Chapter 6
Prevailing National Laws and Security Concepts

3 hrs

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Content:

1. **Prevailing Laws**
   - ❑ **Electronic Transaction Act (Chapter 9)**
   - ❑ **The Privacy Act, 2075 (Chapter 6, 9, 10)**
   - ❑ **Cybersecurity Policy 2021 *(Draft)***
2. **Other Concepts**
   - ❑ **Cyber Strategy of Government of Nepal**
   - ❑ **The CERT Team**
   - ❑ **Laws related to computers:- CFAA, DMCA, etc.**
   - ❑ **Open-Source Intelligence (OSINT)**
   - ❑ **The OWASP Top ten**

6.1 Prevailing Laws

6.1.1 Electronic Transaction Act (Chapter 9)

6.1.2 The Privacy Act, 2075 (Chapter 6, 9, 10)

6.1.3 Cybersecurity Policy 2021 *(Draft)* *https://api.giwms.gov.np/storage/22/posts/1691665949_27.pdf*

Electronic Transaction

- The **act of buying or selling online or transferring** money electronically from one place to another is called **E-transaction.**
- ATM transactions, bill payments using e-sewa, mobile top-ups, transaction using internet banking and credit cards, etc. are all examples of electronic transactions.

6.1.1. Electronic Transaction Act

- The Electronic Transactions Act 2063 was introduced in Nepal **to ensure the reliability and security of electronic transactions** including the control of unauthorized use of electronic records or alteration in such records through illegal manner.
- The Electronic Transactions Act, 2063 (2008) was introduced in 24th Bhadra 2063 B.S.
- The Electronic Transaction Act came into effect on **02 September 2008.**
- This act was formulated to legalize and to ensure reliability and safety of all sort of electronic transactions and digital signatures and penalize cybercrime.
- It has **12 sections (chapters)** and 80 clauses.

- Electronic Transaction Act consists of below chapters:
  - Chapter 1: Preliminary
  - Chapter 2: Provisions Relating to Electronic Record and Digital Signature
  - Chapter 3: Provision Relating to Dispatch, Receipt and Acknowledgement of Electronic Records
  - Chapter 4: Provisions Relating to Controller and Certifying Authority
  - Chapter 5: Provisions Relating to Digital Signature and Certificates
  - Chapter-6 Functions, Duties and Rights of Subscriber
  - Chapter-7 Electronic Record and Government use of Digital Signature
  - Chapter 8: Provisions Relating to Network Service
  - **Chapter 9: Offence Relating To Computer**
  - Chapter 10: Provisions Relating to Information Technology Tribunal
  - Chapter 11: Provisions Relating to Information Technology Appellate Tribunal
  - Chapter 12: Miscellaneous

- Source: http://www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf
- https://www.lawimperial.com/highlights-of-electronic-transactions-act-2006/#:~:text=The%20Electronic%20Transactions%20Act%202063,such%20records%20through%20illegal%20manner.

परिच्छेद १ : प्रारम्भिक (उपधारा १-२)

परिच्छेद २ : विधुतीय अभिलेख तथा डिजिटल हस्ताक्षर सम्बन्धी व्यवस्था (उपधारा ३-९)

परिच्छेद ३ : विधुतीय अभिलेखको सम्प्रेषण, प्राप्ति र स्वीकार सम्बन्धी व्यवस्था (उपधारा १०-१२)

परिच्छेद ४ : नियन्त्रक तथा प्रमाणीकरण गर्ने निकाय सम्बन्धी व्यवस्था (उपधारा १३-२९)

*परिच्छेद ५ : डिजिटल हस्ताक्षर तथा प्रमाणपत्र सम्बन्धी व्यवस्था (उपधारा ३०-३४)

*परिच्छेद ६ : ग्राहकको काम, कर्तव्य र अधिकार (उपधारा ३५-३८)

*परिच्छेद ७ : विधुतीय अभिलेख र डिजिटल हस्ताक्षरको सरकारी प्रयोग (उपधारा ३९-४१)

परिच्छेद ८ : नेटवर्क सेवा सम्बन्धी व्यवस्था (उपधारा ४२-४३)

*परिच्छेद ९ : कम्प्युटर सम्बन्धी कसुर (उपधारा ४४-५९)

परिच्छेद १० : सूचना प्रविधि न्यायाधिकरण सम्बन्धी व्यवस्था (उपधारा ६०-६५)

परिच्छेद ११ : सूचना प्रविधि पुनरावेदन न्यायाधिकरण सम्बन्धी व्यवस्था (उपधारा ६६-७१)

परिच्छेद १२ : विविध (उपधारा ७२-८०)

Key Provisions:

1. **Legal Recognition of Electronic Records and Digital Signatures**: The act provides legal recognition to electronic records and digital signatures, making them equivalent to paper-based documents and handwritten signatures.
2. **Offenses and Penalties**: The act outlines various cyber offenses, including unauthorized access to computer systems, data theft, cyber fraud, and dissemination of obscene material. It also specifies penalties for these offenses, which can include fines and imprisonment.
3. **Certifying Authorities**: The act provides for the establishment of Certifying Authorities (CAs) responsible for issuing digital signature certificates to ensure the security and authenticity of electronic transactions.
4. **Data Protection and Privacy**: Provisions are included to protect the privacy and integrity of electronic communications and transactions.
5. **E-Governance**: The act promotes the use of electronic means for government transactions and communications to enhance efficiency and transparency.

- **Objectives**
  1. To facilitate electronic commerce by providing legal recognition to electronic documents and signatures.
  2. To ensure the security, integrity, and authenticity of electronic transactions.
  3. To prevent cybercrimes and provide legal recourse for victims of such crimes.
  4. To promote the use of electronic means in government and other sectors to improve service delivery.

Chapter 9: "Offenses Relating to Computer and Cybercrime”

1. **Unauthorized Access**: Gaining access to a computer system without permission. Penalty: Up to 3 years imprisonment or a fine up to NPR 200,000, or both.
2. **Damage to Computer Systems**: Causing harm to computer systems or networks through malicious programs or commands. Penalty: Up to 5 years imprisonment or a fine up to NPR 500,000, or both.
3. **Data Theft**: Illegally obtaining, copying, or extracting data. Penalty: Up to 3 years imprisonment or a fine up to NPR 200,000, or both.
4. **Cyber Fraud**: Conducting fraud using computers or networks. Penalty: Up to 5 years imprisonment or a fine up to NPR 500,000, or both.
5. **Cyber Terrorism**: Acts intended to threaten national security or public order by damaging critical information infrastructure. Penalty: Up to 10 years imprisonment or a fine up to NPR 1,000,000, or both.
6. **Dissemination of Obscene Material**: Publishing or transmitting obscene content. Penalty: Up to 1 year imprisonment or a fine up to NPR 100,000, or both.
7. **Identity Theft**: Using another person’s identity for illegal purposes. Penalty: Up to 3 years imprisonment or a fine up to NPR 200,000, or both.
8. **Interception of Communication**: Unauthorized interception or tampering with communication data. Penalty: Up to 3 years imprisonment or a fine up to NPR 200,000, or both.

6.1.2 The Privacy Act 2075

- The Individual Privacy Act, 2018 (2075) (the "**Act**") came into force on **September 18, 2018** (*Ashwin* 02, 2075) as the first specific legislation of Nepal governing the protection of individual privacy.
- The Privacy Act, 2018 in Nepal **addresses the protection of personal data and privacy rights** of individuals **by regulating the collection, storage, and processing of personal information.**
- It gives directions for keeping personal information and sensitive data safe. The Act **protects everyone's privacy rights and makes sure that sensitive data is kept safe**.
- The law gives us direction towards protecting our privacy of:
  - ✓ body,
  - ✓ family,
  - ✓ home,
  - ✓ belongings,
  - ✓ documents,
  - ✓ data,
  - ✓ messages, and
  - ✓ personal information online.

What does Personal Information mean?

(a) Information about your background, like caste, ethnicity, birth, religion, and marital status.

(b) Details about your education or qualifications.

(c) Your address, phone number, or email address.

(d) Important identification documents like passports, ID cards, or licenses.

(e) Letters you send or receive that mention personal information.

(f) Biometric information like fingerprints, retina scans, or blood groups.

(g) Information about any criminal history or sentences.

(h) Opinions or views expressed by professionals or experts during decision-making.

Key provisions of Privacy Act 2018

1. **Right to Privacy**: Individuals have the right to keep their personal information private and to be informed about the collection and use of their data.
2. **Data Collection**: Entities must obtain consent from individuals before collecting their personal information and must inform them about the purpose of data collection.
3. **Data Use**: Personal data must be used only for the specified purposes for which it was collected.
4. **Data Protection**: Entities are required to implement adequate security measures to protect personal data from unauthorized access, disclosure, or misuse.
5. **Data Retention**: Personal data should be retained only for as long as necessary to fulfill the purposes for which it was collected.
6. **Right to Access and Correction**: Individuals have the right to access their personal data held by an entity and to request correction of any inaccuracies.
7. **Complaints and Redressal**: The law provides mechanisms for individuals to file complaints and seek redressal if their privacy rights are violated.

- This Privacy Act 2075 involves 12 chapters and 36 clauses:
  - Chapter-1 Preliminary
  - Chapter-2 Privacy of Body and Family of Person
  - Chapter-3 Privacy Relating to Residence
  - Chapter-4 Privacy Relating to Property
  - Chapter-5 Privacy Relating to Document
  - **Chapter-6 Privacy Relating to Data**
  - Chapter-7 Privacy Relating to Correspondence
  - Chapter-8 Privacy Relating to Character
  - **Chapter-9 Electronic Means and Privacy**
  - **Chapter-10 Collection and Protection of Personal Information**
  - Chapter-11 Offences and Punishment
  - Chapter-12 Miscellaneous

Chapter 6: Privacy Relating to Data

1. Every person shall have the right to keep the personal data or details related to him or her confidential.
2. While collecting personal or family data of any person, his or her consent shall be obtained.
3. The data collected by a public body or body corporate upon obtaining the consent of the concerned person shall be used only for the purpose for which such data have been collected. Provided that if any data are demanded for the national security or peace and order, it shall not be deemed to bar to provide such data in accordance with the prevailing law.
4. No person shall, without obtaining the consent of another person, provide the personal data related to that person to anyone else or publish, or cause to be published,.
5. Notwithstanding anything contained in sub-section (4), in cases where it is necessary to provide any personal data or details to the court or the agency or official authorized under law in the course of investigation of any criminal offence, such data or details shall be provided.
6. Notwithstanding anything contained in sub-section (4), if there arises a question as to the issues such as age, qualification, character, sexuality, disability of any person, and the authorized official so demands, the concerned person shall provide such details or documents.

Chapter 9: Electronic Means and Privacy

Clause 19: To have privacy of electronic means:

1. Every person shall have the right to maintain privacy of the matter relating to any of his or her personal information, document, correspondence, data or character that remained in electronic means.
2. No one shall obtain the notice, information, correspondence of any person remained in electronic means in unauthorized manner, violate or provide its privacy for anybody in unauthorized manner.
3. Except for the consent given by the concerned person or order issued, under law, by authorized official, no one shall listen to any dialogue or talks held between two or more than two persons through electronic means, or mark or record the sound of such talks by making use of any mechanical device. Provided that in the case of a speech or statement made publicly, the provision of this sub-section shall not be applicable.
4. Notwithstanding anything contained in sub-section (2) or (3), any notice, information or correspondence may be listened to, marked or recorded, or cause to be listened to, marked or recorded with the consent of the concerned person or order of the authorized official.
5. Other provisions relating to the privacy of electronic notice and data shall be as prescribed.

Clause 20: Relating to installing CCTV camera at public place:

1. If it is necessary to install CCTV camera at any public place, such camera may be installed, or caused to be installed, at a place other than the toilet, bathroom or changing room.
2. Provision shall be made to give a notice of such camera installed at the place where the camera has been installed pursuant to sub-section (1) so that all can see and be informed.
3. The provisions relating to the installation of the CCTV camera at any place shall be as prescribed.

Clause 21: Not to make surveillance or espionage:

- In order to make surveillance or espionage of the residence of any person or any office, or for the purpose of obtaining anything confidential pursuant to this Act, no electronic means, photography or method may be used.

Clause 22: Not to use drone:

- No drone of any kind or similar kind of other device shall be used or no act shall be done with the purpose of obtaining any secret information of any public body, archaeologically important place, building of security agency, protected zone or zone of mine or mineral or at the residence of any person, without permission of the authorized official or such a person, except in border area or public place of the country

Chapter 10: Collection and Protection of Personal Information

Clause 23: Not to collect personal information except in accordance with law

No one except the official authorized under law or the person permitted by such official shall collect, store, protect, analyze, process or publish the personal information of any person.

1. **Clause 24: Not to deem to be personal information**

   Except as otherwise provided in the prevailing law, the information regarding the person holding a public post shall not be deemed to be his or her personal information

2. **Clause 25: Protection of collected information**

   The personal information that has been collected by any public body or remained under the responsibility or control of such a body shall be protected by such body.

3. **Clause 26: Not to use personal information without consent**

   the personal information collected by or remained under the responsibility or control of a public body or body corporate shall not be used or given to any one without the consent of the concerned person

4. **Clause 27: Not to process sensitive information**

   A public body shall not process, or cause to be processed, any sensitive personal information remained under its responsibility or control.

5. **Clause 28: Application may be made to correct information**

   If any person thinks that any information related to him or her which is remained under the responsibility, protection or control of any public body is wrong or is not based on the fact, he or she may, at any time, make an application to the concerned public body in the prescribed form to correct such information.

References:

- https://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Privacy-Act-2075-2018.pdf
- https://pioneerlaw.com/individual-privacy-act-2018-2075/
- https://www.nrb.org.np/contents/uploads/2021/07/%E0%A5%A8%E0%A5%AA.%E0%A4%B5%E0%A5%88%E0%A4%AF%E0%A4%95%E0%A5%8D%E0%A4%A4%E0%A4%BF%E0%A4%95-%E0%A4%97%E0%A5%8B%E0%A4%AA%E0%A4%A8%E0%A5%80%E0%A4%AF%E0%A4%A4%E0%A4%BE-%E0%A4%B8%E0%A4%AE%E0%A5%8D%E0%A4%AC%E0%A4%A8%E0%A5%8D%E0%A4%A7%E0%A5%80-%E0%A4%90%E0%A4%A8-%E0%A5%A8%E0%A5%A6%E0%A5%AD%E0%A5%AB.pdf

- The statistics of Nepal Police show that the number of cyberbullies had surged since 2014. Data breach cases of FoodMandu, Vianet, Ministry of Agriculture and Central Library, several cases of ATM hacks and social media cyberbullying have been reported for the last few years due to the loopholes in the cybersecurity system in Nepal.
- Although the cybercrimes issues are handled under the Electronic Transaction Act 2008, this act does not address the changing dynamics and challenges of cyberspace.
- Hence, the Ministry of Communication and Information Technology had drafted a new policy draft named **'National Cyber Security Policy 2021'** with the purpose to govern and address cybersecurity issues.
- The cases of cybercrimes are handled under the Electronic Transaction Act 2008. Currently, an expert group named Computer Emergency Response Team (CERT) under the Department of Information Technology deals with cybersecurity threats like hacking and phishing.
- The team also collaborates with security operations center teams to establish detection rules and coordinate responses.

6.1.3 Cyber security Act 2021

- The Cyber Security Act of Nepal, introduced in 2021, aims to provide a comprehensive legal framework for addressing cyber crimes, enhancing cyber security, and protecting critical information infrastructure.
- https://api.giwms.gov.np/storage/22/posts/1691665949_27.pdf

लक्ष्यः

विश्वव्यापी साइबर सुरक्षा सूचकाङ्क (Global Cyber Security Index-GCI) स्कोर (Score) ४४.९९ बाट आगामी पाँच वर्षभित्र ६०, दश वर्षभित्र ७० र पन्ध्र वर्षभित्र ८० प्रतिशत पुऱ्याउने।

उद्देश्यः

९.१ सुरक्षित साइबर स्पेस निर्माणका लागि कानूनी र संस्थागत व्यवस्था गर्नु,

९.२ साइबर आक्रमणको जोखिम न्यूनीकरण गर्दै संवेदनशील राष्ट्रिय पूर्वाधार संरक्षण गर्नु,

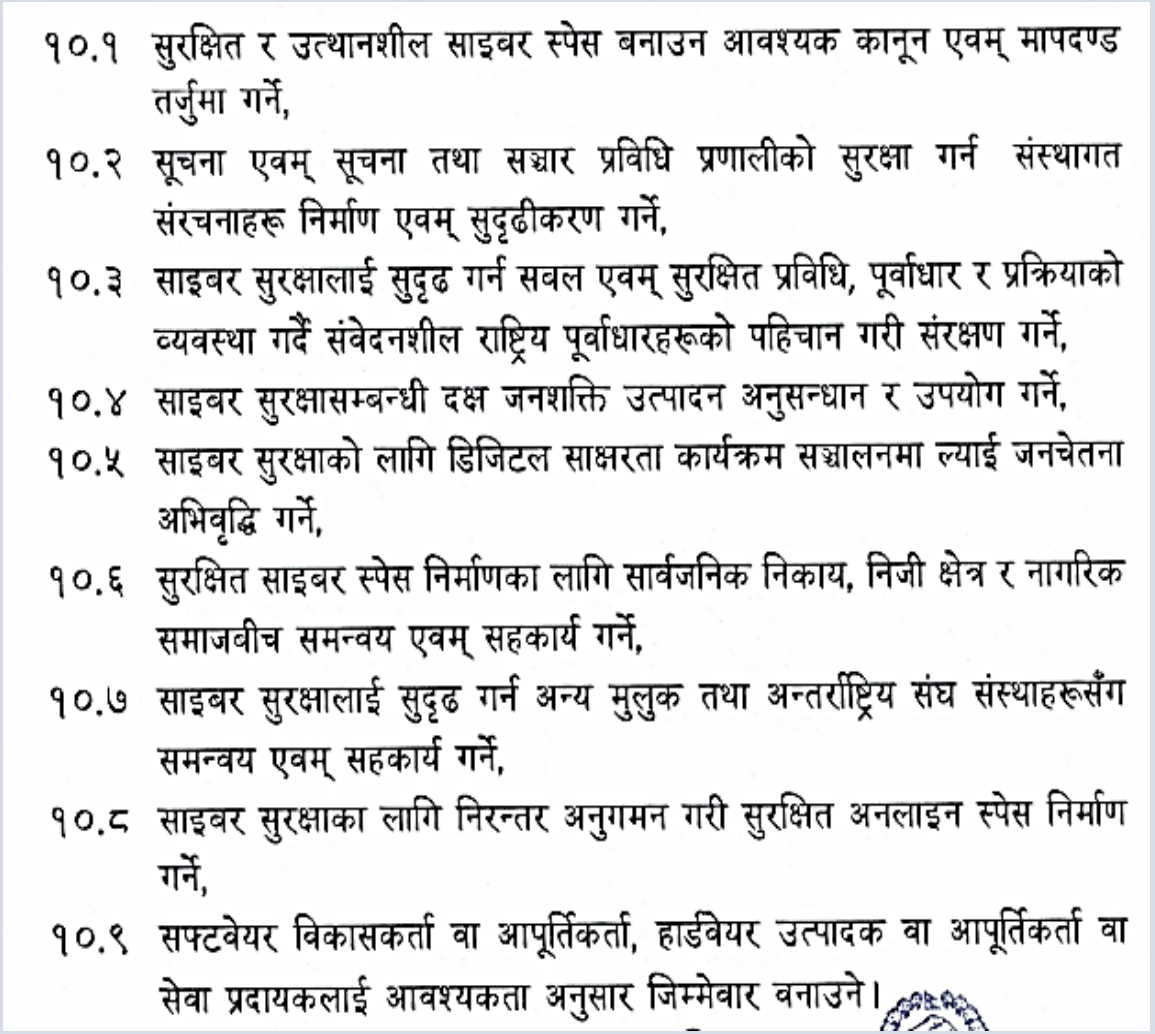
९.३ साइबर स्पेसलाई सशक्त र सुदृढ बनाउन साइबर सुरक्षा क्षेत्रमा अनुसन्धान, जनशक्ति उत्पादन एवम् कार्यरत जनशक्तिको क्षमता अभिवृद्धि गर्नु,

९.४ डिजिटल प्रणालीबाट प्रवाह हुने सेवालाई विश्वसनीय र सुरक्षित बनाउनु,

९.५ साइबर सुरक्षासम्बन्धी जोखिम न्यूनीकरणका लागि द्विपक्षीय, क्षेत्रीय तथा अन्तर्राष्ट्रियस्तरमा समन्वय, अनुभव एवम् सहयोग आदान प्रदान गर्नु।

Strategies:

1. **Strategy 1: To Frame the laws and guidelines for secured and resilient cyberspace**
2. **Strategy 2: Develop institutional and organizational structure based on international guidelines to secure information and Information technology system**
3. **Strategy 3: Build infrastructure and technology to strengthen cybersecurity and prevent them.**
4. **Strategy 4: Develop skilled human resource in the cybersecurity sector**
5. **Strategy 5: To do public awareness campaigns on issues of cybersecurity**
6. **Strategy 6: To collaborate with public entities and the private sector for secure cyberspace**
7. **Strategy 7: Collaborate with international organizations for secured cyberspace**
8. **Strategy 8: To build a safe online space**
9. **Strategy 9: To make software developers/suppliers and hardware manufacturers/suppliers and service providers responsible and accountable.**



१०.१ सुरक्षित र उत्थानशील साइबर स्पेस बनाउन आवश्यक कानून एवम् मापदण्ड तर्जुमा गर्ने,

१०.२ सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा गर्न संस्थागत संरचनाहरू निर्माण एवम् सुदृढीकरण गर्ने,

१०.३ साइबर सुरक्षालाई सुदृढ गर्न सबल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रक्रियाको व्यवस्था गर्दै संवेदनशील राष्ट्रिय पूर्वाधारहरूको पहिचान गरी संरक्षण गर्ने,

१०.४ साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन अनुसन्धान र उपयोग गर्ने,

१०.५ साइबर सुरक्षाको लागि डिजिटल साक्षरता कार्यक्रम सञ्चालनमा ल्याई जनचेतना अभिवृद्धि गर्ने,

१०.६ सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय, निजी क्षेत्र र नागरिक समाजबीच समन्वय एवम् सहकार्य गर्ने,

१०.७ साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ संस्थाहरूसँग समन्वय एवम् सहकार्य गर्ने,

१०.८ साइबर सुरक्षाका लागि निरन्तर अनुगमन गरी सुरक्षित अनलाइन स्पेस निर्माण गर्ने,

१०.९ सफ्टवेयर विकासकर्ता वा आपूर्तिकर्ता, हार्डवेयर उत्पादक वा आपूर्तिकर्ता वा सेवा प्रदायकलाई आवश्यकता अनुसार जिम्मेवार बनाउने।

6.2 Other Concepts

6.2.1 Cyber Strategy of Government of Nepal

6.2.2 The CERT Team

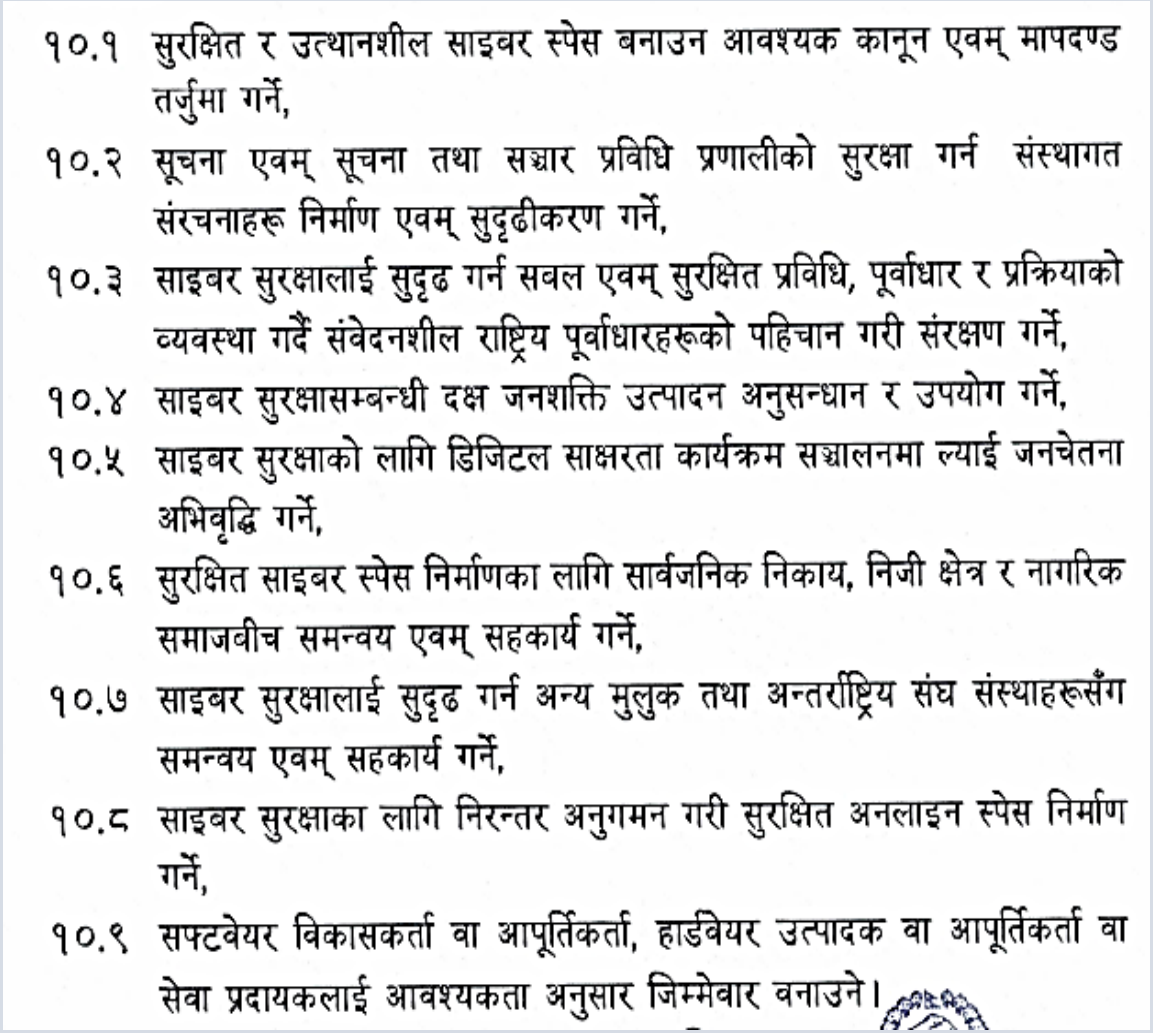
6.2.3 Laws related to computers:- CFAA, DMCA, etc.

6.2.4 Open-Source Intelligence (OSINT)

6.2.5 The OWASP Top ten

6.2.1 Cyber Strategy of Government of Nepal

1. **Strategy 1: To Frame the laws and guidelines for secured and resilient cyberspace**
2. **Strategy 2: Develop institutional and organizational structure based on international guidelines to secure information and Information technology system**
3. **Strategy 3: Build infrastructure and technology to strengthen cybersecurity and prevent them.**
4. **Strategy 4: Develop skilled human resource in the cybersecurity sector**
5. **Strategy 5: To do public awareness campaigns on issues of cybersecurity**
6. **Strategy 6: To collaborate with public entities and the private sector for secure cyberspace**
7. **Strategy 7: Collaborate with international organizations for secured cyberspace**
8. **Strategy 8: To build a safe online space**
9. **Strategy 9: To make software developers/suppliers and hardware manufacturers/suppliers and service providers responsible and accountable.**



१०.१ सुरक्षित र उत्थानशील साइवर स्पेस बनाउन आवश्यक कानून एवम् मापदण्ड तर्जुमा गर्ने,

१०.२ सूचना एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको सुरक्षा गर्न संस्थागत संरचनाहरू निर्माण एवम् सुदृढीकरण गर्ने,

१०.३ साइबर सुरक्षालाई सुदृढ गर्न सवल एवम् सुरक्षित प्रविधि, पूर्वाधार र प्रक्रियाको व्यवस्था गर्दै संवेदनशील राष्ट्रिय पूर्वाधारहरूको पहिचान गरी संरक्षण गर्ने,

१०.४ साइबर सुरक्षासम्बन्धी दक्ष जनशक्ति उत्पादन अनुसन्धान र उपयोग गर्ने,

१०.५ साइबर सुरक्षाको लागि डिजिटल साक्षरता कार्यक्रम सञ्चालनमा ल्याई जनचेतना अभिवृद्धि गर्ने,

१०.६ सुरक्षित साइबर स्पेस निर्माणका लागि सार्वजनिक निकाय, निजी क्षेत्र र नागरिक समाजबीच समन्वय एवम् सहकार्य गर्ने,

१०.७ साइबर सुरक्षालाई सुदृढ गर्न अन्य मुलुक तथा अन्तर्राष्ट्रिय संघ संस्थाहरूसँग समन्वय एवम् सहकार्य गर्ने,

१०.८ साइबर सुरक्षाका लागि निरन्तर अनुगमन गरी सुरक्षित अनलाइन स्पेस निर्माण गर्ने,

१०.९ सफ्टवेयर विकासकर्ता वा आपूर्तिकर्ता, हार्डवेयर उत्पादक वा आपूर्तिकर्ता वा सेवा प्रदायकलाई आवश्यकता अनुसार जिम्मेवार बनाउने।

6.2.2 The CERT Team

- **CERT** stands for **Computer Emergency Response Team**.
- A CERT is a group of cybersecurity experts responsible for identifying, responding to, and mitigating security incidents, cyber threats, and vulnerabilities within an organization, sector, or country.
- It is an organization responsible for:
  - **Responding to cybersecurity incidents**
  - **Coordinating security measures** among various stakeholders
  - Providing **early warnings and alerts about threats**
  - **Conducting security awareness** and capacity-building programs
  - Assisting with **prevention, detection, and mitigation of cyberattacks**

Roles and Responsibilities of a CERT Team

1. **Incident Handling & Response** – Detecting, analyzing, and mitigating cyber threats like malware, phishing, and data breaches.
2. **Vulnerability Management** – Identifying and reporting security vulnerabilities in software and systems.
3. **Threat Intelligence** – Monitoring cyber threats and sharing intelligence with relevant stakeholders.
4. **Security Awareness & Training** – Educating users and organizations on best cybersecurity practices.
5. **Forensics & Investigation** – Analyzing security incidents and conducting forensic investigations.
6. **Collaboration & Coordination** – Working with other cybersecurity teams, government agencies, and private organizations to improve security posture.

CERTs in Nepal

1. Nepal CERT (NpCERT)

- **Status**: Government initiative
- **Affiliation**: Under the Ministry of Communication and Information Technology (MoCIT)
- **Website**: https://np-cert.gov.np
- **Role**: National-level CERT for Nepal
- **Responsibilities**:
  - Monitor, detect, and respond to national cybersecurity threats
  - Coordinate cyber incident responses among government, private sector, and international partners
  - Develop national cybersecurity policies and frameworks
  - Provide alerts, advisories, and best practices for cybersecurity
  - Conduct capacity-building, training, and awareness programs

2. NREN CERT (Nepal Research and Education Network)

- **Focus**: Academic and research institutions
- **Role**: CERT for educational networks and university systems
- **Responsibilities**:
  - Provide cybersecurity incident response within the education and research sector
  - Promote secure academic collaboration
  - Coordinate with global education and research CERT networks

3. Banking Sector CERT / NRB-CSIRT

- **Affiliation**: Nepal Rastra Bank (NRB)
- **Role**: Sectoral CERT for the banking and financial industry
- **Responsibilities**:
  - Monitor cybersecurity threats targeting the banking sector
  - Coordinate incident responses among financial institutions
  - Set standards and guidelines for cybersecurity practices in banking

4. Nepal Telecom CERT / NT-CERT

- **Affiliation**: Nepal Telecom (NTC)
- **Role**: Organizational CERT for Nepal Telecom
- **Responsibilities**:
  - Handle cyber incidents targeting telecom infrastructure
  - Secure telecom systems and data
  - Provide internal cybersecurity monitoring and response

Types of CERTs

- **National CERTs** (e.g., **US-CERT**, **CERT-In** in India, **JPCERT** in Japan) – Handle cybersecurity at a national level.
- **Corporate CERTs** (e.g., **Google's CERT, Microsoft's Security Response Center**) – Protect large enterprises from cyber threats.
- **Sector-Specific CERTs** (e.g., **Financial Sector CERT, Energy Sector CERT**) – Focus on cybersecurity within a particular industry.

6.2.3 Computer Fraud and Abuse Act (CFAA)

- The Computer Fraud and Abuse Act (CFAA) is a U.S. federal law enacted in 1986 **to address computer-related offenses.**
- It was originally **designed to protect government and financial institution computers from unauthorized access and cyber attacks** but has since been expanded to cover a broader range of computer systems and activities.
- Key points include:
  1. **Unauthorized Access**: Criminalizes accessing computers without permission.
  2. **Damage and Loss**: Addresses causing harm to computer systems or data.
  3. **Fraud**: Covers using computers to commit fraud or extortion.
  4. **Penalties**: Includes fines and imprisonment based on the offense severity.
  5. **Protected Computers**: Applies to government, financial, and internet-connected computers.

6.2.4 Digital Millennium Copyright Act (DMCA)

- The **Digital Millennium Copyright Act (DMCA)** is a U.S. copyright law enacted in **1998 to address the challenges of digital content protection and online copyright infringement.**
- It implements two key international treaties from the **World Intellectual Property Organization (WIPO)** and **is designed to protect copyright holders** while balancing the interests of users and service providers.
- **Why the DMCA Matters Today?**
  - Used to enforce copyright protection on the internet (e.g., streaming platforms, social media, gaming, and software).
  - Impacts digital rights, including fair use, free speech, and access to information.
  - Relevant in discussions about piracy, DRM restrictions, and online content moderation.

Key Provisions of DMCA:

1. **Anti-Circumvention Provisions (Section 1201)**
   - Prohibits bypassing digital rights management (DRM) or encryption technologies that protect copyrighted materials (e.g., DVD encryption, software protection).
   - Even if you own legally purchased content, breaking its DRM can be illegal.
2. **Safe Harbor for Online Service Providers (Section 512)**
   - Protects internet service providers (ISPs), websites, and platforms (like YouTube) from liability for copyright infringement **if** they comply with takedown notices.
   - Requires platforms to remove infringing content when notified through a **DMCA takedown notice**.
3. **DMCA Takedown Notice and Counter-Notice Process**
   - **Copyright owners** can issue takedown notices to platforms hosting infringing content.
   - **Users** can submit a **counter-notice** if they believe their content was removed unfairly.
4. **Protections for Libraries, Archives, and Education**
   - Allows limited exceptions for certain institutions to bypass digital locks for preservation and research.
5. **Penalties for Copyright Infringement**
   - Criminal and civil penalties for violating the DMCA, including **fines and imprisonment** for intentional violations.

6.2.5 Open Source Intelligence (OSINT)

- **Open Source Intelligence (OSINT)** **refers to the process of collecting, analyzing, and utilizing publicly available information** from various sources to generate intelligence.
- It is widely used in cybersecurity, law enforcement, military operations, corporate security, and ethical hacking.

- It refers to the process of collecting and analyzing information from publicly available sources to gather actionable intelligence.
- OSINT techniques involve using a variety of tools and methods to gather data from sources such as social media platforms, websites, public records, news articles, and other publicly accessible information.
- Key sources for OSINT include social media platforms (like Twitter, Facebook, LinkedIn), online forums, blogs, publicly accessible databases (such as property records or business registrations), and even satellite imagery.
- OSINT analysts rely on critical thinking, creativity, and the ability to verify information to make sense of the data collected.
- It's important to note that while OSINT relies on publicly available information, ethical considerations, privacy laws, and terms of service agreements must be respected when conducting OSINT activities.
- OSINT is widely used by various entities, including government agencies, law enforcement, corporations, journalists, and researchers, to gather information for various purposes such as threat assessment, competitive intelligence, due diligence, and investigative journalism.

Sources of OSINT

OSINT data is collected from **freely accessible** sources, including:

1. **Publicly Available Websites** – News sites, blogs, forums, social media (Facebook, Twitter, LinkedIn, Reddit).
2. **Government Publications** – Public records, legal documents, court records, company registrations.
3. **Social Media Intelligence (SOCMINT)** – User profiles, posts, interactions, and trends.
4. **Dark Web Sources** – Information from forums and marketplaces using tools like Tor.
5. **Search Engines & Online Databases** – Google Dorking, WHOIS lookups, Wayback Machine, academic research databases.
6. **Satellite Imagery & Geospatial Intelligence (GEOINT)** – Google Maps, Google Earth, satellite imagery.
7. **Corporate & Financial Data** – SEC filings, patents, market reports

Uses of OSINT

- **Cybersecurity & Threat Intelligence** – Identifying vulnerabilities, leaked credentials, phishing campaigns.
- **Law Enforcement & Investigations** – Tracking criminals, identifying threats, digital forensics.
- **Military & National Security** – Monitoring geopolitical threats, adversarial activities.
- **Corporate Security & Competitive Intelligence** – Analyzing competitors, market trends, leaked data.
- **Journalism & Fact-Checking** – Verifying news, investigating misinformation.
- **Ethical Hacking & Red Teaming** – Conducting reconnaissance before penetration testing.

6.2.6 Open Web Application Security Project (OWASP)

- https://owasp.org/www-project-top-ten/
- The Open Web Application Security Project, or OWASP, **is an international non-profit organization dedicated to web application security.**
- The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks.
- The report is put together by a team of security experts from all over the world. OWASP refers to the Top 10 as an ‘awareness document’ and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.

Key Objectives of OWASP

1. **Promote Awareness** – Educating developers and security teams about common web security risks.
2. **Provide Security Standards** – Defining best practices for secure coding.
3. **Develop Open-Source Security Tools** – Offering free tools for security testing and assessment.
4. **Encourage a Security-First Approach** – Integrating security into the Software Development Lifecycle (SDLC).

OWASP Top 10 (Most Popular Project)

1. **Broken Access Control** – Improper enforcement of user permissions.
2. **Cryptographic Failures** – Weak encryption or improper handling of sensitive data.
3. **Injection Attacks** – SQL injection, command injection, and other code injections.
4. **Insecure Design** – Poor security practices in the application's architecture.
5. **Security Misconfiguration** – Default settings, unpatched systems, or exposed configurations.
6. **Vulnerable and Outdated Components** – Using outdated libraries or dependencies.
7. **Identification and Authentication Failures** – Weak passwords, improper authentication mechanisms.
8. **Software and Data Integrity Failures** – Insecure software updates, supply chain attacks.
9. **Security Logging and Monitoring Failures** – Lack of logging, making incident detection difficult.
10. **Server-Side Request Forgery (SSRF)** – Attackers force the server to make requests to unintended locations.

CENTRAL INVESTIGATION BUREAU (CIB)

- CBI is the national investigation agency of Nepal which is run under Nepal Police.
- It is sometimes referred as Central Investigation Bureau of Nepal Police.
- It runs under Nepal Government.
- CBI of Nepal Police aims to sweep away organized crime from the country within a few years. It is responsible for conducting cybercrime investigation in Nepal.
- The **Central Investigation Bureau (CIB)** is a specialized unit of the **Nepal Police** responsible for handling **serious criminal investigations** at the national level.
- It is Nepal's top investigative agency for organized crime, cybercrime, financial fraud, human trafficking, and other high-profile criminal activities.

Key Roles & Responsibilities of CIB

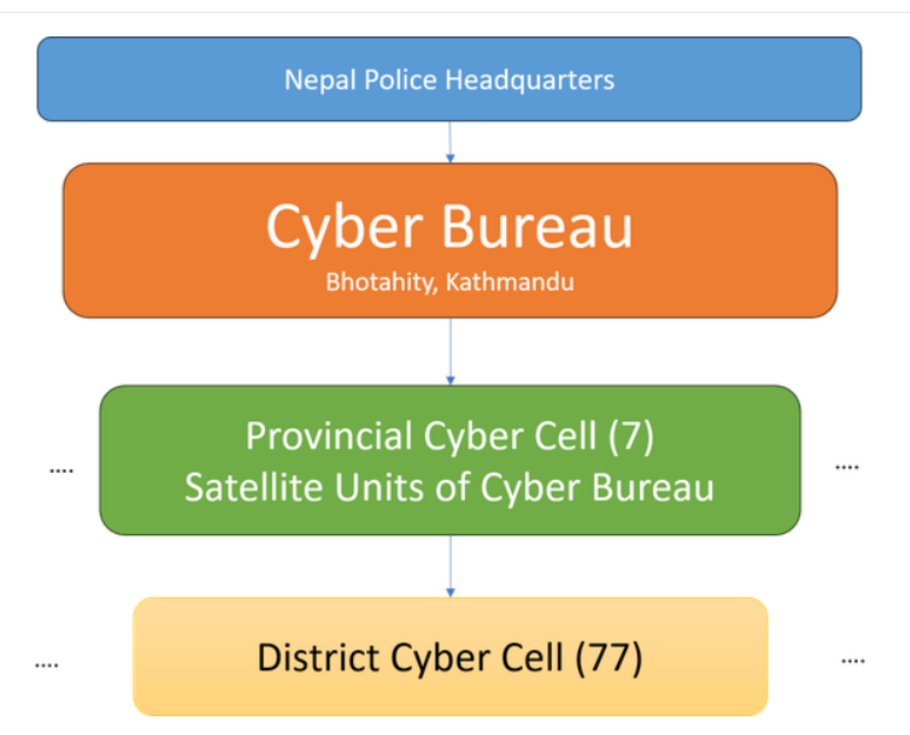
1. **Investigating Organized Crime** – Handling cases related to criminal gangs, drug trafficking, and illegal arms.
2. **Cybercrime Investigations** – Addressing online fraud, hacking, identity theft, and digital forensics.
3. **Financial & Banking Fraud** – Investigating scams, fake currency cases, tax evasion, and money laundering.
4. **Human Trafficking & Smuggling** – Rescuing victims and prosecuting traffickers.
5. **Corruption & White-Collar Crimes** – Working with other agencies to combat corruption.
6. **Counter-Terrorism & National Security** – Monitoring threats that impact national security.
7. **Homicide & High-Profile Cases** – Investigating murder cases and crimes involving influential individuals.
8. **Forgery & Document Fraud** – Dealing with fake passports, visas, land certificates, and academic documents.

CIB's Jurisdiction & Powers

- Operates under the **Nepal Police Headquarters** and works in coordination with agencies like:
  - **Department of Immigration**
  - **Department of Money Laundering Investigation**
  - **Nepal Rastra Bank (NRB)**
  - **Interpol (for international crimes)**
- CIB officers have special legal powers to conduct surveillance, cyber forensics, and undercover operations.

CENTRAL INVESTIGATION BUREAU (CIB)

- **ORGANIZATIONAL STRUCTURE OF CBI**



Reference: https://cyberbureau.nepalpolice.gov.np/about-us/organization-structure/

How to Contact CIB Nepal

- **Headquarters**: Kathmandu, Nepal
- **Hotline**: 100 (Nepal Police)
- **Cybercrime Reporting**: Nepal Police Cyber Bureau
- **Official Website**: https://www.nepalpolice.gov.np/

End of Chapter