INFORMATION WARFARE

Subject Code: CS34325CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Computer Networks, Cyber Security, Information Security Fundamentals

Course Objective: To provide the foundations of information warfare principles, offensive and defensive operations, and strategic aspects of conflict in the information age.

Course Outcomes:

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

CO-1	Understand and analyze the concepts, dimensions, models, and threat actors of information warfare.
CO-2	Comprehend and evaluate offensive information warfare techniques including cyber intrusions, malware, espionage, and influence campaigns.
CO-3	Understand defensive security mechanisms, threat intelligence, and resilience strategies to protect information assets and infrastructures.
CO-4	Analyze the impact of artificial intelligence, emerging technologies, and strategic communication in modern information warfare.
CO-5	Evaluate legal, ethical, geopolitical, and real-world case studies related to information warfare.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	3	2	1	3	1
CO-2	2	3	3	2	2	2
CO-3	2	3	2	1	2	2
CO-4	2	2	2	2	3	2
CO-5	2	3	3	1	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Introduction to Information Warfare:

Concept of data, information, and knowledge; evolution of warfare from conventional to cyber and information warfare; Information as an asset, weapon, target, and strategic resource; dimensions of information warfare: military, political, economic, corporate and societal; threat actors: nation-states, proxies, terrorists, hacktivists, insiders and criminal groups; information warfare models: denial, deception, disruption, degradation and subversion; Attack surfaces and objectives.

Unit-2: Offensive information warfare techniques:

Cyber offensive operations: reconnaissance, OSINT, exploitation, persistence, privilege escalation, lateral movement and exfiltration; malware for information operations: viruses, worms, Trojans, ransomware, logic bombs and botnets; intelligence and espionage: military, economic and

industrial espionage; psychological and cognitive warfare: propaganda, misinformation, disinformation, perception management, social media manipulation and influence campaigns; synthetic media: deepfakes, AI-generated content and automated influence operations.

Unit-3: Defensive Information Warfare and Resilience:

Security objectives: confidentiality, integrity, availability, authenticity and trust; defensive strategies: prevention, detection, response and recovery; security mechanisms: authentication, encryption, access control, auditing and monitoring; intrusion detection and prevention systems; threat intelligence and anomaly detection; bot and deepfake detection techniques; risk and vulnerability assessment; defense of critical information infrastructure; cyber resilience, continuity planning and incident response; limitations and challenges of defense mechanisms.

Unit-4: Governance, Emerging Trends and Case Studies:

National cyber security policies, cyber laws and international norms; ethics of information warfare; information warfare in military doctrines and geopolitical conflicts; AI in information warfare: adversarial AI, predictive analytics, autonomous defense systems; election interference, economic manipulation and strategic communication campaigns; case studies of major global information warfare incidents;

Learning Resources:

Text and Reference Books:

1. Ventre, Daniel. *Information warfare*. John Wiley & Sons, 2012.
2. Farwell, J. Information Warfare. Marine Corps University Press, 2020.
3. Carr, Jeffrey. Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.", 2012.
4. Singer, Peter Warren, and Emerson T. Brooking. LikeWar: The weaponization of social media. Eamon Dolan Books, 2018.
5. Hutchinson, William, and Matthew Warren. Information warfare. Routledge, 2012.