Project Report: Global Cybersecurity Horizons (2025-2035)

Title: The Strategic Evolution of Global Cybersecurity: Emerging Frontiers, Workforce Transformation, and Economic Paradigms 2025-2035

Subject: Cybersecurity Strategic Foresight and Labor Market Analysis

Timeline: 2025 – 2035

Focus Domains: AI-Native Defense, Post-Quantum Cryptography, Space-Based Networks, Internet of Bodies, and 6G Infrastructure.

Date: February 7, 2026

Abstract

This report provides an expert-level analysis of the global cybersecurity landscape for the decade spanning 2025-2035. As the annual revenue from cybercrime is projected to exceed $8 trillion, the industry is undergoing a structural shift from perimeter-based defense to autonomous, self-healing resilience.[1] The report identifies five primary technological frontiers: adversarial AI swarms, the quantum-safe transition, orbital information security, the bio-digital interface (Internet of Bodies), and AI-native 6G infrastructure. Furthermore, it details the economic orchestration of regional deep-tech hubs, specifically focusing on the Bengaluru-Mysuru corridor as a global model for sovereign IP creation. Finally, it provides a definitive matrix of the top 50 specialized cybersecurity job roles required to navigate this era of machine-speed threats and dissolved physical-digital boundaries.[2]

Table of Contents

---

1. Introduction: The Deep-Tech Decade

The global cybersecurity landscape between 2025 and 2035 represents a period of profound structural reconfiguration, characterized by the convergence of autonomous intelligence, quantum-resistant architectures, and the extension of the digital attack surface into the biological and orbital realms.[1] This decade marks a historical transition from reactive, perimeter-based defense to a model of persistent, self-healing resilience.[1] As the annual revenue from cybercrime is projected to surpass $8 trillion—a figure nearly five times the combined revenue of the world's largest technology firms—the economic and geopolitical stakes of digital security have become an existential concern for nation-states and global enterprises.[1]

The broader cybersecurity market is expected to witness substantial growth, with valuations rising from approximately $218.98 billion in 2025 to nearly $700 billion by 2034.[3] North America continues to dominate the market share, accounting for approximately 43.0% in 2025, while the Asia-Pacific region is emerging as the fastest-growing geographical segment due to rapid digital transformation initiatives.[3]

2. The Autonomous Intelligence Frontier: Adversarial AI and Agentic Defense

The role of Artificial Intelligence (AI) in cybersecurity has fundamentally shifted from a functional enhancement to the primary substrate upon which all digital interactions occur.[1] By 2025, approximately 66% of organizations anticipate that AI will have the most significant

impact on their security posture, yet only 37% have implemented robust processes to vet the security of these tools before deployment.[1]

2.1 The Rise of Agent Swarms and Multi-Agent Systems

The year 2025 marks the emergence of "agent swarms"—multi-agent systems where autonomous AI units collaborate to execute complex workflows.[1] Defensive agent swarms can identify anomalies and initiate self-healing protocols in milliseconds, reducing the mean time to respond (MTTR) to near zero.[1] Conversely, attackers leverage these swarms for hyper-personalized social engineering and mutating malware.[1]

2.2 Shadow AI and the Governance of Autonomous Systems

The proliferation of "Shadow AI"—the unsanctioned use of AI tools—presents a critical risk to data sovereignty.[1] By 2030, SOC focus will shift from alert triage to the oversight of autonomous response agents, requiring professionals who can audit AI decisions for bias or adversarial manipulation.[1]

AI Cybersecurity Metrics	2025 Projection	2030 Forecast	Impact Mechanism
Organizations citing AI as top priority	66%	92%	Convergence of AI and security operations [1]
Reduction in MTTR via AI Agents	40-60%	90%+	Shift from human-speed to machine-speed defense [1]
AI in Cybersecurity Market Size	$29.64B	$102B (2030)	Demand for autonomous threat hunting [4]
Average breach cost involving AI	$4.44M	$7.2M	Increased sophistication of adversarial AI [1]

3. The Quantum Transition: Cryptographic Obsolescence and the PQC Deadline

The impending arrival of cryptographically relevant quantum computers (CRQCs) poses a catastrophic risk to modern encryption.[5] The global transition to Post-Quantum Cryptography (PQC) is governed by a strict timeline, with NIST mandating the deprecation of classical public-key cryptography by 2030-2035.[6]

3.1 The NIST PQC Standards and Technical Constraints

In August 2024, NIST finalized the first three standards for quantum-resistant algorithms: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA).[5] These rely on lattice-based math, such as the Module Learning with Errors (MLWE) problem:

$$A\mathbf{s} + \mathbf{e} \approx \mathbf{b} \pmod{q}$$

PQC keys are substantially larger than classical ones; for example, a Dilithium signature requires several kilobytes compared to 64 bytes for ECDSA.[1]

3.2 Crypto-Agility and the Hybrid Infrastructure Phase

Organizations are now in a "Hybrid Phase," deploying both classical and post-quantum algorithms simultaneously to ensure resilience. "Crypto-agility"—the ability to rapidly update cryptographic protocols—has become a core requirement to prevent "harvest now, decrypt later" tactics.

4. The Space-Based Frontier: Securing Orbital Information Networks

The space economy is projected to reach $1.8 trillion by 2035.[1] However, the rapid proliferation of orbital assets has outpaced cybersecurity standards.

4.1 Unique Vulnerabilities of Orbital Assets

Space systems suffer from legacy components with limited Size, Weight, and Power (SWAP) capacity and unencrypted protocols susceptible to jamming and spoofing.[7] The 2022 Viasat incident proved that space networks are now primary targets in hybrid warfare.[7]

4.2 The Shift Toward Cyber-Resilient Satellites

By 2035, the space cybersecurity market is expected to reach $2.5 billion.[8] Focus is shifting toward Zero Trust Architecture (ZTA) and AI-driven anomaly detection on-orbit.

5. The Bio-Digital Frontier: Internet of Bodies and Neural Privacy

The Internet of Bodies (IoB) expands the digital attack surface to sensors implanted or worn on the human body.[9]

5.1 Neural Data as the Final Privacy Boundary

A "neuro-digital" breach could allow adversaries to reverse-engineer intentions or manipulate motor functions via Brain-Computer Interfaces (BCIs). The IoB market is projected to reach $1,800 billion by 2033.[9]

5.2 Ethical Governance and the UNESCO Standard

In 2025, UNESCO adopted the first global framework on neurotechnology ethics to safeguard mental privacy.[10] Future security will rely on neural-specific encryption and zero-trust principles for bio-digital interfaces.[11]

Neurotechnology Market Projections	**2025 Projection**	**2035 Forecast**	**Key Segment**
Market Size (USD)	$15.35B - $17.34B	$33.64B - $53.18B	Healthcare (Largest) [13]
Brain-Computer Interface (BCI) Size	$2.41B - $2.94B	$12.11B - $18.85B	Non-invasive BCI (55%+) [15]
CAGR (2025-2035)	-	13.23% - 19.2%	Cognitive enhancement (Fastest) [15]

6. 6G and the AI-Native Infrastructure of 2030

6G networks, expected by 2030, will provide terabit-per-second speeds and air interface latency as low as 0.1 ms.[19]

6.1 Hyper-Connectivity and the Massive Attack Surface

6G targets a connection density of 10^7 devices per square kilometer, creating an unprecedented attack surface.[21] AI-native management is required to handle real-time resilience across terrestrial and satellite interfaces.

6.2 Privacy-Preserving Technologies in 6G

To secure highly sensitive 6G data, architectures will employ Fully Homomorphic Encryption (FHE) and Secure Multi-Party Computation (SMPC).[22] FHE performance is doubling every two years, making it viable for 2030 deployments.[23]

7. Web3 and the Governance Vulnerabilities of DAOs

Decentralized Autonomous Organizations (DAOs) represent a paradigm shift in trustless decision-making, yet they face systemic plutocratic manipulation via "one token, one vote" models.[17] Future security requires quadratic voting and zero-knowledge proofs for anonymous but verifiable governance.[1]

8. Regional Strategic Orchestration: The Bengaluru and Mysuru Ecosystems

Karnataka's IT Policy 2025-2030 serves as a strategic blueprint for Indian deep-tech leadership.[25]

8.1 Bengaluru: The Deep-Tech Engine

Bengaluru hosts the world's largest tech workforce (2.5 million professionals) and accounts for 46% of all VC activity in India.[25]

8.2 Mysuru: The Designated Cybersecurity Cluster

As part of the "Beyond Bengaluru" mission, Mysuru is designated as the state's cybersecurity and ESDM cluster, anchored by the Mysuru Global Technology Centre (MGTC).[25]

Regional Project	Focus Area	Impact Metric
Global Technology Centre (Mysuru)	Infrastructure for GCCs	3,000-seater facility [28]
Technoverse GIDS	Integrated Tech Campuses	Cybersecurity testbeds [25]
KAN (Accelerator Network)	Startup Support	25,000 startups by 2030 [31]
Tier-2/3 City Investment	Beyond Bengaluru Fund	75 Crore allocated [31]

9. The Future Workforce: Top 50 Cybersecurity Job

Roles (2025-2035)

Global shortages of cybersecurity professionals are estimated to reach 3.5 million unfilled roles by 2025.[33]

Specialized Roles J01 - J13

Role ID	Job Title	Primary Domain	Core Skills	Typical Salary (USD)
J01	AI Security Engineer	AI & ML	LLM hardening, prompt injection defense	$130k-$185k [1]
J02	Quantum Readiness Architect	Quantum	PQC migration, lattice-based math	$180k-$250k [1]
J03	Neurosecurity Ethicist	IoB/BCI	BCI privacy, bio-signal guardrails	$110k-$165k [1]
J04	Space Network Defense Lead	Space	LEO link security, satellite forensics	$155k-$225k [1]
J05	6G Protocol Specialist	6G/Telecom	Network slicing, THz communicatio n	$145k-$210k [1]
J06	Adversarial AI Tester	AI Red Teaming	Model poisoning, evasion attacks	$135k-$195k [1]

J07	Privacy Engineer (GenAI)	PETS	Differential privacy, federated learning	$140k-$205k [1]
J08	DAO Governance Auditor	Web3/DAO	Smart contract formal verification	$130k-$190k [1]
J09	Cloud-Native Security Arch	Cloud	Kubernetes security, policy-as-cod e	$160k-$235k [1]
J10	Autonomous Incident Resp	SecOps	SOAR engineering, AI oversight	$125k-$180k [1]
J11	Zero Trust Architect	Identity	Continuous authentication, DID	$145k-$215k [1]
J12	Bio-Digital Forensic Anal	IoB	Implant forensics, medical IoT	$115k-$170k [1]
J13	Digital Sovereignty Off.	GRC	Localized security stacks, NIS2	$120k-$185k [1]

Specialized Roles J14 - J25

Role ID	Job Title	Primary Domain	Core Skills	Typical Salary (USD)
J14	Crypto-Agility Manager	Quantum	Cryptographic inventory, PQC	$140k-$205k [1]
J15	OT/ICS	Critical Infra	SCADA	$135k-$190k [1]

	Resilience Lead		security, smart grid defense	
J16	Deepfake Analyst	Social Eng.	Synthetic media detection	$105k-$155k [1]
J17	Confidential Comp. Lead	Cloud	Secure enclaves, data-in-use	$165k-$230k [1]
J18	AI Supply Chain Mgr	AI/Third-Party	Model vetting, data origin audit	$130k-$185k [1]
J19	Quantum Cryptographer	Quantum	QKD, quantum-safe random numbers	$120k-$195k [1]
J20	IIoT Lifecycle Specialist	IIoT	Secure firmware, device lifecycle	$125k-$175k [1]
J21	Cognitive Security Off.	Human-Centric	Misinformation defense, neuromorphic	$140k-$210k [1]
J22	Smart City Cyber Lead	Smart Cities	IoT sensor security, urban mobility	$135k-$195k [1]
J23	FHE Research Engineer	PETS	Fully homomorphic encryption	$175k-$245k [1]
J24	Supply Chain Integrity Anal	Hardware	Semiconductor vetting, root of	$120k-$180k [1]

			trust	
J25	Digital Twin Security Spec	Simulation	Threat modeling in virtual cities	$135k-$190k [1]

Specialized Roles J26 - J37

Role ID	Job Title	Primary Domain	Core Skills	Typical Salary (USD)
J26	Quantum Algorithm Dev	Quantum	Circuit optimization, QML	$140k-$210k [1]
J27	Decentralized Identity Mgr	Web3	Verifiable credentials, wallet security	$125k-$180k [1]
J28	Edge AI Security Analyst	6G/Edge	On-device ML threat detection	$120k-$175k [1]
J29	Regulatory Automation Eng	GRC	Compliance-as-code, audit agents	$115k-$170k [1]
J30	Chief Trust Officer	Leadership	Enterprise digital trust strategy	$250k-$450k [1]
J31	BCI Security Developer	IoB	Secure neural encoding, write-in BCI	$140k-$200k [1]
J32	LEO Malware Researcher	Space	Reverse engineering satellite code	$145k-$215k [1]

J33	Smart Grid Cyber Analyst	Critical Infra	Power grid anomaly detection	$125k-$180k [1]
J34	Robotic Security Specialist	Manufacturing	Cobot security, AMR protection	$135k-$195k [1]
J35	Web3 Forensics Specialist	Web3	Blockchain tracing, bridge hacks	$120k-$175k [1]
J36	Quantum Safe Network Eng	Telecom	PQC VPNs, post-quantum TLS	$140k-$205k [1]
J37	AI Governance Auditor	Ethics	Model bias testing, ethical AI logs	$125k-$185k [1]

Specialized Roles J38 - J50

Role ID	Job Title	Primary Domain	Core Skills	Typical Salary (USD)
J38	Biometric Privacy Attorney	Legal	Neuro-rights law, bio-data privacy	$175k-$285k [2]
J39	6G Slice Security Manager	6G	Multi-tenancy isolation, SDN/NFV	$145k-$210k [1]
J40	Shadow AI Risk Specialist	Enterprise	Unsanctioned AI monitoring	$110k-$165k [1]
J41	Human-AI Interaction Spec	Human Factor	Security decision augmentation	$115k-$175k [1]

J42	Space Supply Chain Auditor	Space	Subcontractor vetting, provenance	$125k-$185k [1]
J43	Virtual Ground Station Lead	Space	Software-defined ground stations	$150k-$220k [1]
J44	Federated Learning Engineer	AI/PETS	Collaborative model training security	$160k-$230k [1]
J45	ZK-Proof Architect	Web3/Auth	Privacy-preserving auth systems	$170k-$255k [1]
J46	PQC Security Analyst	Quantum	NIST compliance, hybrid certificates	$135k-$200k [1]
J47	Medical IoT Security Eng	Healthcare	Connected device lifecycle security	$125k-$185k [1]
J48	Smart Traffic System Auditor	Smart Cities	Urban sensor threat modeling	$120k-$180k [1]
J49	Neuro-Digital Ethics Lead	IoB/BCI	Cognitive sovereignty governance	$145k-$220k [1]
J50	Chief Resiliency Officer	Leadership	National-scale cyber-warfare modeling	$300k-$500k [1]

10. Economic Realities and Implementation Hurdles

Realizing this potential faces major restraints, including expert shortages and budget constraints for SMEs.[3] QKD links can cost $100,000 per link, a barrier for smaller organizations.[35]

Cybersecurity Market Segmentation (2025)	Market Share %	Projected Growth (CAGR)	Dominant Factor
Network Security	~18.7%	11.3%	Infrastructure protection [36]
Cloud Application Security	Fastest Growing	18.01%	Remote work & cloud migration [3]
Managed Security Services	Largest Service	High	Skill shortage in enterprises [33]
Healthcare Vertical	High Growth	18.98%	Connected medical devices [3]
SMEs Segment	Fastest Rate	15.47%	Cloud solution adoption [3]

11. Critical Infrastructure and Government Modernization

Modernization of national defense and industrial systems is a primary driver.[39] The global defense cybersecurity market is projected to reach $77.41 billion by 2035.[39] Industrial cybersecurity is also witnessing a surge, projected to reach $61.18 billion by 2035.[40]

12. Conclusion: Strategic Synthesis

Cybersecurity has transitioned from a supporting technical function to a central pillar of global stability.[1] Success in the decade 2025-2035 will be defined by the shift to autonomous resilience, the imperative of quantum readiness, and the protection of the human body and orbital networks as the ultimate frontiers of the digital age.[1]

---

13. References

- [1] *The Strategic Evolution of Global Cybersecurity 2025-2035.* (Expert-Level Internal Analysis).
- [6] National Institute of Standards and Technology (NIST). *NIST PQC: The Road Ahead.* March 2025.
- [11] UNESCO. *Ethics of Neurotechnology: UNESCO Adopts the First Global Standard.* November 2025.
- [3] Fortune Business Insights. *Cybersecurity Market Forecast 2026-2034.* January 2026.
- [8] Market Growth Reports. *Cyber Security for Space Market Size and Growth Report 2035.*
- [35] Market Growth Reports. *Global Quantum Cryptography Market Projections 2035.*
- [3] Fortune Business Insights. *Global Cybersecurity Market Size and Future Outlook.* January 2026.

Works cited

1. The Strategic Evolution of Global Cybersecurity.pdf
2. Cybersecurity Careers: A Booming Field for the Next Decade - California Miramar University, accessed February 7, 2026, https://www.calmu.edu/cybersecurity-careers-a-booming-field-for-the-next-decade
3. Cybersecurity Market Size, Share, Analysis | Global Report 2034, accessed February 7, 2026, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
4. Artificial Intelligence (AI) In Cybersecurity Market Size, Report 2035, accessed February 7, 2026, https://www.precedenceresearch.com/artificial-intelligence-in-cybersecurity-market
5. The State of Post-Quantum Cryptography (PQC) on the Web | F5 Labs, accessed February 7, 2026, https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web
6. NIST PQC: The Road Ahead, accessed February 7, 2026, https://csrc.nist.gov/csrc/media/Presentations/2025/nist-pqc-the-road-ahead/images-media/rwcpqc-march2025-moody.pdf
7. Space Cybersecurity Market Revenue Trends, 2025 To 2030 - MarketsandMarkets, accessed February 7, 2026, https://www.marketsandmarkets.com/Market-Reports/space-cybersecurity-market-175849133.html
8. Cyber Security for Space Market Size and Growth Report, 2035, accessed February 7, 2026, https://www.marketgrowthreports.com/market-reports/cyber-security-for-space-market-112883
9. Internet of Bodies (IoB) Market Size & Industry Growth 2030 - Future Data Stats, accessed February 7, 2026,

https://www.futuredatastats.com/internet-of-bodies-iob-market
10. UNESCO Adopts First Global Framework on Neurotechnology Ethics, accessed February 7, 2026, https://www.globalpolicywatch.com/2026/01/unesco-adopts-first-global-framework-on-neurotechnology-ethics/
11. Ethics of neurotechnology: UNESCO adopts the first global standard in the cutting-edge technology, accessed February 7, 2026, https://www.unesco.org/en/articles/ethics-neurotechnology-unesco-adopts-first-global-standard-cutting-edge-technology
12. UNESCO's Global Neurotechnology Standards - Captain Compliance, accessed February 7, 2026, https://captaincompliance.com/education/unescos-global-neurotechnology-standards/
13. Neurotechnology Market Size, Share, Insights Outlook 2035, accessed February 7, 2026, https://www.thebusinessresearchcompany.com/report/neurotechnology-global-market-report
14. Neurotechnology Market Trends in Advancing Brain-Computer Interfaces (BCIs), accessed February 7, 2026, https://www.towardshealthcare.com/insights/neurotechnology-market-sizing
15. Brain Computer Interface Market Size and Forecast 2025-2035 - Metatech Insights, accessed February 7, 2026, https://www.metatechinsights.com/industry-insights/brain-computer-interface-market-1331
16. Brain Computer Interface Market Industry Trends and Global Forecasts to 2035: Distribution by Type of Product, Type of Component, Type of Application, End-User, Type of Enterprise and Geographical Regions - Research and Markets, accessed February 7, 2026, https://www.researchandmarkets.com/reports/6173316/brain-computer-interface-market-industry-trends
17. Brain-Computer Interface Market Size, Share, Trends & Insights Report, 2035, accessed February 7, 2026, https://www.rootsanalysis.com/brain-computer-interface-market
18. Neurotechnology Market Size, Analysis, Industry Growth, 2035, accessed February 7, 2026, https://www.marketresearchfuture.com/reports/neurotechnology-market-43140
19. 6G Market Share, Size, Trends During Forecast | 2035 - MRFR, accessed February 7, 2026, https://www.marketresearchfuture.com/reports/6g-market-10951
20. 6G Market Size, Share, Trends, & Insights Report, 2035 - Roots Analysis, accessed February 7, 2026, https://www.rootsanalysis.com/6g-market
21. 6G Market Size, Share, Trends, Opportunities, Scope & Forecast, accessed February 7, 2026, https://www.verifiedmarketresearch.com/product/6g-market/
22. Secure Multi-Party Computation - Data for Public Good, accessed February 7, 2026, https://dataforpublicgood.org.in/blog/secure-multi-party-computation/
23. Applications of Homomorphic Encryption and Secure Multi-Party Computation -

CyberArk, accessed February 7, 2026, https://www.cyberark.com/resources/blog/applications-of-homomorphic-encryption-and-secure-multi-party-computation
24. Homomorphic Encryption and Secure Multi-Party Computation: Mathematical Tools for Privacy-Preserving Data Analysis in the Cloud - ResearchGate, accessed February 7, 2026, https://www.researchgate.net/publication/385870239_Homomorphic_Encryption_and_Secure_Multi-Party_Computation_Mathematical_Tools_for_Privacy-Preserving_Data_Analysis_in_the_Cloud
25. Karnataka IT Policy 2025–2030: A Strategic Blueprint to Lead India's ..., accessed February 7, 2026, https://thenfapost.com/karnataka-it-policy-2025-2030-a-strategic-blueprint-to-lead-indias-deep-tech-decade/
26. Karnataka IT policy targets ₹11.5 lakh sr in software exports by 2030, accessed February 7, 2026, https://www.communicationstoday.co.in/karnataka-it-policy-targets-%E2%82%B911-5-lakh-sr-in-software-exports-by-2030/
27. Government of Karnataka notifies the IT Policy 2025–2030 - PwC India, accessed February 7, 2026, https://www.pwc.in/research-insights/news_alert/tax-insights/government-of-karnataka-notifies-the-it-policy-2025-2030.html
28. KDEM MYSURU CLUSTER, accessed February 7, 2026, https://karnatakadigital.in/wp-content/uploads/2024/07/KDEM-MYSURU-CLUSTER-DECK-2024.pdf
29. Karnataka Targets 1.5 Lakh Jobs And $10 Bn In Digital Revenues From Mysuru, accessed February 7, 2026, https://www.businessworld.in/article/karnataka-targets-15-lakh-jobs-and-10-bn-in-digital-revenues-from-mysuru-562391
30. Karnataka offers extensive incentives in its proposed IT policy - ET Telecom, accessed February 7, 2026, https://telecom.economictimes.indiatimes.com/news/policy/karnataka-offers-extensive-incentives-in-its-proposed-it-policy/125340267
31. About Us - KDEM - Technology Enabler, accessed February 7, 2026, https://karnatakadigital.in/about-us/
32. Karnataka unveils Startup Policy 2025-30, charts roadmap for deep tech decade - DQIndia, accessed February 7, 2026, https://www.dqindia.com/esdm/karnataka-unveils-startup-policy-2025-30-charts-roadmap-for-deep-tech-decade-11018513
33. Cyber Security Market Size & Share Report, 2035 - Roots Analysis, accessed February 7, 2026, https://www.rootsanalysis.com/cyber-security-market
34. Cyber Security Market: Industry Trends and Global Forecasts, Till 2035: Distribution by Type of Component, Deployment Mode, Solution Type, Type of Technology, End-user and Geography - Research and Markets, accessed February 7, 2026, https://www.researchandmarkets.com/reports/6089571/cyber-security-market-in

dustry-trends-global
35. Quantum Cryptography Market Size, Share & Trends Analysis, 2035, accessed February 7, 2026, https://www.marketgrowthreports.com/market-reports/quantum-cryptography-market-100150
36. Aerospace and Defense Cyber Security Market | Global Market Analysis Report - 2035, accessed February 7, 2026, https://www.futuremarketinsights.com/reports/aerospace-and-defense-cyber-security-market
37. Cybersecurity Market Size, Share | Industry Report, 2035 - Market Research Future, accessed February 7, 2026, https://www.marketresearchfuture.com/reports/cyber-security-market-953
38. Cybersecurity Market Report 2025-2030, by Application, Geo, Tech - MarketsandMarkets, accessed February 7, 2026, https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
39. Defense Cybersecurity Market Size, Share, Trends & Insights Report, 2035 - Roots Analysis, accessed February 7, 2026, https://www.rootsanalysis.com/defense-cybersecurity-market
40. Industrial Cybersecurity Market Size to Surge USD 61.18 Bn by 2035, accessed February 7, 2026, https://www.precedenceresearch.com/industrial-cybersecurity-market