

Cybersecurity Law and Policy

Prepared by Dr. Kamal Alieyan

Lecture 1



Introduction to Cyberethics

Lecture 1

Prepared by
Dr. Kamal Alieyan

Course Topics



- **Introduction to Cyberethics**
- **Ethical Issues in Cybersecurity**
- **Cybersecurity Ethics: Cyberspace and Other Applications**
- **Introduction to Cyber laws**
- **Risks in Cybersecurity**
- **Cyber Risks and Cyber Insurance**
- **Introduction to Cybersecurity Policies**

Chapter

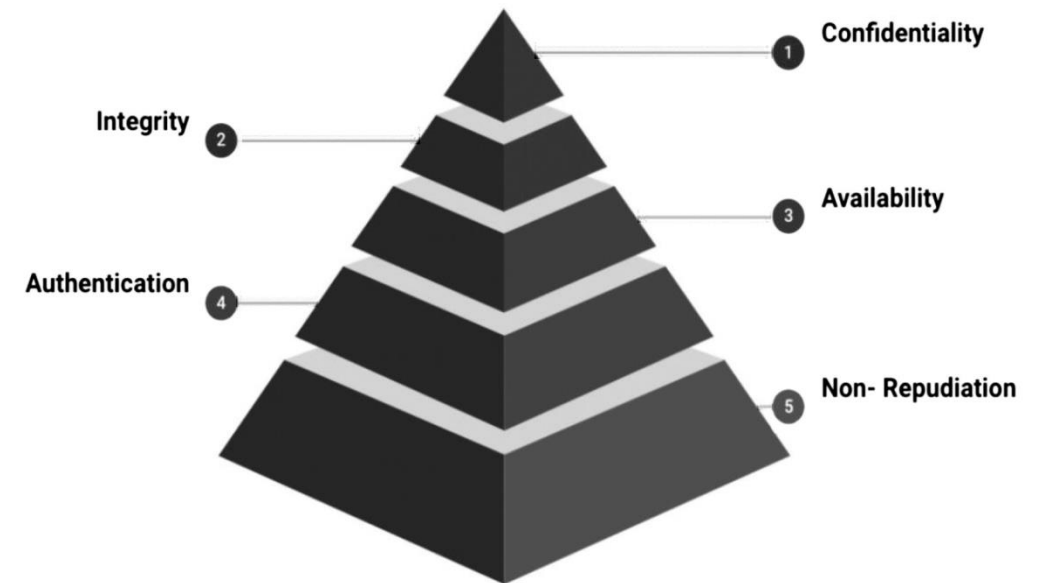
01

Ethics in Cyberspace and Cybersecurity

- The National Institute of Standards and Technology (NIST) defines **cyberspace** as the interconnection and association of networks of information technology (IT) infrastructures.
- It commands safety and reliability due to the huge amount of data traveling across cyberspace. This data may be highly sensitive. Data protection and integrity of computing assets that are a part of an organization's network are critical. Hence, there is a need to defend the assets from any kind of cyber-attacks.
- **Cybersecurity** defined as the process of preventing any damage, followed by protecting, and restoring the computers, electronic communications services, wire communication, electronic communications systems, and electronic communication.

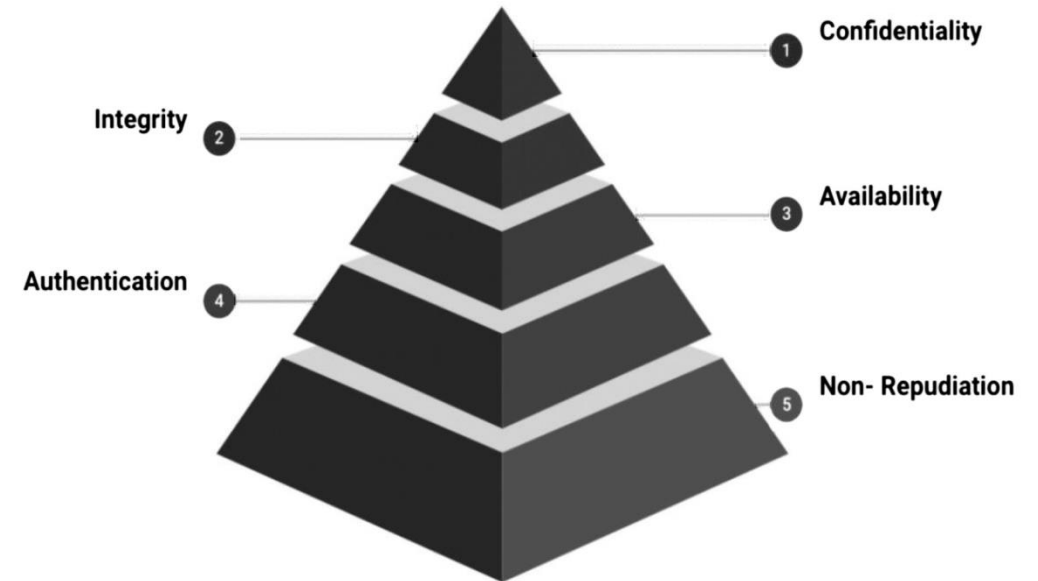
CYBERSECURITY (1/3)

- **Cybersecurity** refers to the collection of technologies, processes, and practices designed for the protection of networks, devices, programs, and data from attack, damage, or unauthorized access.
- It incorporates securing the networks, applications, information, and operations that take place over cyberspace.



CYBERSECURITY (2/3)

1. **Confidentiality:** It refers to protecting the information from disclosure to unauthorized parties. It is associated with the protection of details which should be visible or accessible to people who have appropriate privileges.
2. **Integrity:** It is responsible for ensuring trustworthiness, accuracy, and completeness of the sensitive information. The main objective of integrity is to protect information from being altered by unauthorized or unintended parties and individuals.

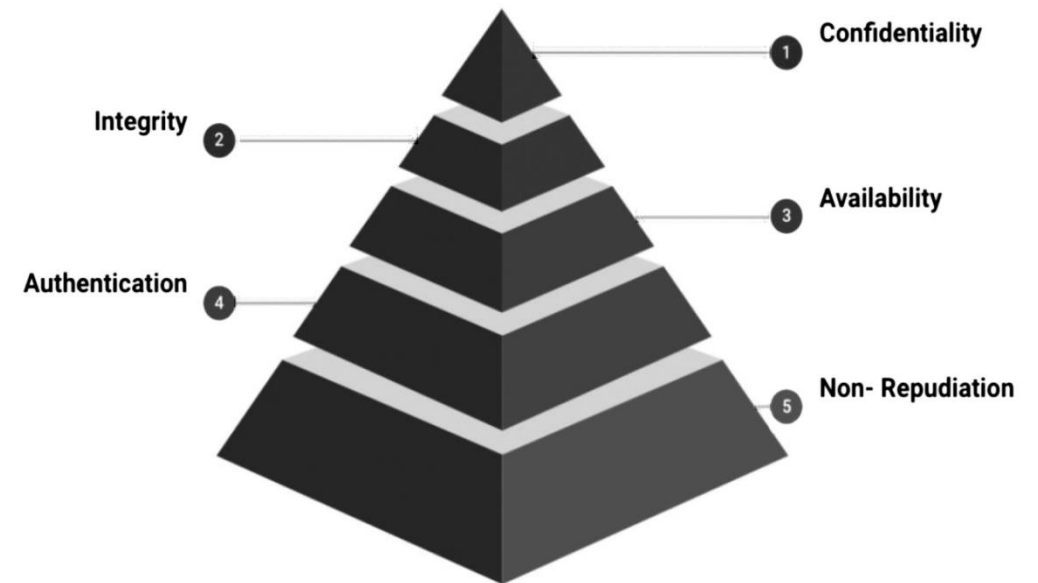


CYBERSECURITY (3/3)

3. Availability: It is responsible for ensuring that only authorized parties can access the information when at the time of need.

4. Authentication: It refers to the process of ensuring and confirming the identity of a user.

5. Non-Repudiation: It can be used to ensure that a party involved in a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.



CYBERETHICS (1/2)

- May be defined as the code of responsible behavior over cyberspace. Laws are the outcomes of Ethics. Ethics are principles that are responsible for guiding a person or society.
- They are created to decide what is good or bad, and what is right or wrong in a given situation.
- It is used for regulating a person's conduct and also assists individuals in living better lives by considering basic moral rules and guidelines.

CYBERETHICS (2/2)

Ethics in cyberspace may be described in the following ways:

1. **Cyberethics** underpins the study of ethics pertaining to computers and networks;
2. **Cyberethics** takes into account user behavior as well as what computers are programmed to do;
3. **Cyberethics** has its effects on individuals and society;
4. **Cyberethics** focuses on responsible behaviors on the internet;
5. **Cyberethics** deal with ethics applied to the Online Environment.

ETHICS, LAW, and POLICY (1/3)

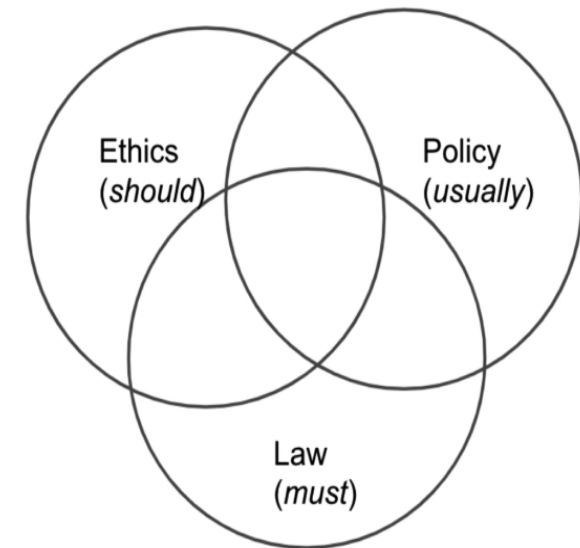
- Laws are the outcomes of ethics.
- **Cyber law** is related to **Cyberethics**:
- While **cyberethics** is concerned with providing foundations for ethical behavior in cyberspace, **Cyber law**, on the other hand, as a discipline, deals with legislations that are passed in different countries.
- **Cyber law** as a discipline, effectively strengthens the foundations of good ethical behavior. This is a requirement for **cyberethics**.
- Moreover, **cyberethics** can be significantly enhanced by deploying cyber legal frameworks, as the ethical principles on their own do not have any respective standing.

ETHICS, LAW, and POLICY (2/3)

- **Cyber Security Policy** is a formal set of rules and must be followed by people who are given access to company technology and information assets.
- The **Cyber Security Policy** serves several purposes, like defining what technology and information assets must be protected.
- It is also responsible for identifying any underlying threats to the assets.
- The **Cyber Security Policy** also describes the responsibilities and privileges that users have.

ETHICS , LAW , and POLICY (3/3)

- There is an interconnection between Ethics, Law, and Policy in the Cyberspace.
- While **Ethics** account for code of conduct and responsible behavior that should be followed in cyberspace,
- **Cyber laws** are legislations that focus on the acceptable behavioral use of technology in cyberspace and must be followed.
- **Policies** are made to achieve some goals and are therefore usually followed.



Chapter

01

PRIVACY and SECURITY (1/2)

- **privacy** and security are **comparable**.
- **Privacy** compares to any rights one has to control the personal information and how it is used.
- Security considers how personal information is protected.
- **Privacy** and **Security** often overlap in the real world; however, they are not the same



PRIVACY and SECURITY (2/2)

- When we deal with personal information, there may be three situations:
 - both **privacy** and **security** are maintained. Your personal information stays with you;
 - privacy may be compromised, but security is still maintained. Your personal information may not be only with you;
 - both privacy and security are compromised.



- Security is essentially about protection against the unauthorized access of data. It is specifically conducted by deploying security controls to limit who can access the information.
- Security is primarily concerned with the protection of data while stored, in transit, and during processing, and the related informational assets like servers and mobile devices



Chapter

01

SECURITY

- Privacy deals with an individual's right to own the data that is originally triggered by his or her life and activities, and for restricting the outward flow of that data.
- Personally identifiable information (PII), personal health information (PHI), Personal Financial Information (PFI), etc., are some private information related to a person.

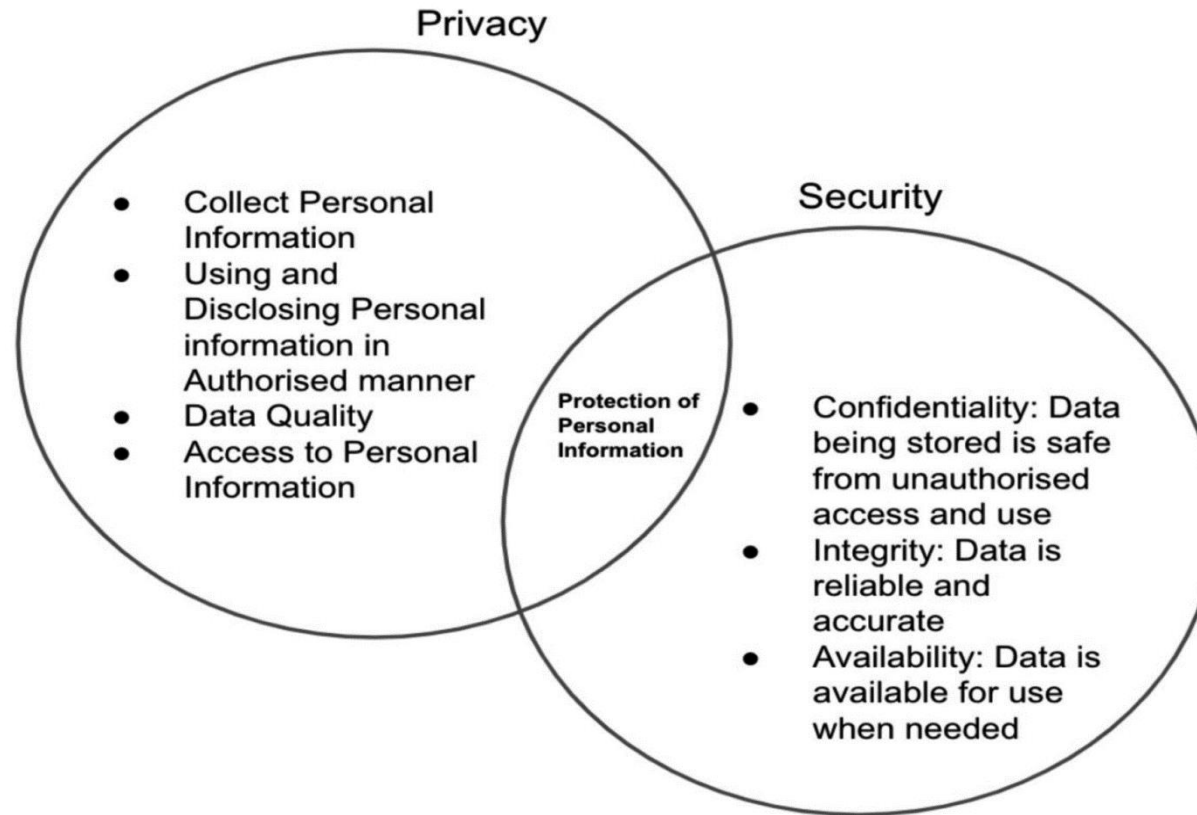


Chapter

01

PRIVACY

THE NEED FOR CYBERETHICS



PRINCIPLES OF CYBERETHICS

❑ The Internet Architecture Board has defined the following activities to be unethical and unacceptable:

1. **Activities seeking to gain unauthorized access to the resources of the internet.**
2. **Activities disrupting the intended use of the internet.**
3. **Activities that lead to wasting of resources (people, capacity, and computer).**
4. **Activities that destroy the integrity of computer-based information.**
5. **Activities that compromise the privacy of users.**

Computer Ethics 10 commandments

1. A computer shall not be used to harm other people;
2. One must not interfere with other people's computer work;
3. It is unethical to snoop around in other people's computer files;
4. A computer must not be used for stealing;
5. A computer must not be used for bearing false witness;

Computer Ethics 10 commandments

6. It is unethical to copy or use proprietary software without permission or paying for it;
7. It is unethical to access an individual's computer resources without authorization;
8. It is unethical to appropriate other people's intellectual output;
9. When writing a program or designing a system, one must think about the social consequences;
10. A computer shall always be used in ways that ensure consideration and respect for fellow humans.

What should be done morally and what should not be done ?

Based on the 10 commandments set of Principles for Cyberethics

Do's:

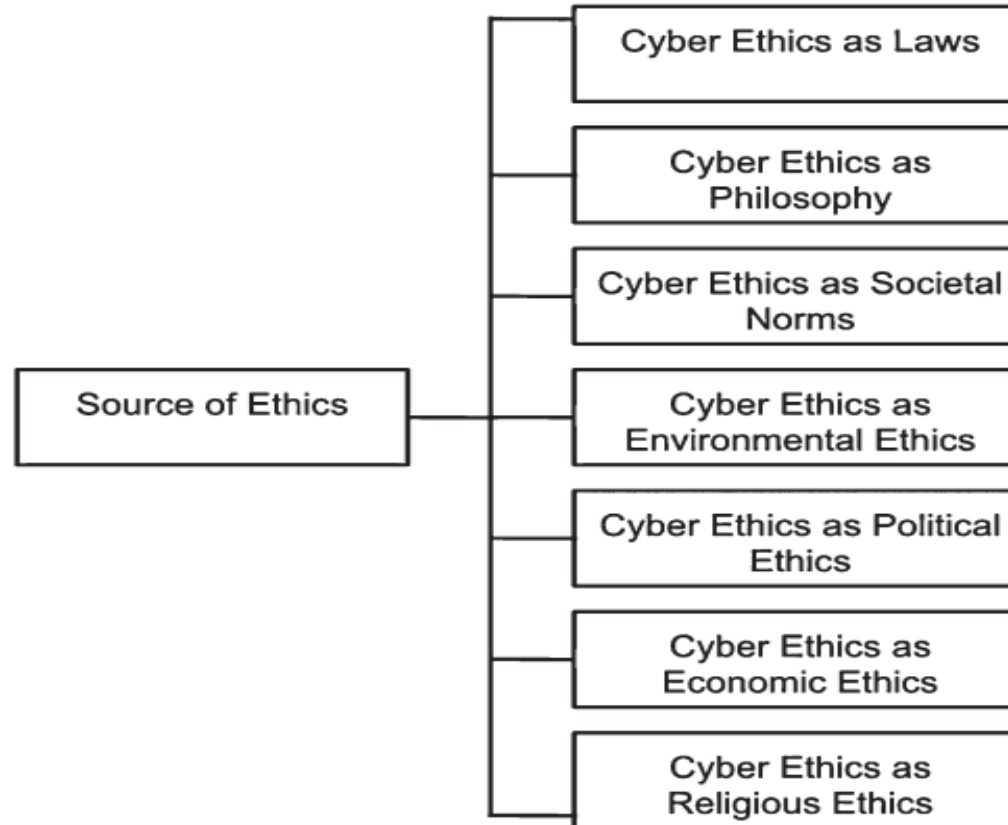
1. Think about the social consequences of writing a program and designing a system.
2. Always use a computer in ways that guarantees consideration and respect for other individuals

What should be done morally and what should not be done ?

Don'ts:

1. Use a computer for harming other people.
2. Interfere with other people's computer work.
3. Snoop around or access other people's computer files.
4. Use a computer for stealing.
5. Use a computer for bearing false witness.
6. Copy or use proprietary software without paying or obtaining permission.
7. Use other people's computer resources without authorization.
8. Appropriate other people's intellectual output.

SOURCES OF ETHICS: WHAT MAKES SOMETHING ETHICAL OR UNETHICAL IN CYBERSPACE?



SOURCE OF ETHICS (1/7)

❑ Cyberethics as Laws:

- It refers to the fact that specific laws are derived from ethics.
- Cyber law and Cyberethics are interconnected and dependent on each other.
- The increasing significance of cyberspace may further bring complex legal, policy, and regulatory issues.
- The need for cyberethics to be strengthened by Cyber laws.

SOURCE OF ETHICS (2/7)

❑Cyberethics as Philosophy:

- It explores the philosophical aspect behind ethics that includes life between birth and death.
- Gaining unauthorized access to someone's account or compromising the privacy of an account are situations that are unethical and Ethics as Philosophy could avert such situations.

SOURCE OF ETHICS (3/7)

❑ Cyberethics as Societal Norms:

- It deals with Community Ethics. These underpin questions of bad and good of social media, how it has an impact on the community life and chances of global communication.
- It also takes into account abuse in terms of cyber bullying, mobbing, etc. It manifests the core values and virtues that usually have their source in the family.

SOURCE OF ETHICS (4/7)

❑ Cyberethics as Environmental Ethics:

- It deals with the impact of cyber technology on human-nature relations.
- It also highlights the environmental negative impact of energy use as well as the positive impact of environmental advantages of weather forecast, scientific research, etc.
- It deals with questions like whether it is ethical to jeopardize natural resources in order to carry out research.

SOURCE OF ETHICS (6/7)

❑ Cyberethics as Economic Ethics:

- It explores the positive and negative impacts of cyberspace.
- The factors taken into account are economic growth, job creation or job losses, financial investments in cybersecurity research, etc.
- The financial sector is frequently hit by data breaches and monetary losses.
- Economic Ethics could be followed while dealing with such situations.

SOURCE OF ETHICS (7/7)

❑Cyberethics as Religious Ethics:

- It looks at the ethical and unethical impact of cyberspace on culture, music, art, dance, language diversity, cultural inclusion or discrimination, religious respect or hate messages through the internet, etc.
- Social media provides platforms for religious and cultural disputes. Keeping in mind Religious Ethics may be a way of avoiding it.



Thank You