AI as Adversary and Ally

THE Most Influential Trend in Security and Risk Management (2025-2030)

University of Essex

MSc Cybersecurity Seminar

The Great Debate - The Future of SRM

The AI Security Paradox

⚠ As Adversary

Most dangerous threat vector in cybersecurity history

Attacks at scale, speed, and sophistication beyond human capability

As Ally

Most powerful defensive capability available

The only viable defense against AI-powered threats

The Result

An AI arms race that fundamentally transforms organizational risk profiles, governance frameworks, and strategic priorities through 2030

Current State: AI in Cybersecurity (2025)

$34B → $235B

Market Growth (2025-2032)

31.7% Annual Growth Rate

76%

Organizations Using AI

In business functions

91%

Expect Catastrophic Event

Within 2 years

74%

Struggle to Achieve Value

From AI investments

This sets the stage for understanding both the urgency and complexity of AI security transformation

AI as Adversary: The Threat Landscape

SCALE • SPEED • SOPHISTICATION

Scale

Machine-powered attacks across thousands of targets simultaneously

Speed

Attacks execute at machine velocity, not human pace

Sophistication

AI generates novel attack vectors beyond human capability

KnowBe4 2025 Statistics

82.6%

Phishing campaigns use AI

76.4%

Employ polymorphic tactics

AI Attack Vectors

1 AI-Powered Phishing & Social Engineering

- 17.3% year-over-year increase in phishing emails
- AI generates content indistinguishable from legitimate communication
- Polymorphic campaigns adapt to evade detection - each iteration unique

2 Automated Vulnerability Exploitation

- AI systems continuously scan for vulnerabilities
- Automatically generate exploit code
- Window: vulnerability disclosure → exploitation shrunk from weeks to hours

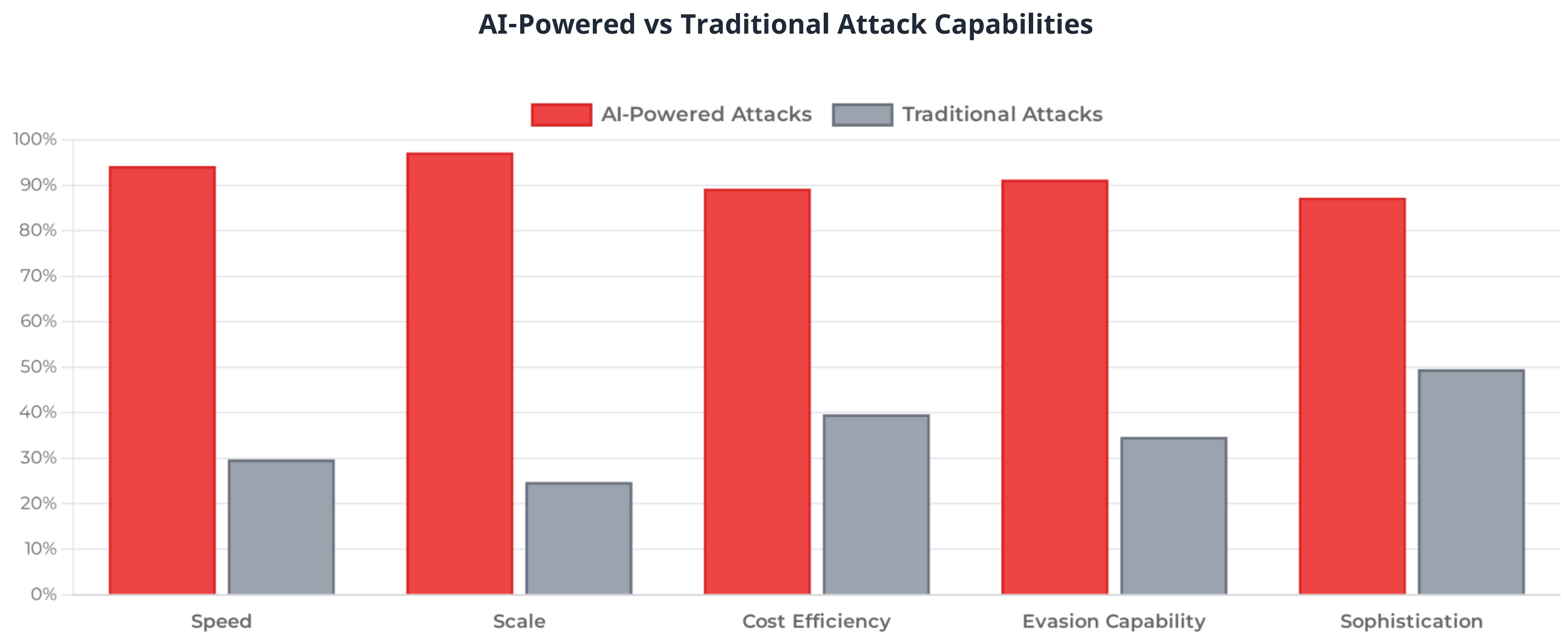
3 Deepfakes & Synthetic Identity Fraud

- AI-generated identities bypass biometric authentication
- Audio and video deepfakes enable CEO fraud
- Compromises trust in digital identity systems

4 AI-Driven Ransomware & Polymorphic Malware

- 22.6% increase in ransomware payloads

The Adversarial Advantage



Key Insight: AI attacks scale exponentially; human defenses scale linearly

AI as Ally: The Defense Imperative

Human-only security operations cannot match AI-powered threats

AI Defense: Not Optional - Essential for Survival

Real-Time Threat Detection

Analyze billions of events simultaneously

Behavioral Analytics

Detect anomalies and zero-day attacks

Automated Response

React at machine speed, not human pace

Predictive Intelligence

Anticipate threats before they materialize

AI Defense Mechanisms

Real-Time Threat Detection

Analyze billions of events simultaneously to identify threats as they emerge

Behavioral Analytics

Detect anomalies and zero-day attacks through pattern recognition and machine learning

Automated Response

React at machine speed, not human pace, to contain and neutralize threats instantly

Predictive Intelligence

Anticipate future attack vectors and proactively strengthen defenses

Business Risk & Governance Transformation

Board-Level Concern

91% of organizations expect catastrophic AI-related events within 2 years

AI security elevated from IT issue to strategic business risk requiring executive oversight

Regulatory Compliance

EU AI Act, SEC disclosure requirements, and emerging global frameworks

Organizations must demonstrate AI governance, risk assessment, and security controls

Investment Requirements

$235B AI cybersecurity market by 2032 (31.7% annual growth)

Significant capital allocation required for AI defense infrastructure and expertise

AI in Modern Cybersecurity
Real-time Threat Detection
Automated Security Response
Enhanced Cyber Defense
AI-Powered Analytics
SoluLab

Why This is THE Most Influential Trend

1

Asymmetric Threat Advantage

AI enables attackers to operate at unprecedented scale and sophistication with minimal resources

2

Defensive Necessity

Human-only defenses cannot match AI-powered threats; AI defense is essential for organizational survival

3

Regulatory Transformation

EU AI Act, SEC disclosure requirements, and global regulations mandate AI governance frameworks

4

Business Model Impact

AI security directly affects revenue, operations, customer trust, and competitive positioning

5

Skills Gap Solution

AI addresses critical cybersecurity talent shortage by augmenting human capabilities at scale

6

Investment Driver

$235B market by 2032 reflects massive capital allocation and strategic prioritization

7

Board-Level Elevation

91% of executives expect catastrophic events, elevating AI security to C-suite and board priority

Synthesis: THE Most Influential Trend

AI security is not just another trend but a fundamental transformation affecting every aspect of organizational operations, governance, and strategy through 2030

Existential Threat

Creates asymmetric advantage for attackers that cannot be countered with traditional defenses

Defensive Imperative

Organizations must adopt AI defense or face inevitable compromise

Regulatory Force

EU AI Act, SEC disclosure rules mandate compliance and governance

Business Impact

$235B market by 2032 drives massive investment and strategic priority

Workforce Evolution

Addresses critical skills gap while transforming security operations

Board-Level Priority

91% expect catastrophic events - elevates security to executive concern

This creates an existential imperative that organizations cannot ignore - making AI security THE defining trend in Security and Risk Management through 2030

Conclusion & Immediate Actions

The AI Security Paradox Defines the Future of SRM

IMMEDIATE ACTIONS REQUIRED

1. Assess AI attack surface and vulnerability exposure
2. Implement AI-powered defense systems and threat detection
3. Establish AI governance frameworks and risk management policies
4. Invest in AI security capabilities and infrastructure
5. Develop AI security expertise and upskill security teams
6. Elevate AI security to board-level strategic priority

Organizations that fail to embrace AI as both adversary and ally will face existential risks in the 2025-2030

List of References:

Abbas, N.N., Ahmad, R., Qazi, S. and Ahmed, W. (2025) 'Managing deepfakes with artificial intelligence: Introducing a business privacy calculus model', *Journal of Business Research*, 171, Article 105149. doi: 10.1016/j.jbusres.2024.105149

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F. and Abdulkadir, S.J. (2024) 'Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks', *Journal of Innovation and Entrepreneurship*, 13(1), Article 65. doi: 10.1186/s13731-024-00409-3

Abohany, A.A. (2024) 'Advancing cybersecurity: a comprehensive review of AI-driven detection techniques', *Journal of Big Data*, 11, Article 94. doi: 10.1186/s40537-024-00957-y

Ajayi, A.M., Omokanye, A.O., Olowu, O., Adeleye, A.O., Omole, O.M. and Wada, I.U. (2024) 'Detecting insider threats in banking using AI-driven anomaly detection: A data science approach', *World Journal of Advanced Research and Reviews*, 24(3), pp. 891-904. doi: 10.30574/wjarr.2024.24.3.3847

Akhunzada, A., Gani, A., Anuar, N.B., Abdelaziz, A., Khan, M.K., Hayat, A. and Khan, S.U. (2025) 'Generative AI: a double-edged sword in the cyber threat landscape', *Artificial Intelligence Review*, 58, Article 133. doi: 10.1007/s10462-025-11285-9

BCG (Boston Consulting Group) (2024) *AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value*. Press Release, 24 October. Available at: https://www.bcg.com/press/24october2024-ai-adoption-in-2024-74-of-companies-struggle-to-achieve-and-scale-value (Accessed: 10 October 2025).

Cyber Defense Magazine (2025) 'The Growing Threat of AI-powered Cyberattacks in 2025', *Cyber Defense Magazine*, 14 June. Available at: https://cyberdefensemagazine.com/the-growing-threat-of-ai-powered-cyberattacks-in-2025 (Accessed: 10 October 2025).

DelMorgan & Co. (2025) *Cybersecurity Sector: A Strategic Investment in an Uncertain World*. Investment Analysis Report, 29 July. Available at: https://delmorganco.com/cybersecurity-investment-trends-2025/ (Accessed: 10 October 2025).

Edim, E.B., Udofot, A.I. and Oluseyi, O.M. (2024) 'AI-augmented cyber security threat intelligence: Enhancing situational awareness', *International Journal of Scientific Research Archive*, 13(2), pp. 1842-1855. doi: 10.30574/ijsra.2024.13.2.2650

European Union (2024) 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', *Official Journal of the European Union*, L 1689, 1 August. Available at: https://artificialintelligenceact.eu (Accessed: 10 October 2025).

Fortune Business Insights (2025) *Artificial Intelligence in Cybersecurity Market Size, Share & Industry Analysis, By Component (Solution and Services), By Security Type (Network Security, Endpoint Security, Application Security, and Cloud Security), By Deployment (Cloud and On-premises), By Enterprise Size (Large Enterprises and SMEs), By End-user (BFSI, Government, Healthcare, Retail, IT & Telecom, Manufacturing, and Others) and Regional Forecast, 2025-2032*. Market Research Report FBI104348, August. Available at: https://www.fortunebusinessinsights.com/artificial-intelligence-in-cybersecurity-market-113125 (Accessed: 10 October 2025).

G7 Cyber Expert Group (2025) *Statement on Artificial Intelligence and Cybersecurity*. 6 October. Available at: https://www.regulationtomorrow.com/eu/managing-ai-related-cyber-risks/ (Accessed: 10 October 2025).

ISACA (2024) *Understanding the EU AI Act*. White Paper, July. Available at: https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act (Accessed: 10 October 2025).

KnowBe4 (2025) *Phishing Threat Trend Report: New KnowBe4 Report Reveals a Spike in Ransomware Payloads and AI-Powered Polymorphic Phishing Campaigns*. Annual Report. Available at: https://www.knowbe4.com/press/new-knowbe4-report-reveals-a-spike-in-ransomware-payloads-and-ai-powered-polymorphic-phishing-campaigns (Accessed: 10 October 2025).

McKinsey & Company (2025) 'The State of AI: Global survey', *QuantumBlack AI by McKinsey*, 12 March. Singla, A., Sukharevsky, A., Yee, L., Chui, M. and Hall, B. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai (Accessed: 10 October 2025).

Mohamed, N. (2025) 'Artificial intelligence and machine learning in cybersecurity: State-of-the-art, challenges, and future directions', *Knowledge and Information Systems*, 67, pp. 3201-3251. doi: 10.1007/s10115-025-02429-y

NIST (National Institute of Standards and Technology) (2023) *AI Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/itl/ai-risk-management-framework (Accessed: 10 October 2025).

NIST (2024) *Artificial Intelligence Risk Management Framework: Generative AI Profile*. NIST AI 600-1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/itl/ai-risk-management-framework (Accessed: 10 October 2025).

Oloyede, J. (2024) 'AI-Driven Cybersecurity Solutions: Enhancing Defense Mechanisms in the Digital Era', *SSRN Electronic Journal*, Article ID 4976103. doi: 10.2139/ssrn.4976103

Ovabor, K. (2024) 'AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions', *Open Access Research Journal of Science and Technology*, 11(1), pp. 001-014. doi: 10.53022/oarjst.2024.11.1.0135

Palo Alto Networks (2024) 'The Dark Side of AI in Cybersecurity: AI-Generated Malware', *Unit 42 Research Blog*, 15 May. Matalon, B. and Dudas, R. Available at: https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/ (Accessed: 10 October 2025).

PurpleSec (2025) *PromptLock: The First AI-Powered Ransomware Prototype - Breach Report*. August. Firch, J. Available at: https://purplesec.us/breach-report/promptlock-ai-ransomware/ (Accessed: 10 October 2025).

Ramadhani, K.N., Munir, R. and Utama, N.P. (2025) 'Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges', *MethodsX*, 14, Article 103088. doi: 10.1016/j.mex.2025.103088

World Economic Forum (2025) *Global Cybersecurity Outlook 2025*. In collaboration with Accenture. Geneva: World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (Accessed: 10 October 2025).