# SNS COLLEGE OF ENGINEERING

**Coimbatore-35**
**An Autonomous Institution**

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

## DEPARTMENT OF CSE ( IoT, Cyber Security including Blockchain Technology)

## 19SB623 – ETHICAL HACKING AND CYBER LAWS

### III YEAR/ VI SEMESTER



## UNIT 4 – INTERNATIONL LAW AND JURISDICTION IN CYBERSPACE

TOPIC 4 –*Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State.*

# 1. Introduction to Cyberspace & Cyber Crime

**Cyberspace**: A global domain within the information environment consisting of the interdependent network of information systems.

**Cyber Crime**: Any criminal activity that involves a computer, networked device, or a network.

**Key Challenges:**

Borderless nature of cyber space

Anonymity of users

Different legal standards across jurisdictions

Lack of international cooperation

# 2. Classification of Cyber Crimes

**Against Individuals:**

- Identity theft (Stealing personal data to impersonate )
- Cyber bullying (harassment using electronic means)
- Phishing (Tricks to gain sensitive info via fake emails/websites)
- Online harassment
- Data theft

**Against Institutions:**

- Hacking
- Ransomware
- Insider threats

# 2. Classification of Cyber Crimes

- Data breaches
- Denial-of-service (DoS) attacks

**Against the State:**

- Cyber terrorism (conduct violent acts that threaten or cause serious harm to national security, infrastructure, or civilian populations)
- Cyber warfare (use of digital attacks by a nation-state or its proxies to damage, disrupt, or disable the information systems of another country.)
- Attacks on critical infrastructure
- Espionage (Spying- the act of finding out secret information about another country or organization)
- Disinformation campaigns

# 3. Jurisdiction in Cyberspace

Jurisdiction determines which court or authority can hear a case.

**Types of Jurisdiction:**

**Territorial Jurisdiction**: Based on location of crime.

**Personal Jurisdiction**: Authority over the individuals involved.

**Subject-Matter Jurisdiction**: Authority to hear a specific type of case.

**Universal Jurisdiction**: Applied to crimes of universal concern (e.g., terrorism).

# 3. Jurisdiction in Cyberspace

**Issues in Cyber Jurisdiction:**

Cross-border data flow

Difficulty in determining location of offense

Cloud storage complexities

Different national laws and enforcement capabilities

# 4. International Legal Frameworks on Cyber Crime

**1. Budapest Convention on Cybercrime (2001)**

**First international treaty** on crimes committed via the internet.

Adopted by the Council of Europe, with non-European states like the USA, Japan, etc. as signatories.

**Key Provisions**:

- Criminalization of specific acts (illegal access, data interference)
- Law enforcement cooperation
- Extradition rules
- Mutual legal assistance

**2. Tallinn Manual (NATO Cooperative Cyber Defence Centre)**

Non-binding academic study

Interprets how international law applies to cyber warfare

Based on UN Charter principles (sovereignty, non-intervention)

# 4. International Legal Frameworks on Cyber Crime

**3. United Nations Efforts**

UN GGE (Group of Governmental Experts): Focus on state behavior in cyberspace.
UN OEWG (Open-Ended Working Group): Promotes dialogue on norms and laws related to cyber.

**4. Other Regional Frameworks**

European Union: GDPR for data protection, NIS Directive for cybersecurity.
African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention).
ASEAN Cybersecurity Cooperation Strategy.

# 5. Enforcement Mechanisms and Cooperation

**1. Mutual Legal Assistance Treaties (MLATs):**
Agreements between countries to help in legal proceedings and investigations.

**2. INTERPOL and Europol:**
International cooperation in tracking cyber criminals.

**3. Regional Cybercrime Centers:**
AFRIPOL (Africa)
ASEANAPOL (Asia)

# 6. Case Studies in International Jurisdiction

**Yahoo! Inc. v. LICRA (France)** – Conflict over content legality across borders.

**Microsoft Ireland Case (USA vs. Ireland)** – Dispute over data stored in foreign servers.

**WannaCry Ransomware (Global)** – Coordinated international response needed.

# 7. Gaps & Challenges in International Cyber Law

Lack of universal treaty on cybercrime

Sovereignty and non-intervention debates

Attribution of cyber attacks to state or non-state actors

Differences in legal standards (e.g., free speech vs. hate speech)

# 8. The Way Forward

Develop binding international cyber law instruments.

Strengthen global cooperation and trust.

Establish universal norms and accountability mechanisms.

Build national capacity and digital diplomacy.

# 9. Conclusion

Cyber crimes against individuals, institutions, and states have global implications.

While national laws are crucial, **international cooperation, harmonized legal standards, and shared jurisdiction frameworks** are essential to effectively combat cybercrime in a borderless digital world.

# *International Cooperation*

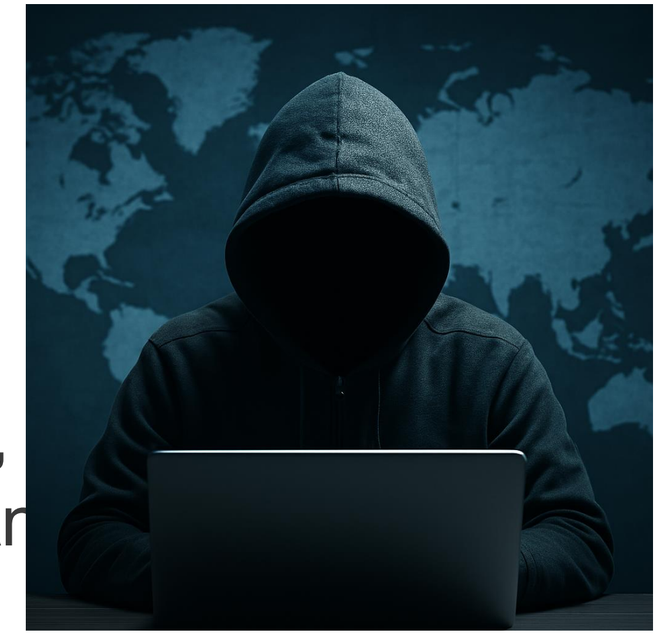
Title: How Countries Work Together Against Cybercriminals
Visual: A hacker being arrested with international police logos (Interpol, Europol, FBI)
Text:
Mutual Legal Assistance Treaties (MLATs)
Budapest Convention on Cybercrime
Extradition agreements
Voiceover: “To solve this, countries sign agreements like the Budapest Convention, allowing them to cooperate in cybercrime cases. But not all nations are on board.”

# *What Happened to Alex?*

Title: Alex’s Fate—A Global Cybercrime Battle
Visual: A judge’s gavel, split into two—one side (France), the other (U.S.)
Text:
France refuses to extradite him
U.S. pressures France for legal action
Alex gets a light sentence under French law
Voiceover: “In real cases like this, the home refuses extradition. Instead, they handle the their own laws, sometimes giving lighter sen

# *The Big Question – Where Do You Go to Trial?*

Title: What If You Commit a Crime Online?
Visual: A question mark over a digital world map
Text:
You can be prosecuted where:
You physically are
The victim is
The crime had an effect
Voiceover: “So, if you commit a cybercrime,
go to trial? The answer isn’t always clear. Ar
makes cyber law so challenging.”



# *Closing & Next Video Teaser*

Title: What’s Next?
Visual: Social media icons, a lock symbol (privacy), and a speech bubble (free speech)
Text:
Next topic: Freedom of Expression vs. Privacy in
Subscribe for more legal cyber stories!

# THANK YOU