CYBERSWITCH TECHNOLOGIES

CRITICAL INFRASTRUCTURE: CHINA IS ALREADY INSIDE

www.cyberswitchtech.com

Why Critical Infrastructure is at Risk

- Legacy Networks: Many systems still run on decades-old technology never designed to withstand modern cyber threats.
- Flat Architectures: Lack of segmentation enables attackers to move laterally once inside.
- Known IPs & Static Routes: Easily mapped and targeted by adversaries.
- Third-Party Access: Vendor maintenance portals are often the weakest link.
- Physical Consequences: Successful attacks can shut down cities, contaminate water supplies, or disable emergency services.

What is RAVID?

RAVID is a security overlay designed to cloak, segment, and continuously change your infrastructure's digital footprint. It is purpose-built for high-stakes, low-tolerance environments like:

- Electric Utilities
- Oil & Gas Pipelines
- Transportation Hubs (Airports, Ports, Rail)
- Water Treatment Facilities
- Public Safety Communications

Core Capabilities:

- Ephemeral Network Tunnels: Constantly rotate device visibility and access points.
- Zero Trust Access: Authenticate every user and device continuously.
- Micro/Macro Segmentation: Isolate systems and departments to contain breaches.
- AI-Powered Behavioral Analysis: Identify threats in real time before they act.
- Non-Disruptive Deployment: Overlay model means no downtime or rip-and-replace.

Use Case Examples

1. Electric Utility – Power Grid Control Systems
Problem: Threat actors attempt to manipulate SCADA systems controlling transformers and substations.
Solution: RAVID makes SCADA interfaces invisible on the network, segments access zones, and requires real-time multi-factor authentication for any command issuance.

2. Water Utility – Remote Treatment Plant Access
Problem: Remote login portal for water quality control accessed through brute-force credential stuffing.

Solution: RAVID blocks unauthorized traffic before the system even becomes visible, and logs behavioral patterns to alert on abnormal access hours or devices.

3. Transportation – Smart Rail Systems
Problem: Sensor spoofing and DDoS attempts against predictive rail traffic systems.
Solution: RAVID cloaks communication paths and dynamically shifts network infrastructure, nullifying external scans and traffic flooding.

4. Emergency Communications – 911 & Dispatch Networks
Problem: Legacy IP systems vulnerable to disruption or spoofing.
Solution: With RAVID, all communications routes are encrypted, identity-verified, and only temporarily available per authenticated session.

How RAVID Deploys

- Works with legacy protocols (Modbus, DNP3, ICCP, SNMP)
- Integrates with SIEMs and Security Operations Centers
- Deployed via appliance, VM, or cloud as needed
- 100% air-gapped options for fully isolated critical assets

Deployment Timeline:

- Evaluate: Identify attack surfaces, high-value assets, and remote entry points.
- Install Overlay: Deploy RAVID layer across priority zones.
- Monitor: Tune behavioral AI with your SOC.
- Scale: Expand segmentation, deploy across remaining zones.

Benefits to Critical Infrastructure Operators

- Invisibility to Hackers – Eliminate discoverable IPs and static services
- No Downtime Needed – Deploy without interrupting critical services
- Reduce Insurance Premiums – Demonstrate measurable risk reduction
- Enhance Regulatory Compliance – Aligns with NERC-CIP, NIST CSF, CISA directives
- Boost Public Trust – Proactively secure essential services

Closing Statement

Cybersecurity for critical infrastructure isn't just about compliance—it's about survival. A breach isn't just a data loss; it's a threat to life, commerce, and national defense. RAVID was engineered by security veterans who understand this reality and built a solution to meet it.

Whether you operate a control room, pump station, switching center, or dispatch desk, RAVID turns your network from a target into a ghost. Threat actors cannot breach what they cannot see.

CYBERSWITCH TECHNOLOGIES

CYBERSECURITY

Cybersecurity is complicated, ever-evolving, and 24/7.

The greatest business value is with an expert partner who can assess your current risks, secure your data and networks, and help you plan for the future.

Our team is comprised of industry experts with successful client implementations in Professional Sports, Entertainment, Media, Commercial, Federal, Civilian and Public Sector.

CONTACT INFORMATION

Marcus Crockett, CEO

Cyberswitch Technologies

678.235.9076

ceo@cyberswitchtech.com