



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



RASHTRIYA RAKSHA UNIVERSITY

An Institution of National Importance

Pioneering National Security and Police University of India

SCHOOL OF INTERNAL SECURITY, DEFENCE AND STRATEGIC STUDIES

Organises

Online Certificate Course On

Information Warfare

Date: 18-23 August 2026



Course Coordinators

Dr. Aparna Varma
Assistant Professor

Dr. Pramjit Singh
Assistant Professor



Scan for Registration

www.rru.ac.in

Concept Note

Information warfare (IW) is defined as the deliberate use and control of information to mislead, divide, or manipulate perceptions and influence political or social outcomes. Recognized as a foundational warfighting function and an instrument of national power, IW is utilized alongside diplomatic, military, and economic tools to achieve strategic goals and impose a commander's will. In the modern era, the shift from the industrial age to the information age has created a landscape of instant and persistent global visibility, where the traditional levels of warfare, strategic, operational, and tactical, are increasingly compressed, allowing local actions to have immediate global impacts. Adversaries now leverage technological and social vulnerabilities to conduct hostile social manipulation, blurring the divide between peace and war through unrestricted methods designed to destabilize institutions and erode public trust.

The mechanics of information warfare involve targeting both thinking processes, such as human cognition and decision-making, and non-thinking processes, which include algorithmic and pre-programmed machine behaviours. A primary challenge in this domain is the distinction between disinformation, deliberate falsehoods intended to cause harm, and misinformation, which is the accidental spread of inaccuracies. Modern campaigns often employ a "firehose of falsehood" strategy, scattering lies and half-truths across numerous channels simultaneously to prioritize bewilderment over persuasion and overwhelm cognitive defences. Generative AI acts as a "force multiplier" in this space, enabling the creation of high-fidelity deepfakes and automated propaganda that saturate the information environment. Furthermore, digital recommendation algorithms do not merely organize content; they "organize perception" by prioritizing emotionally charged information that heightens polarization and ideological extremity.

Strategic competitors often utilize IW to "win without fighting," employing concepts such as Russia's "reflexive control" to manipulate an opponent's perceptions or China's "Three Warfares" (public opinion, psychological, and legal warfare). To counter these threats, organizations must pursue an "information advantage," an exploitable condition resulting from the ability to generate, preserve, deny, and project information more effectively than an opponent. This advantage is built on three primary pillars: systems overmatch, prevailing narratives that elicit trust and credibility, and force resiliency. Ultimately, building resiliency requires an "assault through the ambush" mentality where media literacy and education serve as the primary defence, "inoculating" individuals against malign influence by training them to recognize cognitive biases and reject manipulated media.

Information Warfare (IW) has emerged as one of the most significant dimensions of contemporary conflict, where information itself becomes both a strategic resource and a weapon. Beyond conventional military operations, states and non-state actors increasingly employ information, cyber capabilities, artificial intelligence, social media platforms, and psychological influence campaigns to shape public opinion, manipulate perceptions, influence decision-making, and achieve strategic objectives without necessarily engaging in kinetic warfare. The rapid evolution of digital technologies has blurred the traditional distinction between peace and conflict, making the information domain a continuous arena of strategic competition.

Modern information warfare extends beyond the deliberate spread of disinformation to include cognitive manipulation, algorithm-driven amplification of narratives, deepfake technologies, coordinated influence operations, and psychological targeting of audiences. As AI-enabled content generation and digital platforms continue to evolve, the speed, scale, and sophistication of information operations have increased dramatically, posing serious challenges to national security, democratic institutions, and societal resilience. Consequently, understanding the concepts, doctrines, techniques, and practical applications of information warfare has become essential for policymakers, defence professionals, researchers, media practitioners, and students of strategic studies. This certificate course provides participants with both theoretical foundations and practical analytical tools to understand emerging information warfare strategies, evaluate contemporary case studies, and develop informed responses to evolving information threats.

Learning Outcomes

Upon successful completion of the course, participants will be able to:

1. Explain the fundamental concepts, doctrines, evolution, and strategic significance of Information Warfare in the contemporary security environment.
2. Analyse the role of psychological operations, cognitive influence, perception management, and strategic communication in Information Warfare campaigns.
3. Evaluate the information warfare capabilities, organisational structures, and operational approaches adopted by major state actors through contemporary case studies.
4. Assess the integration of cyber operations, electronic warfare, artificial intelligence, and emerging technologies within the broader Information Warfare ecosystem.
5. Apply analytical tools such as the Target Audience Analysis Worksheet (TAAWS) and the OODA Loop framework to design and evaluate information operations.
6. Develop a comprehensive understanding of social media dynamics, disinformation campaigns, and media literacy to identify, assess, and respond to contemporary information threats.

Date 18.08.2026 | Time : 1030hrs

Welcome Address: Director, SISDSS
Inaugural Address: Vice Chancellor, RRU

Orientation Address by Guest of Honour
Hon'ble Governor of Bihar
Lt Gen Syed Ata Hasnain (Retd), PVSM, UYSM, AVSM, SM, VSM & Bar

Date	Time	Themes	Topic
18.08.2026 Session 01	Morning 1100h - 1300h	Basics of IW	Introduction: Concepts and components of IW
	Evening 1430h - 1700h		The UN as a Theatre of Competing Narratives: Role of Diplomacy as Soft Power
		Assignment 01	
19.08.2026 Session 02	Morning 1030h - 1300h	Psychological Warfare	Psy Ops Planning cycle - I
	Evening 1430 - 1700h		Psy Ops Planning cycle - II and integration with OODA
		Assignment 02	
20.08.2026 Session 03	Morning 1030h - 1300h	IW in India's Neighbourhood	IW structures in West Asia and China - A Comparative Analysis
	Evening 1430h - 1700h		Op Sindoor: A Case Study of IW
		Assignment 03	
21.08.2026 Session 04	Morning 1030h - 1300h	IW and Tech	Cyber Warfare as part of IW
	Evening 1430h - 1700h		Artificial Intelligence and IW
		Assignment 04	
22.08.2026 Session 05	Morning 1030h - 1300h	IW and Tech	Electronic Warfare as part of IW
	Evening 1430h - 1700h		Preparation of TAAWS (Target Audience Analysis Worksheet) - Practical
		Assignment 05	

23.08.2026 Session 06	Morning 1030h - 1300h	Media as Force Multiplier	Perception Management
	Evening 1430h - 1530h		Weaponising social media in IW
		Assignment 06	
	Total hours : 36hrs		
	1645h-1730h Valedictory Session Vote of Thanks		

Chief Patrons



Prof. (Dr.) Bimal N. Patel
Vice-Chancellor
Rashtriya Raksha University

Prof. (Dr.) Kalpesh. H. Wandra
Pro Vice-Chancellor
Rashtriya Raksha University



Organiser



Dr. Ashutosh Mukund Pandey
Director & Assistant Professor
Rashtriya Raksha University

Course Coordinator

Dr. Aparna Varma
Assistant Professor
Rashtriya Raksha University



Course Coordinator

Dr. Pramjit Singh
Assistant Professor
Rashtriya Raksha University



Course Co-Coordinator

Hemshikha Mishra
Junior Research Assistant
Rashtriya Raksha University
For any queries
Email : jra2.sisdss@rru.ac.in

