Security Architecture Portfolio

Dr. Stephen Dietrich-Kolokouris | CCIE | Cybersecurity Professional

---

Professional Summary

Dr. Stephen Dietrich-Kolokouris is a CCIE-certified cybersecurity professional with extensive experience in penetration testing, network security auditing, incident response, and critical infrastructure protection. His career spans classified government contracting environments through private-sector security architecture roles, with particular depth in supply chain vulnerability analysis and adversarial threat modeling.

Core Certifications & Qualifications

- CCIE (Cisco Certified Internetwork Expert) -- Elite-level network infrastructure certification
- Penetration testing expertise across enterprise, OT/ICS, and cloud environments
- Network security audit methodology for critical infrastructure sectors
- Supply chain risk analysis specializing in firmware and hardware-level threats
- Incident response planning, tabletop exercises, and post-breach forensics

Penetration Testing & Red Team Operations

Dr. Dietrich-Kolokouris has conducted penetration testing engagements across multiple sectors including energy, telecommunications, and defense-adjacent networks. His methodology integrates OWASP, NIST SP 800-115, and PTES frameworks with custom tooling developed for OT/ICS environments where standard IT pen-testing approaches are insufficient or dangerous.

Technical Competencies

- External and internal network penetration testing
- Web application security assessment (OWASP Top 10)
- Wireless network auditing (WPA2/WPA3, rogue AP detection)
- Social engineering and phishing campaign design
- Active Directory attack path analysis and privilege escalation
- OT/SCADA vulnerability assessment with safety-first protocols

Network Security Architecture

With CCIE-level expertise, Dr. Dietrich-Kolokouris designs and audits enterprise network architectures with defense-in-depth principles. His work includes zero-trust architecture implementation, network segmentation strategies for mixed IT/OT environments, and firewall rule optimization for organizations with 10,000+ rule sets.

Architecture Deliverables

- Zero-trust network design and microsegmentation planning
- Firewall architecture review and rule-base optimization
- VPN and remote access security hardening
- Network traffic analysis and anomaly detection deployment
- DNS security, BGP route validation, and DDoS mitigation planning
- Cloud-hybrid network security (AWS VPC, Azure NSG, GCP VPC)

Supply Chain Vulnerability Research

Dr. Dietrich-Kolokouris has conducted original research on supply chain threats to critical infrastructure, with particular focus on Chinese sleeper malware embedded in firmware and hardware components. His research examines rare earth element dependency, firmware-level persistence mechanisms, and the intersection of geopolitical strategy with technical exploitation.

Research Focus Areas

- Firmware integrity analysis and backdoor detection methodologies
- Rare earth element (REE) supply chain risk scoring
- Hardware implant threat modeling for critical infrastructure components
- Vendor risk assessment frameworks for defense and energy sectors
- National-level supply chain resilience recommendations submitted to DoD

Incident Response & Crisis Management

Experience designing and executing incident response plans for organizations ranging from mid-market enterprises to government agencies. Particular expertise in developing playbooks for supply chain compromise scenarios, advanced persistent threat (APT) containment, and coordinated disclosure processes.

- IR plan development aligned with NIST CSF and CISA guidelines
- Tabletop exercise design and facilitation for executive leadership
- Digital forensics and evidence preservation procedures
- Threat intelligence integration into detection and response workflows
- Post-incident lessons-learned reporting and control gap remediation

Critical Infrastructure Protection

Dr. Dietrich-Kolokouris specializes in the security challenges unique to critical infrastructure sectors as defined by CISA, including energy, water, transportation, and communications. His work bridges the gap between IT security best practices and the operational constraints of industrial control systems where availability and safety take precedence over confidentiality.

- ICS/SCADA security assessment following IEC 62443 and NERC CIP
- Air-gapped network design and secure data diode implementation
- Physical-cyber convergence threat analysis
- Sector-specific regulatory compliance (NERC CIP, TSA Security Directives)
- DHS National Exercise Simulation platform development for infrastructure resilience testing