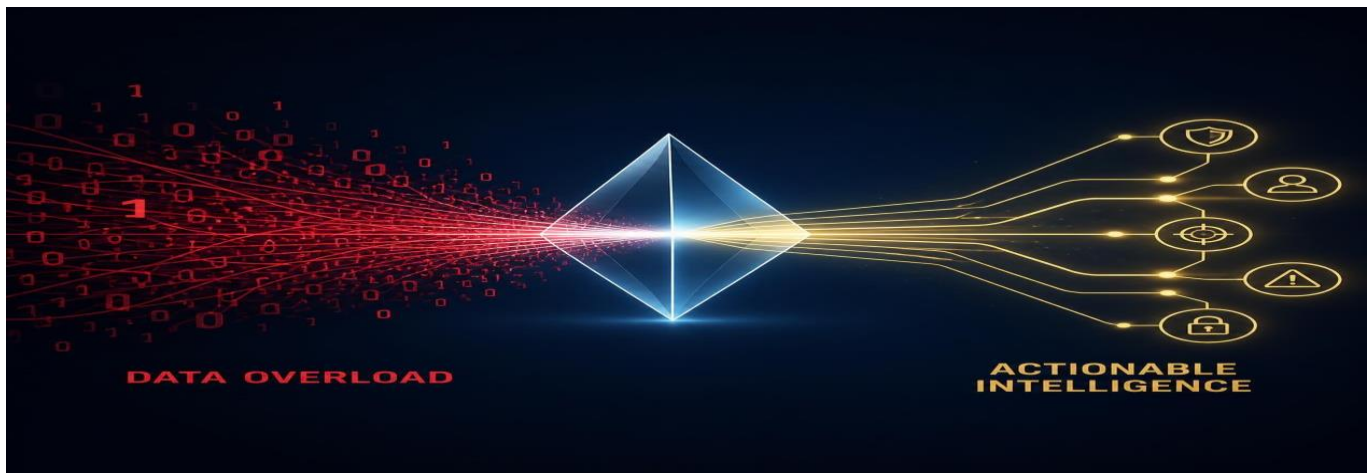


Data vs Intelligence

Strategic Vision & Operational Fundamentals

Redefining Intelligence Sharing & Cross-Sector Collaboration



Executive Overview

For decades, the standard approach across government, law enforcement, and corporate entities to threat intelligence sharing was built on a flawed premise:

THE FLAWED PARADIGM

"Hey – ya know what – just give me all of your data/stuff and we'll figure it out."

Why it fails: Centralized data dumping without direct, domain-specific context creates massive legal liabilities, generates signal-to-noise overload, and breeds deep mistrust among participating organizations.

The National Cyber-Forensics and Training Alliance (NCFTA) was built on a different model—one centered on federated, SME-driven collaboration, mutual trust, and actionable co-location of expertise.

KEY STRATEGIC TAKEAWAY

True intelligence is not raw telemetry—it requires embedded Subject Matter Experts (SMEs) collaborating in a neutral, trust-based ecosystem to deliver real-time operational outcomes.

Key Fundamentals

- **Data vs. Intelligence:** Intelligence is just data without Subject Matter Experts (SMEs) to understand and utilize it. Raw technical telemetry, hashes, or logs without context can create noise rather than clarity.
- **Position & Mindset Shift:** Our fundamental stance must shift from requesting raw assets to inviting collaborative expertise:

"Don't give me your Intelligence (or Data) — bring it with you."

- *"Join our collaborative alliance to make better use of it for our common objectives."*

- **Defining Common Objectives:** Collaboration requires clear alignment. Shared operational objectives must translate into concrete, measurable metrics for success across all participating sectors.

Strategic Model Comparison – Legacy vs The NCFTA approach

Key Dimension	Legacy Data Dump Model	NCFTA Collaborative Alliance Model
Data Philosophy	"Give us your data" (Centralized hoarding)	"Bring your data & SMEs with you"
Space & Environment	Government / Law Enforcement siloes	Neutral, peer-to-peer co-located space
SME Integration	SMEs disconnected from analysts	Direct cross-sector SME co-creation
Outcome / Value	High noise, delay, and liability	High-context, actionable operational value

Lessons Learned from the Field

- **Cross-Sector Collaboration is Vital:** No single organization or government agency possesses full visibility into the threat landscape.
- **Neutral Space Matters:** It is highly unlikely that meaningful and timely bidirectional intelligence exchange will occur strictly inside traditional Government or Law Enforcement spaces. A neutral environment is essential for true peer-to-peer engagement.
- **Inhibitors are Conceptual, Not Actual:** The primary barriers working against effective collaboration are mindset, organizational culture, and legacy assumptions—not technical or legal impossibilities.

The Cross-Sector Strategic Ecosystem



1. Government Partners ● Federal Agencies: FBI, Secret Service, CISA, DOJ ● State & Local: Fusion centers and regional law enforcement ● Defense: Military cyber components and intelligence arms	2. Private Sector ● Financial Services: Banking networks and payment processors ● Critical Infrastructure: Telecom, Energy, Healthcare ● Technology & Commerce: Cloud providers, Retail, Manufacturing
3. Academia ● Research Institutions: Cutting-edge cyber security labs ● Training Hubs: Specialized curriculum development ● Talent Pipeline: Next-generation threat analyst cultivation	4. International Partners ● Global Law Enforcement: Interpol, Europol, allied nations ● Multinational Nodes: Global threat intelligence sharing units ● Cross-Border Operations: Coordinated adversary disruptions

Building the Model for the Future

To sustain this alliance model, we must seek to identify and empower leaders across all four sectors. These efforts must seek to evolve to match the changing landscape across industry and the corresponding adversary environment we collectively seek to dismantle.

THE ASK

Bring your expertise along with the intelligence you already possess. Join the neutral collaborative environment where it can be acted upon together and more impactfully.

EXECUTIVE SUMMARY

By replacing legacy, centralized data dumps with an SME-driven, neutral alliance model bringing Government, Industry, Academia, and international partners together. Through this model, the NCFTA turns static data into decisive, real-time intelligence leading to more sustained threat disruption.