AI in Cybersecurity

Course Module	Content Overview	Duration
Introduction to AI in Cybersecurity	- Role of AI in cybersecurity - Fundamental concepts - Application to security challenges	2 weeks
AI-Driven Threat Detection	- AI models for threat detection - Anomaly detection - Behavioral analysis	3 weeks
Automated Incident Response with AI	- Automating incident response - Threat mitigation - Response orchestration	2 weeks
AI for Vulnerability Management	- AI in vulnerability management - Predictive analytics - Identifying vulnerabilities	2 weeks
Adversarial AI and Security	- Adversarial techniques - Evasion tactics - Countermeasures	2 weeks
Ethical Considerations in AI Security	- Privacy concerns - Data protection - Responsible AI use	1 week
Real-World Applications and Case Studies	- Case studies - Successful implementations - Lessons learned	2 weeks
Hands-On Labs and Tools	- Practical experience - Labs for detection - Response automation	2 weeks

Space Cybersecurity

Course Module	Content Overview	Duration
Introduction to Space Cybersecurity	- Space systems fundamentals - Satellite technology - Space communication security	2 weeks
Threat Landscape in Space Systems	- Cyber threats to space assets - State-sponsored attacks - Space piracy	2 weeks
Satellite and Ground Station Security	- Securing satellite communications - Encryption protocols - Ground station security	3 weeks
AI in Space Security	- AI for monitoring space operations - Real-time threat detection - Automated responses	2 weeks
Cyber Defense Strategies for Space Infrastructure	- Developing policies - Risk management - Securing space assets	3 weeks
Space Security Policy and International Law	- Space security policies - International treaties - Global collaboration	2 weeks

Industrial Cybersecurity

Course Module	Content Overview	Duration
Introduction to Industrial Cybersecurity	- ICS overview - OT security - Industrial cybersecurity challenges	2 weeks
Securing Operational Technology (OT)	- Protecting OT environments - Threat detection - Vulnerability management	3 weeks
Cyber Threats to Critical Infrastructure	- Threats to energy, water, and transport - Impact analysis - Mitigation strategies	3 weeks
AI in Industrial Cybersecurity	- AI applications in industrial settings - Predictive maintenance - Threat detection	2 weeks
Penetration Testing for Industrial Systems	- Simulating attacks - Testing frameworks - Risk assessment	2 weeks
Compliance and Regulatory Frameworks	- Regulations and standards - Compliance requirements - Risk management	2 weeks

Autonomous Remotely Operated Vehicles (AI/ML)

Course Module	Content overview	Duration
Intro to AI and ML	Basics, Key Algorithms (Supervised, Unsupervised, Reinforcement Learning)	3 weeks
Data Prep & Feature Eng.	Data Cleaning, Feature Selection	2 weeks
Supervised Learning	Regression, Classification, Model Tuning	3 weeks
Unsupervised Learning	Clustering, Dimensionality Reduction, Anomaly Detection	2 weeks
Deep Learning	Neural Networks (CNNs, RNNs)	4 weeks
AI/ML in Practice	Predictive Analytics, NLP, AI in Cybersecurity	3 weeks
Ethics and AI Governance	Bias, Ethical Considerations, AI Governance	2 weeks
Capstone Project	Develop and Deploy AI/ML Solution	4 weeks
Intro to ROVs	Overview, History, Types, Applications	2 weeks
ROV Design and Architecture	Components, Power, Control Systems	3 weeks
Navigation and Control	Autonomous Navigation, AI in Control Systems	3 weeks
Sensors and Data	Sensor Types, Data Collection, AI Integration	2 weeks
Communication Systems	Wired/Wireless Communication, Real-Time Transmission, Security	2 weeks
ROV Operations	Mission Planning, Case Studies	3 weeks
Future Trends	AI Advances, Swarm Robotics, Underwater/Space ROVs	2 weeks
Capstone Project	Design and Implement an ROV	4 weeks

Private Secure Infrastructure

Course Module	Content Overview	Duration
Introduction to Private Secure Infrastructure	- Fundamentals of private networks - Security requirements - Designing secure infrastructure	2 weeks
Network Design and Architecture	- Secure network design principles - Architecture for private networks - Segmentation and isolation	3 weeks
Access Control and Identity Management	- Implementing access control mechanisms - Identity management - Multi-factor authentication	2 weeks
Threat Detection and Response	- Detecting threats in private networks - Incident response strategies - Forensics and analysis	2 weeks
Data Protection and Encryption	- Encryption techniques - Data protection methods - Securing sensitive information	3 weeks
Compliance and Risk Management	- Compliance standards - Risk assessment - Policy development	2 weeks

Cloud Security

Course Module	Content Overview	Duration
Introduction to Cloud Security	- Basics of cloud computing - Cloud security fundamentals - Types of cloud services and their security	2 weeks
Securing Cloud Infrastructure	- Securing cloud environments - Infrastructure protection - Cloud architecture and security best practices	3 weeks
Cloud Data Protection and Privacy	- Data encryption in the cloud - Privacy issues - Regulatory compliance	2 weeks
Identity and Access Management in the Cloud	- Managing identities and access - Authentication and authorization - Identity federation and SSO	2 weeks
Cloud Security Threats and Mitigation	- Common threats in cloud environments - Threat mitigation strategies - Incident response in the cloud	2 weeks
Compliance and Governance in Cloud Security	- Compliance frameworks - Governance models - Risk management	2 weeks

Cryptography

Course Module	Content Overview	Duration
Introduction to Cryptography	- Basics of cryptography - Cryptographic algorithms - Key concepts and terminology	2 weeks
Symmetric and Asymmetric Encryption	- Symmetric encryption techniques - Asymmetric encryption methods - Key exchange protocols	3 weeks
Hash Functions and Digital Signatures	- Hash functions - Digital signatures - Integrity and authenticity	2 weeks
Cryptographic Protocols	- Common cryptographic protocols - SSL/TLS - IPsec and their applications	2 weeks
Advanced Cryptography Techniques	- Advanced encryption methods - Quantum cryptography - Emerging trends in cryptographic technologies	3 weeks
Cryptography in Real-World Applications	- Practical applications of cryptography - Case studies - Implementing cryptographic solutions	2 weeks

Module	Topics Covered	Duration
Module 01: Introduction	- Basics of Networking - Basics of Cybersecurity - Cyber Threats Overview - Cybersecurity Terminology - Importance of Cyber Defense	2 weeks
Module 02: Social Engineering & Footprinting	- Concept: Social Engineering & Footprinting - Techniques: Identify Theft, Social Engineer Counter Measures - Concept: Footprinting - Types: Web, Email, Network, Social Media Footprinting - Tools: Footprinting Tools - Counter Measures: Footprinting Counter Measures	2 weeks
Module 03: Vulnerability Analysis & Sniffing	- Concept: Vulnerability Analysis & Sniffing - Types: Vulnerability Assessment - Tools: Assessment Tools - Reports: Assessment Reports - Concept: Sniffing - Types: MAC & DHCP Sniffing, ARP & DNS Poisoning, Spoofing Attacks - Tools: Sniffing Tools - Counter Measures: Sniffing Counter Measures	3 weeks
Module 04: System Security	- Concepts: Privilege Escalation, Gaining Access, Maintaining Access, Clearing Logs - Tools: System Security Tools - Counter Measures: System Security Counter Measures	2 weeks
Module 05: Network Security	- Concept: Network Security - Tools: Scanning Tools, Host & Port Discovery - Techniques: IDS & Firewall Scanning, Fingerprinting - Counter Measures: Network Security Counter Measures	2 weeks
Module 06: Wireless Security	- Concept: Wireless Security - Techniques: Wireless Encryption, Security Threats - Tools: Bluetooth & Wi-Fi Security Tools - Counter Measures: Wireless Security Counter Measures	2 weeks
Module 07: Web Security	- Concept: Web Security - Threats: Server Security Threats - Management: Server Security Management - Counter Measures: Web Security Counter Measures	2 weeks
Module 08: Mobile Security	- Threats: Mobile Platform Threats, Android OS Threats, iOS Threats - Solutions: MDM Solutions	2 weeks

	- Tools: Mobile Security Tools - Techniques: Secure Communication	
Module 09: IoT & OT Security	- Concept: IoT & OT Security - Threats: IoT Threats, OT Threats - Counter Measures: IoT & OT Security Counter Measures	2 weeks
Module 10: Malware Analysis	- Concept: Malware - Types: APT, Virus, Worm, Trojan, Fileless Attack Threats - Techniques: SQL Injection - Tools: SQL Tools, Antimalware Software - Techniques: Evasion Techniques - Counter Measures: Malware Counter Measures	2 weeks
Module 11: Cloud Security	- Concept: Cloud Security - Technologies: Cloud Technology - Techniques: Cloud Security	1 week
Module 12: Threat Detection & Incident Response	- Concepts: Security Operation Centre, Security Information & Event Management - Tools: Endpoint Detection and Response, Extended Endpoint Response - Techniques: Ransomware Detection, Threat Detection, Incident Response	2 weeks
Module 13: Cryptography	- Concept: Cryptography - Algorithms: Crypto Algorithms - Tools: Crypto Tools - Concepts: Public Key Infrastructure, Email Encryption, Communication Encryption, Crypto Analysis	2 weeks
Module 14: Cyber Defence	- Tools: SMC & SMC Lite, Secure Gateway, xFirewall, Endpoint Security, Secure Communication, VPN Technology, Enterprise Messenger	3 weeks