WHITE PAPER: Strategic Infrastructure Resilience

Subject: Cyber-Kinetic Cascades and the CCIE-Defense Framework

Author: Dr. Stephen Dietrich-Kolokouris

Classification: Corporate/Strategic Public Release

1. Executive Summary: The Infrastructure-Conflict Nexus

Modern corporate logistics are no longer merely "supported" by networking; they are **defined** by it. In the same way that **WarSim v5.6** models the collapse of Command Continuity (CCL) during kinetic conflict, corporate entities face "Strategic Darkness" when their networking Control Plane is compromised. This paper outlines the granular technical remediation of systemic degradation in global supply chains.

2. Granular Activity: Layer 3 Pathologies & Logistics

Critical infrastructure failure usually begins at the granular level before cascading into systemic collapse.

A. The BGP Hijack: Logistics Identity Theft

- **The Technical Event:** An adversary utilizes unauthorized Autonomous System (AS) advertisements to reroute the global routing table.
- **The Corporate Cascade:** Shipping telematic streams (AIS) and Warehouse Management Systems (WMS) are intercepted. For a Global Tier-1 Logistics firm, this results in **"Dark Hubs,"** where cargo is physically present but digitally invisible.
- **Remediation (CCIE Logic):** Deployment of **RPKI** for route origin validation and **BGP Prefix Independent Convergence (PIC)**. By tuning BGP timers for sub-second reconvergence, we reduce the "OODA Loop" of the network failure, preventing the port congestion that leads to a $2.5M/day loss.

B. MPLS Label Exhaustion: Energy Grid Blackouts

- **The Technical Event:** Targeted DDoS or kinetic destruction of Label Switch Routers (LSRs) leading to path exhaustion.
- **The Corporate Cascade:** In the Energy sector (OT Plane), the loss of MPLS path protection breaks the **SCADA/DCS** heartbeat. Safety interlocks at power substations, sensing a loss of "Command Continuity," trigger a manual shutdown to prevent physical damage.

- **Remediation (CCIE Logic):** Transitioning from legacy MPLS to **Segment Routing (SR-TE)**. SR-TE allows for source-based routing and automated **Fast Reroute (FRR)**, ensuring that critical energy-grid traffic maintains a 50ms recovery time even if the primary backbone is severed.

3. From Granular to Overview: The Purdue Model Correlation

The degradation of critical infrastructure follows the **Purdue Model** hierarchy. A network-level failure at the CCIE-layer (Level 3.5) creates a "Cyber-Kinetic Bridge" into the physical world.

1. **Level 4 (Enterprise):** Inventory visibility is lost.
2. **Level 3 (Operations):** Just-in-Time (JIT) manufacturing ceases.
3. **Level 0-2 (Physical):** Safety PLCs trip, causing physical asset degradation.

4. WarSim v5.6 Correlation: The 7.5% Threshold

Our simulations indicate that a **7.5% nuclear escalation rate** in military scenarios is almost always preceded by a **total failure of civilian infrastructure**. In a corporate context, this is the "Point of No Return," where the network degradation is so severe that the cost of recovery exceeds the value of the assets. By hardening the granular networking layer (CCIE), we move the "Nuclear" (Total Systemic) failure probability back toward the **Ceasefire (25%)** or **Stability** zones.