PART 1

INTRODUCTION TO CYBERSECURITY LAW AND POLICY (WEEKS 1–2)

---

1. INTRODUCTION TO CYBERSECURITY LAW AND POLICY

1.1 What is Cybersecurity Law?

Cybersecurity law refers to the body of **legally binding rules** made by governments to regulate how computers, networks, and the internet are used. These laws clearly state:

- What actions are **legal or illegal** in cyberspace
- The **penalties** for cyber offenses
- How cybercrimes are **investigated and prosecuted**

In simple terms, cybersecurity law is **the law of the digital world**, just like criminal law is the law of the physical world.

Purpose of Cybersecurity Law

Cybersecurity law exists to:

1. Protect digital assets of individuals, organizations, and governments
2. Prevent cybercrime and punish offenders
3. Build trust in online banking, e-commerce, and digital services
4. Support national security and economic stability

Nigerian Example (Very Important for Exams)

One major cybersecurity law in Nigeria is the:

Cybercrime (Prohibition, Prevention, etc.) Act 2015

This law criminalizes activities such as:

- Hacking
- Phishing
- Identity theft
- Cyber fraud
- Unauthorized access to computer systems

Real-life Nigerian Scenario (Exam Gold ✨):
If a hacker gains unauthorized access to a Nigerian bank's database and steals customer information, the bank can rely on the **Cybercrime Act 2015** to report the case to law enforcement agencies like the EFCC, leading to prosecution.

Recent Case (Lecturer-Impressing Example):
In May 2023, an unemployed man in Abuja, *Idara Sunday*, was sentenced to **7 months imprisonment** for hacking a businessman's bank account and stealing about **₦306,200**. He was also fined and ordered to compensate the victim.
This case shows that **cybersecurity laws are actively enforced in Nigeria**, not just theoretical.

1.2 Key Cybersecurity Terms Explained (With Examples)

- **Hacking:**
  Unauthorized access to a computer or network system.
  Example: Breaking into a bank's internal server without permission.

- **Phishing:**
  Fraudulent messages or emails designed to trick users into revealing sensitive information.
  Example: Fake bank SMS asking customers to "verify their account."

- **Malware:**
  Malicious software designed to damage or gain unauthorized access to systems.
  Example: Ransomware that locks hospital systems until money is paid.

---

2. CYBERSECURITY POLICY

2.1 What is Cybersecurity Policy?

A **cybersecurity policy** is a set of **guidelines and procedures** created by organizations or government agencies to ensure:

- Compliance with cybersecurity laws
- Protection of digital assets
- Proper employee behavior in digital environments

Unlike law, policy does **not create crimes**, but it **guides actions**.

In simple terms:

> Cybersecurity law says *what must be done*,
> Cybersecurity policy explains *how to do it*.

2.2 Purpose of Cybersecurity Policy

Cybersecurity policies:

1. Translate laws into practical daily actions
2. Guide employees on safe use of IT systems
3. Help organizations avoid legal penalties
4. Protect organizational reputation and customer trust

Nigerian Examples of Cybersecurity Policy

1. **NITDA Data Protection Guidelines**
    - Issued by **NITDA (National Information Technology Development Agency)**
    - Established in **2001**
    - Mandate: Regulate and promote IT development in Nigeria
2. These guidelines direct organizations on how to collect, store, and protect personal data.

3. **Banks' Internal IT Security Policies**
    - Password rules
    - Access control
    - Incident reporting procedures

Real-Life Scenario:
A Nigerian bank may require staff to change passwords every 90 days and report suspicious emails immediately. This is **policy**, not law — but it helps the bank comply with the law.

Key Policy Terms

- **Guideline:** Recommended best practices
- **Standard Operating Procedure (SOP):** Step-by-step instructions for implementing policy

---

3. DIFFERENCE BETWEEN LAW, POLICY, AND REGULATION

Term	Meaning	Enforceability	Nigerian Example
Law	Rules made by government	Mandatory, legally binding	Cybercrime Act 2015
Policy	Internal guidelines	Advisory but enforceable internally	NITDA Data Protection Guidelines
Regulation	Specific rules made under a law	Legally binding	NDPR 2019

Easy Way to Remember (Exam Trick 💡):

- **Law** = What the government says
- **Regulation** = How the law must be followed
- **Policy** = How organizations obey the law internally

Applied Nigerian Example

Nigerian banks:

- Follow the **Cybercrime Act** (law)
- Comply with **NDPR** (regulation)
- Create internal IT security rules (policy)

---

4. IMPORTANCE OF CYBERSECURITY LAW AND POLICY

4.1 Importance of Cybersecurity Law

Cybersecurity law is important because it:

1. Protects sensitive digital information
2. Ensures offenders are punished
3. Enables safe online banking and e-commerce
4. Supports international cooperation
5. Promotes ethical behavior online

Nigerian Example:
The **EFCC** regularly prosecutes online fraudsters ("Yahoo Yahoo") under the Cybercrime Act, helping to reduce cyber fraud and protect Nigeria's digital economy.

4.2 Importance of Cybersecurity Policy

Cybersecurity policy:

1. Guides daily IT operations
2. Helps organizations comply with laws

3. Protects reputation and customer trust
4. Manages cyber risks effectively

Example:
Banks enforce internal policies on access control to prevent insider threats and data leaks.

---

5. KEY CONCEPTS IN CYBERSECURITY LAW

5.1 Cybercrime

Definition:
Cybercrime refers to illegal activities committed using computers or the internet.

Common Types in Nigeria:

1. Hacking
2. Phishing and online scams
3. Identity theft
4. Ransomware attacks
5. Cyber terrorism

Cyber Terrorism (Lecturer-Ready Explanation)

Cyber terrorism is the use of digital technology to **attack government systems, critical infrastructure, or the public** with the aim of causing fear or disruption for political or ideological reasons.

Key Features:

- Targets power grids, hospitals, banks, or government agencies
- Uses malware, ransomware, or DDoS attacks
- Motivated by ideology or political goals

Example:
A cyber group hacking into a national power grid and causing a blackout is an act of cyber terrorism.

5.2 Data Protection

Definition:
Data protection refers to laws and rules governing how personal data is collected, processed, stored, and shared securely.

Nigerian Laws:

- **NDPR 2019**
- **Nigeria Data Protection Act (NDPA) 2023**

Example:
Banks encrypt customer data and notify users if a data breach occurs.

5.3 Privacy

Definition:
Privacy is the right of individuals to control how their personal information is used.

Example:
Social media users deciding who can view their posts or personal details.

5.4 Intellectual Property (IP)

Definition:
Intellectual Property refers to legal rights protecting creations of the mind such as software, music, inventions, and digital content.

Importance in Nigeria:
Protects Nigerian software developers, musicians, and tech startups.

Example:
A Nigerian music streaming app copying another app's source code without permission violates IP law.

PART 2 (SIMPLIFIED VERSION)

SOURCES OF CYBERSECURITY LAW, JURISDICTION & REGULATORY BODIES

---

1. SOURCES OF CYBERSECURITY LAW

Cybersecurity law does not come from one place.
In Nigeria, cybersecurity law comes from **three main sources**:

1. Laws made by the government
2. Court decisions
3. International agreements

These sources explain **where cybersecurity rules come from and how they are enforced**.

1.1 STATUTORY LAW (LEGISLATION)

Meaning (Very Simple)

Statutory law means **laws made by the Nigerian National Assembly**.
These laws tell people what is **allowed and not allowed online**.

They are **compulsory**, and anyone who breaks them can be punished.

Important Nigerian Cybersecurity Laws

Cybercrime (Prohibition, Prevention, etc.) Act 2015
This law makes cybercrime a criminal offence in Nigeria.
It covers:

- Hacking
- Phishing

- Identity theft
- Cyber fraud
- Malware attacks

Nigeria Data Protection Regulation (NDPR) 2019
This law controls how organizations:

- Collect personal data
- Store data
- Share data

It protects people's personal information.

EFCC (Establishment) Act 2003
This law created the **EFCC**.
The EFCC investigates and prosecutes:

- Cybercrime
- Online fraud
- Financial crimes

Banks and Other Financial Institutions Act (BOFIA) 2020
This law forces banks to:

- Protect customer data
- Use secure IT systems
- Prevent online fraud

Simple Example (Very Important for Understanding)

If a Nigerian fintech company collects customer data:

- It must protect the data under **NDPR**

- It must not allow hacking or fraud under the **Cybercrime Act**
- If fraud happens, **EFCC** can investigate

If the company fails, it can be **fined or prosecuted**.

Why Statutory Law Is Important

Statutory law:

- Clearly defines cybercrime
- Gives punishment for offenders
- Protects online users
- Supports Nigeria's digital economy

1.2 CASE LAW (COURT DECISIONS)

Meaning

Case law means **decisions made by courts** when they judge cybercrime cases.

These decisions help explain **how cybersecurity laws should be used**.

Once a court decides a case, that decision can guide **future cases**.

Why Case Law Is Important

Case law:

- Explains unclear parts of the law
- Helps judges handle similar cases
- Strengthens punishment for cybercrime

Nigerian Example (Easy to Remember)

In **2018**, a Nigerian court convicted an internet fraudster under the **Cybercrime Act 2015**.

This case showed that:

- Online fraud is a serious crime
- Cybercrime laws are enforced in Nigeria
- Courts support EFCC in fighting cybercrime

👉 In exams, you can write:

> "Through case law, Nigerian courts strengthen cybersecurity enforcement by interpreting and applying the Cybercrime Act."

1.3 INTERNATIONAL CONVENTIONS AND TREATIES

Meaning

International conventions are **agreements between countries** to fight cybercrime together.

This is important because cybercrime often:

- Crosses borders
- Affects people in many countries

No country can fight cybercrime alone.

A. BUDAPEST CONVENTION ON CYBERCRIME (2001)

The Budapest Convention on Cybercrime

The **Budapest Convention on Cybercrime** is the **first international treaty** created to address crimes committed through computers and the internet. It was adopted in **2001 by the Council of Europe** and provides a common legal framework for countries to fight cybercrime effectively.

The Convention focuses on three major areas:

1. **Harmonising cybercrime laws** among countries,
2. **Improving investigation procedures** for digital crimes, and
3. **Enhancing international cooperation**, since cybercrime often crosses national borders.

It defines key cyber offences such as **illegal access (hacking), data interference, system interference, online fraud, and child exploitation offences**, ensuring countries criminalise these acts in their national laws. It also guides law enforcement on how to **collect electronic evidence legally**, while still respecting **human rights and privacy**.

In summary, the Budapest Convention helps countries **work together**, close legal gaps between nations, and respond faster to cybercrime in a coordinated and lawful way.

Meaning

This is the **first international agreement** made to fight cybercrime.

It helps countries:

- Have similar cybercrime laws
- Work together during investigations

Crimes Covered

- Hacking
- Data damage
- Online fraud
- Child exploitation
- Intellectual property theft

Relation to Nigeria

Nigeria has **not officially signed** this convention.
However:

- Nigeria's **Cybercrime Act 2015 follows its ideas**
- Nigeria works with other countries during cybercrime investigations

Simple Example:
EFCC works with Interpol to arrest cybercriminals who target Nigerians or foreigners online.

B. UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE (1996)

Meaning

This law helps countries **recognize online transactions as legal**.

It supports:

- Electronic contracts
- Electronic signatures
- Online business

Why It Matters in Nigeria

Nigeria uses its ideas to:

- Support online banking
- Protect e-commerce
- Make electronic contracts valid

Example:
If a Nigerian company signs a contract online, the contract can be enforced in court.

C. MALABO CONVENTION (2014)

Meaning

This is an **African Union agreement** on:

- Cybersecurity
- Data protection
- Online safety

Relation to Nigeria

Nigeria is a **signatory** to this convention.
Because of this:

- NDPR follows African data protection standards
- Nigeria cooperates with other African countries

Example:
Banks and telecom companies protect customer data to meet African cybersecurity standards.

SIMPLE SUMMARY TABLE

Convention	What It Does	Nigeria's Position
Budapest Convention	Fights cybercrime globally	Cybercrime Act follows its ideas
UNCITRAL Model Law	Supports online transactions	Used for e-commerce laws
Malabo Convention	African cybersecurity rules	Nigeria follows NDPR standards

---

2. JURISDICTION IN CYBERSPACE

Meaning

Jurisdiction means **who has the legal power to handle a case**.

Problems with Jurisdiction Online

- Internet has no borders
- Crimes involve many countries
- Arresting foreign criminals is hard

Simple Example

If a Nigerian hacker attacks a US company:

- Nigerian law applies
- US law also applies
- Countries must cooperate

TYPES OF JURISDICTION (VERY SIMPLE)

Type	Meaning	Example
Territorial	Crime happens in Nigeria	Fraud from Lagos
Personal	Criminal lives in Nigeria	Nigerian resident prosecuted

Subject-Matter	Court handles cybercrime	Federal High Court
Extraterritorial	Crime abroad affects Nigeria	Foreign hacker targets Nigerians

👉 **Easy Explanation:**
Extraterritorial jurisdiction allows Nigeria to punish cybercriminals outside the country if Nigerians are victims.

---

3. REGULATORY BODIES & INTERNATIONAL COOPERATION

Nigerian Agencies Involved

NITDA

- Makes cybersecurity policies
- Enforces data protection laws

EFCC

- Investigates cybercrime
- Arrests online fraudsters

NCC

- Regulates telecom companies
- Ensures network security

NDLEA

- Indirect role when crime uses online platforms

International Cooperation

Nigeria fights cybercrime through:

- Mutual Legal Assistance Treaties (MLATs)
- Interpol cooperation
- International cybersecurity meetings

Example:
Many online fraud cases involve cooperation with the US and UK.