SAVITRIBAI PHULE PUNE UNIVERSITY

(*Formerly University of Pune*)

Advanced Diploma in Cyber and India's National Security

(Credit and Semester System)

SYLLABUS

(To be implemented from the Academic Year: 2025-26)

Department of Defence and Strategic Studies,

Savitribai Phule Pune University,

Dr. Babasaheb Ambedkar Bhavan Pune-411007 (India)

Website: http://ddss.unipune.ac.in

Contact Details:

Telephone:91-20-25621472; 91-20-25690050

Total No. of Seats: 40+
Eligibility: Any Graduate
Fees: As per Savitribai Phule Pune University Rules
Duration: One Year (As Per NEP-2020)

Program Title:

Advanced Diploma in Cyber Security and India's National Security

Program Scope:

This program offers a multidisciplinary and practice-oriented foundation in cybersecurity, digital governance, and emerging cyber threats. It equips learners with the technical, legal, strategic, and investigative skills required to protect digital assets, analyse cybercrime trends, and respond to evolving national and international security challenges. The curriculum blends theoretical modules with hands-on training in VAPT, Forensic Analysis, and Policy Evaluation, preparing students for Careers in Cybersecurity Operations, Compliance, Cyber Law, and Digital Risk Management.

Objectives of the course:

- To provide students with deep understanding on various aspects pertaining to cybercrime, cyber terrorism, crypto-currency, critical infrastructure, cyber law and cyber security.
- Study aspects concerning use of digital technology its abuse and issues pertaining to social media, digital piracy, online privacy and misinformation.
- To acquaint students with the basic concepts of cyber security and national security.
- To acquaint students with the basic concepts of research methodology and help develop spirit of scientific temperament and scientific inquiry.
- To identify key cyber vulnerabilities, assess cyber risk and data protection methods.
- To introduce students the principles, procedures and processes of cyber-forensics and cyber- crime investigations.
- Discuss roles and mandate of various law enforcement groups and cyber defense agencies spanning; civil, military and government.
- To cover the concepts related to cyber-space and cyber-security.
- Gaining understanding of how evolution and access to technology has affected the concept of national security.

Structure of the Course:

The Post Graduate Adavanced Diploma in Cyber Security and India's National Security allows an in-depth study on various aspects pertaining to Cyber Security and National Security. This course has 44 credits, divided into two semesters, over the period of one year. The course focuses upon major thrust areas like, Cyber Security Awareness, Vulnerability Assessment, Cyber Law, Cyber Forensics, Cyber Terrorism, Crypto currency, Cyber Security Policies, Incident Response, Cyber Governance and Compliance, Geopolitics and Cyber Security.

Course Description and Evaluation:

Post Graduate Advanced Diploma in Cyber Security and India's National Security (CSNS) is a part-time program. Medium of instruction is English (Students would, however, be permitted to write their examination in Marathi, as an option). For assessment, the department will follow the choice-based credit system (CBCS). Continuous evaluation system through internal assessment (50%) - assignments, dissertation, term papers and seminars. External assessment -end semester examination (50%).

Method of Teaching:

Utilize a variety of instructional methods- classroom interactions, tutorials, study of classical texts, case method, debates, field visits, open book method, round table discussion, online learning, problem solving, simulation, problem formulation, database searches, comparative studies, prepare monograph, power point presentations and discussions. Special lectures by eminent scholars, conduct seminars, webinars and panel discussions.

Career Prospects:

This course will be beneficial to students and professionals. It will help individuals in pursuing their academic and career growth.

- Opportunities to work in areas of Corporate World and Senior Management.
- Prepare for careers in Regional and International Organizations.
- Prepare for careers in Policy Making Institutions.
- Prepare for careers in Think Tanks and International Research Institutes.
- Prepare for careers in Cyber Forensics.
- Prepare for careers in Security and Cyber Security Consulting.
- Prepare for careers in Civil Services and Competitive Examinations.
- Prepare for careers related to Law Firms, Public Policy, and Digital Governance.

1ST SEMESTER

Course No	Course Title	Course Credit	Total Marks
CSNS 1.1	Fundamentals of Cyber Security	4	100
CSNS 1.2	Cyber Security and India’s National Security	4	100
CSNS 1.3	Cyber Terrorism and its Security Challenges	4	100
CSNS 1.4	Cyber Security, Polices, Governance and Compliance	4	100
	Elective Paper		
CSNS 1.5	Practical Component: Case Studies	2	50
	Research Methodology		
CSNS 1.6	Cyber Security and Research Methodology	4	100
	Total	**22**	**550**

2nd SEMESTER

Course No	Course Title	Course Credit	Total Marks
CSNS 2.1	Geopolitics and Cyber Security	4	100
CSNS 2.2	Emerging and Disruptive Technologies	4	100
CSNS 2.3	Social Media, Disinformation and Cybersecurity	4	100
CSNS 2.4	Dissertation	4	100
	Elective Papers		
CSNS 2.5	Conceptual Framework of National Security	2	50
	On Job Training		
CSNS 2.6	Cyber Internship / On Job Training.	4	100
	Total	**22**	**550**

SEMESTER 1

Course Name: FUNDAMENTALS OF CYBER SECURITY
Course Code: CSNS 1.1
Course Credits: 4 Credit

Course Objectives:
1. Introduce Core Principles and Threat Landscapes: Understand foundational cybersecurity concepts including Confidentiality, Integrity, Availability (CIA Triad), and explore cyber threats such as Trojan, Malware and Zero Day.
2. Develop Cyber Defensive Strategies and Risk Awareness: Learn basic Cyber Security tools and Techniques— Firewalls, Honeypots, Access control and apply risk assessment methods to protect digital systems.

Course Learning Outcomes:
1. The learner will understand the cyber kill chain and all the processes that attackers follow, from initiating an attack to achieving their goals.
2. The learner will begin by gaining an understanding of the need for cybersecurity in every organization, the fundamental procedures that must be followed by cybersecurity professionals.

Teaching Methods:
1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:
1. 50 % of internal assessment will consist of Assignments/Term Papers/Presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Basic of Computer and Cyber Security.
1.1 History of Computer and Generations
1.2 Computer and its Components
1.3 Introduction to Operating Systems
1.4 Introduction to Cloud Security
1.5 Email Security, Web Security and Database Security
1.6 HTTP, HTTPS, SSL and Firewall

Unit 2: Foundations of Cyber Security and Emerging Threats
1.1 Definition, Scope, and Importance
1.2 CIA Triad: Confidentiality, Integrity, Availability
1.3 Threat Landscape: Viruses, Worms, Trojan, Malware, Zero Days
1.4 AI-Driven Attacks: Deepfakes, APTs, RaaS, Internet of Things
1.5 Remote Work Vulnerabilities and Expanded Attack Surfaces

Unit 3: Legal, Ethical, and Governance Frameworks
2.1 Information Technology Act 2000 and Amendments

2.2 International Cyber Law Frameworks: GDPR, WTO, Interpol, WCAG
2.3 Computer Hacking and Bharatiya Nyaya Sanhita, 2023
2.4 Digital Rights, Online Privacy, Right to Forget and Surveillance Debates
2.5 Evolution of Ransomware: Encryption, Data Theft, Extortion, Data Recovery

Unit 4: Network Security: Protocols, Systems, and Applications
3.1 Network protocols: TCP/IP, DNS, HTTPS, P2P
3.2 Cyber Security Tools: Antivirus,VPN, IDPS, IAM, DLP, EDR, Honeypots
3.3 Network attacks: DDoS, DNS/IP/MAC Spoofing, Password Attacks
3.4 Fundamentals of Cloud Security
3.5 Crypto Jacking, E- Commerce and Digital Payment Frauds

Unit 4: Encryption, Cryptography and Cyber Forensics
4.1 Encryption: Symmetric vs. Asymmetric vs. Hashing
4.2 Digital Signatures, Electronic Signatures and Digital Certificates
4.3 Digital Forensics Cycle: Identification, Preservation and Collection of Evidence
4.4 Forensics Tools: Wireshark, Autospy, Cellebrite, Encase, HashKeeper
4.5 Cyber Security Policies and Compliance: ISO 27001, NIST Framework, COBIT

Suggested Reading:

- Bhushan Mayank, Rathore Rajkumar, Jamshed Saurabh Fundamentals of Cyber Security: Principles, Theory & Practices. Publisher: BPB Publications (2017).
- Goyal Krishan, Garg Amit Cyber Security. Publisher: Laxmi Publications (2019).
- Brooks Charles, Grow Christopher, Craig Philip, Donald Jr. Cybersecurity Essentials. Publisher: Wiley (2018).
- Mewises Raef Cybersecurity for Beginners Publisher: Cyber Simplicity (2017).
- William Stallings, Brown Lawrie Computer Security: Principles and Practice, Publisher: Pearson Education (2018).

Course Name: CYBER SECURITY AND INDIA’S NATIONAL SECURITY
Course Code: CSNS 1.2
Course Credits: 4 Credits

Course Objectives:
1. Examine the strategic role of cybersecurity in safeguarding national interests, including critical infrastructure, defence systems, digital sovereignty and national security.
2. Analyse threats posed by cybercrime, non-states actors and state-sponsored attacks and their implications for geopolitical stability and internal security.
3. Explore legal, institutional, and policy frameworks for national cybersecurity governance, including coordination among civil, military, and law enforcement agencies.

Course Learning Outcomes:
1. Define the scope and significance of cybersecurity within national security frameworks.
2. Evaluate real-world incidents involving cyber warfare, sabotage and international cyber-attacks.
3. Assess the vulnerabilities of national infrastructure and propose risk mitigation strategies.
4. Interpret national and international laws, doctrines, and cooperative mechanisms related to cyber defence and sovereignty.

Teaching Methods:
1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:
1. 50 % of internal assessment will consist of assignments/term papers/presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Foundations and Threat Landscape
1.1 Introduction to National Security: Key Concepts and Definition
1.2 Introduction to Cyber Security
1.3 Introduction to Cyber Crime
1.4 Cyber Crimes: Modes and Classification
1.5 Cyber Crime: Tools and Technology
1.6 Cyber Crimes and Bharatiya Nyaya Sanhita 2023

Unit 2: Cyber Warfare, Information Security and Legal Frameworks
2.1 Introduction to Cyber Warfare: Concept and Definition
2.2 Attack Vectors: State-Sponsored, Non-State, Rogue State, Insider, Hacktivist
2.3 Cyber Defense Architecture: CERT, NCIIPC, NTRO, NCCC, I4C, MHA, MoD
2.4 Legal Instruments: IT Act 2000, UAPA, NSA, National Cyber Security Policy
2.5 Comparative Doctrines: NATO Cyber Defense vs India's Joint Cyber Doctrine

Unit 3: Strategic Technology and Disinformation
3.1 Emerging Technologies: Artificial Intelligence, Blockchain, Internet of Things
3.3 Information, Misinformation and Disinformation
3.4 National Cybersecurity Strategy and Capacity Building
3.4 Case Studies: Ukraine Drone Warfare, Stuxnet, Solar Winds Attack
3.5 Activity: Timeline of Major Cyber Incident related to Cyber Warfare

Suggested Reading:

- Khare, Vijay - Dr. B.R. Ambedkar and India's National Security Hardcover Publisher: Kalas Books (2005).
- Mali, Prashant - Cyber Law & Cyber Crimes Simplified: with The Information Technology Act, 2000 Publisher: Cyber Infomedia (2017).
- Taxmann - Bharatiya Nyaya Sanhita (BNS) 2023 – Comprehensive Legal Resource with Bare Act Publisher: Taxman Publication (2024).
- Clarke Richard & Kanke Robert - Cyber War: The Next Threat to National Security and What to Do About It Publisher: HarperCollins (2010).
- NATO Cooperative Cyber Defence Centre of Excellence - Tallinn Manual 2.0 on International Law Applicable to Cyber Operations Publisher: Cambridge University Press (2017).
- Johnson Thomas - Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare Publisher: CRC Press (2015).
- Singer & Friedman - Cybersecurity and Cyberwar: What Everyone Needs to Know Publisher: Oxford University Press (2014).
- Karmalkar Nitin, Khare Vijay - General B.C. Joshi Memorial Lectures on National Security Publisher: Pentagon Press (2022).

Course Name: CYBER TERRORISM AND ITS SECURITY CHALLENGES
Course Code: CSNS 1.3
Course Credits: 4 Credit

Course Objectives:

1. Examine the Nature, Scope, and Evolution of Cyber Terrorism, including its Ideological, Political, Social and Technological dimensions.
2. Analyse the vulnerabilities of Critical Infrastructure and digital systems to cyberterrorism threats, including state-sponsored and non-state actors.
3. Explore national and international Legal Frameworks, Countermeasures, and Strategic responses to Cyber Terrorism and related security challenges.

Course Learning Outcomes:

1. Define Cyber Terrorism and distinguish it from Cybercrime and Cyberwarfare.
2. Evaluate Real-World cyber incidents and threat scenarios involving cyberterrorism techniques and tactics.
3. Assess the impact of Cyber Terrorism on National Security, Public Safety, and Digital Sovereignty.
4. Interpret Legal Instruments, Policy Frameworks, and Institutional Responses to Cyber Terrorism.
5. Propose Technical and Governance-based solutions to mitigate Cyberterrorism Risk and enhance Cyber Resilience.

Teaching Methods:

1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:

1. 50 % of internal assessment will consist of Assignments/Term Papers/Presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Introduction to Cyber Terrorism

1.1 Introduction, Concepts and Definitions on Cyber Terrorism
1.2 Historical Evolution: Early Origins, Growth and Increased Sophistication
1.3 Motivations & Actors: Ideological, Political, Economic, Religious Drivers
1.4 Cyber Terrorism vs. Cybercrime vs. Non-State Actors
1.5 Case Study: Stuxnet Attack

Unit 2: Cyber Infrastructure and Vulnerabilities

2.1 Critical Infrastructure: Power Grids, Banking Systems, Public Transport, Healthcare
2.2 Anomaly Detection, Zero-Day Vulnerability, Exploits & Attacks
2.2 Attack Vectors: Malware, Ransomware, APTs, Wireless Access
2.4 Case Study: Estonia Attack
2.5 Activity: Diagramming India’s Critical Infrastructure and Key Ministers

Unit 3: Legal and Policy Frameworks

3.1 Global Conventions: ITU Resolutions, Budapest Convention, G20 Declarations
3.2 Challenges in Enforcement: Jurisdiction, Anonymity, Speed, Accountability
3.3 Information Technology Act and Cyber Terrorism
3.4 Comparative Framework: India vs. USA vs. China
3.5 Activity: Draft Cyber Security Policy for a Business Organization

Unit 4: Cyber Terrorism and National Security

4.1 Social Media: Misinformation, Disinformation and Online Radicalization
4.2 Psychology of Terror: Understanding Motivation and Counter-Radicalization Measures
4.3 Role of Law Enforcement Agencies and their Mandate
4.4 Activity: Timeline of Major Terror incidents affecting India's National Security
4.5 Case Study: Colonial Pipeline Attack

Suggested Reading:

- Khare, Vijay Terrorism and Counterterrorism. Publisher: Pentagon Press (2019).
- Brewster & Akhgar - Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Publisher: Springer (2016).
- Bingley Richard - Combatting Cyber Terrorism: A Guide to Understanding the Threat Landscape and Incident Response Planning. Publisher: IT Governance Publishing (2024).
- Johnson Thomas - Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Publisher: CRC Press (2015).
- Jeffrey Carr - Inside Cyber Warfare: Mapping the Cyber Underworld. Publisher: O'Reilly Media (2011).
- Lindsay, Cheung, Reveron Derek - China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain. Publisher: Oxford University Press (2015).
- Eoghan Casey - Handbook of Digital Forensics and Investigation Publisher: Academic Press (2010).

Course Name: CYBER SECURITY POLICES, GOVERNANCE AND COMPLIANCE
Course Code: CSNS 1.4
Course Credits: 2 Credit

Course Objectives:
1. Examine strategic frameworks for cybersecurity governance, including risk management, compliance and resilience.
2. Understand the roles of national and international institutions in shaping cybersecurity policy, standards, cooperation and strategic alliances.
3. Explore counterstrategies for mitigating cyber threats, including cyber Defence, incident response planning, threat intelligence and planning.

Course Learning Outcomes:
1. Analyse governance models and assess their effectiveness in managing cybersecurity risks across sectors.
2. Evaluate counterstrategies such as zero trust architecture, layered Defence systems, and threat hunting in organizational contexts.
3. Interpret legal, regulatory, and ethical dimensions of cybersecurity governance at national and international levels.
4. Design strategic cybersecurity policies aligned with business continuity, regulatory compliance, and stakeholder accountability.
5. Recommend improvements and countermeasures based on evolving cyber threat landscapes and technological shifts.

Teaching Methods:
1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:
1. 50 % of internal assessment will consist of assignments/term papers/presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Foundations of Cyber Governance, Risks and Compliance
1.1 Introduction, Definition and Scope of Cyber Governance
1.2 Importance of Cyber Governance in Risks and Compliance
1.3 Key Stakeholders: Boards, CISOs, Regulators, Investors and Audits
1.4 Cyber Governance Frameworks: NIST, ISO/IEC 27001, ZTA, PCI DSS
1.5 Evolution of International Cyber Norms: Budapest Convention, Paris Call, UN-OEWG

Unit 2: Strategic Threats and Policy Responses
3.1 Types of Cyber Threats: Non-State Actors, Supply Chain Attack, CI, Espionage
3.2 National Cybersecurity Strategy and Military Doctrines
3.3 Cyber Threat Intelligence and Incident Response
3.4 Role of Artificial Intelligence, Machine Learning and Quantum Technology.

Unit 3: Cyber Laws of P5 Nations:
3.1 USA, UK, Russian Federation, France, China
3.2 United Nations Charter and Jus Ad Bellum in Cyberspace
3.3 Digital Sovereignty, Piracy, Data Privacy and Countermeasures
3.4 Public-Private Partnerships (PPP)
3.5 Cyber Resilience and Business Continuity Plan

Unit 4: Comparative Frameworks and Future Directions
4.1 Privacy vs. Security: Exploring differences and relationships
4.2 Emerging Trends: Zero Trust Architecture, Quantum Computing Threats
4.3 Social Media Vis-à-vis Human Rights
4.4 Digital Diplomacy, Soft Power and International Relations
4.5 Digital Money Laundering: Modes and Classification

Suggested Reading:

- Indian Institute of Banking & Finance, Anti-Money Laundering and Know Your Customer Perfect Publisher: Macmillan (2023).
- Dehadrai, Jai Prevention of Money Laundering Act, 2002: A Practitioner's Guide Hardcover Publisher: Eastern Book Company (2004).
- Mayank Bhushan, Rathore Rajkumar, Jamshed Saurabh Fundamentals of Cyber Security: Principles, Theory & Practices. Publisher: BPB Publications (2017).
- Goyal Krishan, Garg Amit, Cyber Security. Publisher: Laxmi Publications (2019).
- Brooks Charles, Grow Christopher, Graig Philip, Donald Jr., Cybersecurity Essentials. Publisher: Wiley (2018).
- Mewises Raef, Cybersecurity for Beginners Publisher: Cyber Simplicity (2017).
- William Stallings, Lawrie Brown Computer Security: Principles and Practice, Publisher: Pearson Education. (2018).

Course Name: PRACTICAL COMPONETS: ASSESSMENT AND CASE STUDIES.
Course Code: CSNS 1.5
Course Credits: 4 Credit
Course Objectives:

1. Students perform hands-on scanning and testing systems using tools like Nmap, Metasploit, Burp Suite, McAfee Enterprise Security Manager.
2. They learn to identify security flaws, document findings, and propose remediation strategies. This component builds technical confidence and report-writing skills essential for various cyber industry roles.

Course Learning Outcomes:

1. Learners engage in role play, scenario building, timeline reconstruction and log analysis to trace cyberattack incidents.
2. Leaners engage in understanding various social engineering tactics and engage in role play and scenario building.

2.This module emphasizes analytical thinking and evidence-based reporting, preparing students for roles in law enforcement, compliance, and internal security teams.

1. Incident Response & Management

1.1 Role Play Scenarios building for Security Breach and Response Strategy.
1.2 Draft Incident Reports.
1.3 Hands-on SIEM Tools. (McAfee Enterprise Security Manager)
1.4 Activity: Create Information Security Incident Report Template.

2. Compliance & Audit Simulations

2.1 Mock Audits for ISO/IEC 27000 and PCI-DSS.
2.2 Breach & Attack Simulation for Compliance.
2.3 Policy Drafting, Gap Analysis, Risk Assessment, Review Policies and Control.
2.4 Cybersecurity Compliance Audit Simulation.
2.4 Activity: Create Risk Assessment Templates.

3. Setting up Firewall and Intrusion Detection Systems

3.1 Install and Configure Intrusion Detection System.
3.2 Update Signature and Firmware.
3.3 Install Firewall in Linux.
3.4 Install and Update Windows Firewall Systems.
3.5 Turn On/Off Windows Firewall.

4. Simulate Incident Response Scenarios

4.1 Perform, Protect, Detect, Act and Respond to Malware and Phishing.
4.2 Observe, Orient, Decide and Act (OODA) Loop.
4.3 Protect, Detect, Response (PDR).
4.4 Perform Network Traffic Analysis.
4.5 Activity: Describe Various Networks based Attacks.

5. Social Engineering

5.1 Overview of Social Engineering Attacks.
5.2 Do and Don’ts for Social Media Users.
5.3 Standard Operating Procedures (SOP).
5.4 Role Play Social Engineering Attacks.
5.5 Exercise: Power Point Presentation

Course Name: CYBER SECURITY AND RESEARCH METHODOLOGY
Course Code: CSNS 1.6
Course Credits: 4 Credit

Course Objectives:
1. Introduce foundational research principles, including hypothesis formulation, literature review, and methodological design tailored to cybersecurity contexts.
2. Develop skills in qualitative and quantitative research techniques, including surveys, case studies, statistical analysis, and experimental design for cyber risk assessment.
3. Explore ethical, legal, and practical considerations in cybersecurity research, including data privacy, responsible disclosure, and institutional review protocols.

Course Learning Outcomes:
1. Formulate research questions and hypotheses relevant to cybersecurity challenges such as cyber forensic analysis, policy evaluation, insider threat and non-state actors.
2. Design and conduct empirical studies using appropriate tools and techniques (e.g., SPSS, Python, network simulators, forensic toolkits).
3. Critically review academic, industrial and military literature to identify gaps and emerging trends Cybersecurity Research.
4. Present research outcomes through structured reports, academic papers, policy briefs, monographs demonstrating clarity and relevance.

Teaching Methods:
1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:
1. 50 % of internal assessment will consist of Assignments/Term Papers/Presentations/Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1. Problem Identification
1.1 Define a Precise Research Question (e.g. How do zero-day vulnerabilities propagate across supply chains?)
1.2 Problem Statement
1.2 Align Research with recent Cyber Threats and Technological Shifts
1.3 Conduct Online Research on the said topic

Unit 2. Literature Review
2.1 Survey: Academic Journals, White Papers, Geopolitical Policy Briefs
2.2 Identify Information Gap in areas like Information Security, AI and Forensics Tools
2.3 Conduct Review of Literature on Cyber Security Publications

Unit 3. Research Design
3.1 Choose Research Methodology based on your Objective: Qualitative or Quantitative
3.2 Observational: User Online Behavioral Pattern or Social Media Monitoring Exercise

3.3 Experiment: How People Respond to Disinformation vs. Fact Checking
3.4 Applied: Develop and Test Cyber Security Guidelines, Procedures and SOP's

Unit 4 Data Collection
4.1 Post Events Analysis: Incident Handling Timeline
4.2 Verify Compliance with Privacy Laws and Institutional Board Standards
4.3 Collect Data through Primary and Secondary Sources
4.4 Data Collection Methods: Surveys, Questionnaires, Interviews, Field and Library Visits
4.5 Activity: Visit Various Cyber Crime Reporting Portal (Online)

Unit 5 Academic: Report and Essay Writing
5.1 Book Review
5.2 Article Review
5.3 Commentary
5.4 Blog Writing
5.5 Report Writing
5.6 Essays and Monographs

Suggested Reading:

- Kumar, Ranjit Research Methodology: A Step-by-Step Guide for Beginners. Publisher: SAGE Publication (2024).
- Singh, Ranjit Research Methodology - For Ph.D. Course Work. Publisher: RT Publication (2021).
- Singh, Ranjit Research Methodology. Publisher: RT Publications (2022).
- Metcalf Leigh, Casey William Cybersecurity and Applied Mathematics. Publisher: Elsevier (2016).
- Kohn Loren Designing Secure Systems: Architecting for Security with the Threat Modeling Approach. Publisher: Wiley (2021).
- Eugene, Spafford, Leigh, Dykstra Josiah Cybersecurity Myths Misconceptions: Avoiding the Hazards and Pitfalls That Derail Us. Publisher: Wesley (2023).
- Shoemaker Dan - Cybersecurity: The Essential Body of Knowledge. Publisher: Conklin Cengage Learning (2011).

Semester II

Course Name: GEOPOLITICS AND CYBER SECURITY
Course Code: CSNS 2.1
Course Credits: 4 Credit

Course Objectives:

1. Examine the intersection of global trade, geopolitical tensions, and cyber vulnerabilities, with emphasis on digital infrastructure, supply chains, and strategic technologies.
2. Analyse how cyber threats—including espionage, subversion, and information warfare shaping international relations, economic competition and national security strategies.
3. Explore legal, institutional, and diplomatic frameworks for managing cyber risks in the context of global trade and geopolitical rivalries.

Course Learning Outcomes:

1. Interpret the strategic role of cyberspace in shaping trade policies, technology alliances, and geopolitical rivalries.
2. Evaluate case studies involving cyber-enabled trade disputes, digital sovereignty conflicts, and cross-border data governance.
3. Assess the impact of cyber threats on global supply chains, critical infrastructure, and economic resilience.
4. Analyse national and international responses to cyber challenges, including regulatory frameworks, multilateral cooperation, and strategic deterrence.
5. Propose informed strategies for balancing trade interests, geopolitical stability, and cybersecurity imperatives.

Teaching Methods:

1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:

1. 50 % of internal assessment will consist of Assignments/Term Papers/Presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units

Unit 1: Geopolitical Shifts and Tech Sovereignty

1.1 Basic Concepts of Cyber Security, Geopolitics and Cyber Power
1.2 Understand Geopolitical Shifts and Technological Landscapes
1.3 Case Study: US-China-India Tech Rivalry
1.4 Trade Wars, Market Instability and Strategic Alliances
1.5 Mapping Critical Technologies

Unit 2: Cybersecurity as Economic Strategy

2.1 Global Financial Systems and Supply Chain Risks
2.2 Digital Assets, Blockchain and Money Laundering

2.3 Cyber and Industrial Espionage
2.4 Cyber Space vis-vis Intellectual Property Rights
2.5 Trade Negotiations Amidst Cyber Attack

Unit 3: Regulatory Landscapes, Cryptocurrency and Blockchain
3.1 Data Localization and Cross-Border Compliance
3.2 Comparative Analysis: India's PDP Act vs. GDPR
3.3 Cryptocurrencies, Blockchain, and Sanction Evasion
3.4 Blockchain Forensics and Dark Web Forensics

Unit 4: Global Cyber Norms and Emerging Tech Diplomacy
4.1 Role of WTO, UN, and Regional Blocs in Tech Diplomacy
4.2 Cyber Security Norms across G20, G8, EU, SAARC, SCO
4.3 International Cyber Diplomacy and Quantum Technology
4.4 Activity: Draft International Cyber Ethics Charter
4.5 Case Studies: List Abbreviations on Global Cyber Security Norms

Suggested Reading

- Buchanan Ben – The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Publisher: Harvard University Press (2020).
- Lonergan & Lonergan – Escalation Dynamics in Cyberspace. Publisher: Oxford University Press (2023).
- Siddhartha & Shah Ankit - Geopolitics: Decoding Intents, Narratives, Lies and Future. Publisher: Kitab Mahal (2025).
- Segal Adam - The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. Publisher: PublicAffairs (2016).
- Singer & Friedman - Cybersecurity and Cyberwar: What Everyone Needs to Know. Publisher: Oxford University Press (2014).
- Miller Chris - Chip War: The Fight for the World's Most Critical Technology. Publisher: Scribner (2022).

Course Name: EMERGING AND DISRUPTIVE TECHNOLOGIES
Course Code: CSNS 2.2
Course Credits: 4 Credits

Course Objectives:

1. Examine the foundational principles and transformative potential of emerging technologies such as Artificial Intelligence, Blockchain, Quantum Computing, and the Internet of Things.
2. Analyse the impact of disruptive innovations on industries, governance, and society, including shifts in Business Models, Regulatory Frameworks, and Ethical considerations.
3. Explore strategic approaches for adopting, managing, and regulating emerging technologies in dynamic and competitive environments.

Course Learning Outcomes:

1. Identify and explain key emerging technologies and their technical foundations.
2. Evaluate the disruptive effects of these technologies on sectors such as Finance, Healthcare, Education, and Public Administration.
3. Apply strategic thinking to assess risks, opportunities, and governance challenges posed by emerging technologies.
4. Propose context-sensitive frameworks for responsible innovation, digital transformation, and regulatory adaptation.

Teaching Methods:

1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:

1. 50 % of internal assessment will consist of Assignments/Term Papers/Presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Foundations of Emerging Disruptive Technologies
1.1 Definition, Classification and Identification Criteria
1.2 Strategic Relevance in Defence, Intelligence and War
1.3 Overview of Key Technologies: Virtual Reality, Augmented Reality, 5G & 6G
1.4 Emerging Technologies and Disruptive Strategic Thinking

Unit 2: Risks, Vulnerabilities, and Ethical Challenges
2.1 Job Displacement, Algorithmic Bias and Autonomous Vehicles
2.2 Cyber Warfare Threats and Systemic Vulnerabilities
2.3 Legal and Ethical Issues: Regulation, Privacy, Accountability
2.4 International Norms and Governance Dilemmas

Unit 3: Global Power Shifts and Strategic Competition
3.1 Global Tech Supremacy: US-China-India-Saudi Arabia AI Competition

3.2 Digital Sovereignty, Strategic Alliances and Partnerships
3.3 Role of Global Institutions in Trade Wars: WTO-DSB, G20, G8, BRICS, SCO
3.4 Geopolitical Faultline: Armed Conflicts, Nationalism and Protectionism

Unit 4: Artificial Intelligence in Indian Context and Case Studies
4.1 India's AI Initiatives and Institutional Capacity Building
4.2 Integration of AI in ISR, C3, Training and Simulation
4.3 Case Studies: Autonomous Drone, Border Surveillance and Electronic Warfare
4.4 Contemporary Example: AI Infrastructure, Advanced Computing, Startups and Research

Suggested Reading:

- Armstrong Paul - Disruptive Technologies: A Framework to Understand, Evaluate and Respond to Digital Disruption. Publisher: Kogan Page (2023).
- Clayton Christensen - The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Publisher: Harvard Business Review Press (2016).
- Mittal Himanshu (Ed.) – Smart Computing and Emerging Technologies. Publisher: SCRS Publications (2025).
- Kelly Kevin - The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future. Publisher: Viking (2016).
- Gilder George - Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy. Publisher: Regnery Gateway (2018).
- Wadhwa & Salkever – The Driver in the Driverless Car: How Our Technology Choices Will Create the Future. Publisher: Berrett-Koehler Publishers (2017).

Course Name: SOCIAL MEDIA, DISINFORMATION AND CYBERSECURITY
Course Code: CSNS 2.3
Course Credits: 4 Credit

Course Objectives:

1. Examine the Role of Social Media platforms in shaping public discourse, human behaviour, and information ecosystems.
2. Analyse the mechanisms, techniques, and impacts of disinformation campaigns, including Bot Networks, Deepfakes, and Algorithmic amplification.
3. Explore Cybersecurity Strategies, Legal Frameworks, and Governance Models for detecting and responding to Disinformation and Social Media manipulation.

Course Learning Outcomes:

1. Identify and classify types of disinformation and their propagation methods across digital platforms.
2. Evaluate the cybersecurity risks posed by coordinated inauthentic behavior, data manipulation, and psychological operations.
3. Interpret national and international legal instruments addressing misinformation and disinformation, accountability and digital rights.
4. Apply analytical tools and strategic frameworks to assess and counter disinformation threats in real-world scenarios.
5. Propose policy, technical, and ethical solutions for enhancing information integrity and digital trust in cyberspace.

Teaching Methods:

1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:

1. 50 % of internal assessment will consist of assignments/term papers/presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Understanding the Digital Ecosystem
1.1 Introduction to Social Media
1.1 Evolution of Social Media Platforms
1.2 User Behaviour Patterns, Data Analytics and Infographics
1.3 Comparative Digital Governance: Western vs. Indian Regulatory Platforms
1.4 Activities: Timeline of Major Platforms, Glossary Building & Military Terminology

Unit 2: Anatomy and Impact of Disinformation
2.1 Types of Disinformation: Fake News, Fake Narratives, Viral Content, Hashtags
2.2 Comparative Lens: Democratic vs. Authoritarian Regime Disinformation Tactics
2.3 Activities: COVID-19 Disinformation Case Study
2.4 Suggested Format: Infographic + Case Summaries

Unit 3: Social Media as a Threat Vector
3.1 Types of Social Media: Facebook, Twitter, LinkedIn, Instagram, YouTube
3.2 Social Media Algorithms, Echo Chambers, Online Hate, Misinformation
3.3 Bot Networks, Troll Armies, Dark Room, Micro Blogging, Vlogging, Hangouts
3.4 Impact of Social Media: Digital Activism, Citizen Journalism, Digital Divide
3.5 Activity: Getting Organisation ready for Social Media Content Management

Unit 4: Cyber Security, Ethics, and Digital Resilience
4.1 Cognitive Hacking, Psychological Operations, Hybrid Warfare, Cyber Warfare
4.2 Legal and Ethical Challenges: Speech vs. Harm, Privacy, Accountability
4.3 Building Resilience: Media Literacy, Fact-Checking, Community Interventions
4.4 Activities: Create Disinformation Toolkit

Suggested Reading:

- Khare, Vijay Influence of Social Media on India's Foreign Policy Making Publisher: Pentagon Press (2022).
- Khare, Vijay Impact of Social Media on Peace and Security. Publisher: Pentagon Press (2022).
- Lance, Robert, Flores Claudia The Disinformers: Social Media, Disinformation, Elections. Publisher: Repro Books (2024).
- Losifidis Petros - Digital Democracy, Social Media and Disinformation. Publisher: Taylor & Francis Ltd. (2021).
- Singer & Emerson - Like War: The Weaponization of Social Media. Publisher: Houghton Mifflin Harcourt (2018).
- Woolley Samuel - The Reality Game: How the Next Wave of Technology Will Break the Truth Publisher: PublicAffairs (2020).
- DiResta, Starbird and Others - The Handbook of Disinformation Research. Publisher: Routledge (2025).

Course Name: DISSERTATION
Course Code: CSNS 2.4
Course Credits: 4 Credit

Course Learning Outcomes:
Students are advised to select their topic in consultation with their guide. Dissertation will evaluated by expert in concern field and marks will be given by the quality of research work. Dissertation may be published in Book form without permission of students. It will be the copyright and property of Department of Defence and Strategic Studies and Savitribai Phule Pune University.

Dissertation Submission Format:

- Students are required to submit Two Copies of the dissertation, duly typed and bonded.
- Use A-4 size paper and use Times New Roman script with 12 font size and one and a half spacing for lines.

Evaluation;

A. The evaluation shall be done by the Internal Examiner (Guide) and one External Examiner from within the Department. (Evaluation done in a combined manner for 50 marks).
B. Students would have to make a presentation in the Department. (Evaluation done by the Guide and the External Examiner who evaluates the written report in a combined manner for 20 marks).
C. Dissertation Viva Total; 80 Marks + 20 Marks: 100 Marks.

Course Name: CONCEPTUAL FRAMWORK OF NATIONAL SECURITY STUDIES
Course Code: CSNS 2.5
Course Credits: 2 Credit

Course Objectives:

1. The aim of this course is to introduce fundamental concepts in Security and Strategic Studies.
2. The course will introduce basic theories and approaches of Security and Strategic Studies.

Course Learning Outcomes:

1. Students will learn about various aspects to understand cyber-Security and Strategic Studies.
2. Students will learn about evolution of Strategic Studies during Cold War and Post Cold War period.

Teaching Methods:

1. Teaching will include classroom lectures accompanied with different exercises to learn basic concepts, field visits, etc.
2. Interactive and participative methods will be employed in teaching.
3. Seminars, Conferences, and Workshops will be organized.

Evaluation Pattern:

1. 50 % of internal assessment will consist of assignments/term papers/presentations/ Mid Term Exam and Practical.
2. 50 % External- Examination.
3. Concerned teachers may apply individual internal evaluation methods.

Course Units:

Unit 1: Key Concepts

1.1. Nation
1.2. State
1.3. Nation-State
1.4. Nationalism
1.5. National Power and Sovereignty
1.6. National Interest

Unit 2: Conceptual Understanding of Security

2.1 What is Security
2.2 Concepts and Theories on Security
2.3 Traditional Security vs Non-Traditional Security
2.4 National Security
2.5 International Security
2.6 Humanitarian Crises & Global Interventions

Unit 3: Strategic Studies: Concept and Scope

3.1 Strategic Studies: Key Concept
3.2 Theories and Causes of War
3.3 Key Thinkers; Sun Tzu, Carl von Clausewitz, Thucydides, Chanakya
3.4 Strategic Studies, International Relations and Cold War

3.5 India’s Nuclear Strategy
3.6 Pakistan’s Nuclear Strategy
3.7 China’s Nuclear Strategy

Unit 4: Contemporary Security and Strategic Issues:
4.1 Overview and Timeline of World Wars
4.2 Cyber Threat
4.3 Economic Threat
4.4 Nuclear Threat
4.5 Critical Infrastructure Threat
4.6 Terrorism and Cyber Terrorism

Suggested Readings:

- Khare, Vijay - Defence Studies (Marathi). Publisher: Nirali Prakashan (2007).
- Buzan Barry - People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Publisher: ECPR Press (2007).
- Cavelty, Balzacq and Thierry - Routledge Handbook of Security Studies, Conflict and the International System. Publisher: Lynne Rienner (1995).
- Collins - Contemporary Security Studies. Publisher: Oxford University Press (2016).
- Creveld - The Rise and Decline of the State. Publisher: Cambridge University Press. (2004).
- Cohen Eliot and Gray Colin - Strategy in the Contemporary World: An Introduction to Strategic Studies. Publisher: Oxford University Press (2002).
- Booth Ken - Theory of World Security. Publisher: Routledge (2017).

Course Name: ON JOB TRAINING/ INTERNSHIP PROGRAMME
Course Code: CSNS 2.6
Course Credits: 4

Course Objectives:

1. One of the objectives of the Internship Programme is that students will get a chance to spend some time undertaking work related to the discipline and gain practical experience as well as develop resource network
2. Internship programme would also give an opportunity to students to explore the professional and policy space, related to the discipline

Course Learning Outcomes:

1. Students will gain practical experience in a professional setting related to the student's field of study
2. Students will develop research and administrative skills through the completion of tasks assigned by the internship agency
3. It will enhance the ability to work independently as well as a part of the team
4. It will help them to build professional networks and relationships
5. Students will gain a deeper understanding of the practical applications of academic knowledge and skills

Evaluation Pattern:

1. Students will have to complete a minimum 60 hours and maximum 75 hours of work at the internship programme.
2. Internships can be undertaken at Strategic Think Tanks, Research Organizations, Government Bodies and Agencies, Academic Institutions, Policy Organizations or with Individual Academicians and Professionals
3. Students will undertake work as required by the internship agency. This must include research and administrative duties including submission of essays/books reviews/articles/interviews/etc.
4. Students will obtain a certificate from the internship agency indicating the work hours completed and the activities and duties undertaken by them during the internship programme
5. The certificate should be duly signed by the internship authority and submitted by the students to the department for evaluation

Suggested Thinks Tanks and Research Organizations:

- Institute for Defence Studies and Analysis
- Cyber Peace Foundation
- Observer Research Foundation
- United Service Institution of India
- Vivekananda International Foundation
- Institute of Peace and Conflict Studies
- National Maritime Foundation