The AI Supply Chain: A National Security Imperative

In an era of unprecedented global disruption, the next frontier of national security isn't just cyber defense—it's how we secure the systems that make AI possible.

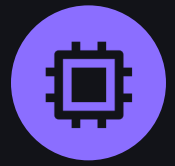
EXIGER

The Era of Global Disruption

Our ability to deploy AI at scale now sits inside a fragile global infrastructure where interdependencies multiply risk.

Geopolitical Tension

Russia-Ukraine conflict exposed critical infrastructure vulnerabilities and semiconductor supply dependencies that ripple across nations.



Semiconductor Fragility

Advanced chip manufacturing concentrated in vulnerable geographic regions creates systemic risk for global AI deployment.

Climate Disruption

Extreme weather events increasingly threaten data centers, power grids, and physical infrastructure supporting AI systems.

The Hidden Backbone: AI's Supply Chain

The future of AI security starts with securing the infrastructure that makes AI possible

Physical Infrastructure

- Semiconductors and advanced chips
- Data centers and compute facilities
- Power generation and cooling systems
- Network connectivity infrastructure

Digital Dependencies

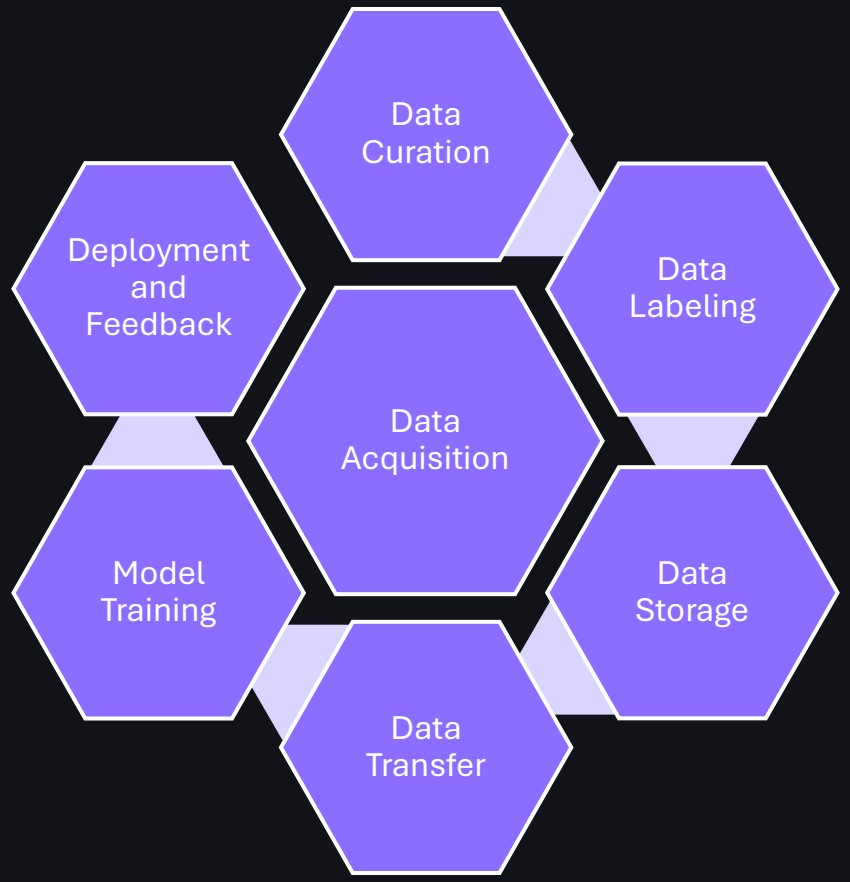
- Training data and datasets
- Open-source software libraries
- Model architectures and frameworks
- Third-party APIs and services

The Expanding Attack and Vulnerability Surface

The Artificial Intelligence Supply Chain is an Evolution of the Traditional ICT Supply Chain

Dimension\	ICT Supply Chain	AI Supply Chain
Physical dependencies	Hardware, firmware	Still critical, but amplified by chip concentration
Software dependencies	Open-source libraries, OS layers	Extended to ML frameworks and toolchains
Data	Input/output of systems	Core raw material – must be trusted, governed, and traceable
Models	Not applicable	New artifact that's trained, shared, and reused
Algorithms	Abstract logic	Toolchain dependency, not a "supply" in itself
Governance	Component certification	Lifecycle assurance – provenance, bias, integrity, explainability

Data is the Key Supply Chain Asset – Managing it Introduces Risk



Risk Profile

- *Integrity Risks* (tampering, poisoning)
- *Privacy Risks* (leakage, exposure)
- *Provenance Risks* (loss of lineage)
- Human Risks (insider, bias)
- Infrastructure Risks (cloud misconfiguration)

From Dependencies to Decisions

We use AI not only to secure the supply chain—but to ensure the AI supply chain itself is trustworthy.

AI Depends on the Supply Chain

Chips, power, data, and infrastructure form the foundation that enables AI capabilities and deployment at scale.

AI Secures the Supply Chain

Advanced analytics, monitoring, and intelligence transform how we identify, assess, and mitigate supply chain vulnerabilities.

Resilience comes from insight—and insight comes from securing the intelligence infrastructure itself

Turning the Lens Around: Using AI to Secure the Chain

Traditional Approach

- Manual vendor assessments
- Periodic compliance reviews
- Reactive incident response
- Limited visibility into sub-tiers

AI-Driven Assurance

- Continuous automated monitoring
- Real-time anomaly detection
- Predictive risk analytics
- Deep supply chain visibility

The good news: AI is also our most powerful tool for identifying and mitigating the vulnerabilities it exposes.

Priorities for Securing the AI Supply Chain

Your Roadmap

- 1. Establish Data Provenance and Lineage
- 2. Secure the Model Lifecycle
- 3. Protect the Data Pipeline
- 4. Strengthen AI Toolchain Assurance
- 5. Diversify and Resilientize Compute Infrastructure
- 6. Integrate Governance and Technical Security

The Challenge

Securing the AI supply chain means safeguarding the integrity of our data, the provenance of our models, and the transparency of our decisions.”

The National Security Frame

Critical Imperatives

- Establish trusted supplier ecosystems
- Implement continuous verification protocols
- Build redundancy into critical dependencies

Public-Private Mission

National resilience depends on whether we can trust the systems that generate and deliver intelligence. This is not a challenge any single entity can solve alone.

Effective supply chain security requires seamless collaboration between government oversight, industry innovation, and shared intelligence frameworks.

The Long Game

Sustained Visibility

Continuous monitoring creates persistent awareness of supply chain health, dependencies, and emerging risks.

Adaptive Defense

AI-driven systems evolve with threats, learning from each incident to strengthen future resilience.

Collaborative Ecosystems

Shared intelligence and coordinated response transform individual vulnerabilities into collective strength.

Building Enduring Resilience

where AI and supply chain resilience reinforce one another—where innovation and security advance together, not in opposition.

If AI is redefining our threats, it must also redefine our resilience.

Winning The Long Game Together

The Exiger Commitment

At Exiger, we're using AI to bridge visibility, trust, and security—transforming supply chain risk from a blind spot into a strategic advantage.

Let's Build Resilience Together

The threats are evolving. Our response must be equally dynamic, intelligent, and collaborative.

We believe that collaboration is how we win the long game. National security and infrastructure resilience require partnerships that span government, industry, and technology innovation.