

Cybersecurity Law, Policy and Ethics

Prepared by **Dr. Kamal Alieyan**

Lecture 03

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Ethical Issues in Cybersecurity



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture objective

- Focusing on the ethical issues that are present in cybersecurity as well as cyberethics frameworks.

Lecture topics

- Ethical Issues in Cybersecurity: Overview
- Types of Ethical Issues in Cybersecurity
- Specific Ethical Issues in Cybersecurity
- Fair Use Doctrine
- The Origin of Cybersecurity Ethics

Ethical issues in cybersecurity: overview (1/3)

- Ethics consider the moral principles that govern a person's behavior.
- Without clear ethical standards and rules, it may not be easy to tell apart cybersecurity professionals from the black-hat criminals against whom they seek to protect systems and data.
- Thus, ethics are a critical part of cybersecurity.



Ethical issues in cybersecurity: overview (2/3)

- The world of cybersecurity is full of ethical challenges, some of which are as follows:
 - **Vulnerability Disclosure:**
When and how should researchers or professionals inform the public about a newly found vulnerability.
 - **Encryption Issues:**
What should be done when law enforcement requests for encrypted data.
 - **Automated Security Tools:**
If it is ethical to release tools that may assist in automating attacks on many systems in the cyberspace and beyond.



Ethical issues in cybersecurity: overview (3/3)

- The world of cybersecurity is full of ethical challenges:
 - **Sale Restrictions:**
What could be the responsibility of cybersecurity professionals for trying to prevent the sale of products they have developed to autocratic governments that may possibly be used to mistreat their citizens?
 - **Incident Responses (IR):**
What is an appropriate level of incident detail to share with customers and other stakeholders?
 - **Roles and Responsibilities:**
What are the roles in your IT department and what are the responsibilities associated with each of those roles?



Types of ethical issues in cybersecurity (1/4)

- The domain of cybersecurity has spanned across several industries related to medicine, education, commerce, government, entertainment, and society at large.
- While it is largely responsible for securing networks, infrastructures, systems, etc. It also invites potential risks.
- Moreover, it presents and makes a few issues identified with morals, and contains three fundamental kinds of moral issues: personal privacy, access rights, and harmful actions
- Let's explore the ways in which they affect society and technological changes.



Types of ethical issues in cybersecurity (2/4)

Personal Privacy

- Cybersecurity, in terms of privacy, allows the exchange of information over cyberspace to different individuals and organizations, to any location of the world, at any given time.
 - Thus, there is an added potential of information disclosure and privacy violation of individuals and organizations due to data diffusion worldwide.
 - Thus, the real challenge is to ensure data privacy and integrity.
- Since this falls within the boundary of ethics, certain precautions may be taken to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals.



Types of ethical issues in cybersecurity (3/4)

Access Rights

- The authorizations an individual client or a computer application holds that permits them to peruse, compose, alter, erase or in any case get to a system record, change arrangements or settings, or remove applications.
- An organization's network or the administrator can define permissions for files, servers, folders, or specific applications on the computer.
- As cyberspace also encourages commerce, access rights are an important issue in cyberspace. Security breaches are normal and large organizations and government associations are at the danger of security assaults.
- Therefore, the implementation of proper security policies and strategies is mandatory. Setting up permissions and access rights confines security attacks to a certain extent.



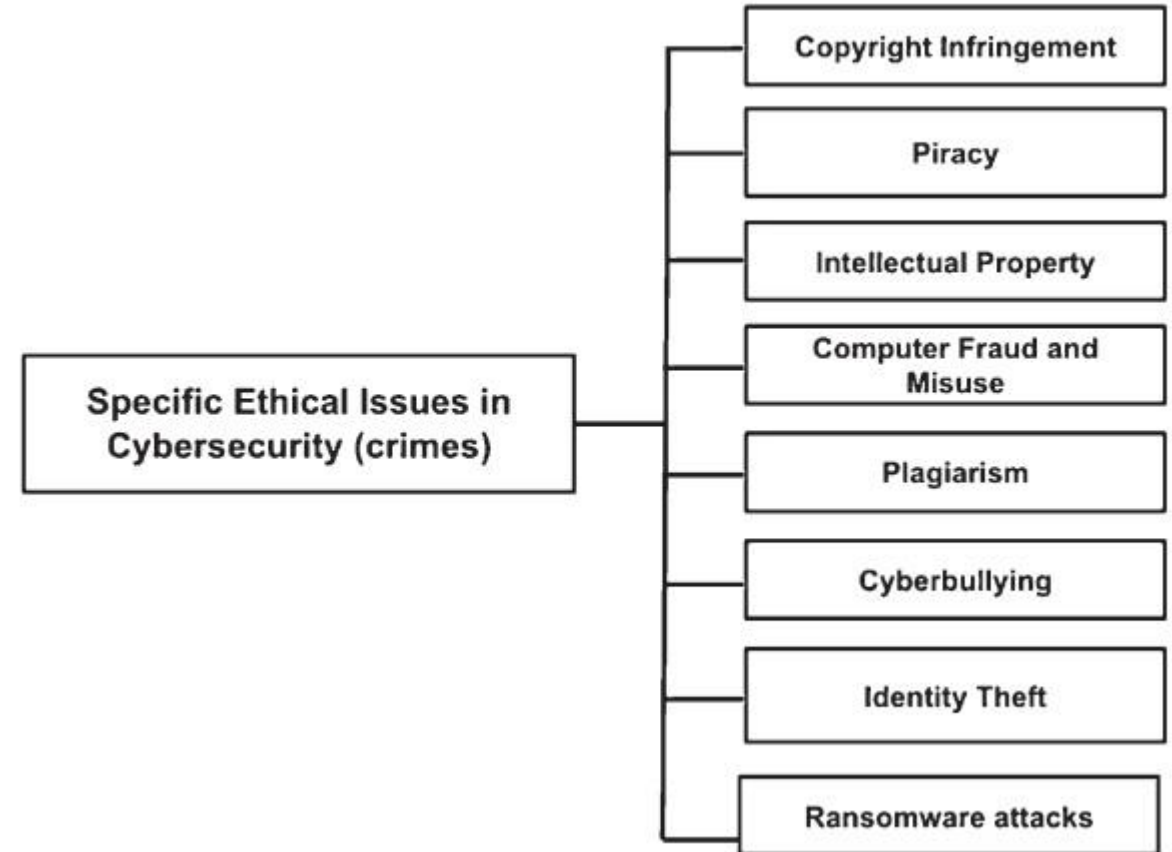
Types of ethical issues in cybersecurity (4/4)

Harmful Actions

- Harmful actions can prompt injuries or negative consequences.
- Some negative consequences pertaining to the same are undesirable loss of information, loss of property, property damage, or unwanted environmental impacts.
- Cybersecurity attacks may lead to such harmful actions.
- **Harmful actions** may also lead to the destruction or modification of files and programs.
- This principle is responsible for prohibiting the use of computing technology that may harm users, the general public, employees, and employers.

Specific Ethical Issues In Cybersecurity (1/14)

- Some specific ethical issues that have cropped up in cybersecurity over the last few years.
- These issues are prevalent in cybersecurity, we also talk about some cases that underpin these ethical issues.
- The following are specific ethical issues in cybersecurity.



Specific Ethical Issues In Cybersecurity (2/14)

Copyright Infringement

- The utilization or creation of copyright-ensured material without the consent of the copyright holder.
- It occurs when a third party breaches the rights afforded to the copyright holder.
- The right could be in the form of an exclusive use of a work for a set period of time.
- The most common copyright infringement in the entertainment industry is in the form of music and movies as they suffer from significant amounts of copyright infringement.
- When new works are developed by individuals and companies, copyright protection is often considered. This ensures that individuals and companies can exclusively profit from their efforts.



Specific Ethical Issues In Cybersecurity (3/14)

Piracy

- Happens because of the unapproved duplication of copyrighted substance that is then sold at significantly lower costs.
- Recently, with the ease of technology, piracy has gotten more common.
- For instance, CD writers are accessible at exceptionally low costs, and music piracy is common in the entertainment industry.
- Music organizations' incomes are hit hard by the overwhelming number of pirated discs and cassettes. This is because of lower costs compared with that at stores.
- So, with this unethical practices of music piracy, many organizations work towards identifying sources of music piracy. Once the sources are identified, they are often confronted with the help of the police.
- However, since convictions are few and the penalties not harsh enough, piracy continues to prevail.

Specific Ethical Issues In Cybersecurity (4/14)

Intellectual Property (IP)

- Intellectual property (IP) may be thought of as ownership of an idea or design by the person who came up with it.
- It may also refer to creations of the mind like inventions.
- Many literary and artistic works as well as designs and symbols could become IP.
- Sometimes names and images used in commerce are also considered IP.
- In order to protect an idea that may not be stolen by someone, one or more of the four different types of IP may be considered.



Specific Ethical Issues In Cybersecurity (5/14)

Intellectual Property (IP)

- There are four types of IP:
 1. **Trade Secrets:** These are valuable information that are not publicly known and of which the owner has taken sensible and rational steps to maintain secrecy.
 2. **Trademarks:** These protect brands. Trademark is the name of the product linked to a product or a service.
 3. **Copyrights:** These are means to protect original works of authorship that may have been authored and written down on a piece of paper or stored electronically.
 4. **Patents:** It is one more type of licensed innovation. Patents grant their owners the legal right to disallow others from making, utilizing, selling, and bringing in a creation for a constrained time of years.

Specific Ethical Issues In Cybersecurity (6/14)

Different types of Intellectual Property

Trade Secrets

Protects Secret
Information
For ex : New Invention,
Coca Cola formula

Trademarks

Protects brands
For ex : Apple for cell
phones

Copyrights

Protects works of
authorship
For ex : books, movies,
drawings

Patents

Protects functional or
ornamental features
For ex : swipe feature or
iPhone design



Specific Ethical Issues In Cybersecurity (7/14)

Computer Fraud And Misuse

- The act of using a computer to access or alter electronic data.
- It usually occurs when a person uses the Internet through a computing device to obtain something valuable to the individual.
- This information may come from a personal computer, government facility or a company.
- For Computer fraud to occur, the person may be able to access and enter a protected computer which is not owned by them;
- With computer fraud, the individual may either access the device without authorization or exceed the timeframe of authorization given by the company;



Plagiarism

- an act of fraud, simply involves taking someone else's work or ideas and using them as your own without giving any credits to the legal possessor or receiving permission before taking the material.
- It involves directly cloning or replicating and then presenting an existing production without proper citation or referencing.
- Paraphrasing without citing, copy, and paste plagiarism, patchwork plagiarism and self-plagiarism are some examples of plagiarism.



Plagiarism

Some forms of plagiarism are as follows:

1. **Direct Plagiarism:** This involves word-to-word transcription of someone else's work without attribution. Direct plagiarism does not involve any quotation marks. Exclusion of quotation marks while performing direct plagiarism is unethical.
2. **Self-Plagiarism:** It occurs when an individual hands over his or her own preceding work, or combines parts of preceding works, without acquiring permission from all authorities involved.
3. **Mosaic Plagiarism:** It is said to occur when an individual borrows phrases from a source unaccompanied by quotation marks.
4. **Accidental Plagiarism:** It is said to occur when individuals disregard citing their sources, or misquote their sources, or accidentally reword a source by using similar words, groups of words, or sentence structure without attribution.

Specific Ethical Issues In Cybersecurity (10/14)

Cyberbullying

- The use of electronic communication for bullying a person.
- It basically includes sending messages of a threatening, intimidating, or compromising nature to the person in question.
- Cyberbullying has been known to occur through SMSs (short message service), text, and apps, or online in social media, forums, or gaming.
- These are the platforms where people can view, participate in, or share content. Hence, it is easy to send, post, or share negative, harmful, false, or mean content about someone else.
- With cyberspace being a home to millions of users, cyberbullying is a common issue that is concerned with cyberethics.

Specific Ethical Issues In Cybersecurity (11/14)

Cyberbullying

- Cyberbullying is extremely unethical due to several reasons.
- It not only affects the victim but also the victims' family and friends if something goes very wrong.
- By using new media, it's simple to irritate, undermine, hurt, embarrass, and defraud another with the expectation to cause mischief, distress, and intimidation.
- We know that harmful actions towards an individual call for ethical issues.
- Cyberbullying is capable of leaving psychological scars on victims, filling them with low confidence and a higher danger of sorrow, uneasiness, and different stress-related issues.



Specific Ethical Issues In Cybersecurity (12/14)

Identity Theft

- The fraudulent act of obtaining the personal or financial information of another person.
- It is performed by assuming that person's name or identity.
- It is usually done to make transactions or purchases.
- There are different types of identity thefts like criminal, medical, financial, and child identity theft.
- Criminal identity theft witnesses a criminal misrepresent himself as another person during arrest for the purpose of steering away from summons.



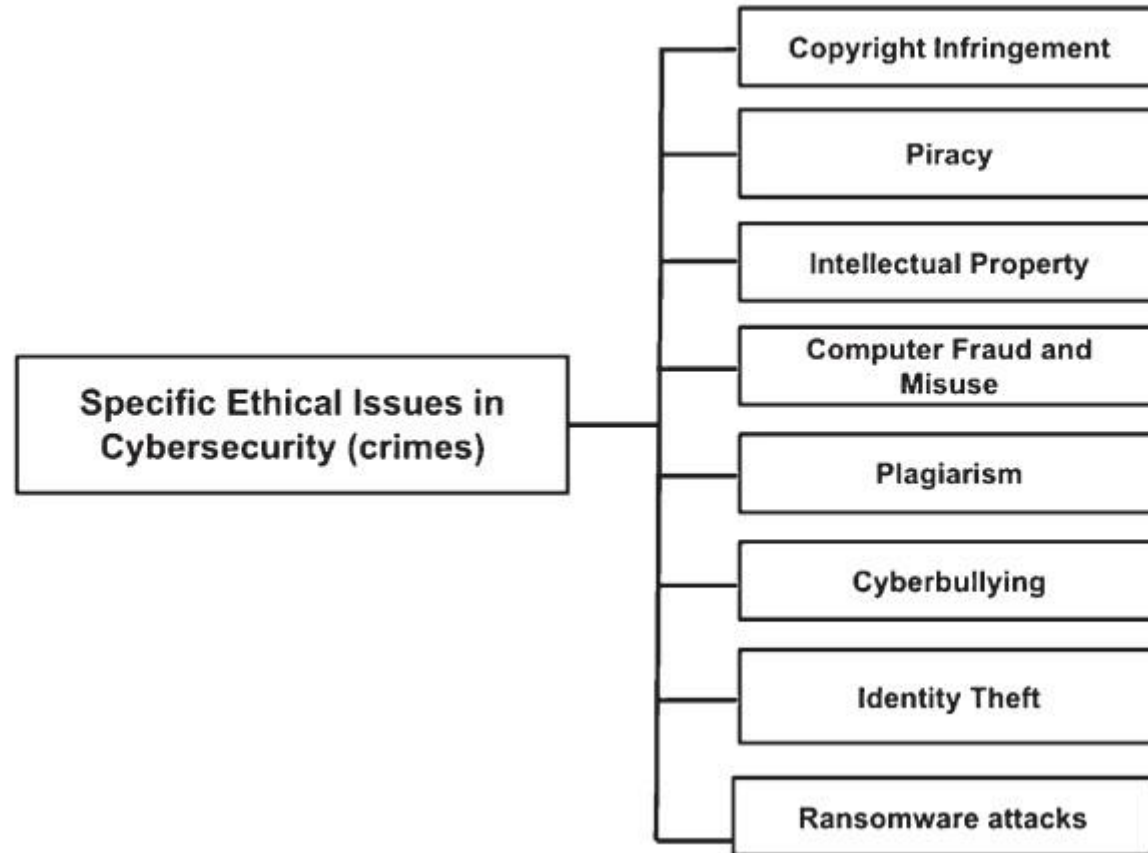
Specific Ethical Issues In Cybersecurity (13/14)

Ransomware Attacks

- Ransomware is a type of malware that is equipped for encrypting files and documents.
- Once the victim's files are encrypted, the attacker demands a ransom from the victim to restore access to the data after payment.
- Explicit directions with respect to payment to get to the decryption key are followed and the expenses may range from a couple 100 dollars to 1000.
- The cost is usually paid in cryptocurrencies.



Specific Ethical Issues In Cybersecurity (14/14)



FAIR USE DOCTRINE (1/2)

Fair Use Doctrine

- Authorizes restricted use of copyrighted material without the need to acquire permission from the copyright holder.
- It is a legal doctrine that assists in promoting freedom of expression by authorizing the unauthorized use of copyright-protected works in various situations.
- Few examples of proper fair use are:
 1. A film reviewer dispersing clips of a movie throughout a film review.
 2. A professor copying a single chapter from a book and giving it to his students.
 3. A researcher quoting passages from another article to support a claim.
 4. A musician taking the melody of a popular song and recording new lyrics.

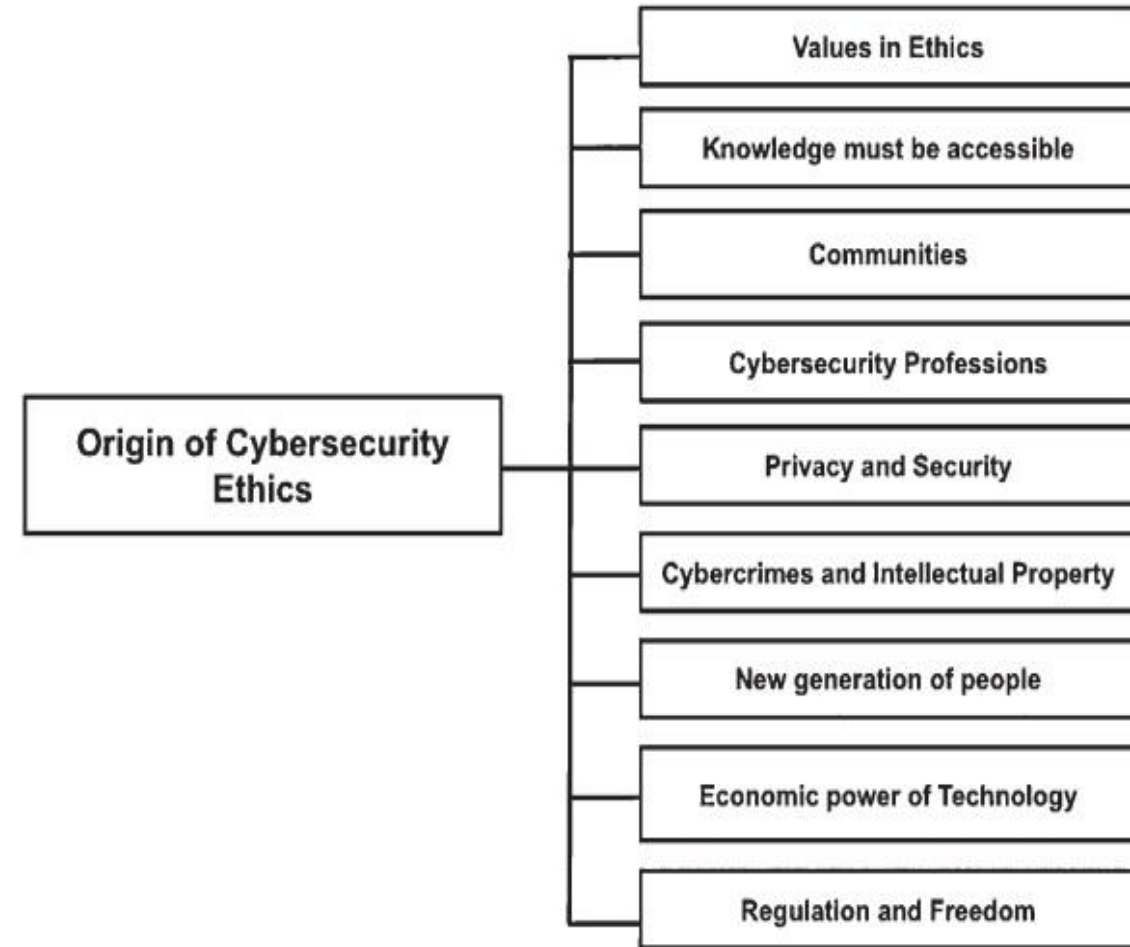


FAIR USE DOCTRINE (2/2)

- There are four factors for determining whether a work is fair use or not.
 1. The Purpose and Character of the Use.
 2. The Nature of the Copyrighted Work.
 3. The Amount and Substantiality of the Portion Used in Relation to the Copyrighted Work as a Whole.
 4. The Effect of the Use Upon the Market.

THE ORIGIN OF CYBERSECURITY ETHICS (1/8)

- Knowledge, information, and communication are the primary drivers of development in globalized, multicultural, knowledge-based societies, which are some key aspects of cyberspace.
- Ethics in information and knowledge has seven core values, namely equity, freedom, care, and compassion, participation, sharing, sustainability, and responsibility.
- The origin of cybersecurity ethics may be attributed to the following subsections.



THE ORIGIN OF CYBERSECURITY ETHICS (2/8)

(1) VALUES IN ETHICS

- Knowledge societies over cyberspace that are based on ethical values must be innovative, sustainable, coherent, and integrative.
- Cyberspace is a global forum, and hence due to the globalized multicultural world, the values must be global and respect the diversity of contextual values.
- Cybersecurity ethics is capable of promoting public awareness of such fundamental values and principles.
- Cybersecurity ethics is responsible for fostering trust among human beings and for strengthening care and action for global environmental protection.



THE ORIGIN OF CYBERSECURITY ETHICS (3/8)

(2) Knowledge Must Be Accessible To Everyone

- Cyberspace promotes access to information, communication, and education.
- This is because knowledge must be thought of as a basic right and public good.
- Open access for free or for affordable costs enables participation of all in the development of societies.

(3) Communities People:

- Community, identity, gender, generation, education people, and systems are the key actors of information, communication, and knowledge over cyberspace.
- For interacting in the cybersecurity domain, there must be sufficient understanding about how to refine, contemplate, and absorb information and knowledge.



THE ORIGIN OF CYBERSECURITY ETHICS (4/8)

(4) Ethics of Cybersecurity Professions

- Professions that are specific to information, communication, processing, creation, dissemination, control, renewal, preservation, archiving, policy-making, and cybersecurity have a special ethical responsibility in implementing core values.
- Cybersecurity engineers, analysts, scientists, social media personnel, security researchers, IT hardware and software developers, curricula developers, politicians, philosophers, and several other professionals in cybersecurity have an impact on private and public opinions.
- However, in the modern information society, professionals must strengthen values, virtues, and rights themselves *through* their professional work.



THE ORIGIN OF CYBERSECURITY ETHICS (5/8)

(5) Cybercrimes and Intellectual Property (IP)

- Piracy has the potential to become an existential threat to prevailing business models for novel content creation and use.
- Piracy usually occurs when potential users see information or material as too expensive and rights protection as excluding the poor.
- New technology has intensified the IP piracy problem. However, it has also provided solutions for the same.



THE ORIGIN OF CYBERSECURITY ETHICS (6/8)

(6) The New Generation of People

- The Internet is a popular platform for connecting computers, smartphones, and tablets, and young people are connecting with each other and the wider society in different ways.
- While the digital world promises to bring people together, there are certain issues that come with it.
- There may be a situation where children, young people and young adults may face specific risks and hazards related to the Internet.
- Some of these issues may be in the form of cyber-bullying and potential addiction to online networks.

THE ORIGIN OF CYBERSECURITY ETHICS (7/8)

(7) Economic Power of Technology

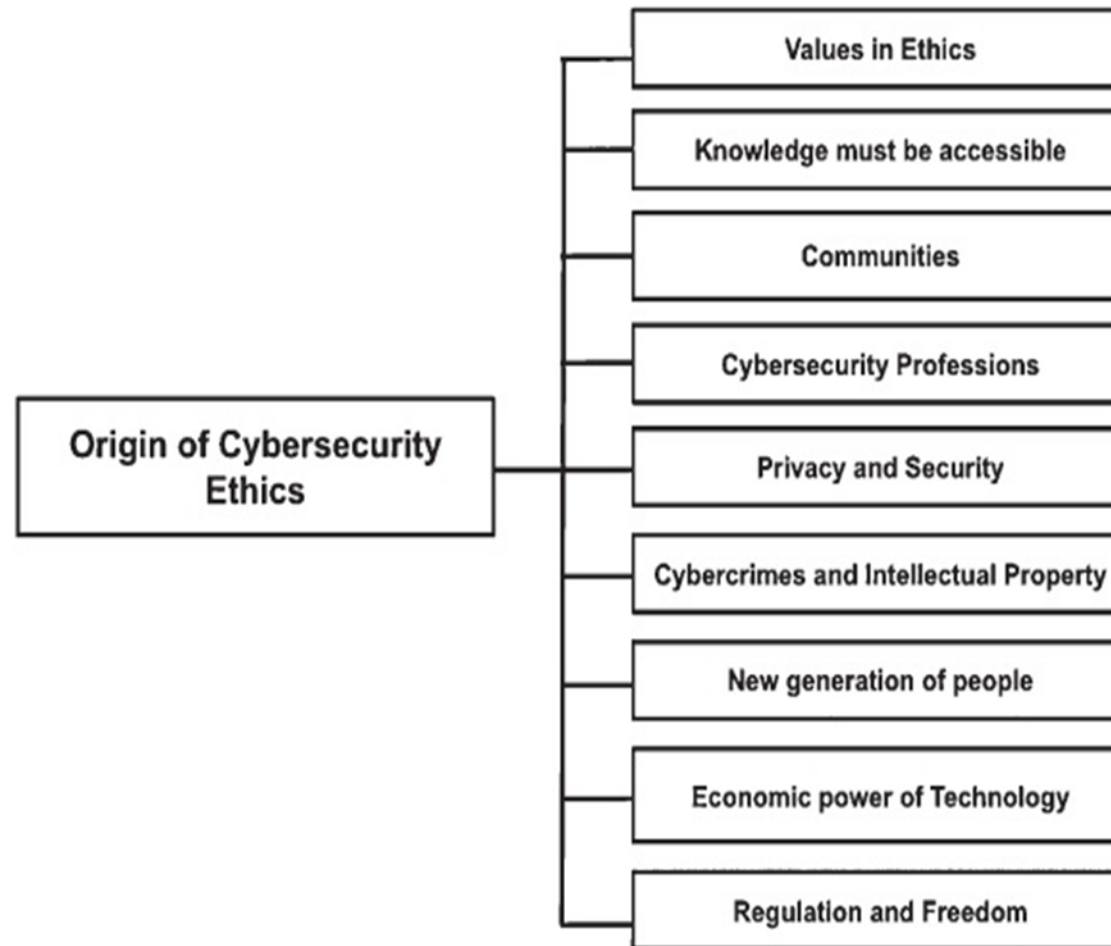
- Key actors in the cybersecurity domain may be in the form of investors and managers of companies and institutions.
- These actors have specific responsibilities in using their entrusted power.
- Greater the power, more will be responsibilities and accountability.

(8) Ethics of Regulation and Freedom

- Educated users in cyberspace must guarantee that administrative estimates bolster freedom of expression, freedom of association in cybersecurity-related advancements, and the option to look for, get, and impart data and thoughts.



THE ORIGIN OF CYBERSECURITY ETHICS (8/8)



THANK YOU

