

Cybersecurity Law, Policy and Ethics

Prepared by **Dr. Kamal Alieyan**
Lecture 04

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يبنى مبدأ المجتمع التعليمي
التعاوني ويخدم العلم مقابل العمل للتربية وبناء المجتمعات

Cybersecurity Ethics: Cyberspace
and Other Applications_(1)



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture Objective

- Target more aspect of cybersecurity ethics.
- The cybersecurity is an advancing field and makes its presence felt in various other domains and applications, we will highlight ethics in those domains and applications.

Lecture topics

- 3.1 CYBERSECURITY ETHICS: A DETAILED STUDY (DOMINS)
- 3.2 CYBERSECURITY ETHICS IN APPLICATIONS

Lecture topics

- 3.1 CYBERSECURITY ETHICS: A DETAILED STUDY (DOMAINS)
- 3.2 CYBERSECURITY ETHICS IN APPLICATIONS

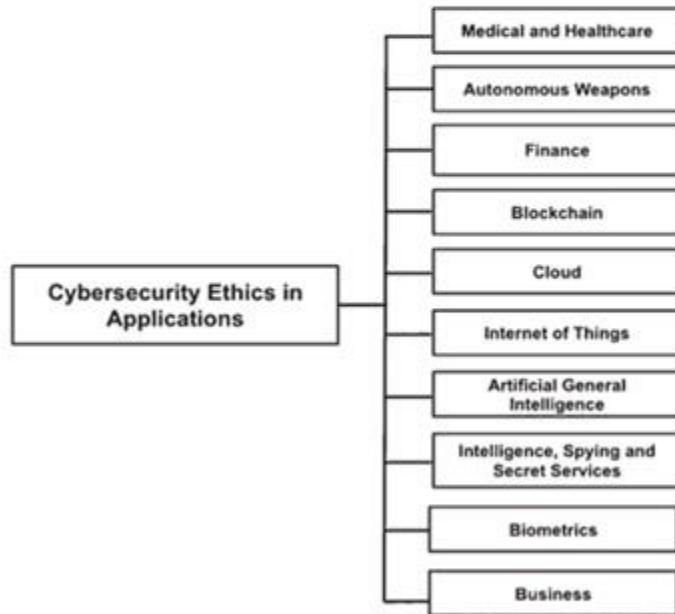


FIGURE 3.2 Cybersecurity ethics in applications.

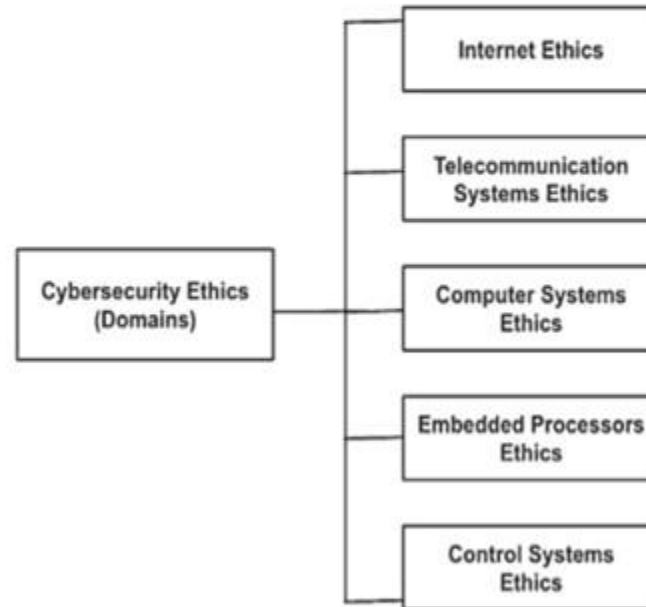


FIGURE 3.1 Cybersecurity ethics (domains).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

- **Cyberspace** incorporates the Internet, telecommunication systems, computer systems, embedded processors, and control systems.
- Each of these domains have specific functionalities and operates in various ways.
- Thus each of these have their own ethics and standards.
- Each of these components are responsible for establishing cyberspace and their applications traverse the globe.
- Therefore, a detailed study on ethics for these components is of great significance.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

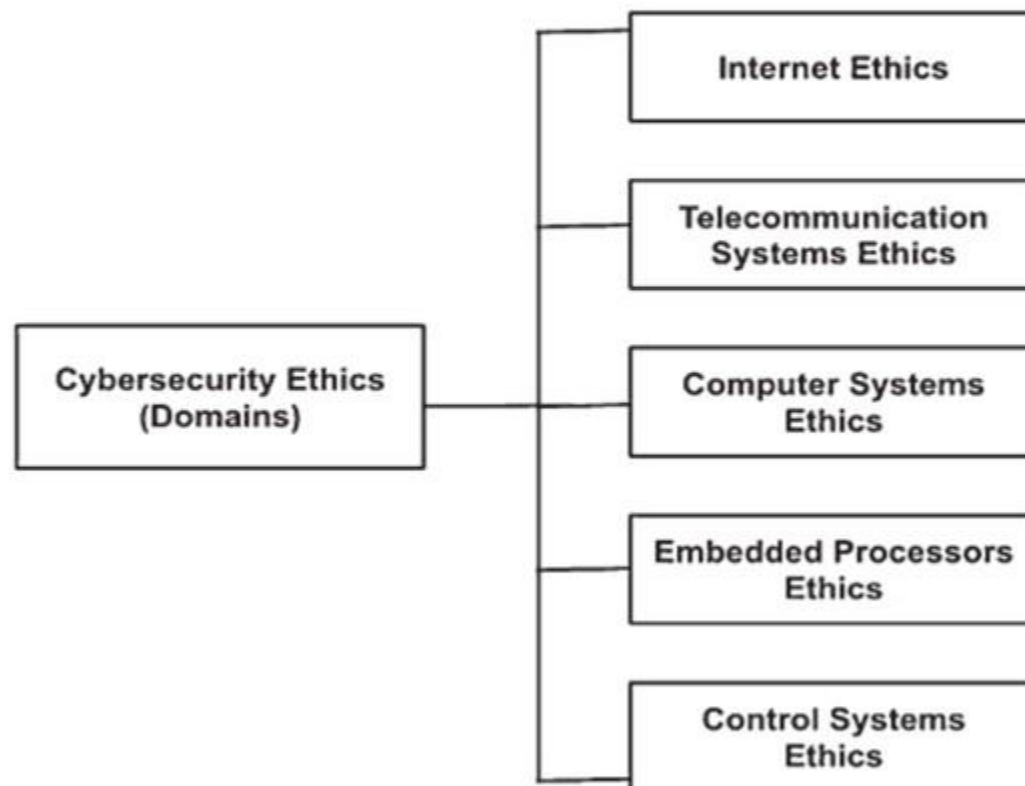


FIGURE 3.1 Cybersecurity ethics (domains).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- One of the most remarkable and active components of cyberspace is the Internet.
- In fact, the majority of the communication among devices and users takes place over the Internet.
- Since the Internet harbors millions of users and devices, exchange of information over the platform must be performed in an ethical way.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- Definition of the Internet:
 - ☐ The Internet might be characterized as a method for interfacing a computer to any other computer anywhere in the world by means of dedicated routers and servers.
 - ☐ At the point when two computers are associated over the Internet, they can send and receive a wide range of information like text, design, voice, video, and computer program.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- Many times ethics over the Internet referred as Internet Etiquette or Netiquette.
- As Etiquette corresponds to the code of polite behavior in society, netiquette concerned with code of good behavior on Internet.
- Netiquette takes into account various aspects of the Internet, like email, social media, and web forums. Also, online chat, website comments.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.1 CYBERSECURITY: INTERNET ETHICS

- There are no specific netiquette rules or guidelines, however the overall idea is to respect others online:
 1. Remember the Human
 2. Following the Same Standard of Behavior online as in Real life
 3. Knowing that You are in Cyberspace
 4. Appreciating the Other Peoples Time and Bandwidths
 5. Making your self Good online
 6. Sharing Expert knowledge
 7. Helping Keep Flame Wars Under Control
 8. Respecting Other People's Privacy
 9. Not Abusing Power
 10. Be Forgiving of Other People's Mistakes
- Good netiquette is useful for everyone in Cyberspace, and it ensures a healthy environment.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- Definition of Telecommunications:

- ☐ Telecommunications is referred to as the transmission of information. This information may be in the form of signs, signals, messages, words, writings, images, and sounds.
- ☐ The information is usually transmitted through means of a wire, radio, optical or other electromagnetic systems.
- ☐ Telecommunication occurs when there is an interchange of information between communication parties which includes the use of technology.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- A telecommunications system operates as a cluster of nodes and links to facilitate telecommunication.
- Telecommunication incorporates **three important aspects**, namely information, communication, and technology, and they are related to one another.
- **Information** is produced due to an interpretation process. Usually, a receiver interprets data during a specific time-space based on the total amount of knowledge and experience of the receiver.
- **Communication** may be defined as the interaction between elements and the repercussion of the effect that the performance of one element has on the performance of another element.
- **Technology** is a field of knowledge and skills that includes design, construction, and use of created artifacts, and the theoretical science of technology itself.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- When technology-based environments are considered, and the complexity that emerges in the cross between humans, between technology and humans, and between information, communication, and technology, a cultural focus emerges where human attitudes, values, and behavior sets the conditions for communication and interaction.
- Inside the ethical circle of information, the issue of suitable or right conduct related to information, creation of information, and transfer of information is considered primarily.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- In a changing technological infrastructure, ethical considerations have an effect on the outcome of human communication.
- Common norms and rules must be respected to enable humans to live and act together in Cyberspace.
- Rules or norms can be both explicit and implicit.
- Society depends on technology. This dependence brings to the fore ethical considerations of its design, use, and implementation.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.2 CYBERSECURITY: TELECOMMUNICATION SYSTEMS ETHICS

- One way of dealing with ethics when designing ICT environments is through a framework for ethical guidance in development projects and the design of information systems.
- The framework includes a method with four steps:
 - Identify the different needs that can be associated with the situation;
 - Identify where conflicts may occur;
 - Solve the problems that can cause conflicts;
 - Let the common needs to be included in a requirement catalog and perform a requirement analysis for the situation to be designed.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

- All the operations in Cyberspace take place due to the interaction of computer systems over the network.
- Definition of Computer Systems
 - ☐ Computer systems are shaped by an arrangement of interconnected systems that share a central storage system.
 - ☐ It also supports various peripheral devices like printers, scanners, and routers.
 - ☐ Every system associated with the system can work autonomously, however, it can communicate with other external devices and computers.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

- Cyberspace continues to grow as more and more computer systems are added.
- More computer systems mean increased usage as well as more communication among users.
- Therefore, it is mandatory to take care of ethical considerations in Cyberspace with respect to computer systems.
- Some ethical considerations are as follows:
 1. **Contributing to Society and Human Well Being:** While designing or implementing systems, it is mandatory that computer experts guarantee that the results of their endeavors will be utilized in socially mindful manners, will address social issues, and will stay away from destructive impacts to wellbeing and welfare.
 2. **Avoiding Harm to Others:** The use of computing technology should not harm users, the general public, employees, employers. Harmful actions incorporate intentional destruction or modification of files and programs. This may have severe consequences in the form of serious loss of resources and unnecessary expenditure of human resources (HR).

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

3. **Being Honest and Trustworthy:** Honesty and trust go hand in hand. For an organization to function effectively, trust is very important. Honest computing professionals do not make intentionally bogus or tricky cases about a system or system design. Rather, they give complete honesty of all appropriate system constraints and issues.
4. **Being Fair and Taking Action Not to Discriminate:** Discrimination between different groups of people may be the result of use or misuse of information and technology. All individuals are entitled to equivalent opportunity to participate in, or take advantage of, the utilization of computer resources irrespective of their race, sex, religion, age, disability, national origin, or other such comparative elements. These standards, however, do not legitimize unapproved access and utilization of computer resources. Further, they do not give an adequate motivation to infringement of some other ethical objectives of this code.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

5. **Honoring Property Rights Including Copyrights and Patents:** Violating copyrights, patents, trade secrets, and the terms of license agreements is prohibited by law in most circumstances. The violations are contrary to professional behavior even if the software is not so protected. Copies of software must be made and distributed only with proper authorization. Unauthorized duplication of materials must be discouraged.
6. **Giving Proper Credit for Intellectual Property (IP):** Computing experts must ensure the integrity of protected innovation. Hence it is not ethical to assume acknowledgment for other's ideas or work, even in situations where the work has not been unequivocally ensured by copyright, patent, and so on.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.3 CYBERSECURITY: COMPUTER SYSTEMS ETHICS

7. **Respecting the Privacy of Others:** This principle is significant for electronic communications, including electronic mail. It denies strategies that capture or monitor electronic client information, including messages, without the consent of clients or approval identified with system activity and support. Client information must be treated with strictest secrecy, aside from in situations where it is proof for the infringement of law or authoritative guidelines. In such cases, the nature or contents of the sensitive information must be disclosed only to proper authorities under the right circumstances.
8. **Honoring Confidentiality:** Honesty and confidentiality are interconnected. It is necessary to honor confidentiality. Computer professionals must regard all commitments of secrecy to employers, customers, and clients except if released from such commitments by necessities of the law or different standards of this code.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- An embedded system may be thought of as a combination of computer hardware and software, which is either fixed in capability or programmable, designed for a specific function or functions within a larger system.
- Embedded system hardware can be microprocessor- or microcontroller-based.
- Definition of Embedded Processor:
 - ☐ An embedded processor is primarily a microprocessor designed into a system that is responsible for controlling electrical and mechanical functions.
 - ☐ An embedded processor can be programmed specifically for the specific operations.
 - ☐ It may support many different CPU (central processing unit) architectures.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- Since embedded processors are deep-seated in critical hardware, such systems can be remarkably tricky to safeguard. Hence cybersecurity and cyber resiliency must be considered toward the start of the plan and design process.
- Embedded processors are known to be powerless against cyber-attacks because of a few reasons, which may go from the electronic system's capacity to withstand cyber threats to the side effects of processor pipeline designs to empower cyber-attacks.
- In addition, fixes may bring about inadvertent impacts, including expanding power utilization and influencing processing or timing, all of which can constrain hardware performance. Therefore, ethical considerations must be kept in mind while designing such embedded processors.

3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- This is important since each person involved in the working of an embedded system acts assuming that the other team members have done their job properly, e.g., a captain sails a ship accepting the originator/designer/maker have planned, created, responsibility and that the ship control works perfectly, etc.
- It is the ethical obligation of all team members to release their obligations with the most noteworthy honesty and meticulousness.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.4 CYBERSECURITY: EMBEDDED PROCESSORS ETHICS

- Each individual included must adhere to the most elevated moral norms to forestall the odd practices inside his/her obligation:
 1. **Communicating Information Responsibly:** When there are many team members, there is a collective obligation that requires the architects/engineers/makers, clients, and software writers to interface capably, particularly without ambiguity, to guarantee the safe operations of the embedded processors. Protocols with respect to communication must be created for this reason, and correspondence must be kept up in any event until the activity of the processors is steady.
 2. **Attributing Responsibility to Software:** Embedded systems must be accompanied by suitable (self) regulatory mechanisms that will guarantee their moral conduct.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- Control systems are an integral part of the automation industry.
- Different control loops that regulate these processes may be in the form of industrial control systems (ICS).
- Supervisory control and data acquisition (SCADA) and distributed control systems (DCS) are some examples of control systems.
- **Definition 3.5: Control Systems**
 - ☐ A control system is made of a set of mechanical or electronic devices that controls other devices or systems using control loops.
 - ☐ It consists of many elements that may be combined together to form a system for producing desired outputs.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- The advancement of Control systems has significantly increased the cyber-attack surfaces.
- The challenges may be in forms like increasing cyber threats, lack of visibility and control, difficulty in securing control layer protocols and unsecured networks.
- Therefore, addressing the issues from an ethical point of view is mandatory:

1. Machine Design Ethics:

- Machine ethics are to be considered from the earliest starting point of the research work and the meaning of the necessities, past classical safety studies.
- For each stage of the machine design process, it is advised to realize a risk assessment and to implement redundant technological barriers to contain possible machine ethical risks.
- It is important to consider how the designed control system could be misused by error or rendered harmful (hijacked) using cyber-attack technologies, for example.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

- 2. Human-Centered Approach:** Researchers must design the control system using a human-centered approach rather than a techno-centered one. This will guarantee utilizing the possible capacity of people when confronting the unexpected while at the same time confining automatic and deliberate abuses of the control system.
- 3. Design Process:** It is encouraged to define a ventured design process, containing distinctive approval stages. Although it is a classical design way, adding exaggerated tests at each of the steps could be yet another approach. This approach would be beneficial for testing the robustness of the designed elements facing exaggerated risks, before the final targeted implementation of the control systems



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

4. **Safety, Responsibility, and Liability:** Safety aspects should be one of the primary concerns such that control systems and humans can work together without accidents. Since control systems increasingly operate in close proximity to humans, safety is very important. Control systems are not only large and complex, but also intelligent and self-learning. But it is equivalently important to understand that these systems may fail, and neither the systems nor humans can be blamed for it. Besides, it is much harder to locate the underlying reason and attribute liability. It is equally hard to find who is accountable for the failures and malfunctions. Therefore, these questions need to be addressed from an ethical point of view.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

3.1.5 CYBERSECURITY: CONTROL SYSTEMS ETHICS

5. Privacy Concerns:

- Control Systems require immense measures of information to work successfully, and this poses several privacy questions.
- For instance, in order to build smart home security systems, smart home systems need to keep track of the times when residents are away. This information may be private, but valuable for burglars. Robots spying on the working habits of their human co-workers may be yet another privacy concern since they may manipulate humans to work harder.
- The ethics behind reviewing medical professional secrecy concerning the health data stored on connected parts of medico-technical systems also raises many privacy concerns and questions.
- Thus, collecting data on an individual's lifestyle and physical parameters may contribute towards improving their health, but it is not ethical to take advantage of the data shared on medico-technical systems.



3.1 CYBERSECURITY ETHICS: A DETAILED STUDY

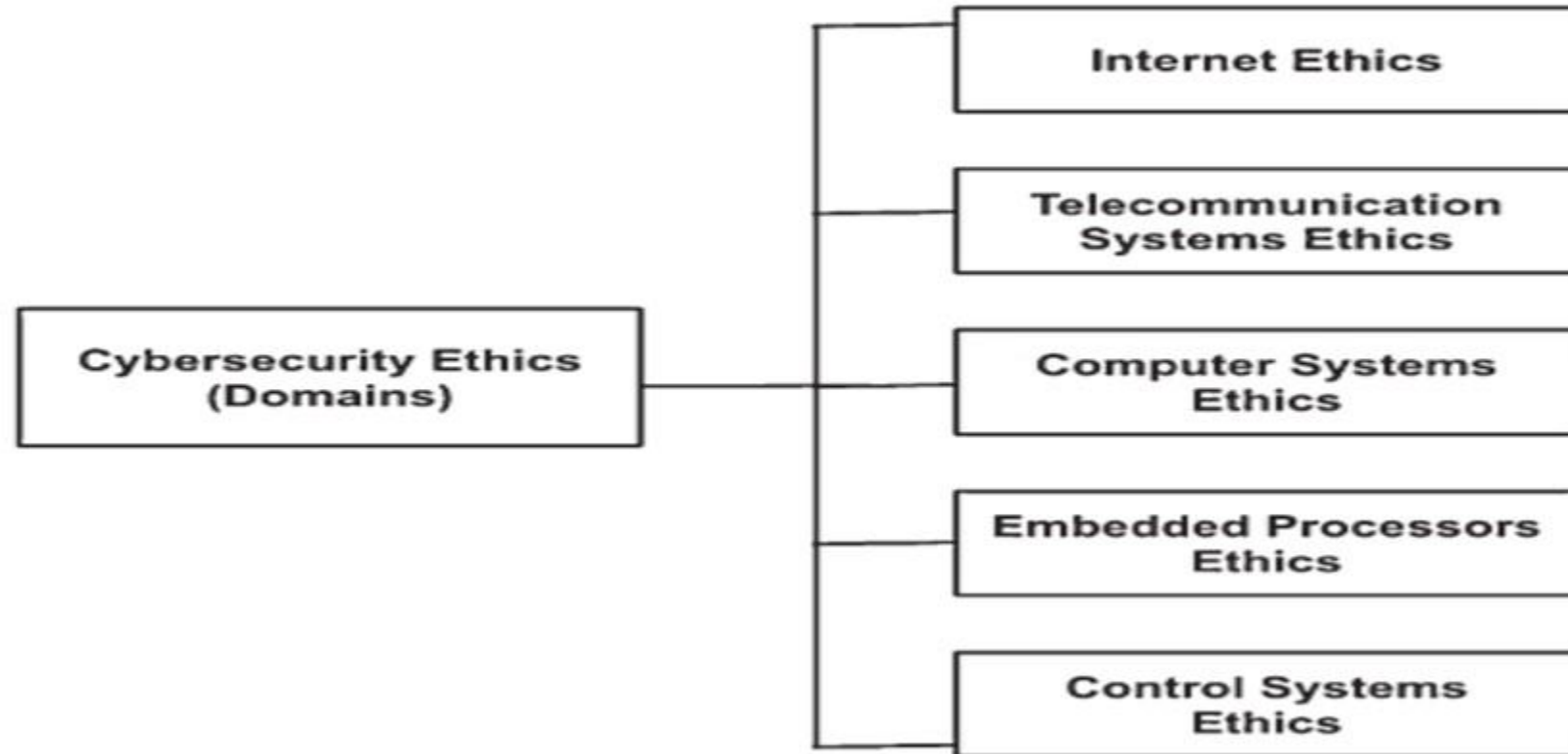


FIGURE 3.1 Cybersecurity ethics (domains).

3.2 CYBERSECURITY ETHICS IN APPLICATIONS

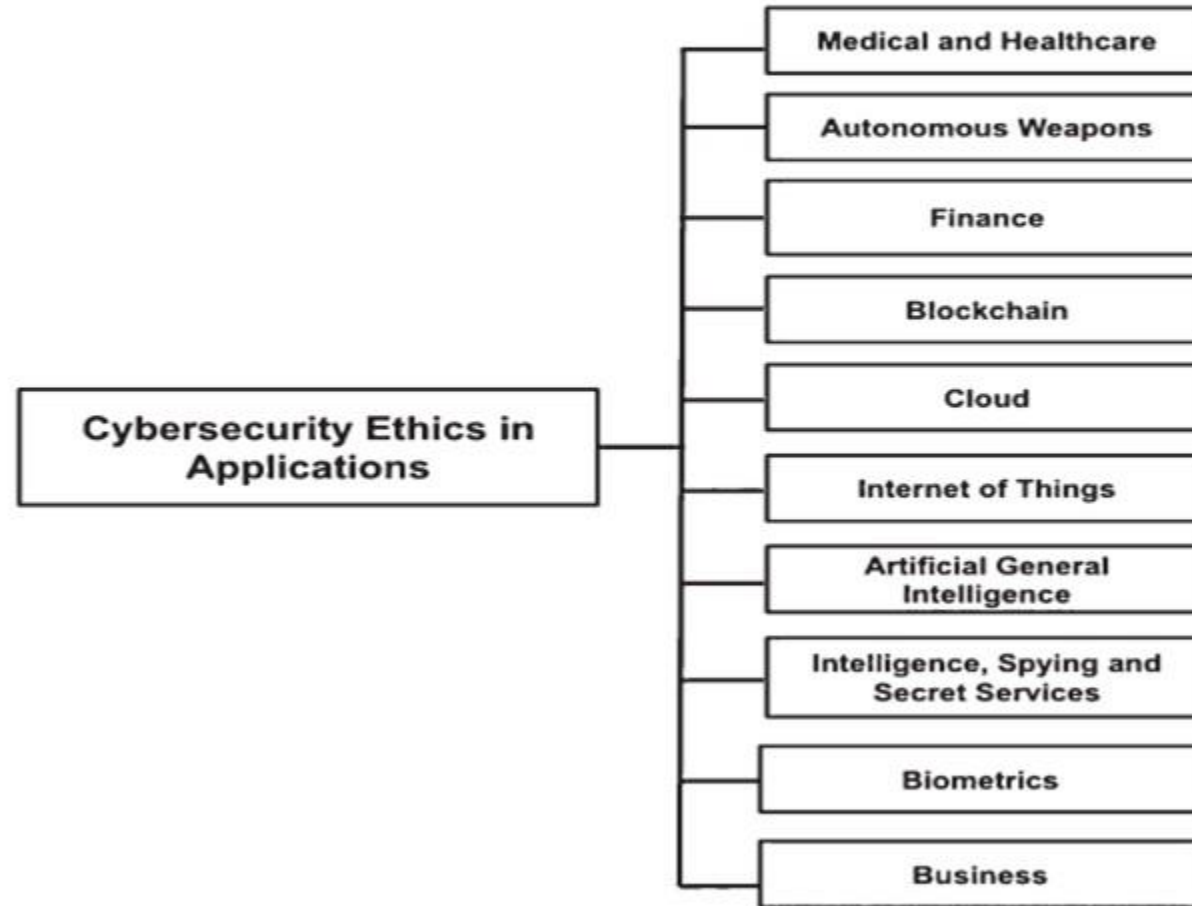


FIGURE 3.2 Cybersecurity ethics in applications.

THANK YOU

