MAHARSHI DAYANAND UNIVERSITY, ROHTAK
Diploma in National and Cyber Security

Skill

India is the home to some of the biggest IT companies that have quite some global reckonings. Now, most recently, some of these IT giants like Wipro, TCS, and Capgemini suffered cyber-attacks. There is no question whatsoever that such cyber-attacks deter the global credibility of this company.
In recent years, India has witnessed a sharp rise in the number of cyber-attacks. The expansion of the digital ecosystem has accentuated the need for companies to hire trained cyber security professionals to deal with new threats. As per a PwC study, the instances of cyber-attacks on Indian enterprises surged by 117 percent in 2019 compared to the previous year. However, due to insufficient funding and a crunch of skilled resources, the availability of skilled workforce does not live up to the demand in the industry. As thousands of companies look to hire cyber security professionals, the gap in the availability of skilled workforce has widened.

According to an estimate, the shortage of cyber-security workforce in India is 9 percent higher than the global average. Considering that India is home to several IT companies and addresses the technology requirements of several global companies, this shortage of skilled cyber-security workforce can be devastating in the long term. Thus, there is an immediate need to rethink the strategy and address the mismatch in the demand and supply of cyber-security professionals.

Professional Competency

The Post Graduate Diploma in Cyber Security and India's National Security is designed to cover the range of cyber incidents and frauds that commonly affect individuals, organizations and nations on a practically daily basis. The course will provide a compressive view of Cyber Security in Indian scenario – how it affects national security at different levels from individual to state and how the evolution and access to technology has affected the scenario of security.

The aim of the course is to identify basic vulnerabilities, learning to assess the risks to data and self. The course will also cover basic everyday measures to mitigating these risks. The focus of the diploma remains on the following points:

- The course will be beneficial to students and professionals. It will help individuals for pursuing their academic and career goals.
- Opportunities to work in area of corporate infrastructure and management.
- Prepare for careers related to Cyber-Laws, Cyber Security and National Security policy at corporate and government sector.
- Prepare for careers in international/regional organizations.
- Prepare for careers in policy organizations.
- Prepare for careers in Think tanks and research-oriented institutes.

Value Addition and Competitive Edge

- To provide students a deeper knowledge on various aspects pertaining to cyber security.

- To cover vulnerability detection and analysis of web applications, mobile applications and other computer systems.
- Study aspects concerning the freedom of expressions using digital technology, the use and abuse of the Internet and the issues of digital piracy, data usage and privacy.
- Discuss the role of multiple cyber agencies, spanning the civil, government and defence domains.
- To acquaint students with the basic concepts of research methodology and help them develop the spirit of scientific inquiry.
- To identify basic vulnerabilities, learn to assess the risk to data and self.
- To introduce students to the principles, procedures and processes of cyber -forensics and cyber- crime investigations.
- To cover the concepts of how cyber-space, cyber-security and cyber-warfare are emulated by various threat actors.
- Gain and understanding of how the evolution and access to technology has affected the scenario of security.

Semester	**Discipline-Specific@4 credits**	**Skill Enhancement Courses (SEC) / Internship@4credits**	**Value-Added Courses (VAC)@2 credits**	**Total Credits**
1	23CPDS11DSC1 Basic of Computer and Cyber Security	23CPDS11SEC1 Non-Traditional Security Threats	23CPDS11VAC1 Introduction to Defence and Security Studies	22
	23CPDS11DSC2 National Security of India			
	23CPDS11DSC3 Cyber Security in Indian Context			
	23CPDS11DSC4 Practicum			
2	23DPDS12DSC5 Security Mechanism in India	23DPDS12SEC2 Internship	23CPDS11VAC2 Animation and Web Designing	22
	23DPDS12DSC6 Cyber Law			
	23DPDS12DSC7 Cyber Crime			
	23DPDS12DSC8 Project Report			
				44

Scheme of Examination
Semester-I Session 2023-24

Course Code	**Course Name**	**Course Credit**	**Internal Assessment**	**Theory**	**Max. Marks**	**Duration of Exam.**
23CPDS 11DSC1	Basic of Computer and Cyber Security	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23CPDS 11DSC2	National Security of India	04	30 Attendance-5	70	100	3Hrs

			Assignments/ Seminars Presentations-5 Sessional Examination-20			
23CPDS 11DSC3	Cyber Security in Indian Context	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23CPDS 11DSC4	Practicum	04	30 Practical Assignments/ Practical File-25 Attendance-5	Examination – 70 Practical Examination- 50 Vova Voce- 20	100	3Hrs
23CPDS 11SEC1	Non-Traditional Security Threats	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23CPDS 11VAC1	Introduction to Defence and Security Studies	02	15 Attendance-5 Sessional Examination-10	35	50	3Hrs

Semester-II

Course Code	Course Name	Course Credit	Internal Assessment	Theory	Max. Marks	Duration of Exam.
23DPDS 12DSC5	Security Mechanism in India	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23DPDS 12DSC6	Cyber Law	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23DPDS 12DSC7	Cyber Crime	04	30 Attendance-5 Assignments/ Seminars Presentations-5 Sessional Examination-20	70	100	3Hrs
23DPDS 12DSC8	Project Report	04			100	
23DPDS 12SEC2	Internship	04			A course requiring students to participate in a professional activity or work experience, or	

					cooperative education activity with an entity external to the education institution, normally under the supervision of an expert of the given external entity. Internship is a course to develop a professional ability through an appropriate learning. The duration of Internship is of 120 hours during summer vacation.	
23DPDS 12VAC2	Animation and Web Designing	02	15 Attendance-5 Sessional Examination-10	35	50	3Hrs

Name of the Department: - Defence Studies
Name of the Course: - Basic of Computer and Cyber Security
Semester: - 01

Course Code	23CPDS11DSC1	Course Credit	(L: 4 T: 0 P: 0)
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:

1. To provide the clarity about the conceptual framework of computer, components of computer, operating system, and network.
2. To create better understanding about the various aspects of application software and search engines.
3. To create understating about computer and cyber security.

Learning Outcomes:

1. Clearly understand the conceptual framework of computer, components of computer, operating system, and network.
2. Better understanding about the various aspects of application software and search engines.
3. After Undergoing the course a student will be able to know use of computer network in electronic payment system, domain name system, digital signature, and electronic signature.

Unit-I

History of Computers, Areas of Application.
Computers and its Components, Application Software and System Software.

Unit-II

Introduction to Operating System.

Basics of Networks and Internet, Types of Networks.

Unit-III

Search Engines, E-mails and WWW; Internet-working Devices, Internet Service provider, IP Address, Working of Email system, Domain Name System, Blogs.
Use of Computer Network in Electronic Payment System and Taxation.
Digital Signatures and Electronic Signatures.

Unit-IV

Computer & Cyber Security:

- Types of Cyber Attacks
- Network Security
- Overview of Security Threats
- Hacking Techniques and Ethical Hacking
- Password Cracking
- Insecure Network Connections
- Malicious Code
- Concept of Fire wall Security

Email Security:

- Web Authentication
- Database Security
- Operating System Security
- Advance Computers, Network & Mobile Security Techniques.

Suggested Readings:

1. Priti Sinha and Pradeep Sinha, Computer Fundamentals, BPB Publications, Noida, 2004.
2. Kumar Janglu, Basic Networking Concepts, Independently Published, 2019.
3. Prashant Mali, Cyber Law & Cyber Crimes, Snow White publications, Mumbai, 2015.
4. Farooq Ahmad, Cyber Law in India, Allahabad Law Agency, 2017.
5. N. Renuka and others, Cyber Crime and Cyber Laws in India, Red Shine Publication, Lunawada, 2022.
6. Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2016.
7. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House, New Delhi, 2022.
8. P.M. Bukshi and R.K. Suri, Guide to Cyber and E – Commerce Laws, Bharat Law House, New Delhi, 2002.
9. Rodney D. Ryder, Guide to Cyber Laws, Wadhwa and Company, Nagpur, 2001.
10. The Information Technology Act, 2000, Government of India, Educreation Publishing, New Delhi, 2020.
11. Linda Volonino and others, Computer Forensics: Principals and Practices, Pearson, Noida, 2006.
12. Eoghan Casey, Digital Evidence and Computer Crime, Third Edition, Academic Press, Waltham, 2011.

13. Andrew Murray, The Regulation of Cyberspace Andrew Murray, Rutledge, London, 2006.

14. Shinder Debra Littlejohn, Scene of the Cybercrime: Computer Forensics, Syngress, 2002.

15. Jones Keith J. and others, Real Digital Forensics: Computer Security and Incident Response, Addison-Wesley Educational Publishers Inc., Boston, 2005.

Name of the Department: - Defence Studies
Name of the Course: - National Security of India
Semester: - 01

Course Code	**23CPDS11DSC2**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:
1.To provide the clarity about the conceptual framework of National Security of India.
2. To create comprehensive knowledge about changing nature of security and security discourses
3. To create understating about India’s major security threats.

Learning Outcomes:
1. Clearly understand the conceptual framework of India’s national security.
2. Better understanding about the various aspects related to India’s security
3. After Undergoing the course a student will be able to know the global and regional security environment and its implications on Indian security.

Unit-I

National Security: Meaning, Definition and Concept.

Major Threats to India’s National Security:

- Internal Threats
- External Threats

Unit-II

Conceptual Framework of Indian Security.
Global and Regional Strategic Environment and Its impact on Indian Security Thinking.
India’s Strategic Culture and National Security Policy.

Unit-III

Major Components of India’s National Security:

- Economic Security
- Cultural Security
- Institutional Security
- Human Security

Unit-IV

Strategic Environment in Indian Ocean Region
Threats to India’s National Security in Indian Ocean.

Military Alliances and Pacts, Peace Treaties, Defence Cooperation, Strategic Partnership and Security Dialogue.

Suggested Readings:

1. Barry Buzan, People, States, and Fear: The National Security Problem in International Relations, University of North Carolina Press, 1983.
2. Abdul-Monem Mohamed, National Security in The Third World, Routledge, New York, 2018.
3. Shahrbanou Tadjbakhsh and Anuradha Chenoy, Human Security: Concepts and Implications, Taylor & Francis, UK, 2007.
4. Sitakanta Mishra and Anshuman Behera, Varying Dimensions of India’s National Security: Emerging Perspectives, Springer Nature, Singapore, 2022.
5. S.K. Shah, India's External and Internal Security Policy in 21st Century, Alpha Editions, Marousi, 2018.
6. Shrikant Paranjpe, India's strategic culture: the Making of National Security Policy, Routledge New Delhi, 2020.
7. Annual Reports of Ministry of Home Affairs, Ministry of Defence and Ministry of External Affairs of India.
8. G.D. Bakshi, The Rise of Indian Military Power: Evolution of an Indian Strategic Culture, KW Publishers Pvt Ltd., New Delhi, 2015.
9. Navnit Gandhi, National Security: Emerging Dimensions and Threats, Pentagon Press, 2010.
10. Archana Upadhyay, India's Fragile Borderlands: The Dynamics of Terrorism in North East India. Vol. 39, IB Tauris, 2009.
11. Suresh R, Maritime Security of India: The Coastal Security Challenges and Policy Options, Vij Books India Pvt. Ltd., New Delhi, 2014.
12. Mohit Nayal, Security of India's Ports, Coast and Maritime Trade Challenges in the 21st Century, Vij Books India Pvt. Ltd., New Delhi, 2021.
13. Alexander Lanoszka, Military Alliances in the Twenty-First Century, Polity Press, Cambridge, 2022.

Name of the Department: - Defence Studies
Name of the Course: - Cyber Security in Indian Context
Semester: - 01

Course Code	**23CPDS11DSC3**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:

1.To provide the clarity about the nuances of the cyber world by understanding cyber threats, to state, institution and individuals.
2. To create comprehensive knowledge about cyber security and cyber warfare.
3. To create understating about cyber policy and preparedness mechanisms.

Learning Outcomes:

1. Clearly understand the cyber world by understanding cyber threats, to state, institution and individuals.
2. Better understanding about the various aspect cyber security and cyber warfare.
3. After Undergoing the course a student will be able to know various cyber security threats to India and India’s cyber security policy.

Unit-I

Cyber Security: Meaning, Definition and Concept.

Major Threats to India’s Cyber Security.

Unit-II

Cyber Warfare: Meaning, Definition and Concept.

Ecosystem of Cyber Warfare:

- Cyber Terrorism
- Cyber Fraud
- Cyber Spying
- Cyber stalking or Bullying
- Cyber Assault

Unit-III

Cyber Warfare Threat to Indian Defence Sector and Challenges.

Cyber Related Crimes in India.

Unit-IV

Indian Government’s Measures taken to Maintain Cyber Security.

India’s International Collaboration on Cyber Security.

Suggested Readings:

1. Kapender Singh (Eds.), Cyber Terrorism and National Security, Mohit Publications, New Delhi, 2015.
2. Scott W. Beidleman, Defining and Deterring Cyber War, Master’s thesis, U.S. Army War College, 2009.
3. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley India, New Delhi, 2017.
4. Lin V Choi ed., Cyber Security and Homeland Security, Nova Publishers, New York, 2005.
5. Sanjay Kumar and others, Cyber Security, Book Bazooka Publication, Kanpur, 2019.
6. Sanjeev Relia, Cyber Warfare: Its Implications on National Security, Vij Books India Private Limited, New Delhi, 2016.
7. Vikas Sharma, Browsing the Cyber Laws of India: A User’s Guide, E-book, 2023.
8. Shantesh Kumar Singh and Shri Prakash Singh, Nontraditional Security Concerns in India: Issues and Challenges, Springer Nature, Singapore 2022.
9. Prashant Mali, Cyber Law & Cyber Crimes, Snow White publications, Mumbai, 2015.
10. Farooq Ahmad, Cyber Law in India, Allahabad Law Agency, 2017.
11. N. Renuka and others, Cyber Crime and Cyber Laws in India, Red Shine Publication, Lunawada, 2022.
12. Sameer Patil, Securing India in the Cyber Era, Taylor & Francis, New Delhi, 2021.
13. Ramnath Reghunadhan, Cyber Technological Paradigms and Threat Landscape in India,

Springer Nature, Singapore, 2022.

14. N. Casarini and others, Moving Forward EU-India Relations: The Significance of the Security Dialogues, Edizioni Nuova Cultura, Ciampino, 2017.

Name of the Department: - Defence Studies
Name of the Course: - Practicum
Semester: - 01

Course Code	**23CPDS11DSC4**	**Course Credit**	**(L: 0 T: 0 P: 4)**
Max. Marks	**100** **Theory-70** Practical Examination- 50 Vova-Voce- 20 **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Learning Objectives:
1. To make students capable to report cyber-crimes at cyber police station and online.
2. To make student efficient in privacy and security setting to prevent cyber threats.
3. To aware students about various aspects of cyber security threats related to their computer and mobile

Learning Outcomes:
1. After Undergoing the course a student will be to create password and cyber security management system.
2. After Undergoing the course a student will be capable to prevent cyber-attacks.
3. After Undergoing the course a student will become capable to tackle cybers crime and cyber-attacks.

Note: - Practicum/Practical examination should be conducted by concerned department/institution as per the direction of university. The assessment shall be jointly undertaken by the internal and external examiners. The External examiners shall be invited from amongst the panel of examiners recommended by the concerned Board of Studies. In case of unavailability of external examiners due to unavoidable circumstances, the Controller of Examinations may allow the conduct of practical examination by the internal examiners so that the conduct of examination and declaration of results is not delayed.

Checklist for Reporting Cyber Crime at Cyber Crime Police Station.
Checklist for Reporting Cyber Crime Online.
Reporting Phishing E-mails.
Demonstration of E-mail Phishing Attack and Preventive Measures.
Privacy and Security Settings for Popular Social Media Platforms.
Configuring Security Settings in Mobile Wallets and UPIs.
Checklist for Secure Net Banking.
Setting, Configuring and Managing Three Password Policy in the Computer (BIOS, Administrator and Standard User).
Setting and Configuring Two Factor Authentication in the Mobile Phone.
Security Patch Management and Updates in Computer and Mobiles.
Managing Application Permissions in Mobile Phone.
Installation and Configuration of Computer Anti-virus.
Installation and Configuration of Computer Host Firewall.
Wi-Fi Security Management in Computer and Mobile.
Registering Complaints on a Social Media Platform.
List out Security Controls for Computer and Implement Technical Security Controls
in the Personal Computer.

List out Security Controls for Mobile Phone and Implement Technical Security Controls in the Personal Mobile Phone.

Name of the Department: - Defence Studies
Name of the Course: - Non-Traditional Security Threats
Semester: - 01

Course Code	**23CPDS11SEC1**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:

1. To create deep understanding about non-traditional security threats.
2. To create understand about the magnitude of non-traditional security threats.

Learning Outcomes:

1. After Undergoing the course a student will be able to realizes that there are nontraditional threats to nation's security other than military which are of equally grave consequences.
2. Clearly understand the various non-traditional security threats drug trafficking, money laundering, narco terrorism and human trafficking are equally dangerous as war.

Unit-I

Human Security: Definition, meaning and concept

Environment Security: Definition, meaning and concept

Unit-II

Energy Security: Definition, meaning and concept

Illegal Migration: Definition, meaning and concept

Unit-III

Narco-Terrorism: Definition, meaning and concept

Small Arms Proliferation: Definition, meaning and concept

Unit-IV

Organized Crimes: Definition, meaning and concept

Money Laundering: Definition, meaning and concept

Suggested Readings:

1. Anthony J. Masys (Eds.), Exploring the Security Landscape: Non-Traditional Security Challenges, Springer International Publishing, Germany, 2018.
2. Hanns-Seidel-Stiftung and V. R. Raghavan (Eds.), India and ASEAN: Non-traditional

Security Threats, East West Books Chenni, 2007.

3. Mely Caballero Anthony (Eds.), Non-traditional Security in Asia: Issues, Challenges, and Framework for Action, Institute of Southeast Asian Studies, Singapore, 2013.
4. Mely Caballero Anthony (Eds.), An Introduction to Non-Traditional Security Studies: A Transnational Approach, SAGE Publications, United Kingdom, 2015.
5. Shebonti Ray Dadwal, Non-Traditional Security Challenges in Asia: Approaches and Responses, Taylor & Francis, India, 2017.
6. Shekhar Adhikari (Eds.), South Asia: Traditional and Non-traditional Security Threats, Pentagon Press, India, 2015.
7. Tamara Nair and Alistair D. B. Cook (Eds.), Non-traditional Security in The Asia-pacific: A Decade of Perspectives, World Scientific Publishing Company, Singapore, 2021.
8. Michel R. Gueldry and others (Eds.), Understanding New Security Threats, Taylor & Francis, United Kingdom, 2019.
9. Shahar Hameiri and Lee Jones, Governing Borderless Threats: Non-Traditional Security and the Politics of State Transformation, Cambridge University Press, United Kingdom, 2015.
10. Ralf Emmers, Non-Traditional Security in Asia: Dilemmas in Securitization, Taylor & Francis, United Kingdom, 2017.
11. Shri Prakash Singh and Shantesh Kumar Singh, Nontraditional Security Concerns in India: Issues and Challenges, Springer Nature, Singapore, 2022.

Name of the Department: - Defence Studies
Name of the Course: - Introduction to Defence and Security Studies
Semester: - 01

Course Code	**23CPDS11VAC1**	**Course Credit**	**(L: 2 T: 0 P: 0)**
Max. Marks	**50** **Theory-35** **Internal Assessment-15**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set five questions in total. Answer to question no. 1 shall be compulsory comprising of five short answer questions from all two units and remaining four questions shall be set by taking two questions from each unit. The students have to attempt three questions in total, first being compulsory and selecting one from each unit. All questions **(Except Q. No.1)** shall carry equal marks.

Learning Objectives:

1.To acquaint to introduce students about the basic concept of Defence and Security Studies.
2. To create deep understanding about war and Defence mechanism of India.

Learning Outcomes:

1. Clearly understand the basic concept of Defence and Security Studies.

2. The course also creates the good understanding among students about war and Defence mechanism.
3. After Undergoing the course a student will be able to understanding the Defence and Security Studies relations with others disciplines.

Unit-I

Defence and Security Studies: Concept, Scope, and Importance.
Defence and Security Studies: Its relations with other disciplines –Geography, Economics, Political Science, History, Psychology and Sociology.

Unit-II

Meaning and Concept of War.
Principles of War.
ABC Warfare (Atomic, Biological and Chemical).
Defence Mechanism of India.

Suggested Readings:

1. JFC Fuller, The Conduct of War: 1789-1961: A Study of The Impact of The French, Industrial, and Revaluations on War and Its Conduct, Da Capo Press, 1992.
2. Carl Von Clausewitz, Principal of War Army Publication New Delhi,1972.
3. Lallan Singh, Art of War in India, 1947 up to date, Parkash Books Depot, Bareilly, 2003.
4. Col. Ravi Nanda, Evolution of National Strategy, South Asia Books; 1st edition,1987.

Name of the Department: - Defence Studies
Name of the Course: - Security Mechanism in India
Semester: - 02

Course Code	**23DPDS12DSC5**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:
1. To create comprehensive knowledge about organizational structure of Indian armed forces.
2. To create better understanding about higher Defence organizations of India.
3. To create deep understanding about major operations of Indian armed forces.

Learning Outcomes:
1. Clearly understand the Defence mechanism of India and evaluate its strengths and weaknesses.
2. Better understanding about higher Defence organizations of India.
3. After Undergoing the course a student will be able to know the Rank Structure of the Three Services and Recruitment methods for Defence Services.

Unit-I

Indian Armed Forces:

- Rank Structure of Indian Armed Forces (Army, Navy and Air Force).
- Responsibilities of Indian Armed Forces.
- Major Operations of Indian Armed Forces.

Unit-II

Organization of Indian Armed Forces:

- Organization of Indian Armed Forces (Army, Navy and Air Force).
- Commands of Indian Armed Forces.
- Static and Field formation of Indian Armed Forces.

Unit-III

Weapon Systems of Indian Armed Forces:

- Weapon Systems of Indian Army.
- Weapon Systems of Indian Navy.
- Weapon Systems of Indian Air Force.

Unit-IV

Higher Defence Organizations of India:

- Power of the President of India in Relation to Security and Defence.
- Role and Function of Ministry of Defence.
- Composition and Function of Defence Committees:
    - Cabinet Committee on Security (CCS).
    - National Security Council (NSC).
    - Chief of Defence Staff (CDS).

Suggested Readings:

1. Ashok Krishna, India's Armed Forces: Fifty Years of War and Peace, Lancer Publishers, New Delhi, 1998.
2. Indian Armed Forces, United Service Institution of India, Vij Books India, New Delhi, 2010.
3. Bharat Verma, G. M. Hiranandani and B. K. Pandey, Indian Armed Forces, Lancer Publishers & Distributors, New Delhi, 2008.
4. R. Venkataraman, India's Higher Defence: Organization and Management, KW Publishers, New Delhi, 2011.
5. Bharath Gopalaswamy, Rajesh M. Basrur (ed.), India’s Military Modernization: Strategic Technologies and Weapons Systems, Oxford University Press, India, 2015.
6. Hemant Kumar Pandey and Manish Raj Singh, India’s Major Military & Rescue Operations, Horizon Books, New Delhi, 2017.

Name of the Department: - Defence Studies
Name of the Course: - Cyber Law
Semester: - 02

Course Code	**23DPDS12DSC6**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Learning Objectives:

1. To create comprehensive knowledge about information technology act, 2000 and cyber security policy of India.

2. To create the basic clarity and understanding of cyber and data protection laws of India and World.
3. To create good understanding about limitations of cyber laws.

Learning Outcomes:

1. The student is able to understand the technicalities of law in cyber-World.
2. Extensive knowledge regarding jurisdictional issues in IT Act.
3. Various important national and international cyber laws.
4. Understands the scope of cyber and data protection laws.
5. After Undergoing the course a student will be able to understand the limitations of cyber laws.

Unit-I

Evolution of the IT Act: Genesis and Necessity.
Objectives, Applicability, Non-applicability of the Information Technology Act, 2000.
Cyber Security Policy of India.

Unit-II

Regulatory Framework of Information and Technology Act 2000:

- Digital Signature
- E Signature
- Electronic Records
- Electronic Evidence
- Electronic Governance
- Controller, Certifying Authority and Cyber Appellate Tribunal. (Rules announced under the Act)

Unit-III

Offences and Penalties under Information and Technology Act 2000:

- Offences under the Information and Technology Act 2000
- Penalty and adjudication
- Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed).

Limitations of Cyber Law

Unit-IV

Data Protection Laws in India:

- Scope and Applicability
- Personal Data under SPDI Rules
- Key Compliance Obligations
- Personal Data Protection Bill, 2019

Cyber Law: International Perspective:

- EDI: Concept and legal Issues
- UNCITRAL Model Law
- Electronic Signature Laws of Major Countries
- Cyber Laws of Major Countries

Suggested Readings:

1. Janine Kremling and Amanda M. Sharp Parker, Cyberspace, Cybersecurity, and Cybercrime, Sage Publications, New York, 2017.
2. Vivek Sood, Cyber Law Simplified, McGraw Hill Education, Noida, 2017.

3. Brian Craig, Cyber Law: The Law of the Internet and Information Technology, Pearson, London, 2012.
4. Talat Fatima, Cyber Law in India, Wolters Kluwer India Pvt. Ltd., Gurugram, 2017.
5. Pavan Duggal, Cyber Law: The Indian Perspective, Saakshar Law Publications, New Delhi, 2002.
6. Pavan Duggal, Artificial Intelligence, Cybercrimes and Cyberlaw, Independently Published, 2018.
7. Nilakshi Jain and Ramesh Menon, Cyber Security and Cyber Laws, Wiley, New York, 2020.
8. J.P. Sharma and Sunaina Kanojia, Cyber Laws, Ane Books Pvt. Ltd., New Delhi, 2016.
9. J.P. Sharma and Sunaina Kanojia, E-Business & Cyber Laws, Bharat Law House Pvt. Ltd., New Delhi, 2018.
10. Kamath Nandan, Law Relating to Computers, Internet and E-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with Rules, Regulations and Notifications (2nd ed.). Universal Law Publishing Co., New Delhi, 2007.
11. Aparna Viswanathan, Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes, Lexis Nexis, New York, 2012.
12. Peter Stephenson and Keith Gilbert, Investigating Computer Related Crime A Handbook for Corporate Investigators, CRC Press Taylor & Francis, Boca Raton, 2013.
13. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, Information Resources Management Association, 2018.
14. Sushma Devi, National Security in the Digital Age: A Study of Cyber Security Challenges in India, Academica Press, United Kingdom, 2018.
15. Nitin Desai, India's Cyber Security Challenge, IDSA Task Force Report, New Delhi, 2012.

Name of the Department: - Defence Studies
Name of the Course: - Cyber Crimes
Semester: - 02

Course Code	**23DPDS12DSC7**	**Course Credit**	**(L: 4 T: 0 P: 0)**
Max. Marks	**100** **Theory-70** **Internal Assessment-30**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set nine questions in total. Answer to question no. 1 shall be compulsory comprising of seven short answer questions from all four units and remaining eight questions shall be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit. All questions shall carry equal marks.

Learning Objectives:

1. Acquainting students with the cyber-crimes.
2. Providing students the necessary understanding of freedom of speech in cyber space.
3. To create understanding among the students about effects of cyber-crimes on national security and business.
4. To create understanding about India’s measures to prevent cyber-crimes.
5. To understand social media and its role in cyber-World

Learning Outcomes:

1. The student is able to understand the cyber-crimes and its effects on various field.
2. Extensive knowledge regarding India's measures to prevent cyber-crimes
3. After Undergoing the course a student will be able to understand the tools of cyber-crimes and impact of cyber-crimes on social media.

Unit-I

Cyber Crimes: Meaning, Definition and Concept.

Types of Cyber Crimes:

- Cyber Crimes Against Individual
- Cyber Crimes Against Property
- Cyber Crimes Against Government

Unit-II

Impact of Cyber Crimes on Social Media.

Tools of Cyber Crimes Related to Social Media.

Reasons of Cyber Crimes at Social Media.

Unit-III

Effects of Cyber Crimes on National Security.

Effects of Cyber Crime on Business.

Unit-IV

Public-Private Partnership in Cyber Security: Opportunities and Challenges.

India's Measures to Prevent Cyber Crimes.

Suggested Readings:

1. Sushma Arora and Raman Arora, Cyber Crimes & Laws, Taxman Publications Pvt. Limited, Delhi, 2021.
2. Grainne Kirwan and Andrew Power, The Psychology of Cyber Crime: Concepts and Principles, Information Science Reference, Pennsylvania, 2012.
3. Janine Kremling and Amanda M. Sharp Parker, Cyberspace, Cyber security, and Cybercrime, Sage Publications, New York, 2017.
4. David J. Loundy, Computer Crime, Information Warfare, and Economic Espionage, Carolina Academic Press 2003.
5. Akash Kamal Mishra, An Overview on Cybercrime & Security, Volume - I, Notion Press, Chennai, 2020.
6. M. Dasgupta, Cyber Crime in India: A Comparative Study, Eastern Law House, New Delhi, 2009.
7. Nir Kshetri, The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives, Springer Nature, Berlin, 2010.
8. Peter Stephenson and Keith Gilbert, Investigating Computer Related Crime A Handbook for Corporate Investigators, CRC Press Taylor & Francis, Boca Raton, 2013.
9. Aparna Viswanathan, Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes, Lexis Nexis, New York, 2012.
10. Jack Balkin and others (Eds.), Cybercrime: Digital Cops in a Networked World, NYU Press, 2007.
11. Ralph D. Clifford, Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime Second Edition, 2006.

Name of the Department: - Defence Studies
Name of the Course: - Project Report
Semester: - 02

Course Code	**23DPDS12DSC8**	**Course Credit**	**04**

Max. Marks	**100** **Project Report-70** **Viva-Voce-30**	**Time of end term Examination**	**--**

Learning Objectives:

1. Acquainting student with research skills in the concerned field.
2. Providing student an opportunity to learn the writing skills.
3. To make the student understand the major developments in the chosen area.
4. To make the student competent to document his findings and suggestions in a research project and present the same with efficiency.

Learning Outcomes:

1. The student is more efficient in dealing with problems in the chosen field.
2. The student builds up a professional approach in presentation of the subject of research.
3. The student evolves in the relevant area with complete understanding of the topic.
4. After Undergoing the course a student will be able to understand the project's goals, activities, timelines, resources used, challenges faced, and the results achieved.

Students are advised to select their topic in consultation with their guide. The Project report submitted by the candidates will be sent to the external examiner for evaluation. Students would have to make a presentation in the Department before the submission of Project Report.

Format of Submission:

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

Evaluation:

- The evaluation shall be done by the Internal Examiner (Guide/Supervisor) and one External Examiner.
- External Examiner shall conduct the Viva-voce.

Name of the Department: - Defence Studies
Name of the Course: - Internship
Semester: - 02

Course Code	**23DPDS12SEC2**	**Course Credit**	**04**
Max. Marks	**100** **Internship Report-70** **Viva-Voce-30**	**Time of end term Examination**	**--**

Learning Objectives:

1. Acquainting student with practical aspects in the concerned field.
2. Providing student an opportunity to work with expert in the concerned field.
3. To acquaint students about professional development.
2. To create deep understanding about how to work in specified field with expert.

Learning Outcomes:

1. The student knows about the concerned subject in practical sense.
2. The student is more efficient in dealing with problems in the area.
3. The student builds up a professional approach.
4. The student evolves in the relevant area with complete understanding of subjects

5. After Undergoing the course a student will be able to understand his/her duty and responsibility.

Internship is a course to develop a professional ability through an appropriate learning. The duration of Internship is of 120 hours during summer vacation. Each student is advised to pursue mandatory Internship with IT organization or Cyber Police Station and obtain a certificate from the concerned on his/her performance during the internship period. The student has to prepare a detailed internship report which will carry 70 marks. The Viva-Voce Examination/Presentation of the report for 30 marks shall be conducted by a committee of three examiners.

Name of the Department: - Defence Studies
Name of the Course: - Animation and Web Designing
Semester: - 02

Course Code	**23CPDS11VAC2**	**Course Credit**	**(L: 2 T: 0 P: 0)**
Max. Marks	**50** **Theory-35** **Internal Assessment-15**	**Time of end term Examination**	**3 Hours**

Note: Examiner will set five questions in total. Answer to question no. 1 shall be compulsory comprising of five short answer questions from all two units and remaining four questions shall be set by taking two questions from each unit. The students have to attempt three questions in total, first being compulsory and selecting one from each unit. All questions **(Except Q. No.1)** shall carry equal marks.

Learning Objectives:

1. To acquaint to introduce students about the basic concept of web designing and web technologies.
2. To create deep understanding about computer graphics and animation techniques.

Learning Outcomes:

1. Clearly understand the basic concept of web designing and web technologies.
2. The course optimizes the creative talent of the individual and helps build attractive web pages.
3. After Undergoing the course a student will be able to learn to register domain name, website hosting and database design

Unit-I

Basics of Web Designing.
Multimedia and its Applications.
Web Technologies.
Introduction to Web Design & Applications

Unit-II

Computer Graphics and Animation Techniques.
HTML, HTTP, WWW & Principles of Web design, Static Vs Dynamic Pages.
Client- side Vs Server-Side programming.
Domain name registration, website hosting and database design.

Suggested Readings:

1. Abhishek R. Mehta, Web Design- A Practical Approach: Beginner’s Guide to HTML, CSS, JavaScript, jQuery and Animation, Notion Press, 2020.
2. Kogent Learning Solutions Inc., Web Technologies: HTML, JAVASCRIPT, PHP, JAVA, JSP, ASP.NET, XML and Ajax, Dreamtech Press, 2009.
3. Satish Jain and M. Geetha Iyer, Web Designing and Publishing, BPB Publisher, 2020.
4. Ben Frain, Responsive Web Design with HTML5 and CSS: Build future-proof responsive websites using the latest HTML5 and CSS techniques, 4th Edition, Packt Publishing, 2022.

- The Internal Assessment for theory shall consist of the following components with marks indicated against each:

<table>
<tr><th>Credit Hours</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td><b>Total Marks</b></td><td><b>100</b></td><td><b>75</b></td><td><b>50</b></td><td><b>25</b></td></tr>
<tr><td><b>Criteria</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Attendance
<table>
<tr><th>% of attendance</th><th>Marks</th></tr>
<tr><td>Below 65</td><td>0</td></tr>
<tr><td>65 to < 70</td><td>2</td></tr>
<tr><td>70 to < 75</td><td>3</td></tr>
<tr><td>75 to < 80</td><td>4</td></tr>
<tr><td>80 and above</td><td>5</td></tr>
</table></td><td>5</td><td>5</td><td>5</td><td>5</td></tr>
<tr><td>Assignments/Seminars Presentations</td><td>5</td><td>5</td><td>-</td><td>-</td></tr>
<tr><td>Sessional Examination</td><td>20</td><td>15</td><td>10</td><td>-</td></tr>
<tr><td><b>Total</b></td><td><b>30</b></td><td><b>25</b></td><td><b>15</b></td><td><b>5</b></td></tr>
</table>

- The Internal Assessment for practical shall consist of the following components with marks indicated against each:

<table>
<tr><th>Credit Hours</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td><b>Total Marks</b></td><td><b>100</b></td><td><b>75</b></td><td><b>50</b></td><td><b>25</b></td></tr>
<tr><td><b>Criteria</b></td><td><b>100</b></td><td><b>75</b></td><td><b>50</b></td><td><b>25</b></td></tr>
<tr><td>Attendance
<table>
<tr><th>% of attendance</th><th>Marks</th></tr>
<tr><td>Below 65</td><td>0</td></tr>
<tr><td>65 to < 70</td><td>2</td></tr>
<tr><td>70 to < 75</td><td>3</td></tr>
<tr><td>75 to < 80</td><td>4</td></tr>
<tr><td>80 and above</td><td>5</td></tr>
</table></td><td>5</td><td>5</td><td>5</td><td>5</td></tr>
<tr><td>Practical Assignments/ Practical File</td><td>25</td><td>20</td><td>10</td><td>-</td></tr>
<tr><td><b>Total</b></td><td><b>30</b></td><td><b>25</b></td><td><b>15</b></td><td><b>5</b></td></tr>
</table>

- The minimum percentage of marks to pass the examination in each semester shall be:
  (i) 40% in each theory paper
  (ii) 40% in each practical examination.
  (iii) 40% in the aggregate of each theory paper and internal assessment (and practical where practical is a component of theory paper).
- **Mechanism for Computation of Work-load:**

The following mechanism shall be adopted for computation of work-load:

- 1 Credit: 1 Theory period of one hour duration/week/semester;
- 1 Credit: 1 Tutorial period of one hour duration/week/semester;
- 1 Credit: 1 Practical period of two hours duration/week/semester;

- 1 Credit: Internship of 30 hours per semester.

Eligibility Criteria

- Bachelor degree from recognized University with at least 45% marks (42.75% for SC/ST candidates of Haryana only).