comms without relying on pre-staged infrastructure
- Security policies are enforced at the platform level, ensuring protected, audit-ready data in even the most unpredictable environments



Conclusion and recommendations



Strengthens secure coalition collaboration across domains



Combines zero trust and rapid deployment for real-time agility



Scalable solution for contested, multi-domain operations

Image source: The Noun Project

Questions and discussion

Contact:

Marqus Hutchinson, CTO

Intelligent Waves

703.766.7999

marqus.hutchinson@intelligentwaves.com