Add on Course on Digital Forensics and Cyber Intelligence organised by Department of Commerce, Shivaji College

Cybercrime refers to criminal activities conducted through digital means, targeting computer systems, networks, or data. It includes hacking, phishing, and identity theft. The distinction from conventional crimes lies in the use of technology as a tool or target. Cybercrimes often transcend borders, have global impacts, and require specialized expertise for investigation and prosecution, setting them apart from traditional criminal activities.

Learning Objectives:

- To build foundational knowledge in cybersecurity by delving deeper into the specialized areas of digital forensics and cyber intelligence.
- To provide students with advanced skills and techniques necessary to conduct comprehensive digital investigations
- To gather actionable intelligence in a rapidly evolving cyber landscape.
- To know various laws and statutes regarding cyber crime

Learning Outcomes:

- By the end of this add-on course, students will have developed advanced expertise in digital forensics and cyber intelligence, enabling them to lead complex investigations, mitigate sophisticated cyber threats, and provide strategic intelligence to support organizational security objectives.

- Through practical exercises and case studies, students will deepen their understanding about cyber crime and learn how to deal with cyber criminals.

Module 1: Introduction to Cybercrime (2 hours)
- Defining Computer Crime and Cybercrimes
- Distinction between Cybercrime and Conventional Crimes

Module 2: Types of Cybercrimes(4 hours)
- Overview of Cyber Stalking
- Understanding Cyber Terrorism
- Forgery and Fraud in Cybercrime
- Crimes Related to Intellectual Property Rights (IPRs)
- Computer Vandalism
- Cyber Forensics

***Module 3: Legal Framework and Concepts* (6 hours)**
- Definitions under IT Act, 2000
- Significance of E-Business and Electronic Governance
- Risks associated with Instant Messaging, Social Networking, and Mobile Applications

- Introduction to Internet of Things (IoT)
- Cyber Jurisdiction and Domain Name Disputes

***Module 4: Secure Operations in Cyberspace* (4 hours)**
- E-Money and Regulations of Pre-Payment Instruments (PPI) by RBI
- Electronic Money Transfer and Privacy of Data
- Authentication of Electronic Records
- Legal Recognition of Digital Signatures
- Role of Certifying Authorities and Controller's Powers

Module 5: Cybercrime Enforcement(4 hours)
- Prioritizing Cybercrime Enforcement
- Reasons for Cybercrimes
- Overview of GDPR and Indian Data Protection Regime

Module 6: Understanding Cybercriminals(2 hours)
- Profiling Cybercriminals
- Categorizing Cybercriminals
- Characteristics of Cyber Victims
- Making Victims Part of the Crime-Fighting Team

Module 7: Cyber Investigators and Investigation Process(2 hours)
- Role and Skills of Cyber Investigators
- Demystifying Computer and Cybercrime
- Investigation Methodology and Evidence Securing

***Module 8: Conducting Forensic Investigations*(2 hours)**
- Professional Conduct in Investigations
- Investigating Company Policy Violations
- Policy and Procedure Development
- Conducting Computer Forensic Investigations

***Module 9: Digital Evidence Collection and Preservation* (2 hours)**
- Understanding the Role of Evidence in Criminal Cases
- Admissibility of Digital Evidence
- Forensic Examination Standards
- Collecting and Preserving Digital Evidence

***Module 10: Building the Cybercrime Case*(2 hours)**
- Major Factors Complicating Prosecution
- Overcoming Obstacles to Effective Prosecution
- Investigative Tools and Steps
- Defining Areas of Responsibility