CYBER INTELLIGENCE			
Semester	**IV**	CIE Marks	**50**
Course Code	**24MCPE672**	SEE Marks	**50**
Teaching Hrs/Week (L:T:P)	**3:0:0**	Exam Hrs	**03**
Total Hrs	**42**	Credits	**03**

Course Learning Objectives:

This course is designed to:

1. Impart knowledge on the building blocks of the threat intelligence life cycle and its associated strategies.
2. Provide methods and approaches for generating intelligence requirements that drive a typical project.
3. Familiarize with incorporating an established threat intelligence framework within the security ecosystem
4. Instill the ability to create a secure and resilient system capable of withstanding potential attacks while ensuring the protection of valuable assets.
5. Familiarize with the types of data required for intelligence gathering and the sources from which it can be collected.

Module 1: Introduction to Cyber Intelligence	**No. of Hrs: 08**

Need for Cyber Intelligence: Intel stories in military, Types of Intelligence: HUMINT, OSINT, SIGINT, COMINT, Intelligence drives operations, Understanding the maneuver warfare mentality.

Textbook 1 - Ch 1

Module 2: Intelligence Development	**No. of Hrs: 08**

The Intelligence Cycle Steps: Planning and direction, Collection, Processing, Analysis and production, Dissemination, Utilization.

Textbook 1 - Ch 2

Module 3: Integrating Cyber Intelligence, Security and Operations	**No. of Hrs: 08**

Developing a strategic cyber intelligence capability, Introduction to Operational Security (OPSEC), Applications of OPSEC in business environments, Cyber Intelligence Program Roles.

Textbook 1 - Ch 3

Module 4: Active Defense and Threat Response	**No. of Hrs: 10**

General principles of Active Defense, Enticement and entrapment in Active Defense, Types of Active Defense, F3EAD Process, F3EAD and the Kill Chain, Applications of F3EAD in the commercial space.

Textbook 1 - Ch 4, 5

Module 5: Threat Intelligence and Collaboration	**No. of Hrs: 08**

Capability Maturity Model, Purpose of Collaboration Capability, Collaboration at the strategic level, Collaboration at the tactical level, Collaboration at the operational level.

Textbook 1 - Ch 6, 7

Course Outcomes:

At the end of the course, the student will be able to:

CO1: Apply concepts like maneuver warfare and the OODA Loop to real-world scenarios for analyzing and improving organizational security responses.

CO2: Build and manage intelligence requirements by applying the steps of the intelligence cycle for effective data collection and analysis.

CO3: Use the OPSEC framework to analyze and address potential threats and vulnerabilities within an organization's security operations.

CO4: Utilize the principles of Active Defense and the F3EAD process to design proactive measures against identified threats.

CO5: Make use of threat intelligence data from various sources to build a collaborative and effective threat response framework within security operations.

Textbooks:

1. Wilson Bautista Jr., "*Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents"*, Packt Publishing, 2018

Reference Books:

1. Aaron Roberts, "*Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers"*, Apress, 2021
2. Jean Nestor M. Dahj, "*Mastering Cyber Intelligence"*, Packt Publishing, 2022

Web Links:

1. Threat Intelligence, Why It Matters: https://www.paloaltonetworks.com/cyberpedia/what-is-cyberthreat-intelligence-cti
2. Cyber Threat Intelligence: https://arcx.io/courses/cyber-threat-intelligence-101
3. Mastering Cyber Threat Intelligence: https://www.my-mooc.com/en/book/mastering-cyber-intelligence
4. Mastering Cyber Threat Intelligence, Scratch To Master: https://www.udemy.com/course/mastering-cyber-threat-intelligence-scratch-to-master/?couponCode=LETSLEARNNOWPP