Dr. Stephen Dietrich-Kolokouris

CCIE | PhD | Former CIA Contractor | Published Author | AI Engineer

A complete professional profile spanning hands-on technical operations through enterprise architecture, policy development, intelligence analysis, AI engineering, and published research.

This document provides a comprehensive view of Dr. Dietrich-Kolokouris's capabilities across the full IT spectrum. From desktop support and system administration through CCIE-level network engineering, security architecture, AI/ML system design, intelligence operations, policy authorship, and academic research -- each discipline reinforces the others. The thread connecting everything is the ability to understand systems at every layer, communicate across technical and executive audiences, and deliver results in high-stakes environments where precision matters.

Part 1: Foundation -- Desktop Support & Systems Administration

Every senior technologist who can't troubleshoot a broken workstation has a blind spot. Dr. Dietrich-Kolokouris built his career from the ground up, starting with hands-on desktop support and systems administration across both Windows and Linux environments. This foundation is not a historical footnote -- it informs every architecture decision, every security assessment, and every conversation with operations teams.

Windows Environment

Deep operational experience across the full Microsoft ecosystem, from individual workstation troubleshooting through enterprise Active Directory design.

- Windows desktop support (Windows 7/8/10/11) -- hardware diagnostics, driver conflicts, OS recovery, user profile migration
- Active Directory design, Group Policy management, OU structure, delegation models
- Windows Server administration (2012 R2 through 2022) -- DHCP, DNS, file services, print services
- Microsoft 365 administration -- Exchange Online, SharePoint, Teams, Entra ID (Azure AD)
- PowerShell scripting for automation, bulk user management, log analysis, and compliance reporting
- SCCM/Intune endpoint management -- deployment, patching, compliance baselines, application packaging
- Windows event log analysis for security monitoring and incident investigation
- Hyper-V virtualization -- VM provisioning, snapshot management, live migration
- BitLocker encryption management and TPM configuration
- WSUS and Windows Update for Business patch management strategies

Linux Environment

Production Linux experience spanning server administration, security hardening, and development environment management. Comfortable at the command line in environments where GUI tools don't exist.

- Linux server administration -- Ubuntu, CentOS/RHEL, Debian, Kali Linux
- Bash scripting for system automation, log rotation, backup procedures, and monitoring
- Package management (apt, yum/dnf, snap) and dependency resolution
- SSH hardening, key-based authentication, jump host configuration
- iptables/nftables firewall configuration and traffic analysis
- systemd service management, journalctl log analysis, cron scheduling
- Apache/Nginx web server configuration, virtual hosts, reverse proxy, SSL/TLS
- Docker container deployment, Dockerfile creation, docker-compose orchestration
- File system management -- LVM, RAID configuration, disk encryption (LUKS)
- SELinux and AppArmor security policy configuration
- Python environment management -- virtualenv, conda, pip dependency management
- Kali Linux for penetration testing toolsets -- Nmap, Metasploit, Burp Suite, Wireshark

Cross-Platform & Helpdesk Operations

- Ticketing system management and SLA compliance in enterprise helpdesk environments
- Hardware troubleshooting -- laptops, desktops, printers, peripherals, docking stations
- Network troubleshooting from the endpoint -- DNS resolution, DHCP leases, proxy configuration, VPN connectivity
- Remote support tools -- RDP, TeamViewer, VNC, SSH tunneling
- Asset management, inventory tracking, and lifecycle planning
- End-user training and documentation for both technical and non-technical audiences
- Imaging and deployment -- PXE boot, WDS, Clonezilla, Fog
- Mobile device management (MDM) for iOS and Android in enterprise environments

Why this matters: When Dr. Dietrich-Kolokouris designs a security architecture or reviews an AI deployment, he understands the operational reality at every layer. Desktop support experience means he can talk to the help desk, the sysadmin, the network engineer, the CISO, and the board -- because he has been each of those roles.

Part 2: Network Engineering -- CCIE-Level Expertise

The Cisco Certified Internetwork Expert (CCIE) is the most demanding networking certification in the industry, held by fewer than 3% of networking professionals worldwide. Dr. Dietrich-Kolokouris earned this certification and has applied that depth of knowledge across enterprise, government, and critical infrastructure networks.

Routing & Switching

- BGP -- multi-homed enterprise design, route filtering, prefix-list and route-map policy, community-based traffic engineering
- OSPF -- multi-area design, stub area optimization, NSSA, virtual links, LSA filtering
- EIGRP -- wide metric, stub routing, route summarization, named mode configuration
- Spanning Tree Protocol -- RSTP, PVST+, MST, root guard, BPDU guard, loop prevention
- VLAN design -- access/trunk/native VLAN architecture, VTP, private VLANs, Q-in-Q
- EtherChannel -- LACP, PAgP, L2/L3 port-channel design, load balancing methods
- First Hop Redundancy -- HSRP, VRRP, GLBP configuration and failover design
- QoS -- DSCP marking, queuing (LLQ, CBWFQ), policing, shaping, end-to-end QoS design
- Multicast -- PIM sparse mode, IGMP snooping, RP placement, multicast troubleshooting

Network Security

- Cisco ASA and Firepower NGFW -- access policy, IPS, malware defense, VPN termination
- Zone-based firewall design on IOS/IOS-XE platforms
- 802.1X port-based network access control with RADIUS/TACACS+ integration
- Network segmentation and microsegmentation for zero-trust architectures
- IPsec and SSL VPN design -- site-to-site, remote access, DMVPN, FlexVPN
- DNS security -- DNSSEC, DNS sinkholing, encrypted DNS (DoH/DoT) policy
- Network forensics -- packet capture, flow analysis, NetFlow/sFlow, traffic baseline deviation

Wireless & Cloud Networking

- Cisco wireless LAN controller (WLC) design, RF planning, rogue AP detection
- Wi-Fi 6/6E enterprise deployment and security (WPA3-Enterprise, RADIUS)
- AWS VPC architecture -- subnets, route tables, NACLs, security groups, Transit Gateway
- Azure virtual networking -- NSGs, VNet peering, ExpressRoute, Azure Firewall
- Hybrid cloud connectivity -- Direct Connect, ExpressRoute, SD-WAN overlay
- Software-defined networking concepts -- Cisco ACI, DNA Center, intent-based networking

Professional Experience

Applied CCIE-level networking at Cisco Global Services and L3Harris Technologies, working on networks where downtime is not an option and security is not optional. This includes classified government networks, defense contractor environments, and critical infrastructure sectors where network reliability has direct operational and safety implications.

Part 3: Cybersecurity & Security Architecture

Security is not a layer bolted on top -- it is a design principle that must be present at every level, from endpoint configuration through network architecture to organizational policy. Dr. Dietrich-Kolokouris brings this philosophy to every engagement.

Offensive Security

- External and internal penetration testing using OWASP, NIST SP 800-115, and PTES methodologies
- Web application security assessment -- injection, authentication bypass, SSRF, IDOR
- Active Directory attack path analysis -- Kerberoasting, AS-REP roasting, DCSync, Pass-the-Hash
- Social engineering campaign design -- phishing, pretexting, physical security testing
- Wireless network auditing -- WPA2/WPA3 attacks, evil twin, deauth, credential capture
- OT/SCADA vulnerability assessment with safety-first protocols for industrial environments
- Red team operations -- adversary emulation, C2 framework deployment, lateral movement
- Exploit development fundamentals -- buffer overflow, ROP chains, shellcode analysis

Defensive Security & Architecture

- Zero-trust architecture design and implementation roadmaps
- Network segmentation and microsegmentation for IT/OT convergence environments
- SIEM deployment and tuning -- log correlation, alert fatigue reduction, use case development
- Endpoint detection and response (EDR) deployment and policy configuration
- Threat intelligence integration into detection and response workflows
- Vulnerability management program design -- scanning, prioritization, SLA tracking
- Security architecture review for cloud, hybrid, and on-premises environments
- Encryption strategy -- data at rest, in transit, key management, certificate lifecycle

Incident Response

- IR plan development aligned with NIST CSF, CISA, and SANS incident handling frameworks
- Tabletop exercise design and facilitation for technical teams and executive leadership
- Digital forensics -- disk imaging, memory analysis, timeline reconstruction, chain of custody
- Malware analysis fundamentals -- static analysis, behavioral analysis, indicator extraction
- Post-incident reporting, root cause analysis, and control gap remediation
- Breach notification coordination and regulatory reporting requirements

Supply Chain Security Research

Original research on supply chain threats to critical infrastructure, with particular focus on Chinese sleeper malware embedded in firmware and hardware components. This research examines rare earth element

dependency, firmware-level persistence mechanisms, and the intersection of geopolitical strategy with technical exploitation. Findings have been submitted to Department of Defense and Department of Homeland Security contacts.

- Firmware integrity analysis and backdoor detection methodologies
- Rare earth element (REE) supply chain risk scoring algorithms
- Hardware implant threat modeling for defense and energy sector components
- Vendor risk assessment frameworks with quantitative scoring
- National-level supply chain resilience recommendations
- WarSim Algorithm -- conflict simulation system submitted to DoD incorporating supply chain variables

Part 4: AI Engineering & RAG System Development

Dr. Dietrich-Kolokouris designs and deploys production AI systems with an emphasis on retrieval-augmented generation, where every AI response is grounded in real source material. This is not theoretical -- these are deployed, user-facing systems.

Production RAG Systems

- End-to-end RAG pipeline design: document ingestion, chunking, embedding, indexing, retrieval, generation
- LangChain framework -- chains, retrievers, prompt templates, output parsers, agent tooling
- Vector databases -- FAISS (local), ChromaDB (persistent), with metadata filtering and MMR retrieval
- Embedding models -- OpenAI text-embedding-ada-002, text-embedding-3-small, cost/performance optimization
- Chunking strategy -- RecursiveCharacterTextSplitter with optimized parameters for different document types
- Evidence pack formatting -- source deduplication, page-level citation, context window management
- Guardrail systems -- regex-based output filtering to prevent hallucinated URLs and fabricated citations
- Index persistence -- SHA-256 manifest system that rebuilds only when source documents change
- Streaming response delivery for real-time user experience

LLM Application Architecture

- GPT-4o and GPT-4o-mini integration with cost-optimized routing (heavy model for answers, light model for preprocessing)
- System prompt architecture -- layered constraints, action modes, tone control, context injection
- Structured JSON extraction from natural language using LLM function calling
- History-aware query rewriting for multi-turn conversations
- Action mode switching -- chat, fit summary, outreach drafting, verification
- Recruiter intent extraction -- silent per-turn analysis of roles, domains, locations, requirements
- Prompt engineering -- few-shot, chain-of-thought, constraint layering, guardrail design

Agent Frameworks & Automation

- OpenAI function calling and tool-use agent patterns
- Browser automation agents for web research and data collection
- Multi-agent orchestration with tool selection, error recovery, and human-in-the-loop flows
- YouTube Script Generator for content creation across paranormal, true crime, and history genres
- NAMECOMMS (Neural Anomaly Manifold Entropy Communication System) -- custom research instrumentation

- Streamlit application development for user-facing AI interfaces
- Python full-stack development -- API integration, data processing, PDF generation, web deployment

Data Engineering

- PDF document processing pipelines -- PyPDF, pdfplumber, text extraction, table extraction
- Data cleaning, deduplication, and preprocessing for ML pipelines
- Vector database administration -- index optimization, retrieval parameter tuning
- API integration -- OpenAI, Anthropic, LangChain ecosystem
- Cost monitoring and optimization for production LLM applications

Part 5: Intelligence Operations & Analysis

Dr. Dietrich-Kolokouris served as a CIA contractor supporting counterterrorism operations during the Al-Qaeda and ISIS operational theaters. This experience provides a dimension that most IT professionals simply do not have: the ability to operate in environments where information is incomplete, stakes are existential, and analytical rigor is the difference between mission success and catastrophic failure.

Operational Experience

- CIA contractor supporting counterterrorism (CT) operations
- Operational experience during Al-Qaeda and ISIS active threat periods
- Classified environment work requiring strict compartmentalization and need-to-know protocols
- Intelligence analysis -- structured analytical techniques, hypothesis testing, alternative analysis
- Secure communication protocols and operational security (OPSEC) best practices
- Cross-functional collaboration with intelligence community partners
- Experience working within SCIF and classified processing facilities

Analytical Tradecraft Applied to IT

Intelligence analysis tradecraft directly transfers to cybersecurity threat analysis, incident investigation, and strategic technology planning:

- Structured Analytical Techniques (SATs) -- Analysis of Competing Hypotheses, key assumptions check, devil's advocacy
- Indicator development -- translating threat intelligence into actionable detection signatures
- Pattern-of-life analysis applied to network traffic and user behavior analytics
- Open source intelligence (OSINT) collection and validation methodologies
- Report writing for multiple audiences -- technical detail for operators, executive summary for leadership
- Threat modeling that accounts for adversary capability, intent, and opportunity
- Decision support under uncertainty -- probabilistic assessments, confidence levels, information gaps

Security Clearance

Held security clearance as required for CIA contractor roles. Experienced with the personnel security process including SF-86, polygraph procedures, and periodic reinvestigation requirements. Specific clearance level and current status should be verified directly with Dr. Dietrich-Kolokouris.

Part 6: Policy Development, Governance & Compliance

Technical skills without policy understanding create blind spots. Policy without technical depth creates shelfware. Dr. Dietrich-Kolokouris bridges both -- he can write the firewall rule and the policy that governs it, draft the incident response plan and execute it, design the compliance framework and implement the controls.

Security Policy & Governance

- Information security policy development -- acceptable use, access control, data classification, incident response
- Security program design aligned with NIST CSF Identify, Protect, Detect, Respond, Recover functions
- Risk management frameworks -- NIST RMF, ISO 27005, FAIR quantitative risk analysis
- Security awareness training program design and phishing simulation campaigns
- Vendor risk management -- third-party security assessments, questionnaire design, continuous monitoring
- Board-level and executive security briefing development
- Security metrics and KPI frameworks for program effectiveness measurement
- Business continuity and disaster recovery planning -- BIA, RTO/RPO, tabletop exercises

Compliance Frameworks

Federal & Defense

- NIST Cybersecurity Framework (CSF) -- risk management, security control mapping, maturity assessment
- NIST SP 800-53 -- security and privacy controls for federal information systems
- NIST SP 800-171 -- protecting CUI in nonfederal systems, CMMC alignment
- FISMA -- Federal Information Security Management Act compliance and reporting
- FedRAMP -- cloud service provider authorization for federal use
- ITAR/EAR -- export control regulations for defense-related technical data

Critical Infrastructure

- NERC CIP -- power grid cybersecurity standards (CIP-002 through CIP-014)
- TSA Security Directives -- pipeline and transportation sector requirements
- IEC 62443 -- industrial automation and control systems security lifecycle
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs)
- CFATS -- Chemical Facility Anti-Terrorism Standards

Industry Standards

- ISO 27001/27002 -- ISMS implementation, certification audit preparation, control selection
- SOC 2 Type II -- trust service criteria, audit evidence collection, gap remediation
- PCI DSS -- cardholder data environment scoping, SAQ, compensating controls
- HIPAA Security Rule -- ePHI protection, risk analysis, BAA requirements

- GDPR -- data protection impact assessments, DPO responsibilities, cross-border transfer mechanisms

Policy Drafting & Implementation

Dr. Dietrich-Kolokouris has experience drafting, reviewing, and implementing security policies for organizations at various maturity levels. His approach combines regulatory requirements with operational reality:

- Gap analysis between current state and target compliance framework
- Policy document authorship -- clear, enforceable language that technical and non-technical staff can follow
- Standard operating procedure (SOP) development for security operations
- Control implementation roadmaps with prioritization based on risk and resource constraints
- Audit preparation and evidence collection strategies
- Policy exception management and compensating control documentation
- Change management for security policy rollout -- communication plans, training, enforcement timelines

Part 7: Publications, Research & Academic Work

Dr. Dietrich-Kolokouris is the author of seven published books and holds a PhD from Goethe University Frankfurt. His published work demonstrates research methodology, analytical writing, and subject matter expertise that directly reinforces his technical capabilities. Each publication is summarized below.

The American Paranormal

Genre: Investigative Research / Consciousness Studies

A comprehensive 400-page scholarly investigation into 150 years of American spiritualism and consciousness research. The book documents field investigations conducted alongside evidential medium Cindy Kaza, applying rigorous analytical frameworks to anomalous experiences typically dismissed by mainstream academia. Research locations included Skinwalker Ranch, where Dr. Dietrich-Kolokouris conducted EMF analysis and sensor data collection.

The work bridges scientific inquiry with consciousness research, maintaining evidentiary standards throughout. Published with a Halloween 2025 launch, supported by media appearances including Fox 4 Dallas.

Key skills demonstrated: Primary source research, field investigation methodology, sensor data analysis (EMF), evidence-based argumentation, long-form scholarly writing, media engagement and public communication.

Chicago Ripper Crew: Reboot

Genre: True Crime Investigation

A re-examination of one of Chicago's most notorious serial murder cases, incorporating previously unexplored documentation and witness accounts. Dr. Dietrich-Kolokouris revisited original case evidence with fresh analytical perspectives, applying investigative techniques honed in intelligence work to cold case analysis.

Key skills demonstrated: Evidence re-evaluation, source verification, witness testimony analysis, investigative methodology, narrative reconstruction -- skills directly applicable to digital forensics and incident investigation.

Behind the Mask: Hitler the Socialite

Genre: Historical Analysis

An academic analysis examining Adolf Hitler's social persona and the networks that enabled his rise to power. Drawing on German-language primary sources and archival materials accessed through Goethe University Frankfurt connections, the work provides original scholarship on the social dynamics of authoritarian power consolidation.

This research required fluency in German and the ability to navigate European archival systems -- capabilities that also position Dr. Dietrich-Kolokouris for roles with German companies or requiring German language skills.

Key skills demonstrated: German language fluency, archival research, cross-cultural analysis, primary source evaluation in foreign languages, academic publication standards.

Additional Published Works

Dr. Dietrich-Kolokouris has authored a total of seven books spanning true crime, historical analysis, and investigative research. Each work applies the same core methodology: deep primary source research, rigorous evidence evaluation, clear analytical writing, and the ability to synthesize complex information into accessible narratives for general audiences.

The breadth of published work -- from WWII history to modern true crime to consciousness research -- demonstrates intellectual versatility and the ability to rapidly develop subject matter expertise in new domains. This is the same capability that allows Dr. Dietrich-Kolokouris to move between cybersecurity, AI engineering, and intelligence analysis with equal confidence.

PhD -- Goethe University Frankfurt

> Johann Wolfgang Goethe-Universitat Frankfurt am Main

Doctoral research in History at one of Germany's leading research universities. The PhD program provided rigorous training in primary source analysis, archival research methodology, hypothesis construction and testing, peer review processes, and the production of original scholarship meeting the highest academic standards.

The doctoral experience also provided deep immersion in German academic culture, professional German language fluency, and familiarity with European research institutions and methodologies.

> Key skills demonstrated: Research methodology, hypothesis-driven analysis, academic writing at the highest level, peer review, German language fluency, cross-cultural professional competence.

WarSim Algorithm -- Department of Defense Submission

The WarSim Algorithm is a quantitative conflict simulation system designed for strategic planning and training applications. Dr. Dietrich-Kolokouris leads data modeling for this system, which was submitted to the Department of Defense for evaluation.

- Multi-variable scenario modeling for force projection and resource allocation
- Integration of historical conflict data with predictive modeling frameworks
- Quantitative risk scoring applied to geopolitical and military variables
- Demonstrates ability to conceptualize, develop, and deliver research products at the national security level
- Applied data modeling skills transferable to threat simulation, risk quantification, and security architecture

Consciousness & Paranormal Research Program

Following a transformative near-death experience during cardiac arrest in November 2022, Dr. Dietrich-Kolokouris has pursued rigorous research into consciousness studies and anomalous phenomena. This research program applies the same evidence-based methodology used in his academic, intelligence, and cybersecurity work.

- Collaboration with evidential medium Cindy Kaza on consciousness research protocols

• Field investigation at Skinwalker Ranch -- EMF analysis, sensor deployment, data collection

• Development of NAMECOMMS (Neural Anomaly Manifold Entropy Communication System) -- custom ITC research instrumentation using numerical coherence detection

• Content creation for YouTube covering paranormal investigation, true crime, and historical analysis

• Fox 4 Dallas television appearance for expert commentary and book promotion

• Development of professional media kits, marketing materials, and social media strategies

Part 8: The Complete Picture -- Why It All Connects

Most professionals specialize. Dr. Dietrich-Kolokouris integrates. The value proposition is not any single skill -- it is the compound effect of all of them working together.

From Desktop to Boardroom

The career progression from desktop support through systems administration, CCIE-level network engineering, cybersecurity architecture, intelligence operations, AI engineering, policy development, and academic research is not a scattered resume. It is a deliberate accumulation of capabilities that allows Dr. Dietrich-Kolokouris to:

- Troubleshoot a workstation at 8am, review a firewall architecture at 10am, brief a CISO at noon, and write policy by 3pm
- Translate between technical operations teams and executive leadership without losing fidelity
- Design security architectures that account for real-world operational constraints
- Build AI systems that solve actual business problems, not just demonstrate technology
- Apply intelligence analysis tradecraft to cybersecurity threat assessment and incident investigation
- Write documentation, policy, and reports that are clear, enforceable, and actionable
- Operate in classified, regulated, and high-stakes environments where precision is non-negotiable
- Rapidly develop expertise in new domains -- proven by published work across five distinct subject areas

Professional History

- Cisco Global Services -- CCIE-level network engineering and architecture
- L3Harris Technologies -- cybersecurity in defense contractor environment
- CIA Contractor -- counterterrorism intelligence operations (Al-Qaeda, ISIS theaters)
- StahlTek Consulting -- independent cybersecurity consulting and AI development
- DHS Research -- supply chain vulnerability analysis, emergency management simulation
- Goethe University Frankfurt -- PhD research and academic publication
- Published Author -- seven books across true crime, history, and investigative research

Language & Cultural Competence

- German language fluency -- professional and academic proficiency, including technical and archival German
- Lived and studied in Germany (Frankfurt am Main) -- deep familiarity with German business culture
- Positioned for roles with German companies, German-American joint ventures, or requiring DACH region engagement
- Cross-cultural communication skills developed through international academic and intelligence work

Certifications & Credentials

- CCIE (Cisco Certified Internetwork Expert) -- elite network engineering certification
- PhD, History -- Goethe University Frankfurt (Johann Wolfgang Goethe-Universitat)
- Former CIA Contractor -- counterterrorism operations, security clearance holder
- Published Author -- seven books in print

For questions about any aspect of this portfolio, visit the AI Portfolio Assistant at skdietrich.streamlit.app or connect on LinkedIn.