LL.M. Two year course

New Specialization in Cyber Law
Group F : Cyber Law

Semester – I
Paper - I
Title : INVESTIGATION AND CYBER CRIME

Total Marks : 100
Theory: 80
Internal Assessment : 20

COURSE OBJECTIVES: The learner is expected to -

1. **Understanding Cyber Crime:** Gain a comprehensive understanding of the nature, types, and impact of cyber crimes in digital environments.
2. **Developing Investigative Skills:** Acquire expertise in cyber crime investigation, including digital forensics, electronic evidence collection, and advanced investigative techniques.
3. **Navigating Legal Frameworks:** Analyse national and international legal frameworks governing cyber crime investigations, including jurisdictional challenges, ethical considerations, and privacy concerns.
4. **Enhancing Prevention Strategies:** Learn proactive strategies to prevent cyber crimes through robust cybersecurity measures, risk assessment, and incident response mechanisms.
5. **Exploring Emerging Trends:** Study new-age cyber crime threats, such as AI-driven attacks, IoT vulnerabilities, deepfake frauds, and cryptocurrency-related crimes, and their implications for law enforcement and regulatory bodies.

COURSE OUTCOMES:

1. **Comprehensive Knowledge of Cyber Crime:** Demonstrate a thorough understanding of cyber crimes, their methodologies, motivations, and societal impact.
2. **Proficiency in Investigation Techniques:** Develop hands-on skills in digital forensic analysis, evidence handling, and cyber crime investigative methodologies.
3. **Legal and Ethical Expertise:** Understand the legal and ethical aspects of cyber crime investigations, including cross-border jurisdiction issues, digital privacy laws, and compliance with international conventions.
4. **Effective Cyber Security and Response Planning:** Gain the ability to design and implement cyber security measures and incident response frameworks to mitigate cyber threats.
5. **Adaptability to Emerging Threats:** Stay updated with evolving cyber crime tactics and demonstrate the ability to analyse and address novel cyber threats using technological and legal interventions.

COURSE CONTENTS:

Unit I: Introduction to Cyber Crime and Investigation

- Definition and classification of cyber crimes.
- Prevalence and impact of cyber crimes on individuals, organizations, and national security.
- Investigative methodologies and digital forensic tools used in cyber crime cases.
- Role of digital evidence in cyber crime investigation.
- **Dark Patterns** – The role of deceptive digital interfaces in cyber crimes.
- **AI Ethics & Accountability** – Use of AI in crime prediction and bias in forensic algorithms.
- **Cyber Terrorism & Digital Warfare** – Threats posed by cyber terrorism and hacking groups.
- Case studies of landmark cyber crime investigations.

Unit II: Legal Frameworks Governing Cyber Crime Investigations

- Overview of national and international cyber laws and treaties.
- Jurisdictional challenges and cross-border cyber crime investigations.
- Ethical and legal considerations in digital evidence collection and forensic examination.
- Comparative analysis of cyber crime laws in different jurisdictions.
- Privacy rights and data protection laws vs. investigative needs in cyber crime cases.

Unit III: Investigation of Specific Cyber Crimes

- Detailed examination of common cyber crimes, including hacking, phishing, ransomware, financial frauds, identity theft, and cyber terrorism.
- Techniques and tools used for investigating specific types of cyber crimes.
- Case studies illustrating real-world investigative techniques.
- Challenges in evidence preservation and chain of custody in digital environments.
- Use of AI, machine learning, and blockchain technology in cyber crime investigations.
- **Deepfake Regulations** – Challenges of deepfake videos in criminal investigations.
- **Encryption Debate** – Balancing law enforcement needs and encryption in cyber investigations.

Unit IV: Cyber Crime Prevention and Incident Response

- Cyber security frameworks and risk assessment strategies.
- Incident response planning and execution: roles and responsibilities.
- Legal and regulatory requirements for reporting cyber incidents.

- Collaboration between law enforcement, the private sector, and international agencies in combating cyber threats.
- Case studies of effective cyber crime prevention and mitigation strategies.
- **Platform Accountability** – The role of digital platforms in aiding forensic analysis.
- **The Pegasus Spyware Investigation** – Case study of state surveillance and forensic evidence.

Unit V: Emerging Trends and Future Directions in Cyber Crime Investigation

- IoT vulnerabilities, and deepfake-related frauds.
- Cryptocurrency crimes: legal challenges and investigation methods.
- Future directions in cyber crime investigation and law enforcement strategies.
- Ethical dilemmas in cyber crime investigations and evolving legal standards.

SUGGESTED READINGS:

1. **Robert Moore**, *Cybercrime: Investigating High-Technology Computer Crime*
2. **Dr. Erdal Ozkaya**, *Cybersecurity: The Beginner's Guide*
3. **Karnika Seth**, *Cyber Laws and IT Protection*
4. **R. K. Srivastava (Ed.)**, *Cyber Crime: Concepts, Methodologies, Tools, and Applications*
5. **Dr. Pavan Duggal**, *Cyber Law: Law of Information Technology and Internet*
6. **Dr. K. Jaishankar**, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*
7. **Shubhankar Dam**, *Information Technology Law: Perspectives on Cyber Law in India*
8. **Jonathan Clough**, *Principles of Cybercrime*
9. **Michael Cross**, *Social Engineering: How to Hack the Human Brain*
10. **Brett Shavers**, *Computer Forensics and Digital Investigation with EnCase Forensic 7*
11. **Thomas J. Holt & Adam M. Bossler**, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*
12. **David S. Wall**, *Cybercrime: The Transformation of Crime in the Information Age*

Semester – I
Paper - II
Title : INTERNATIONAL PERSPECTIVES ON CYBER LAW

Total Marks : 100
Theory 80
Internal Assessment : 20

COURSE OBJECTIVES:

1. **Understanding the Foundations of Cyber Law:** Develop a strong understanding of fundamental cyber law principles, including jurisdiction, sovereignty, and international legal frameworks.
2. **Comparative Legal Frameworks:** Examine the evolution and structure of cyber law across different jurisdictions, identifying key differences and similarities.
3. **Analysis of Cyber Crimes:** Analyse various cyber crimes, their transnational nature, and international cooperation mechanisms for investigation, prosecution, and prevention.
4. **Privacy and Data Protection:** Study international privacy laws and regulations, including their implications for data security, surveillance, and consumer rights.
5. **Emerging Trends and Future Challenges:** Explore emerging technological threats such as AI-driven cyber threats, blockchain-based crimes, cyber warfare, and their legal implications on global cyber governance.
6. **Global Internet Governance:** Examine the roles of global organizations such as ICANN, ITU, and UN bodies in regulating cyberspace.
7. **Instruction to Course In charge** : Encourage students to compare international and national frameworks through research-based presentations.

COURSE OUTCOMES:

1. **Comprehensive Knowledge of International Cyber Law:** Demonstrate an in-depth understanding of core principles and legal frameworks governing cyberspace, including jurisdictional issues and enforcement mechanisms.
2. **Comparative Legal Analysis:** Analyse and compare cyber law frameworks across multiple countries and assess their effectiveness in regulating cyberspace.

3. **Expertise in Cyber Crime Investigations:** Identify, evaluate, and apply international strategies for the prevention, investigation, and prosecution of cyber crimes.
4. **Mastery of Privacy and Data Protection Laws:** Gain proficiency in international privacy laws, including GDPR, CCPA, and their impact on digital rights and compliance mechanisms.
5. **Understanding Emerging Issues:** Develop expertise in addressing legal challenges posed by new technologies such as AI, cryptocurrency, the dark web, and digital warfare.
6. **Policy and Governance:** Critically analyse global efforts toward harmonizing cyber laws and internet governance through multilateral treaties and international cooperation.

COURSE CONTENTS:

Unit I: Foundations of International Cyber Law

- Definition, scope, and significance of cyber law in an international context.
- Evolution of cyber law and international regulatory frameworks.
- Comparative analysis of cyber laws in different countries (e.g., US, EU, India, China, Japan).
- Challenges in enforcing international cyber law: jurisdictional conflicts, sovereignty issues, and extraterritorial reach.
- **Budapest Convention on Cybercrime (2001)** – The first global treaty against cybercrime.
- **General Data Protection Regulation (GDPR)** – EU's landmark data privacy framework.
- **California Consumer Privacy Act (CCPA)** – U.S. privacy law and its global influence.

Unit II: Jurisdiction and International Cyber Treaties

- **International internet governance** jurisdiction in cyberspace.
- Key international conventions and treaties (e.g., Budapest Convention on Cybercrime, Malabo Convention, ASEAN Cybersecurity Cooperation).
- Case studies of landmark international cyber law cases.
- Regional and global efforts toward harmonizing cyber laws (e.g., GDPR in the EU, APEC Privacy Framework).
- **The UN Guiding Principles on Business & Human Rights** – Cyber law's human rights perspective.
- **Crypto Regulations** – How different countries regulate cryptocurrencies

Unit III: Transnational Cyber Crimes and Enforcement Mechanisms

- Classification of cyber crimes: hacking, cyber terrorism, identity theft, online financial frauds, and misinformation campaigns.
- Role of INTERPOL, EUROPOL, UNODC, and private sector cooperation in combating cyber crimes.
- Challenges in cross-border cyber crime investigations, mutual legal assistance treaties (MLATs), and extradition laws.
- Digital evidence collection and forensic methodologies in transnational cyber investigations.

Unit IV: Privacy and Data Protection Regulations (from global perspectives)

- Evolution of global privacy laws: GDPR, CCPA, PDP Bill (India), and other regional frameworks.
- Balancing individual privacy rights with national security concerns.
- Regulations on data transfers across borders and enforcement of privacy rights.
- International best practices for data breach management and corporate compliance.

Unit V: Emerging Technologies, Cyber Warfare, and Global Internet Governance

- Regulatory approaches to emerging technologies: blockchain, artificial intelligence, and quantum computing.
- Cyber warfare and its implications under international humanitarian law.
- Role of ICANN, ITU, and the UN in internet governance and digital policy frameworks.
- Future challenges and policy responses to cyber threats at the global level.
- **Internet Governance Forum (IGF) Reports** – UN reports on internet policies.
- **The Right to Digital Access** – International movement for internet as a fundamental right.

SUGGESTED READINGS:

1. **Karnika Seth**, *Cyber Laws and IT Protection*
2. **R. K. Srivastava (Ed.)**, *Cyber Crime: Concepts, Methodologies, Tools, and Applications*
3. **Dr. Pavan Duggal**, *Cyber Law: Law of Information Technology and Internet*
4. **Dr. K. Jaishankar**, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*
5. **Shubhankar Dam**, *Information Technology Law: Perspectives on Cyber Law in India*

6. **Ruth Boardman, Eduardo Ustaran, and Arty Rajendra**, *International Cybersecurity and Privacy Law in Practice*
7. **Philippe Gillieron and Guillermo Jimenez (Eds.)**, *Cyber Law: International and Transnational Perspectives*
8. **Michael Rustad and Michael D. Scott**, *Global Internet Law in a Nutshell*
9. **Tadashi Iino**, *Cyber Law in Japan*
10. **Jonathan Clough**, *Principles of Cybercrime*
11. **Brett Shavers**, *Cybercrime Investigations: A Comprehensive Resource for Everyone*
12. **Orin S. Kerr**, *Computer Crime Law*
13. **David S. Wall**, *Cybercrime: The Transformation of Crime in the Information Age*
14. **Thomas J. Holt & Adam M. Bossler**, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*
15. **Michael G. Solomon**, *Security Strategies in Cybersecurity and Information Systems*

Semester – II
Paper - III
Title : CYBER LAW AND DIGITAL FORENSICS

Total Marks : 100
Theory 80
Internal Assessment : 20

COURSE OBJECTIVES:

1. **Understanding Cyber Law and Digital Forensics:** Develop a strong understanding of cyber law principles, international regulations, and their applications in the digital ecosystem.
2. **Classification of Cyber Crimes:** Identify, classify, and analyze various cyber crimes such as hacking, ransomware, identity theft, financial fraud, cyber terrorism, and deepfake crimes.
3. **Legal and Ethical Considerations:** Examine jurisdictional complexities, privacy concerns, and ethical issues involved in cyber crime investigations and the use of digital evidence.
4. **Practical Digital Forensics Skills:** Acquire proficiency in digital evidence collection, forensic analysis, data preservation, and court-admissible documentation.
5. **Emerging Trends in Cyber Forensics:** Explore the role of AI in cyber-attacks, blockchain applications in cyber security, IoT vulnerabilities, and other technological advancements impacting cyber law and forensic investigations.
6. **Judicial and Investigative Challenges:** Understand the role of cyber forensic experts in litigation, legal proceedings, and policy recommendations for strengthening cyber crime investigations.
7. **Notes for Course In charge : Hands-on Training in Digital Forensics & Cyber Investigation -** Introduce **mandatory forensic lab assignments** in Cyber Forensics

---

COURSE OUTCOMES:

1. **Comprehensive Knowledge of Cyber Law and Digital Evidence:** Demonstrate a deep understanding of legal frameworks and regulations governing digital investigations and forensic methodologies.
2. **Proficiency in Cyber Forensics:** Develop hands-on skills in forensic techniques, including evidence acquisition, chain of custody, data recovery, and expert testimony.
3. **Analytical and Investigative Abilities:** Critically analyse different cyber crimes, their methodologies, and investigative approaches in national and international contexts.

4. **Application of Legal and Ethical Principles:** Apply best practices in digital forensics while ensuring compliance with cyber laws, privacy laws, and human rights frameworks.
5. **Technological Awareness and Adaptability:** Stay updated with emerging trends in cyber security, forensic tools, and challenges posed by emerging technologies such as cloud computing and the dark web.
6. **Role of Cyber Forensics in Legal Proceedings:** Develop an understanding of how forensic evidence is presented in court, the admissibility of digital evidence, and the role of forensic experts in judicial processes.

COURSE CONTENTS:

Unit I: Introduction to Cyber Law and Digital Forensics

- Definition, scope, and importance of cyber forensics.
- Evolution of cyber forensics and its role in the legal system.
- Legal principles governing digital evidence and forensic investigation.
- Challenges in cyber forensic investigations: data integrity, encryption, anonymity, and jurisdictional issues.
- Role of digital forensics in cyber crime detection and law enforcement.

Unit II: Digital Evidence Collection and Admissibility

- Types of digital evidence: volatile vs. non-volatile evidence.
- Legal aspects of digital evidence: admissibility, authenticity, and reliability in courts.
- Chain of custody and best practices in handling digital evidence.
- Tools and techniques for data acquisition, extraction, and forensic imaging.
- International best practices in digital evidence handling (e.g., ISO 27037).
- **Data Breach Notification Laws** – Legal obligations to report cybersecurity breaches.
- **The Cambridge Analytica Scandal** – How digital forensics uncovered mass data misuse.

Unit III: Cyber Forensic Investigation Process

- Cyber forensic investigation lifecycle: identification, collection, preservation, analysis, and presentation of evidence.
- Case studies of cyber forensic investigations in India and globally.
- Challenges in digital forensics: encryption, cloud computing, and anti-forensic techniques.
- Use of artificial intelligence and machine learning in cyber forensic investigations.

- Investigating financial cyber crimes: online fraud, cryptocurrency scams, and digital money laundering.

Unit IV: Cyber Forensics Tools and Techniques

- Overview of forensic tools: EnCase, Autopsy, FTK, Sleuth Kit, Wireshark, and Volatility.
- Techniques for forensic data recovery, steganography detection, and mobile forensics.
- Cloud forensics and IoT forensics: challenges and solutions.
- Role and qualifications of forensic experts in cyber crime investigations.
- International frameworks for cyber forensic investigations and cooperation (e.g., INTERPOL, EUROPOL, CERTs).
- **Algorithmic Bias** – How forensic AI tools can produce biased results.
- **Mass Surveillance Programs** – The balance between national security and privacy.

Unit V: Cyber Forensics and Legal Proceedings

- Role of cyber forensic experts in court proceedings and litigation.
- Expert testimony and admissibility of forensic evidence in legal proceedings.
- Cyber forensics in corporate investigations and regulatory compliance.
- Case law analysis: landmark judgments on digital forensics and cyber evidence.
- Future challenges and policy recommendations for digital forensic investigations.

SUGGESTED READINGS:

1. **Thomas J. Holt & Adam M. Bossler**, *Cybercrime and Digital Forensics: An Introduction*
2. **Dr. Pavan Duggal**, *Cyber Law: Law of Information Technology and Internet*
3. **R. K. Srivastava (Ed.)**, *Cyber Crime: Concepts, Methodologies, Tools, and Applications*
4. **Dr. K. Jaishankar**, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*
5. **Karnika Seth**, *Cyber Security and Cyber Laws*
6. **Marjie T. Britz**, *Computer Forensics and Cyber Crime: An Introduction*
7. **Brett Shavers**, *Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis*
8. **Michael G. Solomon**, *Security Strategies in Cybersecurity and Information Systems*
9. **Eoghan Casey**, *Handbook of Digital Forensics and Investigation*

10. **Orin S. Kerr**, *Computer Crime Law*
11. **Journal of Digital Investigation** – Research-focused journal covering the latest advancements in cyber forensics.
12. **Journal of Cyber Security** – Covers cyber security threats, forensic investigation techniques, and legal perspectives.

Semester – II
Paper - IV
Title : CYBER LAW AND THE INFORMATION TECHNOLOGY ACT, 2000
Total Marks : 100
Theory 80
Internal Assessment : 20

COURSE OBJECTIVES:

1. **Understanding the Cyber Law Framework in India:** Develop a comprehensive understanding of the legal framework governing cyber law in India, focusing on the Information Technology Act, 2000, and its amendments.
2. **Analyzing Key Provisions of the IT Act:** Examine significant provisions related to electronic signatures, digital governance, cyber crimes, and data protection under the IT Act.
3. **Legal Compliance and Liabilities:** Understand the compliance requirements for businesses and individuals under the IT Act, including obligations and liabilities in the digital domain.
4. **Cyber Crimes and Enforcement Mechanisms:** Identify different types of cyber crimes recognized under the IT Act and analyze enforcement mechanisms, legal remedies, and judicial interpretations.
5. **Application of Cyber Law in Practical Scenarios:** Develop the ability to apply theoretical knowledge through case studies and real-world legal issues related to cyber law and digital governance.
6. **Comparative Analysis of Global Cyber Laws:** Compare Indian cyber law with international regulatory frameworks to understand global best practices and legal challenges in cyberspace.

COURSE OUTCOMES:

1. **Comprehensive Knowledge of the IT Act, 2000:** Demonstrate an in-depth understanding of the legal definitions, scope, and objectives of the IT Act and its amendments.
2. **Legal Interpretation and Application:** Apply legal principles to analyze issues related to electronic transactions, cyber contracts, digital signatures, and data security.
3. **Regulatory Compliance Expertise:** Develop skills to identify legal and regulatory compliance requirements under the IT Act, ensuring adherence to laws on electronic transactions, cybersecurity, and data protection.
4. **Cyber Crime Investigation and Remedies:** Evaluate various cyber crimes under the IT Act, such as unauthorized access, identity theft, hacking, phishing, and online fraud, along with corresponding legal remedies.

5. **Case Law Analysis and Practical Implementation:** Assess judicial pronouncements and real-world case studies to apply cyber law principles effectively in litigation and policy-making.
6. **Understanding International Cyber Law Perspectives:** Gain insights into global cyber law frameworks, treaties, and international best practices to ensure harmonization with India's digital economy policies.

COURSE CONTENTS:

Unit I: Cyber Law – Indian and International Perspectives

- Definition, scope, and significance of cyber law.
- Evolution and importance of cyber law in India and its alignment with global legal frameworks.
- Comparative study of Indian cyber law with international treaties, conventions, and best practices.
- Role of international organizations in regulating cyber laws (e.g., ITU, UNCITRAL, Budapest Convention).

Unit II: The Information Technology Act, 2000 – Key Provisions

- Overview and objectives of the IT Act, 2000, including recent amendments.
- Legal recognition of electronic records and digital signatures.
- Electronic governance and its implications for legal documentation and business transactions.
- Role of Certifying Authorities and the framework for digital authentication.
- **Safe Harbour Doctrine** – Liability protection for intermediaries under IT Act.
- **The IT Rules, 2021 (India)** – New social media accountability framework.
- Regulation of AI & Machine Learning in Cyber Law

Unit III: Use of Electronic Records and Validity of Contracts

- Legal validity of electronic contracts and digital documentation.
- Concept of e-contracts, clickwrap agreements, and smart contracts under the IT Act.
- Role and powers of the Controller of Certifying Authorities.
- Regulations governing the use of electronic records in financial transactions and governance.

Unit IV: Cyber Crimes, Penalties, and Legal Liabilities

- Classification of cyber crimes: hacking, identity theft, cyber terrorism, phishing, and cyber defamation.

- Legal consequences of cyber crimes: penalties and enforcement under the IT Act.
- Case studies of landmark cyber crime judgments in India.
- Role of law enforcement agencies, cyber cells, and forensic experts in cyber crime investigations.
- Interplay between the IT Act and IPC provisions concerning cyber crimes.
- **Fake News & Misinformation Laws** – IT Act provisions against fake news.
- **Surveillance Capitalism** – How companies profit from mass data collection.

Unit V: Data Protection, Privacy, and Emerging Challenges

- Data protection laws in India and their alignment with international frameworks (e.g., GDPR, PDP Bill).
- Legal framework for cybersecurity, breach notifications, and compliance measures.
- Issues of confidentiality, privacy, and surveillance in the digital age.
- Emerging legal challenges in cyber law: artificial intelligence, blockchain regulation, deepfake crimes, and cryptocurrency fraud.
- The future of cyber law: policy recommendations for strengthening digital governance.
- Cover legal issues in **AI-generated content, automated decision-making, and bias in AI systems**.

SUGGESTED READINGS:

1. **Dr. Karnika Seth**, *Cyber Crimes and Law in India*
2. **Andrew Murray**, *Information Technology Law: Text, Cases, and Materials*
3. **Dr. Pavan Duggal**, *Cyber Law: Law of Information Technology and Internet*
4. **R. K. Srivastava (Ed.)**, *Cyber Crime: Concepts, Methodologies, Tools, and Applications*
5. **Karnika Seth**, *Cyber Security and Cyber Laws*
6. **Orin S. Kerr**, *Computer Crime Law*
7. **Eoghan Casey**, *Handbook of Digital Forensics and Investigation*
8. **Michael Rustad**, *Global Internet Law in a Nutshell*
9. **Journal of Cyber Law & Policy** – Covers research articles and legal analysis on cyber law issues.
10. **Asian Journal of Cyber Law** – Focuses on legal developments and case studies in cyber law within the Asia-Pacific region.

Semester – III
Paper - V
Title : DIGITAL HUMAN RIGHTS AND CYBER FREEDOMS

Total Marks : 100
Theory 80
Internal Assessment : 20

COURSE OBJECTIVES:

1. **Understanding Digital Human Rights:** Develop a comprehensive understanding of fundamental human rights in the digital age, including freedom of expression, privacy, and access to information.
2. **Legal Frameworks Governing Cyber Freedoms:** Examine international conventions, national legislations, and judicial pronouncements related to digital rights and cyber governance.
3. **Challenges in the Digital Landscape:** Analyse threats to digital freedoms, including censorship, internet shutdowns, mass surveillance, and the role of social media in human rights violations.
4. **Regulation of Online Speech and Misinformation:** Evaluate the balance between free speech and regulations against hate speech, misinformation, and cyber radicalization.
5. **Data Sovereignty and Digital Inclusion:** Explore the legal and policy challenges of data localization, digital divide, and accessibility rights in cyberspace.
6. **The Role of Technology in Human Rights Advocacy:** Assess the use of blockchain, AI, and digital forensics in safeguarding cyber freedoms and upholding justice.

COURSE OUTCOMES:

1. **Comprehensive Knowledge of Digital Rights:** Understand the evolution and current state of human rights in cyberspace, including national and international protections.
2. **Analytical Skills for Digital Law Application:** Critically analyse cyber laws related to online privacy, freedom of speech, and internet governance.
3. **Legal Response to Digital Challenges:** Evaluate the role of courts, regulatory authorities, and policy frameworks in combating cyber threats to human rights.
4. **Regulatory and Ethical Considerations:** Assess the ethical and legal implications of government surveillance, content moderation, and cybersecurity policies.

5. **Role of International and Regional Bodies:** Understand the role of organizations like the UN, ITU, and regional cyber governance frameworks in protecting digital freedoms.
6. **Policy Recommendations for Digital Freedom:** Formulate policy approaches to enhance digital rights, cybersecurity governance, and fair access to the internet.

COURSE CONTENTS:

Unit I: Foundations of Digital Human Rights and Cyber Freedoms

- Definition, scope, and evolution of digital human rights.
- Key principles of cyber freedoms: privacy, access to information, and digital autonomy.
- International treaties and conventions on digital rights (UDHR, ICCPR, European Convention on Human Rights).
- Role of state and non-state actors in protecting digital freedoms.
- Right to Internet as a Fundamental Right
- **The Right to Be Forgotten** – Legal rights to remove personal data from the internet.

Unit II: Legal Frameworks for Digital Rights and Governance

- National and international legislations on digital rights (IT Act, GDPR, Freedom of Speech laws).
- Cybersecurity laws and their impact on human rights.
- Comparative analysis of digital rights frameworks in leading jurisdictions (EU, USA, India, China).
- Role of courts in interpreting and upholding cyber freedoms.

Unit III: Threats to Digital Freedoms and Legal Safeguards

- Internet censorship, content takedown laws, and their impact on freedom of expression.
- Internet shutdowns and the legality of access restrictions.
- Mass surveillance programs and their implications for privacy rights.
- Role of encryption laws and policies in securing online communication.
- **Internet Shutdowns & Censorship** – The legal and ethical debates over government-imposed shutdowns.

Unit IV: Regulation of Online Speech, Hate Speech, and Misinformation

- Defining hate speech, misinformation, and disinformation in the cyber domain.

- Legal frameworks governing online speech and content moderation.
- Case studies on digital speech regulations and their impact on civil liberties.
- Balancing freedom of expression with the need for cybersecurity and counter-radicalization.

Unit V: Data Sovereignty, Digital Divide, and Emerging Challenges

- Concept of data sovereignty and its impact on digital freedom.
- Digital divide and accessibility rights in the context of internet governance.
- Emerging trends: Artificial Intelligence, blockchain, and their impact on human rights.
- Policy recommendations for securing digital freedoms and inclusivity.

SUGGESTED READINGS:

1. **David Kaye**, *Speech Police: The Global Struggle to Govern the Internet*
2. **Ethan Zuckerman**, *Digital Cosmopolitans: Why We Think the Internet Connects Us, Why It Doesn't, and How to Rewire It*
3. **Jack Goldsmith & Tim Wu**, *Who Controls the Internet? Illusions of a Borderless World*
4. **Lawrence Lessig**, *Code and Other Laws of Cyberspace*
5. **Bruce Schneier**, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*
6. **Jeff Kosseff**, *The Twenty-Six Words That Created the Internet*
7. **Cass Sunstein**, *Republic.com 2.0*
8. **Yochai Benkler**, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*
9. **UNESCO Reports on Internet Freedom and Human Rights in Cyberspace**
10. **Journal of Digital Human Rights & Cyber Law** – Covers research on digital governance, privacy policies, and cyber freedoms.
11. **International Review of Law, Computers & Technology** – Focuses on comparative cyber law issues.

Semester – III
Paper - VI
Title : EMERGING ISSUES IN CYBERSPACE

Total Marks : 100
Theory 80
Internal Assessment : 20

COURSE OBJECTIVES:

1. **Understanding the Evolution of Cyberspace:** Gain insights into the rapid developments in cyberspace and the legal, ethical, and regulatory challenges they present.
2. **Addressing Cybersecurity Risks:** Identify and analyse emerging cyber threats such as AI-driven cyber attacks, deepfake technology, and ransomware.
3. **Enhancing Data Privacy Protections:** Understand global data protection frameworks, including GDPR, CCPA, and India's proposed data privacy regulations.
4. **Examining Intellectual Property Rights (IPR) in the Digital Domain:** Explore the challenges of protecting copyrights, trademarks, and patents in the era of digital content and piracy.
5. **Regulatory and Legal Developments:** Study evolving legal frameworks, international treaties, and global efforts to regulate cyberspace and mitigate cybercrime.
6. **Technological Innovations and their Legal Implications:** Assess the role of emerging technologies like blockchain, the Internet of Things (IoT), and quantum computing in cyberspace.
7. **Bridging the Digital Divide:** Address inequalities in digital access, cybersecurity literacy, and the ethical responsibilities of governments and corporations.

COURSE OUTCOMES:

1. **Enhanced Legal and Policy Frameworks:** Critically evaluate new laws, amendments, and policies related to data privacy, cybersecurity, and digital rights.
2. **International Cybersecurity Cooperation:** Understand global efforts in managing cross-border cybercrime and establishing international security standards.
3. **Adapting Legal Frameworks to Technological Advances:** Analyse how laws and regulations evolve with advancements in artificial intelligence, blockchain, and cybersecurity best practices.

4. **Challenges in Cybercrime Enforcement:** Identify the difficulties faced by law enforcement in tackling cybercriminal activities in an increasingly anonymous digital world.
5. **Application of Ethical and Legal Principles:** Develop a research-based understanding of ethical dilemmas related to emerging technologies, privacy concerns, and surveillance policies.
6. **Addressing the Future of Cyberspace:** Gain proficiency in analysing future trends, policy recommendations, and governance models to ensure a secure digital environment.

COURSE CONTENTS:

Unit I: Introduction to Cyberspace

- Definition, scope, and significance of cyberspace.
- Evolution and history of cyberspace.
- Key components: Internet, intranet, extranet, and emerging digital ecosystems.
- Internet governance: regulatory bodies, frameworks, and challenges in governance..

Unit II: Cybersecurity Threats and Risk Management

- Advanced cyber threats: AI-driven attacks, deepfake technology, ransomware, and quantum computing.
- Case studies of major cyber attacks and their global implications.
- Threat detection and mitigation techniques.
- Cybersecurity policies and regulations: national and international perspectives.
- Role of government agencies and private sector collaboration in combating cyber threats.
- **Regulating Social Media** – Legal frameworks for content moderation.
- **AI Ethics & Accountability** – The role of AI in cyber security governance

Unit III: Data Privacy and Global Regulations

- Fundamentals of data privacy and security.
- Comparative analysis of major global regulations: GDPR, CCPA, India's Personal Data Protection Bill.
- Compliance strategies for organizations and businesses.
- Digital rights, surveillance policies, and privacy challenges.
- Ethical dilemmas in data governance and information security.
- Digital Currency & Regulation of Cryptocurrency

- Crypto Bill (India), FATF Travel Rule, EU's MiCA Regulation, SEC regulations in the U.S.

Unit IV: Intellectual Property Rights in the Digital Age

- Introduction to digital intellectual property laws.
- Copyright, trademarks, and patents in cyberspace.
- Cyber piracy and digital content protection.
- Legal frameworks for combating digital piracy and counterfeiting.
- International cooperation and treaties related to intellectual property enforcement.
- **Regulating OTT Platforms** – Frameworks for digital streaming regulations.
- **Cyber Piracy and Enforcement** – Laws for protecting digital content

Unit V: Future Trends, Ethical Considerations, and Global Governance

- Emerging technologies and their legal implications: blockchain, AI, IoT, and quantum computing.
- Cyber warfare, state-sponsored cyber attacks, and the implications for international law.
- Global cybersecurity governance and treaties: UN, ITU, and ICANN's role in internet governance.
- Bridging the digital divide: ensuring cybersecurity awareness and equal access to technology.
- The future of cyberspace: predictions, innovations, and policy recommendations for a secure digital future.
- **Digital Sovereignty** – Nations exerting control over their digital ecosystems.
- **Technological Adaptation in Cyber Law** – Evolving legal responses to digital innovations.
- **future trends of internet governance, such as decentralized web, Web3**

SUGGESTED READINGS:

1. **Robin Hanson**, *The Age of Em: Work, Love, and Life when Robots Rule the Earth*
2. **Michael Patrick Lynch**, *The Internet of Us: Knowing More and Understanding Less in the Age of Big Data*
3. **P.W. Singer & Allan Friedman**, *Cybersecurity and Cyber War: What Everyone Needs to Know*
4. **Jon Erickson**, *Hacking: The Art of Exploitation*
5. **Manuel Castells**, *The Network Society: From Knowledge to Policy*
6. **Sanjay Kaushik**, *Internet and Society: Social Theory in the Information Age*

7. **Bruce Schneier**, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*
8. **Richard Clarke & Robert Knake**, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*
9. **Eoghan Casey**, *Handbook of Digital Forensics and Investigation*
10. **David S. Wall**, *Cybercrime: The Transformation of Crime in the Information Age*
11. **Journal of Cybersecurity & Digital Law** – Covers legal developments and case studies in cybersecurity regulations.
12. **Global Internet Law & Policy Journal** – Focuses on international cyber law challenges and emerging policies.

Suggestions for Course Outcomes and Instructions

General Course Instructions:

1. **Practical Approach**
    - Every course should include at least **one mock cyber crime investigation case study**.
    - Encourage students to **write policy papers** on contemporary issues.
2. **Interdisciplinary Approach**
    - Include discussions on **economics of cybercrime, cyber psychology, and geopolitical aspects of cyber law**.
3. **Hands-on Training in Digital Forensics & Cyber Investigation**
    - Introduce **mandatory forensic lab assignments** in Paper III (Cyber Forensics).
    - Encourage collaboration with **cybersecurity firms, law enforcement agencies, or CERT-In** for practical training.