

Code War: The AI Revolution in Cybersecurity

Index

Chapter 1-The Digital Battlefield: Old Rules, New Weapons

- 1.1 The Evolution of Cybersecurity
- 1.2 Traditional defense models and their limitations
- 1.3 Enter Artificial Intelligence

Chapter 2-Rise of the Machines: AI in the Hands of Hackers

- 2.1 How cybercriminals are using AI
- 2.2 Deepfakes, polymorphic malware, and AI-enhanced phishing
- Deepfakes
- 2.3 Case studies: Real-world AI-assisted attacks

Chapter 3-Defensive Intelligence: AI on the Cybersecurity Frontlines

- 3.1 Defensive AI applications
- 3.2 Threat detection and behavioral analytics
- 3.3 AI in Security Operations Centers (SOC)
- 3.4 Real-time Response Automation

Chapter 4-Ethics and Exploits: The Dark Side of AI

- 4.1 Vulnerabilities in AI models
- 4.2 Adversarial machine learning
- 4.3 Model poisoning and evasion attacks
- 4.4 Managing AI risk

Chapter 5-Man and Machine: Augmented Cybersecurity in Action

- 5.1 Privacy vs. protection
- 5.2 The ethics of predictive policing and AI surveillance
- 5.3 Regulatory and governance issues

Chapter 6-Cybersecurity by Design: Embedding AI into Infrastructure

- 6.1 Red and blue teaming with AI
- 6.2 AI in cyber simulations and war games
- 6.3 The role of digital twins and threat emulation

Chapter 7-AI Governance and Global Cyber Norms

- 7.1 AI in national cybersecurity strategies
- 7.2 State-sponsored cyber operations
- 7.3 International norms and digital cold wars

Chapter 8-The Future of Cyber Offense: AI-Powered Digital Warfare

- 8.1 Adaptive and predictive defense systems
- 8.2 AI for automated patching and system hardening
- 8.3 SOC of the future: human-AI collaboration

Chapter 9-Building Resilience: Adaptive Defense Strategies in the AI Era

- 9.1 Quantum computing and cybersecurity
- 9.2 Integrating AI with blockchain and Zero Trust
- 9.3 Autonomous threat hunting and self-healing systems

Chapter 10-Tomorrow's Threatscape: AI, Quantum Computing, and the Next Digital Frontier

- 10.1 Implementing AI responsibly
- 10.2 Vendor selection and evaluation
- 10.3 Upskilling Teams for the AI Age
- 10.4 Governance and accountability frameworks