ETI EMERGING TECHNOLOGIES INSTITUTE | NDIA

March 2026

FIGHT THE BASE

UNIFIED CONSTRUCT FOR USAF INSTALLATIONS AS FORWARD OPERATING WEAPONS PLATFORMS

Authors: Brian Stites, Chair, Cyber Warfare Division, NDIA and
Daryl Haegley, Technical Director, Control Systems Cyber Resilience, Department of the Air Force

Bottom Line Up Front (BLUF)

Peer adversaries possess the capability to disrupt or deny U.S. combat power generation at the installation level through coordinated multi-domain attacks combining precision strike weapons, cyber operations, space-enabled targeting, and/or infrastructure disruption. Their objective is not necessarily to destroy aircraft in flight, but to deny or degrade sortie generation by targeting the infrastructure that enables it.

Department of the Air Force installations are still largely governed, funded, and evaluated as support infrastructure rather than combat platforms operating within an adversary's weapons engagement envelope.

This creates a strategic gap: Installations generate combat power but are not doctrinally treated as warfighting systems required to sustain operations under attack.

The Fight the Base Concept

Fight the Base (FtB) reframes Air Force installations as forward operating weapons platforms responsible for generating combat power while operating in contested environments.

The concept draws from the Navy's "Fight the Ship" doctrine, which assumes platforms within an adversary's engagement envelope must continue executing missions while conducting damage control and recovery operations.

Applied to installations, the operational premise is straightforward: Air Force bases must be able to generate combat power while under attack, disruption, or infrastructure degradation. Under the Fight the Base construct, installations must be designed, resourced, and exercised to:

- Generate combat sorties under degraded conditions
- Conduct infrastructure damage control during mission execution
- Maintain situational awareness across cyber and physical infrastructure systems
- Rapidly recover degraded capabilities within operational timelines
- Validate survivability through operational exercises

This reframes resilience from a facility management or compliance issue into a combat readiness requirement.

Operationalizing the Concept: Fight the Base Mission Readiness Index (FBMRI)

The Fight the Base Mission Readiness Index (FBMRI) provides a framework for measuring an installation's ability to sustain combat power under contested conditions. FBMRI integrates existing initiatives including:

- Installation Infrastructure Action Plans (I2AP)
- Energy Resilience and Readiness Exercises (ERRE)
- Cyber Resiliency Readiness Exercises (CRRE)
- Mission assurance programs

Building on the above, FBMRI unifies these initiatives to form a mission-focused readiness construct that evaluates infrastructure resilience based on each infrastructure element's impact on combat sortie generation and operational continuity. Key dimensions include:

- Mission generation continuity
- Cyber-physical infrastructure resilience
- Energy sustainment
- Infrastructure interdependencies
- Recovery timelines
- Redundancy depth

FBMRI produces a composite readiness score for an installation's ability to generate combat power under stress.

Strategic Value

Adopting the Fight the Base construct enables senior leaders to:

- Understand capacity for sustained combat power generation during degradation of infrastructure
- Align infrastructure investments with operational mission outcomes
- Incorporate installation survivability into readiness reporting
- Prioritize resilience investments during POM and MILCON cycles

Fight the Base converts installation resilience from a compliance activity into a measurable warfighting capability for sustained global combat power projection.

Crosswalk of Critical Infrastructure Protection / Installation Resiliency

Policy / Strategy	"President Trump's Cyber Strategy for America"	DoD Cyber Strategy	"CISA National Infrastructure Protection Plan (NIPP)"	"USAF Installation Resilience / ERRE / CRRE frameworks"	"Fight the Base Mission Readiness Index (FBMRI)"
Date	**March 2026**	**September 2023**	**December 2013**	**2022-2023 (Primary policy set)**	**"Concept / Project Framework (2025-2026)"**
Summary	Establishes six policy pillars focused on adversary disruption, regulatory reform, federal network modernization, critical infrastructure protection, emerging technology leadership, and cyber workforce development.	Current Department of Defense cyber strategy. Focuses on defending the nation, campaigning in cyberspace, and building enduring cyber advantages.	Core national critical infrastructure risk-management framework. Still the governing document for the sector risk management model used by DHS/CISA and sector agencies. NIPP is a critical infrastructure risk-management framework rather than a cyber strategy.	Driven primarily by the Department of the Air Force Installation Infrastructure Action Plan (I2AP) - March 2022, along with associated DAFI guidance governing installation resilience exercises and infrastructure resilience.	"FBMRI is an overall unifying construct similar to ""Fight the Ship"" that directly translates base and installation combat power generation during periods of disruption, destruction and attack. Translates adversary cyber activity into installation-level mission readiness impact metrics. Not an official DoD or DAF policy document."
Pillar 1	**Shape Adversary Behavior**	**Very Strong** Direct alignment with Defend the Nation and Campaign in Cyberspace lines of effort. Emphasizes proactive disruption and cyber deterrence.	**Limited** Limited direct alignment; NIPP focuses on infrastructure risk management and resilience rather than adversary disruption or cyber operations.	**Limited** Limited alignment; installation exercises simulate adversary effects to validate resilience and response.	**Very Strong** Very Strong: Quantifies mission impact of adversary cyber campaigns on installations and operational readiness. CONUS and OCONUS bases, installations and sites are combat power projection platforms.
Pillar 2	**Promote Common Sense Regulation**	**Limited** Limited direct overlap; DoD cyber doctrine is operational rather than regulatory.	**Moderate** Moderate alignment through public-private partnership governance and sector risk management standards.	**Limited** Limited direct linkage; installation frameworks implement resilience and operational policy rather than regulate industry.	**Strong** Strong: FBMRI smoothes and fast-tracks technology piloting, evaluation (exercises), certification, and ATO by using test & evaluation exercises to validate regulatory processes. Enables mission commanders and critical commercial support services to streamline regulatory processes for mission readiness.
Pillar 3	**Modernize & Secure Federal Networks**	**Strong** Strong alignment with secure and resilient DoD Information Network (DODIN), Zero Trust implementation, and enterprise cyber defense.	**Limited** Limited; NIPP promotes infrastructure security and resilience but does not focus on federal network architecture modernization.	**Moderate** Moderate alignment with installation IT modernization, cyber resilience exercises, and IT/OT integration.	**Strong** Strong: Provides measured KPIs to directly link networks to power projection capacity and mission readiness.
Pillar 4	**Secure Critical Infrastructure**	**Strong** Strong alignment with DoD Defense Critical Infrastructure (DCI) protection and resilience of infrastructure supporting military operations.	**Very Strong** Very strong alignment - central mission of NIPP through sector risk management and infrastructure resilience.	**Very Strong** Very strong alignment - ERRE/CRRE focus on base infrastructure resilience, utilities, ICS/OT systems, and recovery.	**Very Strong** Very Strong: Primary integration point. FBMRI translates infrastructure disruption into mission readiness metrics for installations as combat power projection platforms.
Pillar 5	**Sustain Superiority in Critical & Emerging Technologies**	**Strong** Strong alignment with DoD objective to build enduring cyber and technological advantage.	**Moderate** Moderate alignment through supply chain security and protection of infrastructure technologies.	**Moderate** Moderate indirect alignment through adoption of secure infrastructure technologies and OT cybersecurity practices.	**Strong** Strong: Measures mission readiness KPIs and provides clear path for emerging technologies evaluation, adoption and implementation for mission readiness.
Pillar 6	**Build Talent & Capacity**	**Moderate** Moderate alignment through cyber workforce development and operational capability.	**Moderate** Moderate alignment via sector partnership capacity building.	**Moderate** Moderate alignment through installation exercises, training, and resilience planning.	**Strong** Strong: Develops, trains and certifies cyber operators, defenders and recovery teams as combat mission operators and power projection readiness multipliers.