

Cybersecurity Law and Policy

Prepared by Dr. Kamal Alieyan

Lecture 6



Introduction to Cyber Laws

Lecture 6

Prepared by
Dr. Kamal Alieyan

Lecture Objective



- **Introduce cyber law in the realm of cyberspace and cybersecurity.**
- **To Introduce the needs for cyber laws, and the differences between ethics and laws.**
- **To explain some typical examples of cybercrimes.**
- **Discuss why they are illegal and unethical.**
- **Discuss some challenges in cyber law.**

Lecture topics



- **6.1 Cyber Laws**
- **6.2 The Need for Cyber Laws**
- **6.3 Cyberethics and Cyber Law**
- **6.4 Need for Cyber Regulation Based on Cyberethics**
- **6.5 Cybercrime Categories from The Legal Perspective**
- **6.6 Cyber Law and Intellectual Property (IP)**
- **6.7 Challenges in Cyber Law**

Chapter

06

6.1 CYBER LAWS

- **Ethics** is a code of responsible behavior, while **law** is an outcome of ethics.
- Since cyberspace operates on a global level, the number of cybercrimes increases widely.
- Several activities over cyberspace like illegal access, illegal interception, data interference, misuse of devices, computer-related forgery, computer-related offenses, computer-related fraud, and offenses related to copyright and neighboring rights may be termed as **cybercrimes**, which may have a drastic impact over the society.
- Therefore, there is a need to introduce some kind of legislation that mandates acceptable behavioral use of technology over cyberspace.

Chapter

06

6.1 CYBER LAWS

Definition of Cyber law:

- Cyber law legislation that underpins acceptable behavioral use of technology like computer hardware and software, the Internet, and networks.
- It guarantees that users are protected from any harm by empowering the investigation and indictment of online crime.
- Further, it applies to the activities of people, gatherings, general society, government, and private associations.

Chapter

06

6.1 CYBER LAWS

- **Cyber law** has a role in society and business.
- Cybercrimes like fraud, forgery, money laundering, theft, and other illegal activities are performed via computers, the Internet, and networks.
- **Cyber law** is responsible for investigating crimes perpetrated in the physical world but enabled in cyberspace.
- From the business perspective, cyber law is used to protect companies from unlawful access and theft of their intellectual property (IP).

Chapter

06

6.1 CYBER LAWS

- Although cyberspace is global, cyber law is different in different countries. While cybercrime impacts the global community, the adoption of cybercrime legislation varies among countries.
- Most of the countries have cyber laws, few have draft legislation, and some even have no cyber laws.
- Numerous states are involved in developing new cyber laws as addenda to their present codes.

Chapter

06

6.1 CYBER LAWS

- Many countries revise their already existing national codes with legislative language on cybercrime.
- .
- In the past several nations have instituted their own national cyber laws remembering their own national prerequisites.
- Countries vary widely in their ability to investigate and punish cybercrime.
- Further, changing levels of risks across different countries make it difficult to pass common cyber laws all over the globe.

6.2 THE NEED FOR CYBER LAWS

- **Cyber law** is worried about the law governing the Internet. It addresses several issues like cybercrimes, electronic commerce, IP and data protection, and privacy.
- **Cybercrime** predominantly deals with computer crimes, computer-related crimes, and computer abuse.
- **E-commerce** involves electronic data used in commercial transactions. Electronic commerce laws are responsible for addressing issues of data authentication by electronic and digital signatures.
- **IP** deals with copyright law pertaining to computer software, computer source code, websites.
- **Data protection and privacy** laws are responsible for addressing legal issues that emerge while gathering, putting away and communicating sensitive personal information. This is usually done by data controllers like banks, hospitals, email service providers, etc.

6.2 THE NEED FOR CYBER LAWS

- Due to the advancement in technology, especially cybersecurity, it may be said that current criminals can take more with a computer than with a firearm, and tomorrow's terrorists might have the option to accomplish more harm with a keyboard than with a bomb.
- Cyber-crimes that aim at stealing valuable data and vandalizing the economy are a threat not only to cyberspace but various other domains too that harbor sensitive information.
- Thus, enforcing cyber laws in cyberspace is mandatory:
 - **Cyber laws are vital** because they touch almost all aspects of transactions and behavior on and concerning the Internet, the World Wide Web and Cyberspace.
 - **Cyber laws ensure the right** to enter into legally enforceable digital contracts.

6.2 THE NEED FOR CYBER LAWS

- **Cybercrimes**, for example, malware attacks, computer frauds, phishing, hacking, unauthorized access, email hijacking, denial of service are **becoming frequent**, and may **potentially harm sensitive data, the economy** as well as the reputation of an individual or an organization, hence cyber laws may help prevent them.
- Almost **all transactions are in electronic form and accountability is significant**.
- In numerous non-cyber crime cases as well, significant proof might be found in systems, mobile phones, for example, in instances of separation, murder, abducting, tax avoidance, and so on.
- Cyber law is an **important part of Digital Forensics**.

6.3 CYBERETHICS AND CYBER LAW

- Figure 4.1 mentions how **ethics** are a code of responsible behavior and should be followed.
- **Law** being an outcome of ethics is something that must be followed.
- **Policies** are guidelines that organizations usually follow to promote cybersecurity in their environments.
- We see how these three are connected to each other.
- Although they all aim to ensure better cybersecurity in a given environment, they are very different from each other.

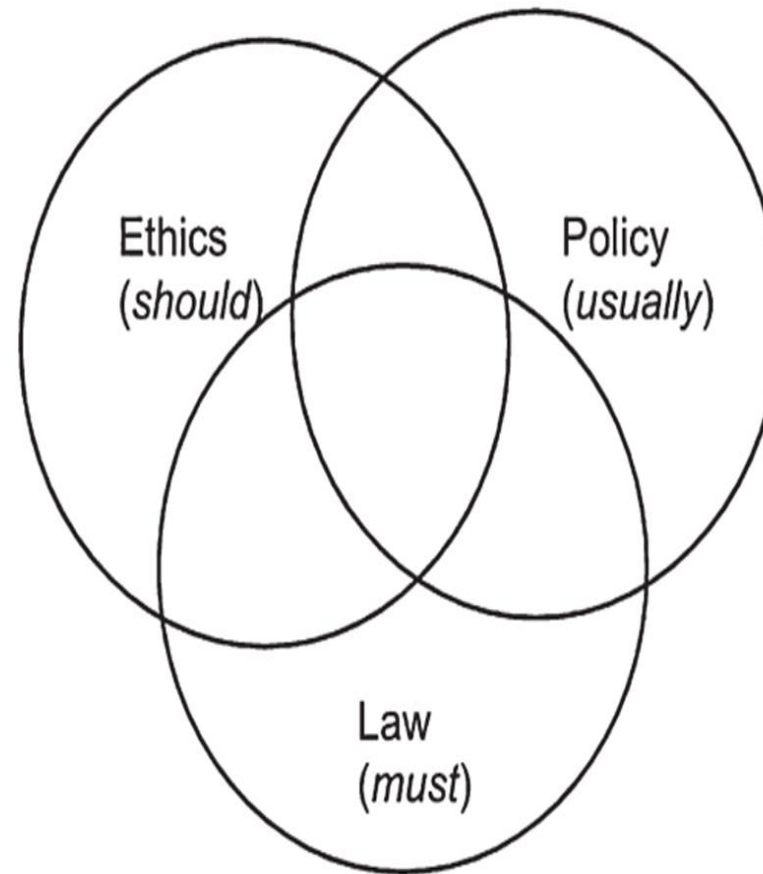


FIGURE 4.1 Ethics, law, and policy triad.

6.3 CYBERETHICS AND CYBER LAW

- **Ethics** are rules that control an individual or society, created to decide what is good or bad, right or wrong, in a given circumstance.
- **Ethics** are also responsible for regulating an individual's behavior or conduct and helps them live a good life. This may be done by applying the moral rules and guidelines.
- **Law** systematic set of universally accepted rules and regulations.
- These principles and guidelines might be made by a suitable authority, for example, government.
- It might be utilized to oversee the activity and conduct of the individuals and can be upheld, by imposing penalties.
- Further, there is a difference in scope and application of ethics and laws.

Ethics versus Legal:

- While **Legal** can apply to a more widespread scope, **Ethical** applies on an individual basis.
- The two of them judge a specific conduct or activity either right or wrong in their respective opinions.
- **Legal** may be said to have more of an objective view, while **Ethics** has a personal as well as varied view depending on the individual.

6.3 CYBERETHICS AND CYBER LAW

- Due to the significant increase in the number of cyber-criminal activities in cyberspace that are not just unethical but also illegal, the role of ethics becomes even more significant. Therefore, there is a need to combine ethics and Law in regulating the activities of the cyber world.
- Information technology (IT) has made the world a global village and has enhanced every sphere and sector of society like the economy, commerce, social, and educational sectors.
- However, this is one space where a lot of work is required to be done.
- It is high time now for careful inspection of the legal and ethical aspects since not enough guidelines are available in this field as compared to those available in conventional branches of science and technology.
- There is a **significant need for cyberethics** to be strengthened by cyber laws.

6.3 CYBERETHICS AND CYBER LAW

- Many countries have come up with new legal national frameworks to govern and regulate cybersecurity.
- Hence, it is imperative that cyber legal frameworks and cybersecurity legal frameworks must now be evolved keeping in mind the evolved principles of cyberethics.
- Consider the following example: obtaining data from networks. Here, there are two separate concerns:
 - **First**, collecting network measurement data (e.g., packet traces), and
 - **Second**, it is publishing the data.
- Clearly, the ethical issues, in this case, are respecting users privacy and respectful uses of published traces, while the legal issue is communication privacy laws.
- Most cybercrimes have some components of **Illegal** as well as **unethical behavior**.

6.3 CYBERETHICS AND CYBER LAW

- Keeping in mind the growing number of cyber laws in the world, including cybersecurity laws, it is increasingly clear that the said legal frameworks incorporate cyber ethical principles and standards, e.g., a demonstration of not hacking a system is a moral guideline.
- If an ethical principle is violated, then such an act is prescribed as a cybercrime which is punishable with imprisonment and fines.
- If a person does any cybercrime activity, then it becomes an offense under the existing cyber laws.
- Further, the increased focus of people on protection and preservation of personal privacy as also data privacy has brought forward the need for effectively codifying ethical considerations pertaining to the protection of privacy.
- For example, it is ethical not to invade anyone's privacy, however, in case if someone does invade someone else's privacy, that becomes an actionable wrong for which various remedies are provided under different cyber legal frameworks.

6.3 CYBERETHICS AND CYBER LAW

- Further, extraordinary cyber laws have specified that an individual, who does not follow anticipated cultural moral standards and behavior concerning activities on cyberspace, would be held to **legal consequences**.
- The domain of cyber law is concerned with providing adequate, strong, validity, and sanction for cyber ethical principles and cyberethics as an evolving discipline.
- For ensuring proper cyber laws, governments in every country, public policymakers, computer professionals, organizations, and private citizens must all take an interest and contribute.
- There is a need to exploit this global information in a socially and ethically sensitive way for our future benefit and applications.

Chapter

06

6.4 NEED FOR CYBER REGULATION BASED ON CYBERETHICS

- Cyber law calls for the safe and lawful collection, retention, processing, transmission, and use of personal data of individuals.
- Cyberethics, therefore, provides the foundation for cyber legal principles concerning the protection of data and other aspects of human endeavor in cyberspace.
- Cyber law will play a very important role in the evolution of cyberethics.
- The obligation will be on officials and administrators to begin perceiving the convergence between cyber law and cyberethics and increasingly grant legal recognition, validity, and sanction to cyberethics principles.
- This becomes although more significant, as we are coming across times where cybercrimes are going to be far more difficult and dangerous. Cybercrime as a paradigm is constantly evolving.

Chapter
05

6.5 CYBERCRIME CATEGORIES FROM THE LEGAL PERSPECTIVE

- The Internet is not a safe place, as it witnesses cybercrime growing at a rapid rate since people are connected to devices as well as each other digitally.
- Cybercrimes influence associations, organizations, and governments **billions of dollars every year**.
- These crimes target the organizations **economy and their reputation**.
- In fact, cybercrime is growing more and more.
- From the Legal perspective, cybercrime can be classified into the following types (Figure 4.2).

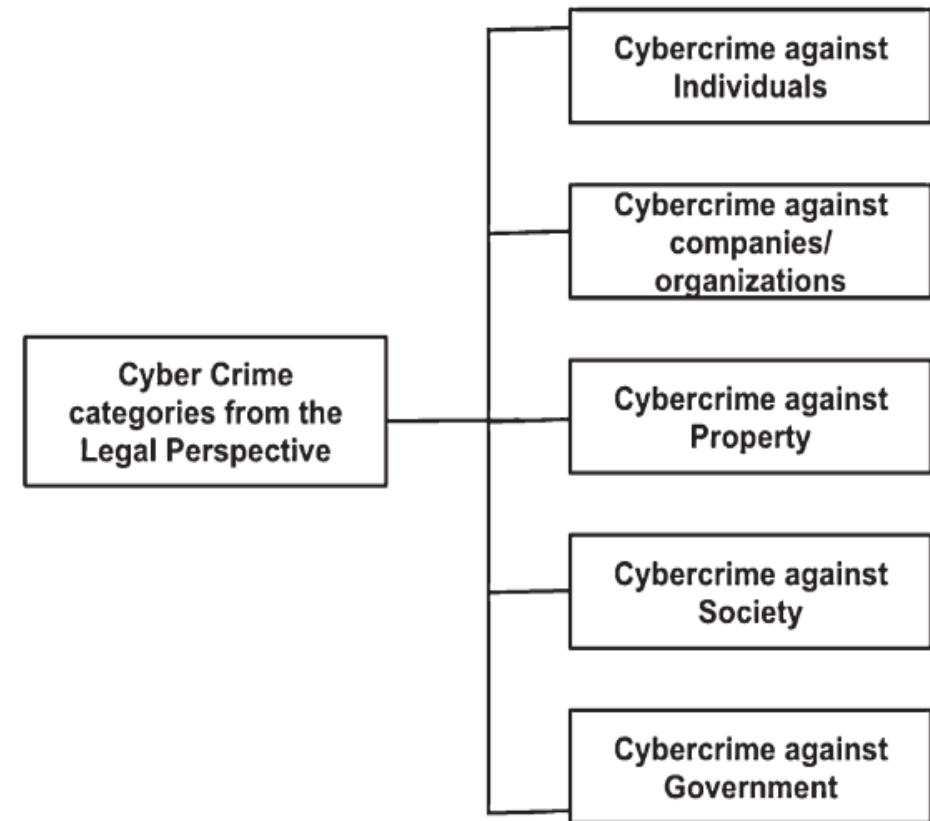


FIGURE 4.2 Cybercrime categories from legal perspective.

6.5 CYBERCRIME CATEGORIES FROM THE LEGAL PERSPECTIVE

- **The Cybercrime Against Individuals:** social engineering, phishing, email harassment, cyberstalking, and spreading illegal adult materials, Credit Card extortion, human trafficking, social engineering, data fraud.
- **Cybercrime Against Companies/Organizations:** company website is hacked, data breaches, cyber extortion, malware distribution.
- **Cybercrime Against Property:** computers, servers, systems. DDOS attacks, hacking, malware transmission, cyber, system vandalism and copyright infringement.
- **Cybercrime Against Society:** Financial crimes against open associations, selling unlawful products, trafficking, web-based betting, fraud.
- **Cybercrime Against Government:** cyber terrorism and include breaking into government systems and networks, destroying, and closing down military sites, and spreading publicity.

6.6 Cyber Law and Intellectual Property (IP)

- Cyberspace is prone to crimes related to IP.
- **Definition 4.2: Intellectual Property (IP)**
 - Intellectual property defined as the domain of the Law that manages ensuring the privileges of the individuals who make unique works.
 - It considers everything from unique plays and books to creations and company identification marks.
 - IP laws are capable of encouraging new technologies, artistic expressions, and inventions for promoting economic growth.
- Individuals who know that their creative work will be safeguarded and that they can benefit from their work may feel encouraged to produce novel things so as to enhance technology.
- IP is a field of legal practice and cyber law. It is an extremely new territory of Law.

6.6 Cyber Law and Intellectual Property (IP)

- Since Internet users can promptly duplicate material on the web, copyright questions have gotten complicated.
- Cyber law has evolved over the last few decades for responding to the wide range of offenses that can be committed online.
- Both IP and cyber law, subsequently, are currently growing fields of expanding significance.
- IP rights identified with cyber law for the most part fall into the accompanying classifications (Figure 4.3).

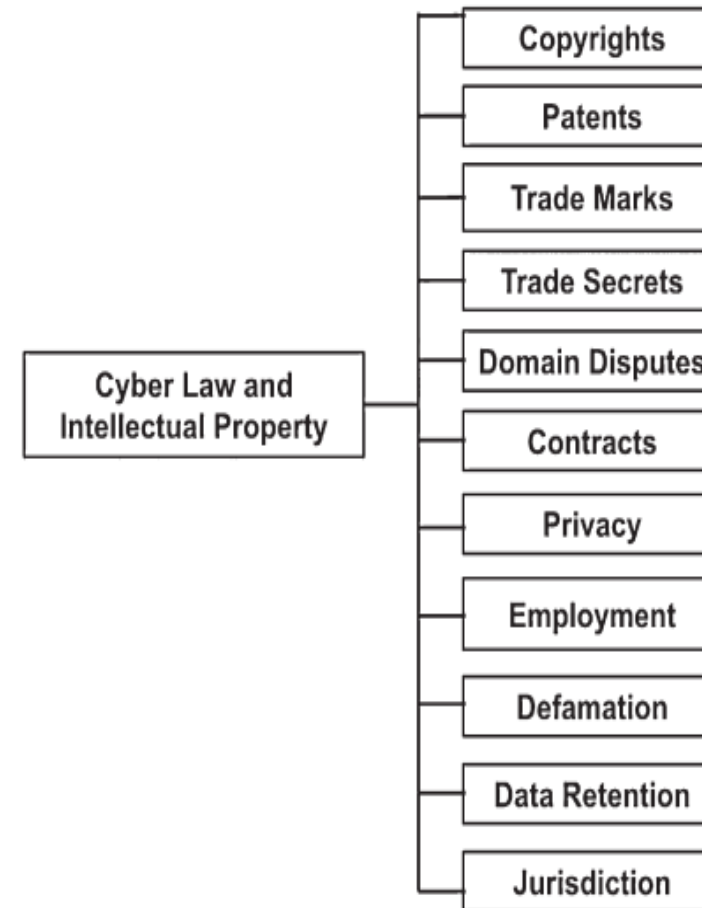


FIGURE 4.3 Cyber law and intellectual property.

Chapter

06

6.7 Challenges in Cyber Law

- One of the **biggest challenges in developing cyber laws** is the concept of jurisdiction.
- **Jurisdiction** might be characterized as the official capacity to settle on lawful choices and decisions.
- Jurisdiction seems challenging for developing cyber laws because the Internet is virtual.
- Further, it does not have any territories. Thus, while mediating the legitimate network regularly faces a contention of Law.
- In a situation where two jurisdictions agree that an individual's action is illegal, it is hard to foresee which Law will apply if both jurisdictions have different severity of punishment or fines.
- Conflict may likewise fall back on who has authority over a case in a digital world that has no physical boundaries. With the issue of jurisdiction it makes the activities of law enforcement officers and agencies daunting when pursuing a cybercrime, every law enforcement staff or agency has their area of authority.

Chapter

06

6.7 Challenges in Cyber Law

Some cyber law Issues requiring discussions are mentioned as follows:

1. Are all the crimes recognized that we see every day in cyber-space?:

- Cyber Crime is an evolving field, and therefore, as technology moves, new types of crimes surface. Therefore, it is practically incomprehensible for the Law to precisely distinguish various kinds of violations and propose remedies accordingly.
- Cyber law needs to depict offenses just as a general term. Thus, corresponding incidents must be interpreted and mapped to different offenses mentioned in the Act.

Chapter

06

6.7 Challenges in Cyber Law

2. Are our police responsive to the public when a complaint is made?

- It is important to train the Police force when it comes to Cyber Crimes so that it yields results.
- One of the greatest underlying issues that many citizens still face is the inability to get their complaints registered with all Police Stations as well as the presence of Cyber Crime Police Stations.
- Sometimes citizens in some places are encouraged by some officers to avoid registration of cases. Cyber Crimes must be reported by the public without hassles.

6.7 Challenges in Cyber Law

3. Are intermediaries and corporates co-operative with law enforcement?:

- Intermediaries and Corporates avoid working with law enforcement as it seems like an intrusion to their work. Therefore, there may not be enough cooperation even if the corporate interest is involved.
- More often than not, Crimes perpetrated inside the corporate system are not announced.
- Even if some crimes are reported and identified, the criminal is just backed out of the activity and not handed over to the law enforcement.
- Commercially minded business entities must look at the crimes from the human perspective and set aside some investment for information security and consumer education.

6.7 Challenges in Cyber Law

4. Are the expertise in cyber law and cyber forensics being amplified?:

- For creating the right pool of talents in cyber law and cyber forensics, the educational plan in training needs to be geared up:
 - i. Creating awareness of cybercrimes at the high school level
 - ii. Presenting cyber laws in the curriculum in graduation level
 - iii. Presenting information security in the educational program at the technical and management instruction.

Chapter

06

6.7 Challenges in Cyber Law

5. Are cyber laws being misused for internet censorship and privacy invasion?:

- It is important to ensure that reasonable steps are being taken by an individual in order to satisfy a legal requirement. However, the notification has come for severe criticism. This is because it can also be misused as a means of Internet Censorship.
- The fear is a result of a few cases in the past where the intensity of the executive to give directions to block websites has been utilized without legitimate governing rules.
- There is a need to guarantee citizen participation in the usage of delicate controls, for example, hindering of sites to evade the provisions being misapplied .

6.7 Challenges in Cyber Law

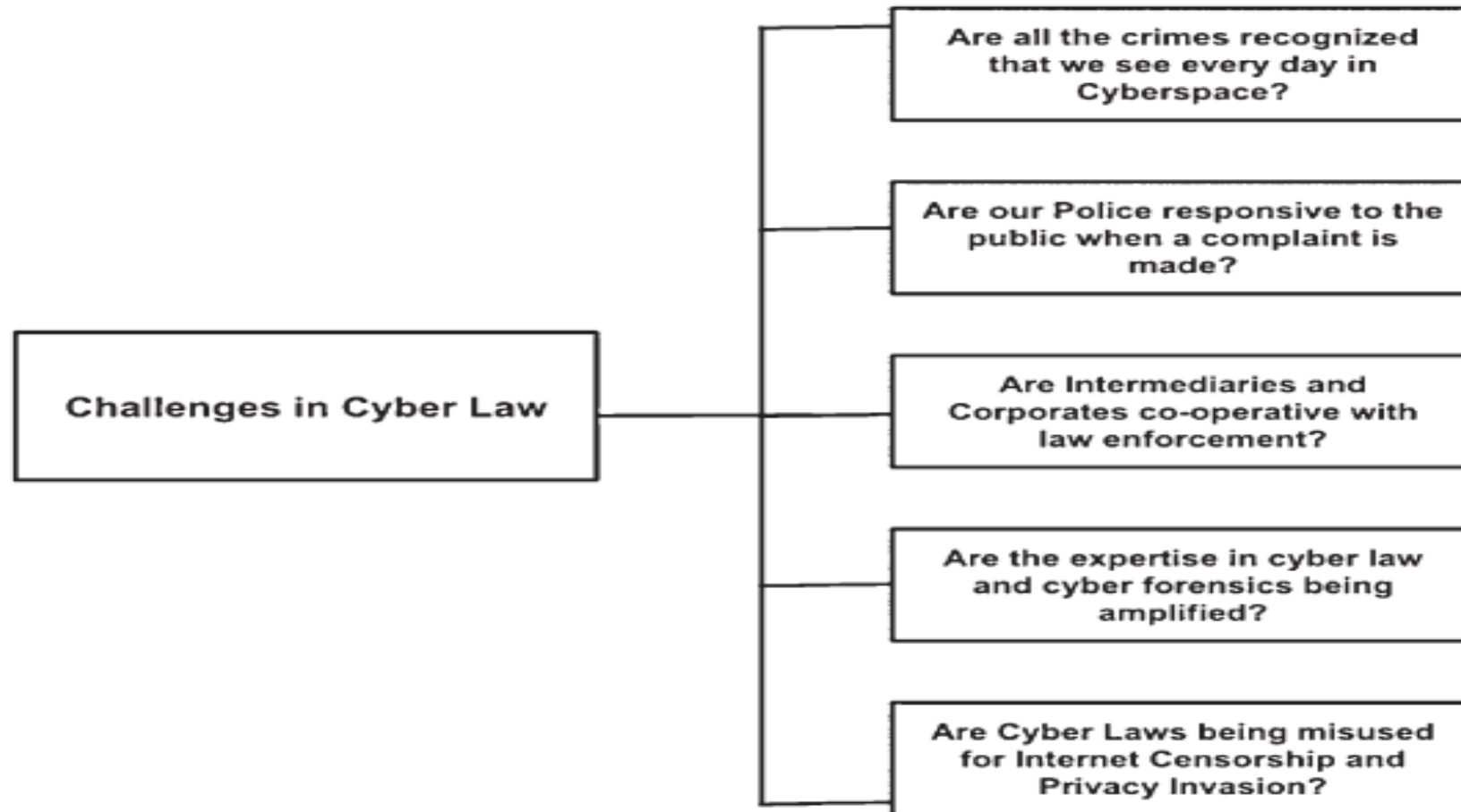


FIGURE 4.4 Challenges in cyber law.



Thank You