IBLADES WHITEPAPER · GOVERNMENT & PUBLIC SECTOR

Sovereign, Quantum-Safe National Security Infrastructure

Protecting multi-agency communications, critical national infrastructure, and the field edge against quantum and AI-era threats — without disrupting essential public services.

← Government & Public Sector

In this paper

1. Executive summary

National digital transformation is accelerating economic growth — and expanding the attack surface of government faster than most agencies can defend it. Security functions across defense, intelligence, law enforcement, and civilian agencies increasingly face escalating AI-augmented cyberattacks and denial-of-service campaigns, sophisticated threats to critical national infrastructure, fragmented governance and compliance requirements, severe cybersecurity skills shortages, and the urgent need to future-proof against quantum computing threats.

iBlades secures this environment with a single, hardware-anchored, AI-Threat and post-quantum cryptography (PQC) resilient fabric that overlays existing systems. **NetTron**

provides an intelligent secure network fabric and centralized command; **GuardTron** delivers plug-and-play edge security for critical national infrastructure; and **ManoTron** enables secure mobile and critical communications for field and coordination teams. Together, these solutions simplify complexity, enforce sovereignty and compliance through hardware roots of trust, and enable autonomous resilience against AI-driven and quantum threats — without requiring agencies to replace the systems they already run.

---

2. The 2026 threat landscape

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing thousands of APIs and services at once, generating evasive malware, and mapping trust relationships to move laterally after a foothold. Governments and critical infrastructure operators increasingly report sustained, multi-vector distributed denial-of-service (DDoS) campaigns, identity-led attacks, AI-generated phishing, business email compromise, and ransomware — often at volumes far above what existing teams can manually triage.

> **The real target is complexity.** AI attacks feed on exposed APIs, admin consoles, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Harvest Now, Decrypt Later (HNDL)

Adversaries capture encrypted classified, intelligence, and citizen data today to decrypt once quantum computers mature. Government is acutely exposed: national security communications, intelligence products, and citizen records must often remain confidential for decades, making today's encrypted traffic a long-term liability if it isn't already quantum-resistant.

Fragmented systems and the field edge

Cybersecurity responsibilities are frequently dispersed across multiple agencies and regulators, leading to duplicated effort, information silos, and inconsistent response. Underneath this coordination challenge sits a technical one: legacy government systems and public-facing platforms often can't be patched without halting essential services, and

field operations for security and emergency-response teams depend on communications that must withstand interception, jamming, and partial connectivity in contested or austere environments — while still supporting rapid, coordinated response.

---

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM for key exchange, ML-DSA/Dilithium for signatures; FIPS 203/204) with keys generated locally and rotated autonomously.

- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh and centralized command and control; enables autonomous key management, policy enforcement, and real-time visibility and coordinated defense across distributed agencies.
- **GuardTron™** — plug-and-play hardware edge node that isolates legacy systems and critical national infrastructure nodes; agentless, tamper-resistant, and built to ease the operational and skills burden on security teams.
- **ManoTron™** — hardware-secured mobile and critical communications for field teams, intelligence operatives, and executives, maintaining secure voice, data, and messaging under network stress or adversarial conditions.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement even after a compromise.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, EDR/XDR, SASE, and identity tools.

---

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric
ISO 27001	Information security management	Zero-trust access, immutable audit trails
IEC 62443 (OT)	Security for operational technology and industrial systems	Hardware isolation and segmentation for critical infrastructure nodes
National cybersecurity strategy / CNI protection	Governance, incident management, and protection of critical national infrastructure	Hardware-enforced boundaries, autonomous key rotation, and auditable compliance evidence

---

5. A low-risk pilot path

- **Select** a non-critical subsystem or a single designated critical-infrastructure node as an initial scope.
- **Deploy** the edge node inline — a fast install with no changes to production or mission-critical systems.
- **Validate** isolation with a red-team exercise; legitimate traffic passes, attacks are blocked.
- **Demonstrate** post-quantum key rotation and audit evidence; reverse cleanly if desired.

Ready to secure your national security infrastructure?

Request a briefing to see how a low-risk pilot would work in your environment.

Request a briefing

⬇ Download PDF

Back to overview

Prefer email? Reach us at hello@iblades.ai

---

iblades.ai™

Safe, effective, secure.

Next-generation cyber architecture making cybersecurity simple, reliable, and accessible for everyone.

hello@iblades.ai

Products

- NetTron™
- GuardTron™
- ManoTron™
- Pricing

Solutions

- Financial Institutions
- Healthcare
- Infrastructure
- Government & Military

Company

- About Us
- Partners
- Documentation
- Contact

Compliance

- NIST Approved
- SOC 2 Type II
- HIPAA Compliant
- ISO 27001
- FedRAMP Ready

HEADQUARTERS
127 Spring Street, Suite 120
Pleasanton, CA 94566

R&D CENTER
795 24th Street
Ogden, UT 84401