20-8-23

Ethics and cyber law: To the point ans করলেই Number দেবে স্যার।

*) Ethics কী ? [অনেক সময় Accident নিয়ে analysis]

*) As a software engineer, কী কী ethical issue আসতে পারে ?

⇒ (i) Privacy concerns
(ii) Security
(iii) Transparency
(iv) Environmental impact
(v) Data manipulation

[প্রাধিকারের সামগ্রী নিয়ে বিভিন্ন মতামত দেওয়া → Publicity যে Availability করা হয়েছে, Society তে তার impact কী? [Point আকারে] → Positive দিক এবং negative দিক]

5- Unethical Examples in the Sector of Software Development:

① Plagiarism and code theft:

Copying and or using someone's else code without permission and presenting it as your own is unethical.

② Backdoor- implementation:

Intentionally adding hidden vulnerabilities to software for malicious purposes such as unauthorized access or data theft, ~~highly~~ is highly unethical.

③ Data privacy violation:

Developing software that collects or shares users personal data without their consent is unethical.

④ Developing Malware:

Developing malware/virus with the intent to harm ~~with~~ users system is highly unethical and ~~illega~~ illegal.

(4) ~~Neglecting Accessibilities~~:

~~Developing software that doesn't prioritize~~ do accessibility for individuals ~~with~~ disabilities. ~~This can lead discrimination~~

(5) Addictive Design:

Addictive Design involves intentionally designing software, or application in a way that exploits psychological triggers to keep users engaged for extended periods, often at the expense of their well-being.

Q3

The use of polythene, also known as plastic bags, raises ethical ~~cons~~ concerns due to its environmental impact.

① Negative Ethical Aspects:

(i) Environmental harm: Polythene is ~~non-~~ non-Bio degradable and can persist the environment for hundreds of years, also polluting the environment and harm to wild life.

(ii) Resource depletion: The production of polythene requires fossils, causing carbon emissions and resource depletion.

~~(iii) Negative Externalities:~~

② Positive Ethical Aspects:

(i) convenience and Accessibility: Polythene Bags are Lightweight, portable, and affordable making them convenient for everyday USE.

(ii) Affordability: Polythene bags are relatively inexpensive to produce, which can benefit consumers who may have limited financial resources.

Ethical conclusion:

While there may be certain advantages to use polythene in terms of convenience, affordability, its negative impacts are significant ethical concerns. Counting ~~environmentally~~ on environmentally replacements of plastic/polyethene. from my ethical standpoints, instead of using polythene/plastic ~~wh~~ we should use their replacements, such as staff made by jutes, bags made by jute etc.

Ethics (10-9-23)

* কীভাবে engineering এর সাথে ethics যায়? ⇒

(i) build product → একটা ওটা তৈরি করা।

(ii) Develop Process → পানি দিয়ে turbine ঘুরানো, (হাইড্রো বিদ্যুৎ) পানির সাহায্যে হাত মেশিনের ন্যায় ব্যবহার করা।

Main → To the point any fact হবে।

Consequence → গ্যাস লাইন blast
→ bridge ভেঙে যাবে
→ Nuclear Power Plant
→ medical equipment

Example : Earthquake
Health & safety

Conclution : কিছু Guide line follow করতে হবে।

Practical Reasoning : It uses different methods from mathematics and science.

[mam: reasoning কী কী?]

Ethical Reasoning: It is a type of practical Reasoning that concerns certain societal or life-~~from~~ form goals, such as justice, equality, freedom, health and safety.

Essence of engineering:

** ~~একজন~~ engineer এর social responsibility কী কী?

⇒ Public and Social safety maintain;

⇒ Environmental issue check;

⇒ Data privacy maintain;

⇒ Risk analysis;

⇒ Honesty maintain in project or work.

*) Software field এ: Camuration এর মত ক্ষতিকর কাজ Project এ involve না হওয়া, ~~sequrity~~ sequrity maintain করা, abusive content যাতে spread না হয়।

** একটা engineer কী type এর ethical issue face করে?

⇒ safety (user data share করবো না।)

⇒ acceptable risk (~~কতটুকু~~ "মাত্রা ছাড়া" নিচ্ছি, data যে share করছি তার risk টা মেনে নিলাম। যে তো অন্য ক্ষতিও করতে পারে, bridge or অন্য কিছু নির্মাণে environmental ~~risk এ~~ hazard এর risk টা মেনে নিচ্ছি। অর্থাৎ chemical product বানালে environment এর PH নড়বে তবুও hazard এর risk টা মেনে নিচ্ছি।)

⇒ Complaince

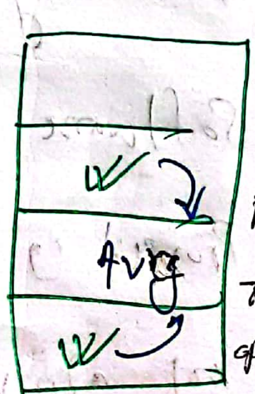
⇒ Confidentiality (চুক্তিতে যে এই Data নিয়ে অন্যের কাজে করতে পারবো না)

⇒ environmental health

⇒ Data integrity

⇒ Conflict of interest

⇒ Honesty / Dishonesty



Data stream যেত কিছুক্ষণ ঠিক থাকে এমন কোন operation করে যেকোনো দুটি করে Apply করা যাবে না।

গুরুত্বপূর্ণ Point এর সাথে example দিতে। ***

⇒ Social impact

⇒ fairness

⇒ Accounting for uncertainty.

*) কোন Language এ কি করলো তা planning হতে নিয়ে আসলো হস্তক্ষেপ

কী জানাতে চাই, কী কী থাকবে, single.

format ⇒ motivation → কী দেখে জানালো / কী জন্য

⇒ Description

Ethics (17-9-23)

[আমি uni এর একটা Project এ আছি, বাইরেও আছি, আমি বাইরেরটা ভালোভাবে করছি → conflict of interest]

* professional responsibility : কী ?

[Acceptable risk → change করে software field এঃ অনেক বেড়েছে]

* Social " " ?

(*) The code of ethics for engineers : FRP

(I) Fundamental canons;

(II) Rules of Practise;

(III) Professional Obligations;

(*) True false type Qstn থাকবে। (*) 2 marks এর প্রশ্ন explanation চাইবে।

(*) Example টা নিয়ে পড়বো → PDF এ একটা example case দেয়া আছে ওটা।

(*) Law vs Morality :

① Legal & Moral	② Legal & Immoral
③ Illegal & Moral	④ Illegal & Immoral

① → Medical Doctor, Designing a system to be safe

④ → killing an innocent person. → Human trafficking.

② → Owning a slave pre-civil war in the US. → Tobacco Company Executive. White-hat hacker.

③ → Parking in a no parking zone, to come to the aid of an injured person. Robinhood.

→ record এ evidence conflict.

→ Policy এর সাথে conflict হয় কারো (and my decision)

Society এর duty আর career এর conflict

আমার Project আর client এর conflict

[ethics → 8-10-23]

[H.W → telling the truth in public statement]

Senario 1:

আমি একটা এডুকেশনের owner, আমাকে নিয়োগ দিবো দুইজন Student.

একজন এমন গুণমানের মেয়ে অনেক ভালো Conception হয়, ↳ A পাইছে

অন্যজন Grade B পাইছে, এর অভিভাবকের সুনাম অনেক

কাকে নিয়োগ দেবো?

→ আমার আর আমার boss এর মধ্যে

Senario 2: একটা Project এ কাজ দিল, 1M dollar দেয়া হবে bridge করার জন্য, আমি দেখলাম 1M এ করলে ব্রিজ ভেঙে যাবে, 1.2 M দেয়া হলে মজবুত হবে, কিন্তু মান কম হবে, → Career এর ~~ethics এর সাথে~~ boss এর সাথে

কোন কোন Point এ conflict আছে? → আমার সাথে আমার boss এর conflict নাকি morality এর সাথে conflict, নাকি decision নিলে কারো চাকরি চলে যাবে সেটা নিয়ে conflict? then decision.

ETHICAL ISSUES THAT ENGINEERS ENCOUNTER FREQUENTLY

- **Safety:** It is important for engineers to be aware of the ethical issues involved in safety. For example, A faulty electrical system could cause a fire or explosion.
- **Acceptable risk:** Engineers must often make decisions about the level of risk that is acceptable in a particular design or project. For example, an engineer might be designing a new type of bridge. The engineer would need to consider the potential risks of the bridge collapsing, also need to consider the impact of a bridge collapse on the people who would be using the bridge.
- **Compliance:** Compliance is a fundamental aspect of responsible engineering practice. For example, an engineer designs a software system that is not accessible to people with disabilities. This could violate discrimination laws.
- **Confidentiality:** Engineers are bound by ethical principles related to confidentiality, which involve respecting and protecting sensitive information obtained in the course of their work. For example, an engineer working on a financial software project steals trade secrets from their employer and starts their own company. This could harm the employer's business.
- **Environmental health:** Engineers play a critical role in promoting environmental sustainability. For example, an engineer working on a software project for a mining company decides to use software that automates the mining process, but this results in the company emitting more pollutants into the water. This could harm the fish and other wildlife in the water.
- **Data integrity:** Engineers' ethics regarding data integrity underscore the importance of accuracy, reliability, security, and transparency in data-related activities. For example, an engineer working on a medical software project accidentally deletes patient data. This could harm the patient's health.
- **Conflict of interest:** Engineers must avoid conflicts of interest that could compromise their ability to make objective decisions about safety. For example, an engineer who is being paid by a client to design a project may have a conflict of interest if the engineer also has a financial interest in the project.
- **Honesty/Dishonesty:** Engineers are expected to demonstrate the highest standards of honesty and to avoid dishonesty in all aspects of their

professional practice. For example, an engineer working on a financial software project knowingly makes false statements about the software's capabilities. This could harm investors.

- **Societal impact**: Engineers' ethics regarding societal impact emphasize the importance of considering the broader implications of their work on communities and the well-being of society. For example, an engineer working on a social media platform decides to design the platform in a way that encourages users to spend more time on it. This could have negative consequences for people's mental health and well-being.
- **Fairness:** Engineers have a vital role to play in advancing fairness, equity, and justice in their professional practice and the broader communities they serve. For example, an engineer working on a predictive analytics software project decides to use data that is biased against certain groups of people. This could lead to the software making unfair decisions about those groups of people.
- **Accounting for uncertainty:** Accounting for uncertainty is a crucial ethical consideration for engineers, as it acknowledges the inherent unpredictability and complexity of many engineering projects. For example, an engineer working on a social media platform does not account for the possibility of misuse of the platform. This could lead to the platform being used to spread misinformation or hate speech.

NATIONAL SOCIETY OF PROFESSIONAL ENGINEERS

Code of Ethics for Engineers

Preamble

Engineering is an important and learned profession. As members of this profession, engineers are expected to exhibit the highest standards of honesty and integrity. Engineering has a direct and vital impact on the quality of life for all people. Accordingly, the services provided by engineers require honesty, impartiality, fairness, and equity, and must be dedicated to the protection of the public health, safety, and welfare. Engineers must perform under a standard of professional behavior that requires adherence to the highest principles of ethical conduct.

I. Fundamental Canons

more important than anything else; supreme

Engineers, in the fulfillment of their professional duties, shall:

1. Hold paramount the safety, health, and welfare of the public.
2. Perform services only in areas of their competence.
3. Issue public statements only in an objective and truthful manner.
4. Act for each employer or client as faithful agents or trustees.
5. Avoid deceptive acts.
6. Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession.

II. Rules of Practice

1. Engineers shall hold paramount the safety, health, and welfare of the public.

a. If engineers' judgment is overruled under circumstances that endanger life or property, they shall notify their employer or client and such other authority as may be appropriate.

b. Engineers shall approve only those engineering documents that are in conformity with applicable standards.

c. Engineers shall not reveal facts, data, or information without the prior consent of the client or employer except as authorized or required by law or this Code.

d. Engineers shall not permit the use of their name or associate in business ventures with any person or firm that they believe is engaged in fraudulent or dishonest enterprise.

encourage or assist (someone) to do something wrong

e. Engineers shall not aid or abet the unlawful practice of engineering by a person or firm.

said, without proof

f. Engineers having knowledge of any alleged violation of this Code shall report thereon to appropriate professional bodies and, when relevant, also to public authorities, and cooperate with the proper authorities in furnishing such information or assistance as may be required.

2. Engineers shall perform services only in the areas of their competence.

a. Engineers shall undertake assignments only when qualified by education or experience in the specific technical fields involved.

stick, attach

b. Engineers shall not affix their signatures to any plans or documents dealing with subject matter in which they lack competence, nor to any plan or document not prepared under their direction and control.

c. Engineers may accept assignments and assume responsibility for coordination of an entire project and sign and seal the engineering documents for the entire project, provided that each technical segment is signed and sealed only by the qualified engineers who prepared the segment.

3. Engineers shall issue public statements only in an objective and truthful manner.

a. Engineers shall be objective and truthful in professional reports, statements, or testimony. They shall include all relevant and pertinent information in such reports, statements, or testimony, which should bear the date indicating when it was current.

relevant

b. Engineers may express publicly technical opinions that are founded upon knowledge of the facts and competence in the subject matter.

c. Engineers shall issue no statements, criticisms, or arguments on technical matters that are inspired or paid for by interested parties, unless they have prefaced their comments by explicitly identifying the interested parties on whose behalf they are speaking, and by revealing the existence of any interest the engineers may have in the matters.

4. Engineers shall act for each employer or client as faithful agents or trustees.

a. Engineers shall disclose all known or potential conflicts of interest that could influence or appear to influence their judgment or the quality of their services.

b. Engineers shall not accept compensation, financial or otherwise, from more than one party for services on the same project, or for services pertaining to the same project, unless the circumstances are fully disclosed and agreed to by all interested parties.

c. Engineers shall not solicit or accept financial or other valuable consideration, directly or indirectly, from outside agents in connection with the work for which they are responsible.

ask for or try to obtain (something) from someone.

d. Engineers in public service as members, advisors, or employees of a governmental or quasi-governmental body or department shall not participate in decisions with respect to services solicited or provided by them or their organizations in private or public engineering practice.

e. Engineers shall not solicit or accept a contract from a governmental body on which a principal or officer of their organization serves as a member.

5. Engineers shall avoid deceptive acts.

a. Engineers shall not falsify their qualifications or permit misrepresentation of their or their associates' qualifications. They shall not misrepresent or exaggerate their responsibility in or for the subject matter of prior assignments. Brochures or other presentations incident to the solicitation of employment shall not misrepresent pertinent facts concerning employers, employees, associates, joint venturers, or past accomplishments.

relating directly to the subject being considered

a request for something, usually money

A brochure is a corporate marketing instrument to promote a product or service

represent (something) as being larger, better, or worse than it really is.

b. Engineers shall not offer, give, solicit, or receive, either directly or indirectly, any contribution to influence the award of a contract by public authority, or which may be reasonably construed by the public as having the effect or intent of influencing the awarding of a contract. They shall not offer any gift or other valuable consideration in order to secure work. They shall not pay a commission, percentage, or brokerage fee in order to secure work, except to a bona fide employee or bona fide established commercial or marketing agencies retained by them.

genuine; real

a fee or commission a broker charges to provide specialized services on behalf of clients

III. Professional Obligations

to keep or continue to have something: She has lost her battle to retain control of the company

1. Engineers shall be guided in all their relations by the highest standards of honesty and integrity.

a. Engineers shall acknowledge their errors and shall not distort or alter the facts.

b. Engineers shall advise their clients or employers when they believe a project will not be successful.

c. Engineers shall not accept outside employment to the detriment of their regular work or interest. Before accepting any outside engineering employment, they will notify their employers.

d. Engineers shall not attempt to attract an engineer from another employer by false or misleading pretenses.

e. Engineers shall not promote their own interest at the expense of the dignity and integrity of the profession.

f. Engineers shall treat all persons with dignity, respect, fairness, and without discrimination.

make great efforts to achieve or obtain something

2. Engineers shall at all times strive to serve the public interest.

a. Engineers are encouraged to participate in civic affairs; career guidance for youths; and work for the advancement of the safety, health, and well-being of their community.

b. Engineers shall not complete, sign, or seal plans and/or specifications that are not in conformity with applicable engineering standards. If the client or employer insists on such unprofessional conduct, they shall notify the proper authorities and withdraw from further service on the project.

c. Engineers are encouraged to extend public knowledge and appreciation of engineering and its achievements.

d. Engineers are encouraged to adhere to the principles of sustainable development[1] in order to protect the environment for future generations.

believe in and follow the practices of

e. Engineers shall continue their professional development throughout their careers and should keep current in their specialty fields by engaging in professional practice, participating in continuing education courses, reading in the technical literature, and attending professional meetings and seminar.

1420 KING STREET, ALEXANDRIA, VIRGINIA 22314-2794 • 888-285-NSPE (6773) • LEGAL@NSPE.ORG • WWW.NSPE.ORG • PUBLICATION DATE AS REVISED JULY 2019 • PUBLICATION #1102

3. Engineers shall avoid all conduct or practice that deceives the public.

a. Engineers shall avoid the use of statements containing a material misrepresentation of fact or omitting a material fact.

b. Consistent with the foregoing, engineers may advertise for recruitment of personnel. just mentioned or stated

c. Consistent with the foregoing, engineers may prepare articles for the lay or technical press, but such articles shall not imply credit to the author for work performed by others.

4. Engineers shall not disclose, without consent, confidential information concerning the business affairs or technical processes of any present or former client or employer, or public body on which they serve. permission for something to happen or agreement to do something

a. Engineers shall not, without the consent of all interested parties, promote or arrange for new employment or practice in connection with a specific project for which the engineer has gained particular and specialized knowledge.

b. Engineers shall not, without the consent of all interested parties, participate in or represent an adversary interest in connection with a specific project or proceeding in which the engineer has gained particular specialized knowledge on behalf of a former client or employer.

5. Engineers shall not be influenced in their professional duties by conflicting interests.

a. Engineers shall not accept financial or other considerations, including free engineering designs, from material or equipment suppliers for specifying their product.

b. Engineers shall not accept commissions or allowances, directly or indirectly, from contractors or other parties dealing with clients or employers of the engineer in connection with work for which the engineer is responsible.

6. Engineers shall not attempt to obtain employment or advancement or professional engagements by untruthfully criticizing other engineers, or by other improper or questionable methods. onischit,samvabbo

a. Engineers shall not request, propose, or accept a commission on a contingent basis under circumstances in which their judgment may be compromised. possibility

b. Engineers in salaried positions shall accept part-time engineering work only to the extent consistent with policies of the employer and in accordance with ethical considerations.

c. Engineers shall not, without consent, use equipment, supplies, laboratory, or office facilities of an employer to carry on outside private practice.

7. Engineers shall not attempt to injure, maliciously or falsely, directly or indirectly, the professional reputation, prospects, practice, or employment of other engineers. Engineers who believe others are guilty of unethical or illegal practice shall present such information to the proper authority for action.

a. Engineers in private practice shall not review the work of another engineer for the same client, except with the knowledge of such engineer, or unless the connection of such engineer with the work has been terminated.

b. Engineers in governmental, industrial, or educational employ are entitled to review and evaluate the work of other engineers when so required by their employment duties.

c. Engineers in sales or industrial employ are entitled to make engineering comparisons of represented products with products of other suppliers. give (someone) a legal right to do something

8. Engineers shall accept personal responsibility for their professional activities, provided, however, that engineers may seek indemnification for services arising out of their practice for other than gross negligence, where the engineer's interests cannot otherwise be protected. compensation for harm or loss

a. Engineers shall conform with state registration laws in the practice of engineering.

b. Engineers shall not use association with a nonengineer, a corporation, or partnership as a "cloak" for unethical acts. hide,disguise,cover

9. Engineers shall give credit for engineering work to those to whom credit is due, and will recognize the proprietary interests of others. relating to an owner or ownership

a. Engineers shall, whenever possible, name the person or persons who may be individually responsible for designs, inventions, writings, or other accomplishments.

b. Engineers using designs supplied by a client recognize that the designs remain the property of the client and may not be duplicated by the engineer for others without express permission.

c. Engineers, before undertaking work for others in connection with which the engineer may make improvements, plans, designs, inventions, or other records that may justify copyrights or patents, should enter into a positive agreement regarding ownership.

d. Engineers' designs, data, records, and notes referring exclusively to an employer's work are the employer's property. The employer should indemnify the engineer for use of the information for any purpose other than the original purpose. compensate (someone) for harm or loss

Footnote 1 "Sustainable development" is the challenge of meeting human needs for natural resources, industrial products, energy, food, transportation, shelter, and effective waste management while conserving and protecting environmental quality and the natural resource base essential for future development.

"By order of the United States District Court for the District of Columbia, former Section 11(c) of the NSPE Code of Ethics prohibiting competitive bidding, and all policy statements, opinions, rulings or other guidelines interpreting its scope, have been rescinded as unlawfully interfering with the legal right of engineers, protected under the antitrust laws, to provide price information to prospective clients; accordingly, nothing contained in the NSPE Code of Ethics, policy statements, opinions, rulings or other guidelines prohibits the submission of price quotations or competitive bids for engineering services at any time or in any amount."

Statement by NSPE Executive Committee

In order to correct misunderstandings which have been indicated in some instances since the issuance of the Supreme Court decision and the entry of the Final Judgment, it is noted that in its decision of April 25, 1978, the Supreme Court of the United States declared: "The Sherman Act does not require competitive bidding."

It is further noted that as made clear in the Supreme Court decision:

1. Engineers and firms may individually refuse to bid for engineering services.
2. Clients are not required to seek bids for engineering services.
3. Federal, state, and local laws governing procedures to procure engineering services are not affected, and remain in full force and effect.
4. State societies and local chapters are free to actively and aggressively seek legislation for professional selection and negotiation procedures by public agencies.
5. State registration board rules of professional conduct, including rules prohibiting competitive bidding for engineering services, are not affected and remain in full force and effect. State registration boards with authority to adopt rules of professional conduct may adopt rules governing procedures to obtain engineering services.
6. As noted by the Supreme Court, "nothing in the judgment prevents NSPE and its members from attempting to influence governmental action . . ."

Note: In regard to the question of application of the Code to corporations vis-a-vis real persons, business form or type should not negate nor influence conformance of individuals to the Code. The Code deals with professional services, which services must be performed by real persons. Real persons in turn establish and implement policies within business structures. The Code is clearly written to apply to the Engineer, and it is incumbent on members of NSPE to endeavor to live up to its provisions. This applies to all pertinent sections of the Code.

What is ethics?
Professional Ethics is a set of standards defined by the professional community which provides a guide for behavior that is expected from the professional.
Why study ethics?
The purpose of study is to familiarize oneself to the professional standards that apply to your profession. These standards vary from state to state, organizations, country and culture. Registration laws incorporate ethics with varying detail, so that what is stated in one jurisdiction may not be stated in another. Knowing the differences will help you grow professionally.

ETHICS IN ENGINEERING

Lecture 1/4

WHAT IS MEANT BY ETHICS?

http://manofthehouse.com/money/career-advice/business-ethics-in-the-workplace

== LAW

- System of moral principles
  - Principles of right and wrong
- Principles of conduct governing behavior of an individual or a group

http://www.yourdictionary.com/library/reference/define-ethics.html

CLICKER QUESTION

A person's behavior is always ethical when one:

A. Does what is best for oneself
B. Has good intentions, no matter how things turn out
C. Does what is best for everyone
D. Does what is legal

ETHICS IN AN ENGINEERING COURSE????

We have been studying engineering, such as design, analysis, and performance measurement.

Where does ethics fit in?

http://www.free-clep-prep.com/Business-Ethics-and-Society-DSST.html

HOW ETHICS FITS INTO ENGINEERING

- Engineers . . .
  - **Build products** such as cell phones, home appliances, heart valves, bridges, & cars. In general they advance society by building new technology.
  - **Develop processes**, such as the process to convert salt water into fresh water or the process to recycle bottles. These processes change how we live and what we can accomplish.

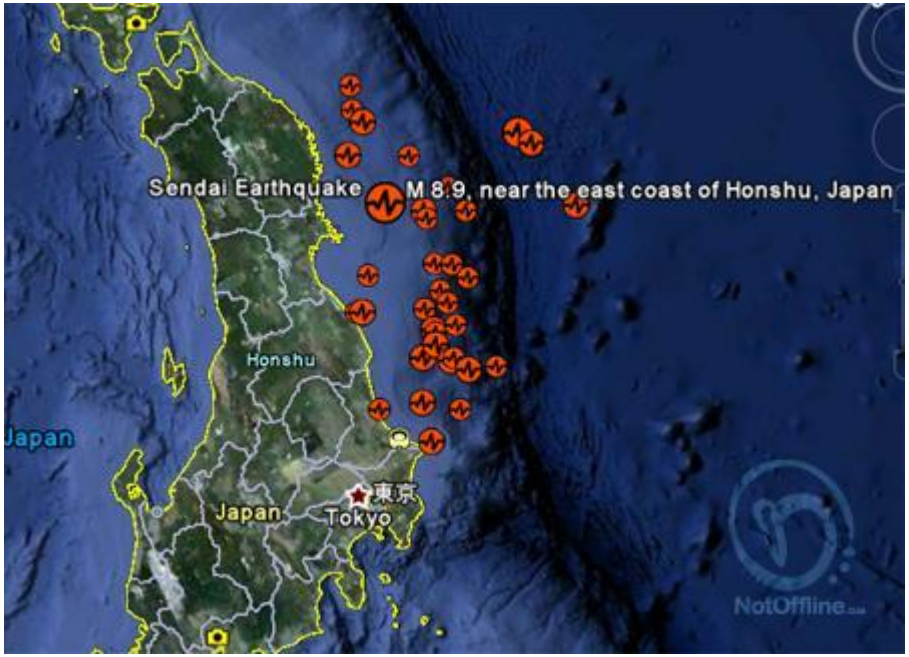
PRODUCTS AND PROCESSES HAVE CONSEQUENCES FOR SOCIETY:

- If the bridge has an inadequate support, it will fail.
- If the gas tank is positioned too close to the bumper, it might explode from a small accident.
- If a medical instrument isn't accurate, improper doses of medication can be given.
- If the process for refining gas, produces too much toxins, it harms the local community.

Decisions made by engineers usually have serious consequences to people -- often to multitudes of people.

Ethics and ethical reasoning guide decision-making.

Consider the March 11, 2011 8.9 magnitude earthquake near Sendai, Japan.



The damage to the Fukushima I Nuclear Power Plant (*Fukushima Dai-ichi*) has led people worldwide to rethink the ethics of nuclear power.

Notice the issues that come up in these discussions:

ISSUE #1: HEALTH AND SAFETY

RISKS: Danger to current and future generations from leakage of radio-isotopes used in nuclear power.

Plutonium-239 (half-life = 24,110 yrs) is a particularly toxic radio-isotope. Normally, 10 half lives are required before a Pu-239 contaminated area is considered safe again, in the case of plutonium, roughly 250,000 years.

So if Pu leaked, -- say, due to an earthquake -- it would cause a health risk for roughly 8000 generations!!

Issues (cont.):

ISSUE #1: HEALTH AND SAFETY RISKS, FURTHER CONSIDERATIONS:

a) The possibility of medical science discovering a cure for cancer sometime in the current or next centuries adds uncertainty to the long-term health risks of leakages of radio-active isotopes.

Issues (cont.):

ISSUE #1: HEALTH AND SAFETY RISKS, FURTHER CONSIDERATIONS:

b) The use of nuclear power may increase our knowledge of radioisotopes used for medical purposes (possible benefit?).

Issues that come up in these discussions:

CONSEQUENCES OF ALTERNATIVES TO NUCLEAR POWER.

ISSUE #2: DEPLETION OF RESOURCES:

Fossil fuels, oil, natural gas and coal, are non-renewable. These resources also affect the goal of *health* because of their impact on pollution and climate changes.

Issues that come up in these discussions:

CONSEQUENCES OF ALTERNATIVES TO NUCLEAR POWER.

ISSUE #3: COMPARATIVE ECONOMIC COSTS OF RENEWABLE SOURCES.

Renewable sources such as hydro-electric-power, wind power, solar power, geo-thermal heat, agricultural biomass and tides do not cause the environmental hazards that fossil-fuels do.

But renewable sources must be balanced with the amount of energy needed to produce and maintain them and consequent environmental hazards. Currently, for example, the energy required to manufacture and install solar energy systems comes from fossil fuels.

REASONING

The kind of reasoning that goes on in such discussions involves certain *goals*
such as, in this case, health, safety and biodiversity.

The reasoning then focuses on finding the best – or at least the reasonably better --
means
for obtaining those goals.

Ethical reasoning is the ability to identify, assess, and develop ethical arguments from a variety of ethical positions."

This type of reasoning is often called *practical reasoning*.

It uses different methods from mathematics and the sciences.

Ethical reasoning is a type of practical reasoning that concerns certain societal or life-form goals, such as justice, equality, freedom, health and safety.

THE ESSENCE OF YOUR ENGINEERING CAREER

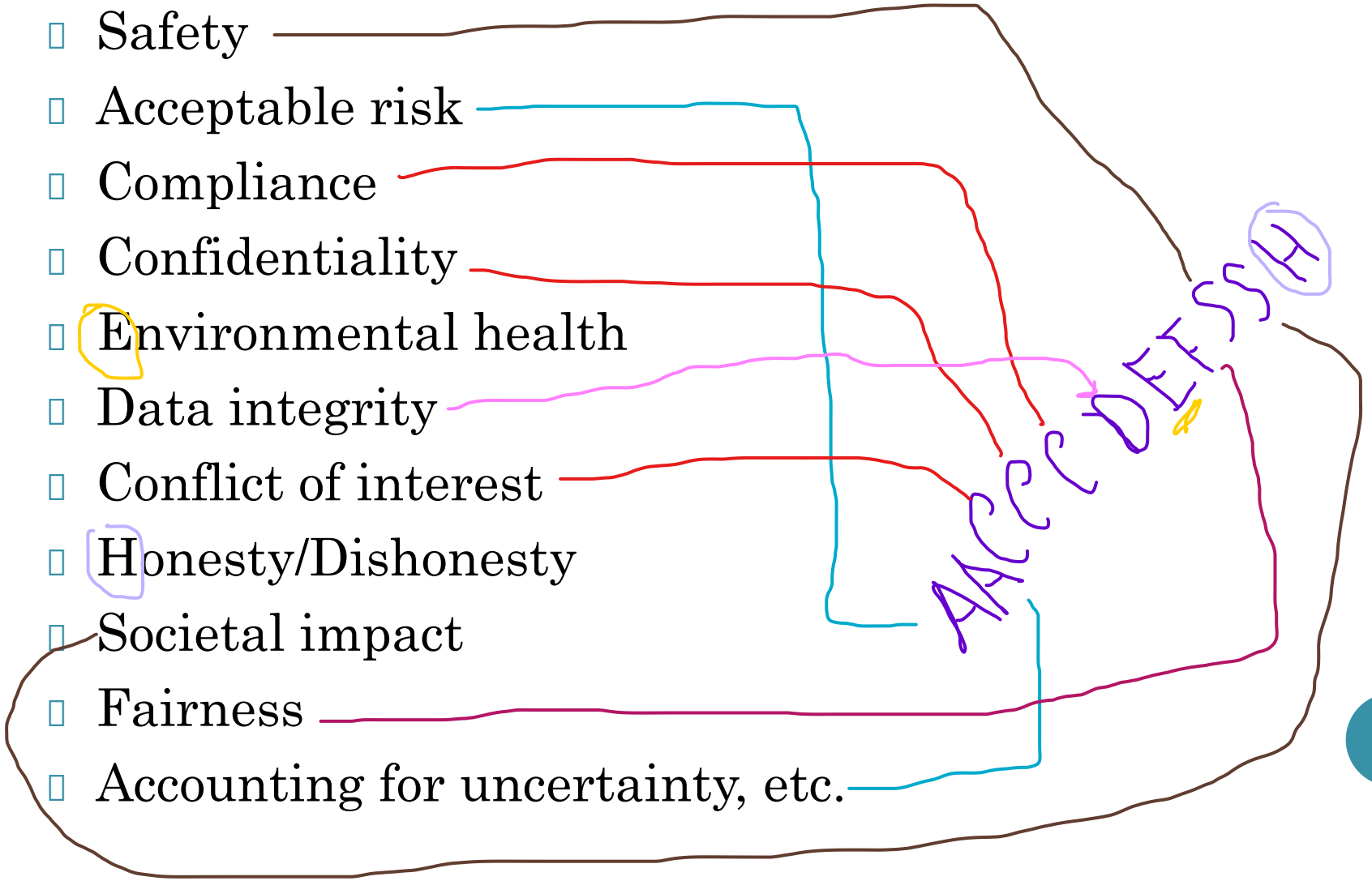
- Engineering is one of the most important professions in society.
- As engineers we *don't just build things and develop processes.*
- We build things and make processes *in order to better society*.
- In order to make society better we have to reflect constantly on the products and processes that we make.

SOCIAL RESPONSIBILITY

- One main connection between ethics and engineering comes from the impact that engineered products and processes have on society.
- Engineers have to think about designing, building, and marketing products that benefit society.
- Social Responsibility requires taking into consideration the needs of society.

TYPICAL ETHICAL ISSUES THAT ENGINEERS ENCOUNTER

- Safety
- Acceptable risk
- Compliance
- Confidentiality
- Environmental health
- Data integrity
- Conflict of interest
- Honesty/Dishonesty
- Societal impact
- Fairness
- Accounting for uncertainty, etc.



PROFESSIONAL RESPONSIBILITY

- Ethics has a second connection with engineering.
- It comes from the way in which being socially responsible puts duties and obligations on us individually.
- Ethics fits into engineering is through professional responsibility.

TWO DIMENSIONS OF ETHICS IN ENGINEERING

- Ethics is part of engineering for two main reasons.

a) Engineers need to be **socially responsible** when building products and processes for society.

b) Social responsibility requires **professional responsibility**.

ABET SAYS . . .

By the time of graduation students will have an understanding of professional and ethical responsibility

http://www.boston.com/news/globe/magazine/articles/2006/09/10/its_the_engineering_stupid/

WHAT WE WILL DISCUSS

- The code of ethics for engineers.
- Practicing ethics as an engineering student.
- How to identify and analyze ethical dilemmas through case analysis.
- Specific examples of ethical situations you may encounter.

Part 1: The Code of Ethics for Engineers

http://www.nspe.org/Ethics/CodeofEthics/index.html

ROLE-RESPONSIBILITIES

- We need to make a distinction between two ways in which ethics can apply to one's life.

- The two ways ethical issues can apply to one's life are based on *role responsibilities*. Role responsibilities are responsibilities that attach to us in virtue of a role that we have. Each of us has different roles that we play in our life.
  - Engineering Student
  - Friend
  - Citizen
  - Employee

Role	Responsibilities
Friend	*Look out for the interests of your friend.*
Athlete	*Play your sport in a professional manner.*
Employee	*Perform the duties of your job.*
Parent	*Look after your children and their interests*
Citizen	*Follow the laws of the country in which you live.*

ETHICS IN ENGINEERING

- There are many fields of engineering, such as
  - Civil
  - Mechanical
  - Electrical
  - Software
  - Industrial

- However, there are many ethical issues that arise across all of these fields of engineering.

- **The code of ethics for engineers pertains to engineers of all kinds.**

CLICKER QUESTION

Engineers should follow their professional code of ethics because:

A. The public will trust engineers more if they know engineers have a code of ethics.

B. It helps them avoid legal problems, such as getting sued.

C. It provides a clear definition of what the public has a right to expect from responsible engineers.

D. It raises the image of the profession and hence gets engineers more pay.

THE ENGINEERING CODE OF ETHICS

The Engineering Code of Ethics has three components:

having or showing the ability to speak fluently

- **The Fundamental Canons:** which articulate the basic components of ethical engineering.
- **The Rules of Practice:** which clarify and specify in detail the fundamental canons of ethics in engineering.
- **Professional Obligations:** which elaborate the obligations that engineers have.

NSPE FUNDAMENTAL CANONS OF ETHICS

Engineers in the fulfillment of their professional duties shall:

- Hold paramount the safety, health, and welfare of the public.
- Perform services only in areas of their competence.
- Issue public statements only in an objective and truthful manner.
- Act for each employer or client as faithful agents or trustees.
- Avoid deceptive acts.
- Conduct themselves honorably, responsibly, ethically, and lawfully, so as to enhance the honor, reputation, and usefulness of the profession.

HPIAAC

TRY IT YOURSELF

- You are supervising a product with specifications that only U.S.-made parts may be used.
- Late in the project you discover a sub-contractor has supplied a part with foreign-made bolts.
- They aren't very noticeable and would function identically to U.S.-made bolts.
- Your customer urgently needs the finished product.

What should you do?

CLICKER QUESTION

Should you:

A. Say nothing and deliver the product with the foreign bolts because the customer won't notice.
B. Find some roughly equivalent violation of the contract/specs for which the customer is responsible and tell them you will ignore their violation if they ignore yours.
C. Tell the customer about the problem, and let them decide what you should do next.
D. Find loopholes in the original specifications so that your company hasn't legally violated the specs.

- C (tell the customer) is the correct answer because it lets the customer decide what is in their best interest given new information.

- This may be tough, because your job may be on the line and your company's reputation may be at stake.

Avoid deceptive acts

Act for each employer or client as faithful agents or trustees

IMPORTANT NOTES ABOUT THE CODE OF ETHICS

- It is not a legally binding document.
- It is not something that we want (or need) engineers to memorize.
- It is something we want engineers to understand and be able to live by as engineers.
- However, in the beginning knowing the code is a guide to understanding how to apply it.

REVIEW THE LAROM CASE

- Hired at Larom because of the promising research with catalysts as a student at SJSU.
- Supervisor, Alex Smith, announces that your unit must make a recommendation within next two days on which catalyst should be used in processing a major product.
- The overwhelming consensus of the engineers in your unit, based on many years of experience, is that catalyst A is best for the job.
- Your research provides preliminary evidence that catalyst B might be more reliable, more efficient, and considerably less costly.

REVIEW THE LAROM CASE

- You ask if the recommendation can be delayed a month to see if firmer evidence can be found.
- Alex asks you to write up the report, leaving out the preliminary data about catalyst B.
- He says, “we've already taken too much time on this project. … we have to be decisive--and we have to look decisive …Besides, we've had a lot of experience in this area."
- You have no desire to challenge your colleagues. You don't necessarily disagree with them about which catalyst is best. BUT you wish you had been given more time to work on catalyst B and feel uncomfortable about leaving the preliminary data out of the report.

WHAT RECOMMENDATION DID YOU MAKE

- Discuss this with a group
- Identify the issues
- Compare courses of action
- Identify best course of action
- One of you may be asked to report out

Ans: option 3 The catalyst (A or B) needs to be used for creating a major product, the catalyst A is tried and

ETHICS TAKES PRACTICE KNOWLEDGE VS. BEHAVIOR

- Unlike robots, no one can just program you to be an ethical engineer that follows the codes.
- It is possible to know the codes of ethics for engineering (or being a student), yet fail to follow them.
- Ethical behavior is about practice and virtue. It is about going beyond the codes, and practicing behavior that leads to an ethical life.

THE EXAMPLE OF INTEGRITY

- A building has structural integrity when it is designed in way such that it appropriately responds to the stresses and loads that it is designed to act under.

- Just as a building can have poor integrity or good integrity. A person can also.

- A person has integrity when she/he can follow the codes he/she is supposed to follow under the stresses and loads of his/her role.

CLICKER QUESTION

Which of the following ensure that behavior is ethical?

I. Following the law
II. Acting in the best interest of society
III. Following non-legal standards for socially appropriate conduct

A. All of the above
B. II and III only
C. None of the above
D. I only

Following the law (I) cannot ensure ethical behavior, because a given law might itself be unethical (example: earlier laws legitimizing slavery.) But both II and III do ensure that behavior is ethical. Hence the correct option is b), "II and III only."

Ethics vs Morality

LAW VS. MORALITY: DON'T CONFUSE THE TWO

Legal & Moral	Legal & Immoral
Illegal & Moral	Illegal & Immoral

morally r8 bt ethically worng

EXAMPLES OF THE CATEGORIES

Legal & Moral	Designing a system to be safe.
Legal & Immoral	Owning a slave pre-civil war in the US.
Illegal & Moral	Parking in a no parking zone, to come to the aid of an injured person
Illegal & Immoral	Killing an innocent person.

Part 2: Practicing ethics as an engineering student

STUDENTS HAVE A CODE OF ETHICS TOO

The SUST University Academic Integrity Policy requires that each student:

1. Know the rules that preserve academic integrity and abide by them at all times. This includes learning and abiding by rules associated with specific classes, exams and course assignments.
2. Know the consequences of violating the Academic Integrity Policy.
3. Know the appeal rights, and the procedures to be followed in the event of an appeal.
4. Foster academic integrity among peers.

S07-2 PREAMBLE

The University emphasizes responsible citizenship and an awareness of ethical choices inherent in human development.

Academic honesty and fairness foster ethical standards for all those who depend upon the integrity of the university, its courses, and its degrees.

University degrees are compromised and the public is defrauded if faculty members or students knowingly or unwittingly allow dishonest acts to be rewarded academically.

PLAGIARISM & CHEATING

- Many components go into being a good engineering student.
- One of the most important, as reflected by the codes of ethics for engineers, is to be ***competent*** in your field of engineering.
- To be competent, it is *necessary* that one actually knows what they claim to know.
- Proving to others that you know what you are supposed to know requires certification through a degree.

WHAT STUDENTS SAY

- 70% of American high school seniors admit to cheating on at least one test
- 95% of the students who said they cheated were never caught.

- An average of 75% of college students report cheating sometime during their college career

ACADEMIC DISHONESTY

- Cheating

At SUST, cheating is the act of obtaining or attempting to obtain credit for academic work through the use of any dishonest, deceptive, or fraudulent means.

CHEATING IS WRONG?

Cheating also undermines the work of fellow students who are honest.

When you cheat, all the other students who didn't cheat are penalized. They end up getting lower grades. As a consequence of lower grades they lose out on scholarships and recommendations.

CHEATING VS. TEAMWORK

- Working on a team for an assigned project is *not* cheating.
- However, failing do due your assigned task on an a team project is a form of cheating. It is called *free-riding*, which is benefiting from the work of others without doing any work of your own.
- Teamwork is important in engineering, but free-riding is wrong, since if everyone did it nothing would get done.

COPYING

One obvious type of cheating that we all recognize is copying someone's work on a homework assignment, exam, or paper.

Submitting someone's work as your own is a kind of cheating.

MULTIPLE SUBMISSIONS

Submitting your own work from one class to another class or submitting one piece of work to two distinct classes is a kind of cheating.

A paper for one class is not a paper for another class.

UNAUTHORIZED SOURCES

consider

Using sources that one is not allowed to use as deemed by the instructor or the university as a whole is a kind of cheating, such as solution manuals.

Also a text message from your friend with the answer to a question on the exam is a form of cheating.

ALTERING GRADES

Altering your grade in any way is a form of cheating.

If you are given a C on your homework, paper, or exam and then you change your grade to a B+, you have cheated.

SURROGATE

Surrogate cheating occurs when someone else either does your homework, takes an exam for you, or writes your paper.

Doing someone's work for them is a kind of cheating.

WHY IS CHEATING WRONG?

Cheating undermines the credibility of the university and the degrees it awards.

If too many people cheat at SUST, then the degrees awarded by SUST won't certify that its students are competent. So, by cheating you not only hurt yourself, you also hurt others.

ETHICS – COURAGE & INTEGRITY

- As we will be seeing more and more being ethical requires:

  - Courage to do the right thing the situation calls for.

  &

  - The integrity to withstand the pressures that push you in the wrong direction.

Ethics in Engineering

Lecture 2/4

Review of Topic from Lecture 1

- You are an employer at a large multinational software firm. You put an ad on Monster.com for software engineers to design a new product.
- You get a bunch of applications, but two stand out based on the applicants' previous internships and the high quality of their communication skills in the interviews.
- The first student has almost all A grades, but came from a university where several cheating scandals have been reported in the paper. The other applicant has mostly B grades, but came from a university well known for strictly enforcing integrity?
- **Who would you hire?**

This really Happens

- *Insider: UNC tolerated cheating* – Charlotte Observer Nov. 18, 2012
- *U.S. News strips George Washington University of ranking for cheating* – Nov 15, 2012
- *Cheating scandal rocks Harvard University – NECN.com* – August 31, 2012
- *An assistant registrar was accused of changing hundreds of student grades at Southern University* – 2003
- *Diablo Valley College students were accused of trading sex for grade changes* - 2007

Outline:

- Review Pentium Case
- From Codes to Cases
- Moral Considerations
- Moral Reasoning & Case Analysis

Pentium Case

Turn to your neighbor(s) and discuss the following:

- What course of action could Intel have taken to satisfy their customers and minimize the negative publicity they received?

Pentium Case

Discuss this with your neighbor(s):

In the literature that comes with a product a manufacturer places a warning such as "This product may contain unexpected flaws and might not operate correctly under all conditions."

- Does this solve the ethical problems for the company?

Clicker Question

What do you think (there is no right answer):

In the literature that comes with a product a manufacturer places a warning such as "This product may contain unexpected flaws and might not operate correctly under all conditions."

Does this solve the ethical problems for the company?

A. Yes
B. Sort of
C. No

Pentium Case

Was there really an ethical dilemma? If so what was it?

- A **dilemma** is a problem offering two possibilities, neither of which is practically acceptable

Part 1: From Codes to Cases

Going Beyond The Code

- The code of ethics for engineers gives us a good set of guides to follow.
- But knowing what the codes say and what exactly to do in a given situation is not always obvious.
- The primary reason is that really hard ethical situations require moral reasoning and conflict resolution.

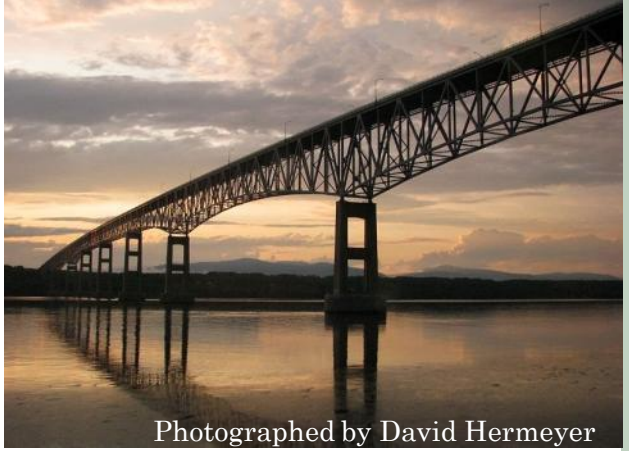
Where we will begin

- To start our exploration into case analysis, we will simply begin by looking at some cases.
- Our goal is to engage in a form of moral reasoning about the cases, which involves:
  - Taking note of which codes of engineering ethics apply.
  - Identifying conflicts.
  - Making a choice of what to do.
- All of this will lead us to a discussion of moral considerations and moral reasoning.

Ethical Frameworks

- Rights Approach
  - Which option best respects the rights of all who have a stake?
- Utilitarian Approach
  - Which option will produce the most good and do the least harm?
- Justice Approach
  - Which option treats people as I want to be treated?
- Ethic of Care Approach
  - Which option is best for those most in need?
- Virtue Approach
  - Which option leads me to act as a responsible person?

Case 1: Protecting the safety of society


Photographed by David Hermeyer

Your employer asks you to design a bridge that will not exceed $1 million to build. After doing a study you determine the following:

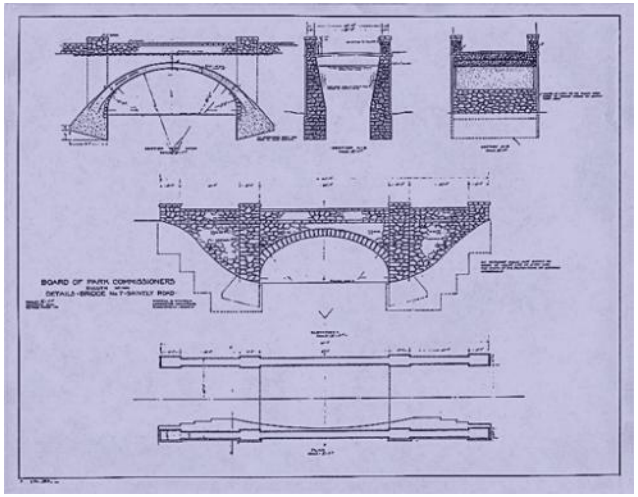
a) An ideal bridge can be built for $1.5 million.
b) Given the design constraints, a bridge built for $1 million will collapse in a moderate earthquake.
c) A bridge built for $1.25 million will survive a moderate earthquake, but will collapse in an infrequent extreme earthquake.

Case 1: Protecting the Safety of Society

Suppose your employer says, “if we don’t build the bridge for $1 million, then we are going to have to lay off half of the staff, including you.”

He further asks you to go ahead with the next stage of the project.

What do you do?



http://www.leydenscience.org/bridges/college.htm

Clicker Question

What do you think is the **primary conflict**:

A. Your duty to your fellow employees vs. your duty to your boss

B. Your duty to society vs. your loyalty to your own career

C. Uncertainty about the maximum magnitude of an earthquake vs. the need to ensure a safe structure.

D. Your duty to be honest to clients vs. your duty to complete the project

What is the conflict?

- The code of ethics for engineers requires:
  - You to take the safety of society as being of paramount importance.
- However, you also feel a personal sense of loyalty to your company and fellow co-workers. You don't want anyone to lose their job.
- **The conflict** is between your duty to society and your loyalty to your own career and the welfare of your other fellow employees.

What is more important?

- The conflict is between your future employment and the employment of others in your company, and the welfare of society.
- In a case like this the welfare of society comes first.
- We have to take into account the fact that your duty to protect the public is *greater than* your duty to your own career, and that of your fellow employees.

Case 2: Telling the Truth In Public Statements

You are asked by the government to verify that a certain nuclear reactor will not leak toxic substances into the neighboring ocean.

After doing a study you discover that:

a) The nuclear reactor likely will leak within the coming 8 years, but there is significant uncertainty.
b) The nuclear reactor cannot be evaluated more carefully unless it is shut down immediately.
c) Both the ocean and the neighboring community are at risk.

Case 2: Telling the Truth In Public Statements

Suppose that upon receiving your report, government officials ask you to modify your report so as to reflect that the nuclear facility is actually safe.

They claim that altering the report will protect the public in the area, preventing panic while the government attempts to shut down and fix the facility.

What do you do?

http://en.wikipedia.org/wiki/File:Diablo_canyon_nuclear_power_plant.jpg

What is the Conflict?

- The code of ethics requires that you
  - Safeguard the public's welfare.

But it also requires that you

- Tell the truth when making public statements concerning your area of engineering.

To solve this conflict, you must

- correctly understand what each code is telling you, and
- choose to act on the obligation that is of priority.

What is the Conflict?

- What does **protecting the public** mean?
  - Making sure that they are safe
- What does issue **public statements in an objective and truthful manner** mean.
  - Telling the public the nuclear reactor may not be safe, but outlining the uncertainties.
- But the government is asking you to alter your report *in order to protect the public*.

What is the conflict?

- Your **obligation** is to safeguard public safety and to tell the truth in your role as an engineer. This means that you cannot alter data as an engineer, and that you must tell the truth about the nuclear reactor.

- The **government** is calling on you as a citizen to alter documents as a way to protect your fellow citizens.

- The **conflict is between** your obligations as an engineer and your obligations as a citizen.

What is more important?

- Role conflicts are hard!!!
- No easy answer!!!
- This is where thinking about other moral considerations matter.
  - What about the public's right to know?
  - What about the government's obligation to tell the truth?
- In this case your duty as an engineer to tell the truth when making public statement *trumps* your civic duty to be loyal to your government.

(*) Cyber crime/sequrity কাকে বলে? (chapter 1) ইটাও definition, according to who — তা লিখতে 3 marks হবে, বেশি marks হলে দুইটাসহ তাও লিখা যেতে পারে।

(*) কত ভাবে cyber crime হয়ে থাকে? (এখান থেকে 10 marks ও আসতে পারে)

(*) Society related crime কী কী? (1 নং 2 No Point)

history → X (3 No. point বাদ)

BD তে কী কী Law আছে, DSA, Digital sequriety Act 2012, recently CSA এখন হতে পারে। *

(*) 4.1, 4.2, 4.3, 4.4 & defination * * *

→ against individual, against poperty, against organization, against society

(*) কিছু Policy, কী কী cyber crime হয়ে থাকে?

(*) Common types cyber crime কী কী আছে? (5 marks)

যেমন হতে, hacking, pshing, spofing, software piracy

(*) 1 নং 5 no point এ present senerio → just reading → BD তে কোন গুলো বেশি বেশি হচ্ছে, Qstn আসতে পারে, Point আকারে লিখবো। (2 marks)

(Chapter-2)

(*) 1 No এ defination দিবো, then ~~font 2 তে~~ → cyber jurisdiction.

(*) তারপর establishment এর যে Point আছে, তারপর Point 2, 3 পড়বো।

(*) Point আকারে লিখবো, বেশি লিখার পড়বার নেই।

(*) Cyber crime হলে কোথায় যাবো → tribunal এ যাবো, bd তে কয়টি, কোথায় আছে, তারা কেমন এই বিষয়গুলো Point 2 হতে জানবো।
→ Establishment & jurisdiction of cyber appeal tribunal Bangladesh

(*) Point 3 এর Punishment কী কী ? ***
↳ i গুরু গুরুত্বপূর্ণ Point কোনোটাই বাদ দেওয়া যাবে না।

Chapter → 3 ✗

(Chapter 4)

(*) Definition (1 No. Point)

(*) 2 No. point internet privacy

(*) 3 No. risk, গুরুত্বপূর্ণ *

(*) Social networking site এ কী কী Privacy issue হয় (4 No.) ?

(*) 5 No. Potential internet privacy risk কী কী ?

Chapter → 5, 6, 7 ✗

(Chapter 8) *

(*) Ch-7 থেকে e-learning এর definition টা পড়বো।

(*) Introduction লাগবে, Point 2 লাগবে (Effects of cyber crime)
economic impact, social impact, ←

Survey, 3 No → বাদ দেবো ✗

(*) Point 4, critical analysis, Point 5 ও পড়বো এবং Point 6

(*) Cyber crime prevention এ কী কী Practice recommend করা হয়. ? ***

(*) 8.1 → education on cyber crimes.

(*) Ch-9 থেকে e-governance এর definition.

(Chapter 10)

* Privacy & cyber security issue in BD, Point 2, 3, Security challenge পুরো কপি

(Chapter 12)

* BTRC এর Point 3 পড়বেন।

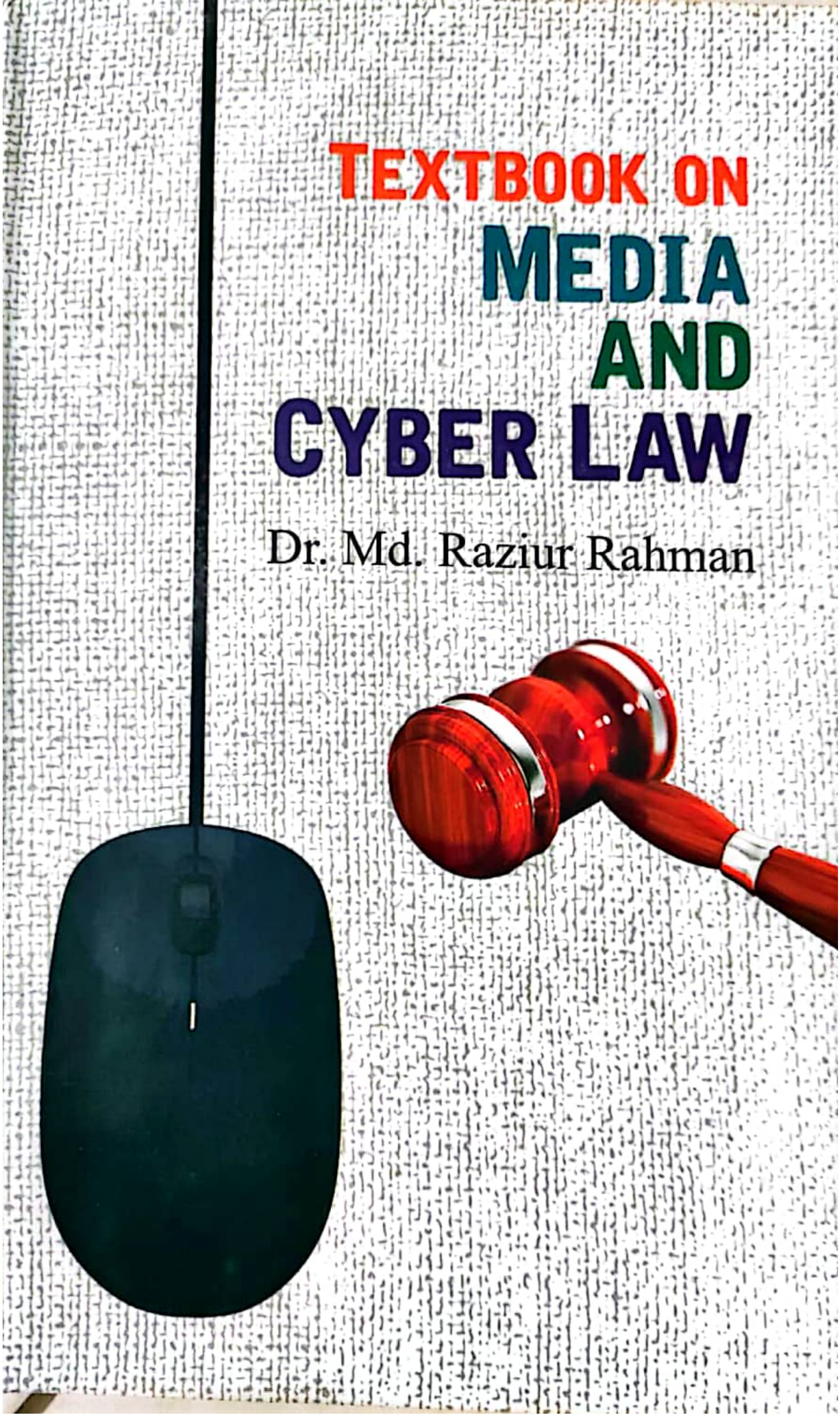
TTZ: 23 পৃষ্ঠা, Ch-1, 2, 4, 8 → Prevention টা

* ethics এর অংশটুকু slide মত পিডিএফ আকারে দিচ্ছি, cyber এর শেষ 3rd slide টা → এটা full syllabus.

* Dr. Md. Razor Rahman (Protecting internal Framework, Back up, Off Internet)
* Cyber crime against Individuals, poperty, society, organizations
* Common Cyber Crimes: Software Piracy, IRC crime (Internet relay chat), Cyber stalking, Phishing, Hacking, Denial of services, E-mail spoofing, Spamming, Cyber Defamation, Harassment & Cyber Stalking, Salami Attack, Intellectual Poperty Crimes, Virus Attack, E-mail Bomling (Logic Bomb; Trajan Horse), Data diddling Forgery, Cyber Terrorism, Web Jacking
* Explains Internet Privacy: Phishing, Pharming, Spyware, Malware
* Effects of cyber crime: Economic Impacts, Social Impacts, Political Impacts.
* Practise recommended for Prevention: Firewalls, Frequent Password changing, Safe surfing, Frequent virus checks, Email Filters, Online Photography. Undergo (back up) Credit card security, Depravation in childrens, Secure the program, Watching Traffic (" ").

TEXTBOOK ON MEDIA AND CYBER LAW

Dr. Md. Raziur Rahman



attracted much more users to the internet world. As of now BTRC has about three hundred and forty five[12] registered ISP license holders[13] and there are approximately 4.5 million users connected to them which is about 0.32% of the total population of the country.

4. Cyber Crime Defined

It is a technological crime and a misnomer[14] term. It is also known as computer crime, electronic crime, hi-tech crime and e-crime. Actually it involves a broad range of potentially illegal activities conducted by the misuse of computers and different types of communication networks. Additionally, cyber crime also includes traditional crimes conducted through the internet. For example, hate crimes, telemarketing and internet fraud, identity theft, and credit card account thefts are considered cyber crimes when the illegal activities are committed through the use of a computer and the internet. Cyber crime is mostly a property related crime. It has no direct contact with the victims and involves less visible and intangible kinds of property such as information, data and computer networks. Victims come to know about their losses long after the actual commission of crimes. Profits from high-tech crimes are vast. Hackers are able to steal greater amounts with greater comfort; a single act can victimize many people in many places at once. It may be divided into two types : (i) crimes that target computer networks or resources directly; and (ii) crimes facilitated by computer networks or devices. Examples of crimes that primarily target computer networks or devices include malware and malicious code, denial-of-service attacks and computing viruses. Examples of crimes that merely use computer networks or devices include, amongst others, cyber stalking, fraud and identity theft and information

12. Report on BTRC, ISP Natiowide-94, ISP Central Zone-79, ISP Zonal-53, ISP Category A-99, ISP Category B-16, ISP Category C-04.
13. Summary of- BTRC licenses, http//www.btr.gov.bd, (accessed 1June 2015).
14. A.R.M Borhanuddin, Cyber Crime and Bangladesh Perspective, Available Online: http ://www.scribd.com/doc/3399476/cyber-crime,(accessed September 2015).

warfare. The Cyber Crime is further subdivided into the following four categories :[15] (i) cyber crime against individuals, (ii) cyber crime against property, (iii) cyber crime against organization, and (iv) cyber crime against society at large. Such a crime can broadly be defined as criminal activities using information and communication technology including the followings, which can be committed against the above mentioned groups :

4.1. Cyber Crime against individuals

Hacking or Cracking, Illegal/Unauthorised access, Illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system),Data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data),E-mail spoofing, Spamming, Cheating and Fraud, Harassment and Cyber stalking, In decedent exposure, Defamation, Drug trafficking, Transmitting virus and worms, Intellectual property crimes, Computer and network resources vandalism, Internet time and information thefts, Forgery, Denial of services, Dissemination of obscene material.

4.2. Cyber Crime against property

Credit card fraud, Intellectual property crimes, Internet time theft.

4.3. Cyber Crime against organizations

Unauthorised control/access over the network resources and websites, Exposing indecent/obscene materials over the web pages, Virus attack, E-mail bombing, Salami attack, Logic bomb, Trojan horse, Data diddling, Blocking from access, Theft of important possessions, Terrorism against government organizations, Vandalising the infrastructure of the network.

---

15. Classification of Cyber crime, Report Cyber crime, http ://www.reportcybercrime.com/case_study_details_user.php,(accessed 1 January 2015).

4.4. Cyber Crime against society

Forgery, Online gambling, Trafficking, Pornography (especially child pornography), Financial crimes, Polluting the youth through indecent exposure, Web jacking.

The crimes mentioned above may be defined briefly as follows :

(a) ***Software Piracy*** : Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

(b) ***IRC Crime :*** Internet Relay Chat (IRC) servers have chat rooms in which people come together and chat with each other. Criminals use it for meeting co-conspirators and hackers use it for discussing their exploits/sharing the techniques. Paedophiles use chat rooms to allure small children.

a person who is sexually attracted to children

fade felano, bimohito kora

(c) ***Cyber Stalking*** *:* In order to harass a woman her telephone number is given to others as if she wants to be friends with males.

(d) ***Phishing*** *:* It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.

(e) ***Hacking*** *:* Hacking is a simple term which means illegal intrusion into a computer system without permission of the owner/user.

(f) ***Denial of Services*** *:* This is an act by a criminal who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide, or when internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(g) ***E-mail Spoofing*** *:* A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

(h) ***Spamming*** *:* Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

not asked for; given or done voluntarily

(i) ***Cyber Defamation*** *:* This occurs when defamation takes place with the help of computers and/or the internet e. g. if someone publishes defamatory matters about someone on a website or sends e-mails containing defamatory information.

manhanikor

(j) ***Harassment & Cyber Stalking*** *:* Cyber stalking mea following every moves of an individual over internet. It can be do with the help of many protocols available such as e- mail, ch rooms, user net groups etc.

(k) ***Salami Attack*** *:* When negligible amounts are removed an accumulated into something larger. These attacks are used for th commission of financial crimes. A criminal makes such program th deducts small amount like Tk. 3.50 per month from the account of a the customers of the bank and deposit the same in his account. In th case no account holder approaches the bank for such small amou but the criminal gains a huge amount.

(l) ***Intellectual Property Crimes*** *:* These include software pira like illegal copying of programs, distribution of copies of softwar and copyright infringement like trademark violations, stealin computer source code etc.

(m) ***Virus Attack*** *:* A computer virus is a computer program th can infect other computer programs by modifying them in such way as to include a possibly evolved copy of it. Viruses can be fi infecting or affecting boot sector of the computer. Worms, unlil viruses do not need the host to attach themselves.

(n) ***E-mail Bombing*** *:* This is another form of internet misu where individuals directs amass numbers of mail to the victim or a address in attempt to overflow the mailbox, which may be a individual or a company or even mail servers there by ultimatel resulting into crashing. There are two methods of perpetrating a email bomb which include mass mailing and list linking.

Logic Bomb *:* It is an event dependent program, as soon as th designated event occurs, it crashes the computer, releases a virus o any other harmful possibilities.

Trojan Horse *:* It is an unauthorized program which function from inside and seems to be an authorized program, thereb concealing what it is actually doing.

(o) ***Data Diddling*** *:* This kind of an attack involves altering ra data just before it is processed by a computer and then changing i back after the processing is completed.

jaliati

oporadhi,kukormokari

(p) ***Forgery*** *:* When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery.

when two or more things come together to form a new whole

(q) ***Cyber Terrorism*** *:* Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attack against computers, and networks where information is stored.

(r) ***Web Jacking*** *:* Hackers gain access and control over the website of another, even they change the content of website for fulfilling political or monetary objectives.

5. Present Scenario of Cyber Crimes in Bangladesh

Bangladesh does not have enough natural resources and has been trying to gain economic development through the utilization of Information Communication and Technology industry. Over the last few years, many nations have taken the advantage of opportunities afforded by ICT within a policy framework, laid down guidelines and preceded with the formulation of a national ICT strategy as a part of overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development.[16] The present Government has also declared the vision-2021 *i.e.* within 2021 this country is desired to become Digital Country and the per capita income equal to that of a middle-income country. In such a situation the Government and other concerns should address the scopes of commission of criminal activities that may be take place in the country as well as rest of the world with the expansion of internet and other networks for the purpose of converting the country into a digital one.

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is

16. Clause 1.3 of the National Information and Communication Technology (ICT) Policy (October, 2002), at http ://sdnbd.org/sdi/issues/IT-computer/itpolicy-bd-2002.htm, (accessed 12April 2015).

thought to be the earliest form of a computer, has been in India, Japan and China since around 3500 B.C. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. It resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime in the world history. A recent survey showed that a new cyber crime is being registered every 10 seconds in Britain. The situation of other countries in the world is almost the same and in some cases it is more critical and miserable. On July 4, 2009 two dozens of websites of South Korea and United States of America were under cyber attack and the attack was remarkably successful in limiting public access to victim websites such as government websites, treasury department, federal trade commission and secret service.[17] Information technology (IT) experts believe that about 90 per cent of cyber crimes remain unreported. In case of Bangladesh, the situation is getting worse day by day. The most common cyber attacks and crimes committed in Bangladesh are listed below :

showing in an insinuating way that one has some secret knowledge that may be harmful or embarrassing

i. Blackmailing girl by capturing their nude photographs and video on the sly and threatening to expose publicly. Such incidents are seen to be caused frequently by their boyfriends and others.

ii. A number of community websites have been introduced, which the young girls and boys are using to exchange phone numbers for posting hidden videos or even pictures with nudity etc.

iii. Hacking in the website of Bangladesh Computer Society, which took place after a few days of a three day-long 'Regional Seminar on Cyber Crime' in Dhaka.[18]

iv. E-mail threatening the Prime Minister Sheikh Hasina from a cyber cafe.[19]

v. Hacking into the internet account of Barisal Deputy Commissioner Office in 2003. The incident was revealed after the Deputy Commissioner Office received a heavily bloated Internet bill whereby a complaint was lodged with the Bangladesh Tar and Telephone Board (BTTB).[20]

vi. Hacking took place in the website of Bangladesh Rapid Action Battalion (RAB) in 2008, during the access to www.rab.gov.bd. The website read : "Hacked by Shahee Mirza."[21]

vii. Hacking the mail of BRAC[22] Bangladesh.

viii. Stealing the transaction report of Dhaka Stock Exchange through hacking.[23]

ix. Inserting naked pictures to the website of Bangladesh National Assembly.[24]

x. Inserting naked pictures into the website of Jamate Islami Bangladesh.[25]

xi. Inserting naked pictures into the website of the Daily Jugantor.[26]

xii. E-mail threatening to the Dhaka Office of the World Bank.[27]

CHAPTER-TWO
Cyber Jurisprudence and Jurisdiction of Cyber Law

1. Cyber Jurisprudence

1. Cyber Jurisprudence

Cyber jurisprudence is a legal term that refers to the concepts that govern cyberspace[1] and the internet.[2] The growth of fresh dimensions in law has been aided by the emergence of cyber jurisprudence around the world. Students and professionals who are interested in learning more about this unique and young subject of study have opened doors to new opportunities all across the world.

Similar issues will arise in the future in a variety of virtual space transactions, and we should psychologically prepare ourselves to adopt new conceptions of virtual property and laws governing virtual property. Of course, the first step is to apply existing physical society notions to virtual space, but we will eventually need to develop separate Cyber Jurisprudence to deal with such issues. For example, if the Bragg case[3] is determined in Bangladesh, the transfer should be governed by the "Transfer of Property Act" and the "Registration Act," as the nature of the property is "Land." The Transfer of Property Act, on the other hand, does not recognize "virtual land" as an immovable property, hence the transaction would be invalid under its terms.

---

1. Cyberspace is interconnected technology. The term entered the popular culture from science fiction and the arts but is now used by technology strategists, security professionals, government, military and industry leaders and entrepreneurs to describe the domain of the global technology environment.
2. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
3. Bragg v. Linden Research, Inc. - 487 F. Supp. 2d 593 (E.D. Pa. 2007).

Because the way the virtual property is used is a "Creation in the thoughts of an imaginative participant," certain of its attributes give it a "Intellectual Property Character." As a result, the disagreement should not be classified as a "Transfer of Property Dispute" or a "Contractual Property Dispute." Even if IPR rules such as copyright are the most closely related to the property, they do not pass the "Meeting of Minds" criteria.

It is observed that in recent judicial reviews, whenever implementation of existing laws of the real space to Cyber Space has encountered a conflict, the laws of the real space has prevailed. This tendency in due course is likely to develop into a principle of "Primacy of Meta Space" and become the bedrock of Jurisprudence.[4] However, when two laws of the real space itself come to conflict in the Cyber Space, the principle of "Primacy of the Meta Space" fails. This is reflected mainly in IPR[5] disputes and Jurisdiction disputes. Instead of fighting legal battles that can only end in victories for the one who has more financial resources, it is necessary to accept that "Real World Laws Cannot be Extended for Every Conflict in Cyber Space"

Now is the time, not when a Crisis occurs, when we should examine cyber jurisprudence in a cyber-society.[6] Left to their own devices, lawyers have a way of siphoning the joy out of anything. Stories like Bragg's probably have most attorneys drafting retainers for the personal injury claims of the 21st century rather than trying to shape a sustainable legal framework for cyber society. As we have discovered in the real world, the Internet has rarely offered easy opportunities to co-opt existing law. Yet, we are presented with an unprecedented opportunity to re-imagine the role of law, to redefine

---

4. Ahmed, Dr. Zulfiquar; Cyber Law in Bangladesh, Published by- Sheikh Mohammad Ali Hasan, National Law Book Company, Nilkhet, Dhaka-1205. P. 36-37
5. Intellectual Property Right.
6. Human-computer interaction has progressed to the point where the term "cyber society" has been coined. This relationship (human-computer interaction) comprises the relationship between a society of humans and a network of computers, not just a single human and a single computer.

its relation with people, to create a legal system heretofore undreamed of. The architects of Second Life, Wikipedia, and others are anything but traditional.[7]

Cyber jurisprudence gives an analysis of the law where, is no land and even there is no border, where all things may be different from the physical world, they may be virtual from origin and nature. We may find virtual world with virtual rules and policies, along with the virtual subject matter, virtual contract, virtual disputes, virtual property, virtual possession and virtual court. Cyber jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace. It emphasis to recognize cyber uniform rules and policies at international level.[8]

Legal issues relating to the electronic and internet in this contemporary world as being necessitated of new kind of jurisprudence, which may be cyber jurisprudence. Cyber jurisprudence gives an analysis of the law where, is no land and even there is no border, where all things may be different from the physical world, they may be virtual from origin and nature.

Cyber jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace. It emphasis to recognize cyber uniform rules and policies at international level, it also discusses with the netizens[9] and netiquates.[10]

2. Claiming new dynamism in jurisprudence

During the preceding decade, the Internet has grown dramatically. Over 9.4 million computers and up to 40 million people are now connected to the Internet, according to estimates. By the end of the century, there will almost certainly be over 200 million Internet users. Without a doubt, cyber law is a promising topic.

---

7. Ibid. P. 38-39
8. http://www.bloggernews.net/11215
9. The term netizen is a portmanteau of the words Internet and citizen as in "citizen of the net". It describes a person actively involved in online communities or the Internet in general.
10. Netiquette is short for "Internet etiquette." Just like etiquette is a code of polite behavior in society, netiquette is a code of good behavior on the Internet.

Cyber law covers cybercrime, online trade, freedom of expression, intellectual property rights, and privacy rights. Cybercrime includes credit card fraud, unlawful access to computer systems, child pornography, software piracy, and cyber stalking. It's worth emphasizing that in order to identify cybercrime and cyber criminals, as well as to resolve jurisdictional confusion, cyberspace architecture and access channels must be addressed.

3. Genesis & the architectural factors of cyber territory

The Internet mechanism can be considered as the global connection of interconnected computer networks straddling state and national borders. The perception of interconnecting computers originally commenced in 1969 as part of a military program called "ARPANET."

4. Territorial monopoly versus cyber space

The law is conceived and spoken of as territorial .the enforcement of law is undoubtedly territorial in the same way as the state is territorial; that is to say the state power is in time of peace exercised only within the territory of the state on its public ships and aircraft and on vessels and aircraft registered under its law.

But the law applicable to the cyber space is quite different form territorial –based law because of the peculiarity of cyber world bearing virtual character of visual nature. It should be considered that the events or activities ensued in cyber world causing legal consequences are not less than those in the real world are.

Accordingly a distinct set of laws and legal principles has become inevitable to be adopted with same mission holding sprit of punishment or remedy. The financial damage sustained by the individual or by corporate body or by governmental organs is claiming billions of dollars, which sometimes surpass traditional territorial-based damage.

5. Jurisdictional confusion

The developing law on jurisdiction must address whether a specific event in Cyberspace is governed by the laws of the state or

country in which the Website is located, the laws of the state or country in which the Internet service provider is located, the laws of the state or country in which the user is located, or perhaps all of these laws.

A number of observers have suggested that cyberspace be considered as a distinct jurisdiction. In practice, the courts haven't agreed with this viewpoint, and legislatures in many states[11] haven't addressed it.

Courts must balance numerous issues when deciding lawsuits involving foreign nationals. Courts must evaluate the procedural and substantive policies of foreign countries whose interests are impacted by the court's assertion of jurisdiction on a case-by-case basis. When extending authority into the international realm, extreme caution and caution are required. When suing a foreign national, there is a greater jurisdictional bar because of the principle of sovereign equality.

6. Cyber terrorism, a real menace

It fear is measureless, its impact is great, its target is human race, it exist somewhere around us, but invisible. It may occur anytime anywhere in the world. It has not been experienced even imagined by man of today, in past. It may reshape in any form. Its alarming aspect is to be developed as an ideology. Its intensity of destruction may severe more than devastation, man of our age ever be thought. No man or country obviously favor or supports it but surprisingly it is being faced by every man and every country. It is unfortunately new phenomenon, it is terrorism in the real world or it may be cyber terrorism in cyberspace.

To define the cyber terrorism many analysts and internet intellectuals draw the almost same parameters, Mark Pollitte of Federal Bureau of Investigation defines the cyber terrorism as follow;

Cyber Terrorism is, "the premeditated, politically motivated attack against information, computer systems, computer programs,

11. http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html

sorasori songghorse lipto noi amon bekti,like a civilian

and data which results in violence against noncombatant targets by sub-national groups or clandestine agents". secret

Computer technology and internet is going to be indispensable part of to-day society and advanced country are becoming more and more dependant and reliant of computer and internet technology. The critics who criticized the John Arquilla who depicted a scenario of mayhem of destruction by cyber terrorism, now are reconsidering their ideas and criticism after the unfortunate terrorist event of 9/11 in USA.[12]

Cyber terrorism can affect a specific community of people as well as entire nation, the example of Australian man in 2001 would be amplify when he used the internet and stolen control software to release one million liters of raw sewage in the public park, but his intention was not to terrorise the people but just to get back it job in the concerned company. A more baleful Cyber Terrorism intrigue that was stymied would have occurred sometime in 1996 in London (2003). Members of the Irish Republican Army were planning to blow up and destroy six key electric substations in London. Had the IRA succeeded in their goal, they would have disrupted power to major portions of London for months. To figure out which substations to bomb, they used libraries and open sources of information to select key nodes that would impact the grid the most. This example would have been a terror attack and would have stuck fear into the people of London. This would also be an example of a physical attack on computer systems.

According to The Guardian, "Nato is treating the threat of cyber warfare as seriously as the risk of a missile strike". If a Governmental Organization like NATO thinks that cyber warfare is that dangerous, then why don't more people think of it that way. The reason for this could be that the general population of the world does not feel the impact of these cyber terrorist attacks.

Cyber terrorism has been accruing with last twenty years and as time progressed and more and more nations become even more computerized, there will be more and more attacks through internet.

---

12. "http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html"

The measures are available to counter the cyber terrorism as US Department Defense charged with the USSD with duty if combating the cyber terrorism. The sensitive data can be safe and secure by the 'air tight' mechanism which has adopted by the FBI successfully. Up to date Antivirus system, firewall and root-kit can play important role to protect the internet and computer system. Intrusion detection system can also help if someone's network has been attacked. A network also requires VPN's if they were people accessing network remotely. In the last but not least exemplary punishments and fine should introduce through the laws against the cyber terrorists as the Pakistan has introduce the Prevention of Electronic Crime Ordinance 2007 where Section 17 exemplary punishments has been provided for the cyber terrorists.[13]

The contemporary world is declared to be a global village, collective efforts of the global nations against this menace to next to this human civilization, can provide potential preventive measures against the cyber-criminal and cyber terrorists. The existence of cyber terrorism cannot be denied it's real but it would be blissful for mankind not to record a single exact cyber terrorist event in its history.

2. Jurisdiction of Cyber Law

6882(1) ICT Act

1. Establishment and Jurisdiction of Cyber Tribunal in Bangladesh

Government of Bangladesh by gazette notification, for the purpose of quick and effective trial of crimes committed under the Act, may establish one or more cyber tribunal, sometimes which is stated later as tribunal under section 68(1) of the ICT Act. The cyber tribunal that is stated in section (1) of the section will comprise of a session judge or an assistant session judge appointed by the government with consulting with the Supreme Court; and such a judge appointed will be introduced —judge, cyber tribunal.[14]

---

13. "http://www.articlesbase.com/cyber-law-articles/cyber-terrorism-a-real-menace-514849.html"
14. The information and Communication Technology Act, 2006, S. 68(2)

The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act.[15]

The special tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order.[16]

2. Establishment & Jurisdiction of Cyber Appellate Tribunal in Bangladesh

The ICT Act envisages the establishment of the Cyber Appellate Tribunal at one or more places as the government may deem fit. Section 82(1) of the ICT Act provides that the government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The cyber appellate tribunal will be comprised of a chairman and two members appointed by the government.[17]

The chairman will be such a person, who was a justice of the Supreme Court or is continuing his post or capable to be appointed as such and one of the member will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed.[18]

The chairman and the members will be in their post minimum 3 years and maximum 5 years and the conditions of their service will be decided by the governments.[19]

The Cyber Appellate Tribunal shall have the power to hear and settle the appeal made against the judgment of cyber tribunal and session courts.[20]

The appeal tribunal will have authority of supporting, canceling, changing, or editing the judgment of the cyber tribunal.[21]

---

15. Ibid., s. 68(3)
16. Ibid., s. 68(4)
17. Ibid., s. 82(2)
18. Ibid., s. 82(3)
19. Ibid., s. 82(4)
20. Ibid., s. 83(1)
21. Ibid., s. 83(2)

come into the possession of

The decision of the appellate tribunal will be final. The Cyber Appellate Tribunal does not seem to be vested with any original jurisdiction; it has been vested with the powers of a Civil Court in respect of, interlay lay between or among

a) Summoning and examining of witnesses
b) Requiring production of document
c) Receiving evidence
d) Issuing commissions and
e) Reviewing its decisions.[22]

3. Punishment for Cyber Crime in Bangladesh ***

The following activities are regarded as offence according to section-54, such as; If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,—

a) Accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so[23]
b) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) Damages or causes to be damaged willingly to any computer, computer system or computer network. data, computer database or any other programmers residing in such computer, computer system or computer network;
e) Disrupts or causes disruption of any computer, computer system or computer network;

---

22. Zulfiquar Ahmed, pp. 150-152
23. The information and Communication Technology Act, 2006, S. 54(a)

f) Denies of causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network, in contravention of the provisions of this Act, rules or regulations made there under;

h) for the purpose of advertisement of goods and services, generates or causes generation of spasm or sends unwanted electronic mails without any permission of the originator or subscriber;

i) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network. If any person commits any of the aforesaid offence, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both. The ICT Act describe punishment for tampering with computer source code is if any person intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network. When the computer source code is required to be kept or maintained by any law for time being in force, then this activity of his will be regarded as offence.[24]

Whoever commits this type of offence shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to Taka three lakhs, or with both. The ICT Act describe punishment for hacking with computer system is if any person, intentionally cause wrongful loss or damage to the public or

24. Ibid., s. 55

any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.[25]

or cause damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him; then such activity shall be treated as hacking offence.[26]

Whoever commits hacking offence, he shall be punishable with imprisonment for a term which may extend to ten years, or with time which may extend to Taka one crore, or withboth.The ICT Act describe punishment for publishing fake, obscene or defaming information in electronic form is if any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene orits effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.[27]

make someone immoral

cause injury

khoti kora, nosto kora

bring about or initiate an action

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to ten years and with fine which may extend to Taka one crore. The ICT Act describe punishment for misrepresentation and obscuring information is if any person makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate shall be regarded as an offence[28]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or

---

25. Ibid., s. 56(1)
26. Ibid., s. 56(2)
27. Ibid., s. 57
28. Ibid., s. 62

the act of trying to achieve something

with fine which may extend to Taka two lakhs, or with both. The ICT Act describe punishment for disclosure of confidentiality and privacy is no person who, in pursuance of any of the powers given conferred under this Act, or rules and regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.[29]

Whoever commits these types of offence he shall be punishable with imprisonment for a term which may extend to two years, or with time which may extend to Taka two lakhs, or with both. The ICT Act describe punishment for using computer for committing an offence is whosoever knowingly assists committing crimes under this Act, using any computer, e-mailor computer network, resource or system shall be regarded as an offence.[30]

jekono bekti, whoever

Whoever aids committing these types of offence he shall be punishable with the punishment provided for the core offence. The ICT Act describe punishment for Offences committed by companies etc then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.[31]

longhon, break

application prochesta

appeal kora, abedon kora

4. Cases under ICT Law in Bangladesh

Bangladesh does not have enough natural resource and has trying to achieve the economic development through the utilization of ICT industry. Over the last few years, many nations have taken advantage of the opportunities afforded by ICT within a policy framework, laid down guidelines and preceded with the formulation

29. Ibid., s. 63
30. Ibid., s. 66
31. Ibid., s. 67

of a national ICT strategy as a part of the overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development.[32]

The present government has also declared the vision2021 i.e. within 2021 this country will become Digital Country and the percaptia income will be equal to a middle income country. But the government as well as other concerns should consider crimes that they may be committed in this world with the expansion of internet and her/networks to convert this country.

The utilitarian approach to ethics is a consequentialist ethical theory that suggests that the moral worth of an action is determined by its overall utility or usefulness. In other words, the rightness or wrongness of an action is judged by the overall happiness or well-being it produces. This approach is associated with thinkers like Jeremy Bentham and John Stuart Mill.

The basic idea behind utilitarianism is to maximize the overall happiness or pleasure and minimize suffering. Utilitarianism is often described by the principle of the greatest happiness or the greatest good for the greatest number.

Here's a simplified example to illustrate the utilitarian approach:

Imagine a scenario where a government has to decide whether or not to build a new hospital. The utilitarian approach would involve weighing the potential benefits and drawbacks of the decision in terms of overall happiness and suffering.

Benefits:

The hospital could provide medical care to a large number of people, improving their health and well-being.
It may create job opportunities for the local community.
Drawbacks:

The construction of the hospital might require the displacement of some residents or the destruction of local businesses.
It will require a significant financial investment.
The utilitarian analysis would involve comparing the overall happiness generated by the benefits against the suffering caused by the drawbacks. If the overall happiness (utility) generated by building the hospital outweighs the suffering, the utilitarian approach would recommend building the hospital.

It's important to note that utilitarianism doesn't always provide clear-cut answers, and critics argue that it may lead to morally questionable decisions if the well-being of a minority is sacrificed for the greater good of the majority. Additionally, determining and measuring happiness or well-being can be subjective and complex.

32 https://www.thedailystar.net/drivers-economy/ict-opens-new-prospects-

CHAPTER FOUR
Internet Privacy

1. Definition

The degree of privacy and security of personal data disclosed on the Internet is referred to as Internet privacy. It's a broad word that encompasses a wide range of elements, methods, and technologies that are used to safeguard sensitive and private data, communications, and preferences.

Users value privacy and anonymity on the internet, particularly as e-commerce grows in popularity. Theft threats and privacy breaches are typical concerns for every website in development. Online privacy is another term for internet privacy.

The internet is one of the most user-friendly communication technologies ever devised by humanity. It's fast, easy, and inexpensive...and it's just as insecure as it is quick, convenient, and inexpensive. A message written months ago may stay on an ISP's server or as a backup, and anybody who knows how to do so may readily recover it. This is information that you have destroyed for a specific reason : you do not want it to be accessible by others once you have done using it. There have been instances when information was recovered up to 6 months later and utilized as evidence in a court case.

If someone wants to, intercepting your communications or information may be very easy. This might just be an administrator from your ISP or your company's network. It may also be a corporate rival, legal adversary, or government entity with much more severe objectives.

There are a plethora of options for safeguarding your online privacy. Some are big and complicated, while others are quite basic. The key point to remember is that certain techniques are nearly completely insecure, while others are almost impenetrable.

It is a widespread misunderstanding that anonymity equates to privacy. Although anonymity and privacy are linked, their meanings are vastly different.

2. Explains Internet Privacy PPSM

Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Internet privacy risks include :

A. **Phishing** : An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.

B. **Pharming** : An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.

C. **Spyware** : An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.

D. **Malware** : An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Internet privacy violation risks may be minimized, as follows :

A. Always use preventative software applications, such as anti-virus, anti-malware, anti-spam and firewalls

B. Avoid shopping on unreliable websites

C. Avoid exposing personal data on websites with lower security levels

D. Clear the browser's cache and browsing history on a consistent basis

E. Always use very strong passwords consisting of letters, numerals and special characters

3. Risks to Internet privacy *

Companies are paid to monitor which websites individuals visit and then utilize the data, such as delivering advertisements depending on one's surfing history. People can reveal personal

conclude (something) from evidence, to make a well informed guess

information in a variety of ways, including through the use of "social media" and by sending bank and credit card information to various websites. Furthermore, directly observed behavior, such as browsing logs, search queries, or Facebook profile contents, can be automatically processed to infer potentially more intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality.[1]. Furthermore, even without any previous behavioral data, tracking onsite user interaction can yield a large number of insights, such as post code, name, and local address.[2]

onadhikarprobes

an accurate and deep understanding

Those worried about Internet privacy often list a variety of privacy hazards — occurrences that may violate privacy — that can occur as a result of using the Internet. These activities vary from the collection of user statistics to more harmful activities such as the distribution of malware and the exploitation of different types of vulnerabilities (software faults).

Several social networking sites make an effort to protect their users' personal information. All registered users on Facebook, for example, have access to privacy settings, which allow them to prevent specific people from seeing their profile, choose their "friends," and limit who gets access to their photos and videos. Other social networking services, such as Google Plus and Twitter, include privacy options as well. When submitting personal information on the internet, the user may utilize these options.

Children and adolescents often use the Internet (including social media) in ways which risk their privacy : a cause for growing concern among parents. Young people also may not realise that all their information and browsing can and may be tracked while visiting a particular site, and that it is up to them to protect their own privacy. They must be informed about all these risks. For example,

---

1. *Kosinski, Michal; Stillwell, D.; Graepel, T. (2013).* "Private traits and attributes are predictable from digital records of human behavior". *Proceedings of the National Academy of Sciences. 110 (15) : 5802–5805.* doi :10.1073/pnas.1218772110. PMC 3625324. PMID 23479631.
2. *Matthees, Robert.* "Cross-Device Tracking : Advanced Client ID/Fingerprint User Identification". *www.robert-matthees.de.* Retrieved 2017-08-29.

on Twitter, threats include shortened links that lead one to potentially harmful places. In their email inbox, threats include email scams and attachments that get them to install malware and disclose personal information. On Torrent sites, threats include malware hiding in video, music, and software downloads. Even when using a Smartphone, threats include geolocation, meaning that one's phone can detect where they are and post it online for all to see. Users can protect themselves by updating virus protection, using security settings, downloading patches, installing a firewall, screening email, shutting down spyware, controlling cookies, using encryption, fending off browser hijackers, and blocking pop-ups.[3]

The privacy concerns of Internet users pose a serious challenge. In an online survey conducted, approximately seven out of ten individuals responded that what worries them most is their privacy over the Internet than over the mail or phone. Internet privacy is slowly but surely becoming a threat, as a person's personal data may slip into the wrong hands if passed around through the Web.[4]

to defend oneself against (someone or something) They succeeded in fending off the attack/attackers

4. Privacy issues of social networking sites

Web 2.0 has resulted in social profiling, which is a rising issue for Internet privacy. Web 2.0 is a system that allows people to share and collaborate on information on the internet via social networking sites like Facebook, Instagram, Twitter, and MySpace. Since the late 2000s, several social networking services have experienced a surge in popularity. Many individuals are disclosing personal information on the internet as a result of these websites.

a sudden powerful forward or upward movement

5. Other potential Internet privacy risks

A. Malware is a term short for "malicious software" and is used to describe software to cause damage to a single

---

3. *Youn, S. (2009). "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents". Journal of Consumer Affairs. 43 (3) : 389–418.* doi :10.1111/j.1745-6606.2009.01146.x
4. *Larose, Robert; Choi, Hyunyi (November 1, 1999).* "Privacy Issues in Internet Surveys". *Social Science Computer Review. 17 (9).* doi :10.1177/089443939901700402

computer, server, or computer network whether that is through the use of a virus, trojan horse, spyware, etc.[5]

B. Spyware is a piece of software that obtains information from a user's computer without that user's consent.[6]

C. A web bug is an object embedded into a web page or email and is usually invisible to the user of the website or reader of the email. It allows checking to see if a person has looked at a particular website or read a specific email message.

D. Phishing is a criminally fraudulent process of trying to obtain sensitive information such as user names, passwords, credit card or bank information. Phishing is an internet crime in which someone masquerades as a trustworthy entity in some form of electronic communication.

camouflage,disguise,pretend to be someone

E. Pharming is a hacker's attempt to redirect traffic from a legitimate website to a completely different internet address. Pharming can be conducted by changing the hosts file on a victim's computer or by exploiting a vulnerability on the DNS server.

F. Social engineering where people are manipulated or tricked into performing actions or divulging confidential information.[7]

revealing

G. Malicious proxy server (or other "anonymity" services).

H. Use of weak passwords that are short, consist of all numbers, all lowercase or all uppercase letters, or that can be easily guessed such as single words, common phrases, a person's name, a pet's name, the name of a place, an address, a phone number, a social security number, or a birth date.[8]

---

https ://technet.microsoft.com

Ibid.

"Social Engineering : The Basics".

I. Using the same login name and/or password for multiple accounts where one compromised account leads to other accounts being compromised.[9]

J. Allowing unused or little used accounts, where unauthorized use is likely to go unnoticed, to remain active.[10]

K. Using out-of-date software that may contain vulnerabilities that have been fixed in newer more up-to-date versions.

L. WebRTC is a protocol which suffers from a serious security flaw that compromises the privacy of VPN-tunnels, by allowing the true IP address of the user to be read. It is enabled by default in major browsers such as Firefox and Google Chrome.[11]

---

9. Digital Tools to Curb Snooping", Somini Sengupta, New York Times, 17 July 2013
10. Top 5 Online Privacy Tips". *Net-Security*. Retrieved 2012-11-23.
11. Huge Security Flaw Leaks VPN Users' Real IP-addresses TorrentFreak.com (2015-01-30). Retrieved on 2015-02-21

CHAPTER SEVEN
E-learning

1. Meaning of E-Learning

E-learning is the transmission of skills and information via a network. E-learning is a method of learning that involves the use of electronic applications and procedures. Web-based learning, computer-based learning, virtual classrooms, and digital collaboration are all examples of electronic applications in e-learning. The internet, audio or video tape, satellite TV, and CD-ROM are all used to provide learning materials. E-learning allows you to study at your own pace.

The term 'E-Learning' means 'electronic Learning' that encompasses all forms of technology enhanced learning. E-Learning is the use of technology to enable people to learn anytime and anywhere. E-Learning can include training, the delivery of just-in-time information and guidance from experts. These services are delivered, enabled or mediated by ICT[1] for the purposes of delivering education.

E-Learning is a catch-all term that covers a wide range of instructional material that can be delivered on a CD-ROM or DVD, over a LAN[2], or on the Internet. It includes CBT[3], WBT[4], EPSS[5], distance or online learning and online tutorials. The major advantage to students is its easy access.

2. The history of E-Learning

The term "e-learning" has only been around since 1999, when it was coined at a CBT systems lecture. Other terms, such as "online

---

1. Information & Communication Technology Act, 2006
2. Local area network
3. Computer-Based Training
4. Web-Based Training
5. Electronic Performance Support Systems

CHAPTER EIGHT

Prevention of Cyber Crimes

1. Introduction :

In recent years, computer crime, also known as cyber crime, has grown in severity and regularity, and as a result, it has become a significant source of worry for businesses, colleges, and organizations. Governments, police departments, and intelligence agencies all around the globe have begun to respond against cybercrime. This chapter offers an introduction of cyber crime and analyzes knowledge of the issue among various respondents in Bangladesh, as well as highlighting the severity of the problem and the urgent need to mitigate its global effect.

Cyber crime is still a low priority in Bangladesh. Though computers are becoming common house hold items and the numbers of internet users have already crossed thirty millions, very few computer related offences are reported to the police. In Bangladesh there is no Computer Emergency Response Team (CERT),[1] no cyber police or virtual police to handle the incidents such as computer abuses, hack attempts and other information security breaches. Bangladesh has enacted the Information and Communication Technology ACT of 2006[2] with a maximum punishment of 14 years of imprisonment or maximum fine of 10 million taka[3] or with both for a cyber crime. Still the legislation seems not to be sufficient to effectively fight cyber crimes in the country.

a failure to do what is required by a law, an agreement, or a duty

act out on stage

---

1. Computer Emergency Response Team' may be called CERT throughout the study.
2. Act no 39 of 2006.
3. Bangladeshi currency.

The present Government is expected to invest millions of taka to materialize its promise to build a digital Bangladesh. This is why the issue of prevention of cyber crime must get due priority and a considerable portion of budget should be allocated to ensure the issue. This chapter finds the policy of prevention of cyber crimes in Bangladesh and also provides some sort of recommendations.

2. Effects of Cyber Crime

Criminals make use of technology in a variety of ways. Scammers and other criminals benefit greatly from the Internet because it enables them to do their business while remaining anonymous online. Cybercrime has an impact on society in a variety of ways, both online and offline.

2. 1. Economic Impacts

Because cybercrime is designed to harm the image of a person, a commercial company, or a government agency, it has a significant economic impact, such as when a financial institution's system, such as a bank, is hacked. In every transaction, banks and their customers must operate in good faith. Banks must maintain their good faith by not leaking a client's information, since this may lead to a cold war. When a cyber-criminal successfully hacks into a bank's system, the bank's good faith is jeopardized, since the criminal may steal a client's money or publish the client's personal information on a website, eroding the customer's confidence. This tarnishes a bank's reputation, since the customer may be ready to seek out better opportunities.[4] put (someone or something) into a situation in which there is a danger of loss, harm,

2. 2. Social Impacts

Trying to overcome a cyber attack for a developing country may not a good experience, as trying to mend the damage might cost repair

4. Nadia Khadam, Insight to Cybercrime, available at http :// www. hanyang.ac.kr/ home_news/H5EAFA/0002/101/2012/29-3.pdf,(accessed 4 February 2016).

millions of dollars which may not be readily available. Due to cyber attacks, the citizens of developed or developing countries start avoiding the advent of technology as they feel insecure. This may destroy the concept of globalization as people might not want to be a part of social networking.[5]

2. 3. Political Impacts

Cyber crime has a big impact on the political world, particularly when governmental computer networks are targeted and attacked. This decreases the ability of international organizations investing resources in developing countries.[6] When this happens it increases white collar criminal activities and funding of anti-government regimes in order to the Government, which will definitely affect the political scenes in a country.

3. Survey

Due to the exploratory nature of the task, survey questions provide a basis for the research in order to find the awareness of cyber crime among the respondents as well as to find out what type of cyber crimes are occurring these days in Bangladesh and what should be done to prevent Cyber Crime.

3.1. Sample and Respondents

The primary target respondents are working professionals who are aware of the various computer crimes and security issues within their organizations. Typically, they are senior managers, IT[7] administrators and IT security consultants. Simple random sampling is the primary sampling method used when selecting the sample for survey.

---

5. Ibid.
6. '*International Journal of Engineering Sciences and Emerging Technologies*,' vol.6, no.2, 2013, pp. 142-153.
7. The term `information technology' may be meant by IT throughout the study.

IT professionals, 59% businessmen and 22% advocates feel that it is spreading very fast; and 33% students, 31% IT professionals, 18.5% businessmen and 52% advocates are of the opinion that it is spreading at an average; whereas 42% students,16% IT professionals, 22.5% businessmen and 26% advocates believe that it is spreading very slow.

4. Critical Analysis

It is true that prevention is preferable than treatment. When using the internet, it is usually a good idea to take some precautions. Bangladesh is a member of the international community, and the country is emerging as an economic and political power in the South Asian region, with an annual GDP growth rate of no less than 6.5 percent in recent years, including 7.05 percent in 2016, and a cyber revolution under the slogan "Digital Bangladesh," as evidenced by her provision of computer and Internet facilities throughout the country. It has the potential to damage not only the Internet environment, but also the country's economic situation and growth, as shown by the recent Reserve Hacking of 80 billion US dollars at the Bangladesh Bank, the country's central bank. All of the nation's economic, social, and political environments, as mentioned above, may become susceptible as a result of cyber criminal actions that occur inside or outside the country. As a result, it is past time for the people of the nation to become not only conscious of the problem but also genuine in their dealings with the Internet or the computer world. The following points should be kept in mind in this regard :

babostha, arrangement

influenced or harmed by a particular thing

1. Children should not give their identifying information such as their names, home addresses, school names, and phone numbers in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive.[9] They should remember that people online might not be who they seem.

---

9. https ://www.privacyrights.org/content/childrens-safetyinternet(accessed 1 July2015).

2. Parents should use content filtering software on their computers so that their child is protected from pornography, gambling, drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3. People should keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4. People should always use latest and update anti-virus software to guard against virus attacks.
5. People should never send credit card number to any site which is not secured.
6. People should not do panic if find something harmful. If there arises any immediate physical danger they should contact local police. Moreover, they should avoid getting into huge arguments online during chat and discussions with other users, and be careful about personal information about themselves online.
7. People should be cautious on meeting online introduced person. They should try to keep record of all communication for evidence and not edit it any way.
8. Big organizations should implement access control system using firewalls, which allow only authorized communications between internal and external network.
9. The use of password is most common for security of network system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.
10. System managers should track down the holes, bugs and weaknesses in the network before the intruders do.

5. Practices Recommended for Cyber Crime Prevention in Bangladesh *****

Cyber attacks could emerge as a major threat to the digital transformation of Bangladesh given the poor knowledge and lack of government initiatives to counter the growing problem, according to the study. Therefore it is always better to take certain precaution while operating the net.

1. **Firewalls**[10] **:** These are programs that protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom the user permits.
2. **Frequent password changing :** With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.
3. **Safe surfing :** Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, and visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimize the risk.
4. **Frequent virus checks** : One should frequently check ones computer for viruses and worms. Also any external medium such as floppy disks and CD[11] ROMS[12] should always be virus checked before running.

---

10. A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
11. A compact disc [sometimes spelled *disk*] (CD) is a small, portable, round medium made of moulded polymer (close in size to the floppy disk) for electronically recording, storing, and playing back audio, video, text, and other information in digital form.
12. Pronounced *rahm*, acronym for *read-only memory*, computer memory on which data has been pre recorded. Once data has been written onto a ROM chip, it cannot be removed and can only be read.

5. **Email filters** : These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
6. **Online photography** : Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
7. **Undergo** : Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
8. **Credit Card security** : To guard against frauds, one should never send credit card number to any site that is not secured.

to make bad : corrupt

9. **Depravation in children** : Always keep a watch on the sites that children are accessing for the purpose of preventing any kind of harassment or depravation in children.
10. **Secure the Program** : It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
11. **Watching Traffic** : Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

onadhikar-probes,trespass

12. **Protecting internal network** : Web servers running public sites must be physically separate and protected from internal corporate network.
13. **Backup** : Make Backups of Important Files and Folders to protect important files and records on computer if one's computer malfunctions or is destroyed by a successful attacker.
14. **Off internet** : Disconnect from internet when not in use.

Some other advises to be addressed while using the Internet or computers :

1. Habitually download security protection update patches & keep your browser and operating system up to date.

2. Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
3. Disable file sharing on computers.
4. Turn off the network during extended periods of non-use, etc.
5. Check online account frequently and make sure all listed transactions are valid. Use a variety of passwords, not the same for all the accounts.
6. Never respond to text messages from someone unknown.
7. Avoid posting cell phone number online.
8. Open email attachment carefully.

6. Policies Recommended for Prevention of Cyber Crime in Bangladesh

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bringing into practical part so that the practices become easier to implement. Policies recommended are as follows :

1. Integrated policies are required to ensure the effective benefits from the information system. The basic challenge and issue in the development of a cyber society is the lack of financial and trained human resources.
2. A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secured and free from cyber crime and within the reach of a common man.
3. Promotion of research & development in ICT[13] area and also in Human Resource is to be a core part of the system.

---

13. ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing : radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

4. Up-to-date, common, and mutually supporting cyber laws should be there to fight with cyber crimes and protection of intellectual property rights towards the creation of cyber-crime free information society.
5. Adoption of ICT standards, regulation, and quality assurance is a necessity to foster high quality of services and productions that keep competition in place for the benefits of the communities within each country.
6. High levels of awareness in each part of the society should be there in regard to information security and cyber crimes and increased exchange of information on information security and cyber crime at the regional and national levels should be there.
7. Effective mechanisms should be there for the detection and prevention of cyber crimes and for improving protection against, detection of, and responses to, cyber crimes, at the lower level itself.
8. Conducting national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and private sector using different media is also a must.
9. The government should educate and involve the media professionals, and then encourage them to increase public awareness.
10. People should engage large private sector corporations and industry associations in the sponsorship of awareness programs.
11. Stress should be laid on less developed countries on effective systems for protection against, detection of and responses to, cyber crime.
12. People should promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.
13. Law enforcement personnel must be trained and equipped in addressing high-tech crimes. Legal systems should

permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

14. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
15. People should use established network of knowledgeable personnel to ensure a timely and effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis.
16. The government should welcome outsourcing initiatives to prepare a galaxy of virtual police officers and establish few cyber police stations across the country as soon as possible. These cyber crime fighters should be given specialized training home and abroad.
17. Awareness raising, education, and technical support to prevent e-crime[14] is essential, but without discouraging the development of e-commerce.

7. Minimizing the Risk of Becoming a Cyber Crime Victim

As widespread as cybercrime appears to be, it would be easy to conclude there is little anyone can do to avoid becoming a victim. However, the prevalence of cybercrime does not mean that victimization is inevitable or that people should avoid using the Internet. Users can make themselves aware of the vulnerabilities its use creates and can take steps to reduce their risks.

1. Use strong passwords : Use separate ID[15]/password combinations for different accounts, and avoid writing them down. Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis.[16]

---

14. E-crime is any form of anti-social behaviour over the internet or via electronic devices. It is an attack or abuse, using technology, which is intended to cause another person harm, distress or personal loss.
15. Own password for access different digital account.
16. The Office of Angel Cruz, Chief Information Security Officer, State of Texas September 2012 , Volume 6, Issue 8

2. To secure computer : Firewalls are the first line of cyber defence; they block connections from suspicious traffic and keep out some types of viruses and hackers.

3. Use anti-virus/malware software : Prevent viruses from infecting computer by installing and regularly updating anti-virus software.

4. Block spyware attacks : Prevent spyware from infiltrating computer by installing and updating anti-spyware software.

5. Secure the mobile device : Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources only. Do not store unnecessary or sensitive information on mobile device. Most importantly, keep the device physically secured; millions of mobile devices are lost each year. In case of loss of dévice, report it immediately to carrier and/or organization. Some devices allow remote data erasing. Always protect mobile device password.[17]

6. Install the latest operating system updates : Keep applications and operating system, e.g., Windows, Mac, Linux,[18] current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

7. Protect the data : Use encryption for most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of important data.

8. Secure the wireless network : Wi-Fi[19] (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid conducting sensitive transactions on these networks.

9. Protect e-identity : Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secured, especially when making online purchases, or ensure that enabled privacy settings, e.g., when accessing/using social networking sites,

---

17. Ibid.
18. Applications of computer operating system may be called Windows, Mac, Linux throughout the study.
19. WiFi is a technology that uses radio waves to provide network connectivity.

such as Facebook, Twitter, YouTube, etc. Once something is posted on the Internet it may be there forever.

10. Avoid being scammed : Never reply to emails that ask to verify your information or confirm your user ID or password. Don't click on a link or file of an unknown origin. Check the source of the message; when in doubt verify the source.

8. Recommendations

The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their "attack surface" and mitigate the risks. For this purpose the following recommendations may be proposed.

prokas, disclosure

8.1 Education on Cyber Crimes :

Education is the most important strategy that can be used in combating crimes in the cyberspace. People can be educated in workshops and seminars specially planned by organizations taking into account cyber safety. It is recommended that this should be done on a regular basis as new employees are always recruited. In doing so employees or system users may learn how to keep personal and organization information safe, then the cyber-criminals will flee. The study shows that most of the cyber-criminals of Bangladesh are youths, students of tertiary institutions, or they have graduated from tertiary institutions. It is recommended that tertiary institutes should introduce studies on cyber crimes, and cyber management and its prevention as part of their course curriculum. In doing so the present social changes happening in the country are to be addressed.

8.2. Creating Cyber Employment :

The Government should act swiftly on domestic cyber crime legislations and enact a comprehensive law on cyber crimes. In order for the law to be effective and efficient the Government should

empower graduates by providing employment or funds to be able to employee themselves with their ideas on cyber-crimes.[20]

8.3. Providing Training :

The Bangladesh Government should also make provisions for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals, whatever intelligent and cunning they may be.

8.4. Cooperation to Government :

For the government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb cyber crimes, it is recommended that there is a need for them to understand the technology and the individuals who engage in such criminal acts. The findings show that cyber criminals are part and parcel of the society, as such, prevention of cyber crimes requires the cooperation of all the citizens and not of the law enforcement agencies alone.

8.5. Identification of Cyber Criminals :

Everyone should watch and report to law enforcement agencies quickly when they feel someone is being involved in the commission of cyber crimes. This enables the government to bring the cyber criminals to the books of law.

8.6. Ensuring Punishment :

The assets of the cyber criminals should be confiscated by the government and the imposition of longer prison terms should be enacted for cyber criminals in domestic legislation. This may serve as deterrent to those youths who want to indulge in heinous cyber crimes.

8.7. Circulating Current Trends :

Innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICT;

---

20. S.J. Schjolberg, 'An International Criminal Tribunal for Cyberspace : Cybercrime Legal Work Group, Geneva, (2007-2008).

through this they can not only be well informed about the current trends in cyber crimes but also gather knowledge on different forms of the said crimes, and the methods how the cyber criminals carry out their bad activities. Thereby they can devise means of protecting their information from cyber criminals.

8.8. Drawing Consciousness :

Internet users should be conscious of security. In simple words, they must learn how not to provide personal or financial information to others unless there is a legitimate and assumed reason. They should not, for instance, throw out cheques, old credit cards, driving licenses, passports, receipts and other numerous documents containing personal data.

8.9. Awareness of Internet Service Provider :

The internet service providers should not just provide broadband connection to their subscribers, but they should also monitor effectively what the subscribers are doing on the internet. They should provide their customers, especially financial institutions and cyber cafes with well guided security codes and packages in order to protect their information and software from hackers and publishers.

9. Conclusion

People in Bangladesh are becoming more vulnerable to cybercrime. Computers have an impact on every aspect of contemporary life. Cybercrime is an issue that affects everyone. Without a question, the Internet provides thieves with unrivaled possibilities. There's a lot that can be done to guarantee a secure and reliable computer environment. It is critical not just for one's own well-being, but also for Bangladesh's national security. In light of recent technological advancements, it is not simple or feasible to eradicate cybercrime from society once and for all, but it is quite possible to fight and monitor it. The first and most important prerequisite for achieving the goal is for people to be aware about cybercrime and the measures that may be taken to avoid it.

CHAPTER NINE
E-governance

1. Introduction

Information and communication technologies are undergoing a global revolution. The Internet, personal computers, and cell phones are all profoundly altering our lives, influencing how we work, study, and connect. The importance of e-Government is being recognized by governments all around the globe. E-Government may increase efficiency in the delivery of government services, simplify compliance with government laws, promote public involvement and confidence in government, and save money for people, companies, and the government itself provided it is properly planned and executed. As a result, policymakers and managers in nations all over the globe, from the most developed to the least developing, are seeking to implement e-Government.

2. Definition

Different academics have defined governance in various ways. The word government comes from the word "govern," which comes from Old French "governer," or Latin "gubernare," which means "to steer or rule," and the Greek word "kubernan," which means "to steer," and is steeped in controlling, or at least having a large (and possibly invasive) role in citizens' lives.

The main criteria that society puts on its government are often used to define governance. Government is defined by the New Oxford English Dictionary (2001) as "the system by which a state or society is ruled" or "the activity or method of governing or regulating a state, organization, or people." Other popular definitions include "the exercise of political power over the acts or affairs of a political unit, people, or other body, as well as the execution of

specific duties for this unit or body" and "the executive policymaking body of a political unit, community, or other body."

In general, e-Government refers to the use of Information Communications Technology (ICT) by the appropriate government entity to provide information and public services to the public. In basic words, e-Government is the use of technology to improve citizen, business partner, and employee access to and delivery of government services. It is the use of information technology to assist government operations, engage people, and deliver more efficient and transparent public services.

3. Benefits of E-Governance

According to the World Bank (2002) E-Governance has the following benefits;

a. It makes the process of gathering information for individuals and companies easier.

b. It empowers people to gather information regarding any department of government and get involved in the process of decision making.

c. E-Governance strengthens the very fabric of democracy by ensuring greater citizen participation at all levels of governance

d. E-Governance leads to automation of services, ensuring that information regarding every work of public welfare is easily available to all citizens, eliminating corruption.

e. This revolutionizes the way governments function, ensuring much more transparency in the functioning, thereby eliminating corruption.

f. Since the information regarding every activity of government is easily available, it would make every government department responsible as they know that every action of theirs is closely monitored.

g. Proper implementation of e-Governance practices make it possible for people to get their work done online thereby

CHAPTER TEN
Privacy Protection and Cyber Security

1. Introduction

Because "cyberspace" has become such an important part of the global information and communication infrastructure, cyberspace security has become a top concern for businesses and governments across the globe.[1] According to the Cyber Security Act of 2015[2] *cyberspace* is "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship. The term "cyber security", though not defined in the *strategy*, is generally understood to encompass any measures taken to protect online information and secure the infrastructure on which it resides.[3]

Technologies that are ubiquitous, interconnected, and allow easy access to the Internet have become deeply integrated in everyday life. As a result, people are increasingly being dependant on cyberspace for social, economic and political interactions. The web

---

1. Deibert, Ron. Distributed Security as Cyber Strategy : Outlining a Comprehensive Approach for Canada in Cyberspace, Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012, Last visited on 25.08.2015
2. Bangladesh Government is to enact a new cyber security law with provisions for tough penalties for cyber crimes. The law will be a compliment to the existing Information & Communication Technology Act of 2006.
3. There is no commonly recognized definition for cyber security. ISO (ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. /IEC 27032/2012 defines cyber security as the "preservation of confidentiality, integrity and availability of information in the Cyberspace."

provides a platform for a whole range of critical infrastructure sectors and services, such as health care, food and water, finance, information and communication technology, public safety, energy and utilities, manufacturing, transportation and government.[1] Cyberspace connectivity augments all of these critical infrastructure sectors and is therefore vital to Bangladesh's future economic growth.

As the online environment has increasingly been subjected to sophisticated and targeted threats; the ever-increasing reliance on cyberspace is creating new and significant vulnerabilities.[2] This risk is magnified by a number of factors : more valuable electronic data is being stored and processed on a massive scale, much of it in the cloud; powerful and portable computing devices such as Smartphone's, tablets and laptops are increasingly integrated into every aspect of our lives; information is shared, combined and linked with other information with greater frequency; and third-party relationships e.g. outsourcing to a cloud provider, are the norm. Unless all components are equally secure, the entire system is vulnerable as cyber criminals are often skilled in exploiting weaknesses in cyberspace.

Privacy protection and cyber security should be thought of as interconnected : as more and more personal information are processed or stored online, privacy protection increasingly relies on effective cyber security implementation by organizations to secure personal data both when it is in transit and at rest.[3] In some cases, cyber security measures underpin critical infrastructure that protects data, thereby safeguarding personal information. However, as with many security measures, certain cyber security efforts can also threaten privacy; the relationship between cyber security and privacy

---

1. Public Safety Canada's website for list of critical infrastructure sectors,(Accessed on 27.08.2015).
2. This is acknowledged in the *Action Plan 2010-2015 for Canada's Cyber Security Strategy (the Action Plan)*, Released April 2013.
3. New Platforms, New Safeguards : Protecting Privacy in Cyberspace (February 23, 2011), https ://www.priv.gc.ca/media/sp-d/2011/spd_20110223_cb_e.asp (Accessed 27August 2015).

is not a completely harmonious one. Cyber security activities can require up-to-the-second monitoring of activities on a network in order to detect anomalies and threats, and in some cases, monitoring of this nature could involve capture and analysis of massive amounts of personal information.

2. Privacy and Cyber Security Issues in Bangladesh

"By allowing the production of enormous quantities of transactional data by and about people, the Internet has enabled the development of numerous possibilities for communication and information exchange. Individuals' personal information, their location and online activities, and logs and associated information about the e-mails and messages they send or receive are all included in this data, which is known as communications data or metadata." This communication data is "storable, accessible, and searchable," and it may be "both extremely revelatory and intrusive" when pooled and aggregated and utilized by the government."[4]

Ever since electronic media were opened to private sector involvement in the early 1990s, successive Bangladeshi governments have encouraged the development of an open internet access and communication regime in the country. Bangladesh currently has 33 million internet users, representing almost 20% of the total population, and ranks 138th out of 190 countries in the Household Download Index compiled by Net Index.[5] The World Economic Forum's 2013 Global Information Technology Report[6] ranked Bangladesh 114th out of 144 countries worldwide, with poor scores for its infrastructure and regulatory environment, even though an affordable and competitive communication service is generating exponential growth for users. In addition, localisation and the

---

4. Frank La Rue, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, in his landmark report on state surveillance and freedom of expression during the 23rd session of the UN Human Rights Council in Geneva in April 2003.
5. www.netindex.com/download/allcountries(accessed 3May 2015).
6. www.weforum.org/reports/global-information-technology-report-2013(accessed 3May 2015).

availability of phonetic Bangla software have contributed to the development of local blog and content hosting services.[7] The current Government in Bangladesh has a plan to establish what it calls a "Digital Bangladesh by 2021", with the aim of integrating internet access with development efforts in various sectors; but with widespread digital communication comes a greater threat to security and privacy, and uncertainty on how state and other institutions will address those issues while protecting the rights of individuals.

Globally there are two models available to protect citizens. One is the authoritarian model, where the problem is addressed through the development of a surveillance regime with filtering at the control points or on the backbone of the internet, and monitoring of the use of computers. A more liberal approach, on the other hand, is to make people aware of the risks, to develop their capacities and to set down punitive measures that require proper evidence and respect individual rights.[8] Bangladesh is often swinging between these two models, and there is a sense in which it is addressing the situation on an ad hoc basis.

3. Status of Bangladesh ICT Policies & Security Challenges

The Government of Bangladesh has established the National Council for Science and Technology in order to enhance the living standards of the general public by expanding development efforts in science and technology and their application (NCST). The Council's Executive Committee has also been established to carry out the Council's policies.

Recently formulated National Information and Communication Technology Policy (2002) has also given enormous importance to the development of ICT[9] for capturing people's share in the multi-

---

7. *Freedom on the Net 2013 : Bangladesh*, www.freedomhouse net/2013/bangladesh#.U4aWAfldXsF.org/report/freedom,(accessed 4May 2020).
8. M. Hassan, (2012, June 30). 'Cybercrime : Implementation must to achieve Vision 2021,' *The Daily Star*, available at archive thedailystar.net/law/2012/06/05/ analysis.htm,(accessed 11 August 2019).
9. Information and Communication Technology be abbreviated as ICT throughout the chapter of the study.

billion dollar software export market, for ensuring good governance, for enacting ICT related policies, special allocation of funds for software projects, development of world class ICT professionals and creation of a world class ICT institution for promoting excellence in the field.

By the year 2006, the Vision of this Policy 2002 is to create an ICT-driven country with a knowledge-based society. To achieve this goal, a country-wide ICT infrastructure was to be developed to ensure that every citizen has access to information, thereby facilitating citizen empowerment and enhancing democratic values and norms for long-term economic development through the use of infrastructure for human resources development, good governance, e-commerce, banking, public utility services, and other on-line ICT-enabled services.

Human resource development, the construction of ICT infrastructure, supporting ICT research and development, and the growth of ICT industries are all addressed in the 2002 National ICT Policy. It also emphasizes the importance of hardware industries, e-commerce, e-governance, ICT legal issues, ICT application in health care, and ICT application in agriculture to maximize the potential for rural economy and agro-business development. The use of ICT in other areas such as social welfare, transportation, and the legal system is also discussed.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL)[10] has adopted a Model Law on Electronic Commerce. This is known as UNCITRAL Model Law of e-commerce. In conformity with UNCITRAL Model Law, Bangladesh drafted an ICT Law, which has been approved by the parliament in February 2005 to facilitate electronic commerce and to encourage growth and development of information technology.

The ICT Law establishes rules and norms that validate and recognize contracts, forms through electronic means, sets default

10. The United Nations Commission on International Trade Law may be called UNCITRAL through the study.

rules for contract formation and governance of electronic contract performances, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes and supports the admission of computer evidence in courts and arbitration proceedings. In addition, the Copy Right Act 2000 has been amended to include computer software.

The Government is committed to mounting a direct and sustainable effort on the reduction of poverty, enhancing livelihood security, removal of hunger and malnutrition and generation of employment. This calls for generation and screening of all relevant technologies, their widespread dissemination through networking and support for the vast unorganized sectors of the economy of the country.

Realizing the importance of ICT and the enormous impact it can create in our everyday life, the name of the Ministry has been changed from Ministry of Science and Technology to the Ministry of Science and Information & Communication Technology. The Ministry of Science and ICT have been entrusted with the responsibility of harmonious growth of this sector in Bangladesh. Bangladesh Computer Council (BCC)[11], the apex body having the responsibility for promotion of all sorts of ICT activities in the country, is also governed by the Ministry of Science and ICT.

Development of Science and ICT depends on the expansion of telecommunication sector. This sector is still under developed due to lack of deregulation and open competition. In 2002, independent telecom regulatory authority, Bangladesh Telecommunication Regulatory Commission (BTRC) has been created.

4. The Government Activities

Cyber diplomacy is one of the foreign policy priorities of Bangladesh's current Government. The Government is planning to

---

11. Bangladesh Computer Council (BCC), an organization established by the government that ensures the use of computers and information technology in order to achieve the necessary policies and activities.

CHAPTER : TWELVE
BTRC

The Bangladesh Telecommunication Regulatory Commission (BTRC) is an independent commission founded under the Bangladesh Telecommunication Act, 2001.[1] The BTRC is responsible for regulating all matters related to telecommunications (wire, cellular, satellite and cable) of Bangladesh.

The BTRC started operating from 31 January 2002 with a vision of facilitating affordable telecommunication services and increasing the teledensity to at least 10 telephones per 100 inhabitants by 2010.

Bangladesh Telecommunication Act paved the way for the establishment of Bangladesh Telecommunication Regulatory Commission (BTRC). There had been hardly any independent monitoring mechanism for the telecommunication sector before BTRC came into being. Bangladesh Telegraph and Telephone Board (BTTB)[2] had the sole monopoly and they were the only telecom operator until mobile phone technology flourished and foreign companies (trans-national corporations) started operating in Bangladesh. Earlier laws and regulation neither neither covered modern aspect of telecommunication nor were the regulatory implementation mechanisms in place.

After foreign mobile operators started their operations in Bangladesh, BTTB faced intense competitions. Consumers were gradually turning their faces towards mobile companies though service charges of these operators were relatively higher in the initial

---

1. Act no 18 of 2001
2. BTCL or Bangladesh Telecommunications Company Limited is the largest telecommunications company in Bangladesh. The company was founded as the Bangladesh Telegraph & Telephone Board (BTTB) following Bangladesh's independence in 1971. On July 1, 2008 the BTTB became a public limited company and was renamed as BTCL.

years. In this changing operating environment, necessity was felt for a regulator. BTTB was unable to be a regulator as it was also service provider and competitor for the private sector. In order to regulate telecommunication sector, Bangladesh Telecommunication Act was promulgated. It has been stated in Section 6 of the Act, "On the commencement of this Act, a Commission to be known as the Bangladesh Telecommunication Regulatory Commission shall be established".

1. Functions and duties of BTRC

The general functions and duties of the commission are as follows :

1. To regulate the establishment, operation and maintenance of telecommunication services in Bangladesh
2. To protect the interests of the local consumers in respect of the charges imposed on them and their access to telecommunication services, and the quality and variety of such services
3. To encourage research and development activities in telecommunication and innovative activities and investment in providing telecommunication services
4. To protect the social and economic interests of the consumers, to respond to their needs and to control and abolish the existing and probable oppressive or discriminatory conduct or activities o the telecommunication service providers
5. To maintain and promote competition among the service providers in order to ensure high-quality telecommunication services
6. To ensure protection of the privacy of telecommunication
7. To collect, from within and outside Bangladesh, information on telecommunication and internet and to analyze and assess their impact on Bangladesh and to take necessary action or, as the case may be , to make necessary recommendations to the government

8. To frame a national scheme of numbering plan to be followed in telecommunication and to modify it whenever necessary.
9. Implementation of guideline about the internet domain name, as the case maybe, its modification and amendment, implementation, settlement of complain and dispute regarding the internet domain name

2. Objectives of the Bangladesh Telecommunication Act 2001

The Bangladesh Telecommunication Act 2001 has delineated its objectives as follows :

1. To encourage the orderly development of Telecommunication System that enhance and strengthens the social and economic welfare of Bangladesh ;
2. To ensure in keeping with the prevalent Social and economic realities of Bangladesh, access to reliable, reasonably price and modern Telecommunication services and internet. Services for the greatest number of people as far as practicable;
3. To ensure the efficiency of the national Telecommunication System and it capability to complete in both the national and international spheres;
4. To prevent and abolish discrimination in providing telecommunication services, to progressively effect reliance and competitive and market oriented system and in keeping with these objectives to ensure effective control of the Commission;
5. To encourage the introduction of new services and to create a favorable atmosphere for the local and foreign investors who intend to invest in the Telecommunication Sector of Bangladesh.

3. Laws regulating BTRC

The legal statues governing the telecommunication industry in Bangladesh which will be applicable to all applicants and Telecommunication value added service Registration Certificate holder is given below :

1. The Bangladesh Telecommunication Regulations Act 2001 (as amended)
2. The Wireless Telegraphy Act 1933[3] and The Telegraph Act 1885[4] for matters which are not covered by the Bangladesh Telecommunication Regulations Act 2001.
3. Any act of parliament or Ordinance and any rules or regulations, made or to be, made by the government.
4. The Bangladesh Telecommunication Regulatory Commission (ANS Operator's Quality of Service) Regulations 2018.
5. The rules/ regulations/ guidelines / directives / orders /instructions and decisions issued or to be issued under the act by the commission.

4. Status of consumers in the telecom sector

Though the number of subscribers is quite huge, consumers have got little attention in the telecommunication sector. Call charges went down due to intense competition, although there are allegations of hidden charges for different offers and packages offered by the different service providers. Giant operators often block access to other networks and consumers fail to get connection during peak hours. There are other forms of exploitation also reported by consumers and the media. There are specific allegations against mobile operators for breaking the laws of the land. One such example is the recently reported case[5], filed by BTRC on Jan 16, 2008 against Grameenphone for illegal VOIP[6] business. It is not the first instance though. Earlier in 2007, most of the private operators paid fines for facilitating illegal VOIPs trading.

---

3. Act no. XVII of *1933*.
4. *Act* no. XIII of *1885*.
5. Case No. 46 under Gulshan Police Station, Dhaka
6. Voice over Internet Protocol (VoIP), also called IP telephony, is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

technology. This unrestricted network access allows certain highly competent criminals to engage in unlawful activities in the cyber realm. Crashing a computer system, stealing information stored in electronic form; e-mail bombing, data tampering, financial fraud such as unauthorized money transfers by cracking credit card security codes, denial of service, and virus attacks are among the most frequent evil deeds. However, in our nation, the institutional and legal foundation for preventing and punishing these crimes is insufficient.

2. An Overview of Cyber Crimes

The terms 'cyber crime' 'computer crime' 'information technology crime' and 'high-tech crime' are often used interchangeably to refer to two major categories of offenses. Firstly; the computer is the target of the offence; attacks on network confidentiality, integrity and/or availability i.e. unauthorized access to and illicit hampering with systems, programs or data, all falling into this category.[3] Secondly; traditional offences such as theft, fraud, and forgery that are committed with the assistance of or by means of computers, computer networks and related information and communications technology; here, the computer is a tool used to commit a conventional crime.[4] Cyber crime is a criminal activity done using electronic devices, computers and the internet. The Council of Europe's Cyber Crime Treaty uses the term 'cyber crime' to refer to offences ranging from criminal activity against data to content and copyright infringement.[5]

A recent study noted, cyber crimes differ from terrestrial crimes in four ways : 'They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be

---

3. M. D. Goodman, 'Why the PoliceDon't Care about Computer Crime', 10 Harvard Journal of Law and Technology, vol.465, 1997, pp.468-469. http ://jolt.law.harvard.edu/articles/10hjolt465.html. See also Criminal Threats to E-Commerce 17, Interpol, Jan. 2001.
4. ibid.
5. T. Krone, High Tech Crime Brief, Australian Institute of Criminology, Canberra, Australia, 2005.

committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.'[6] They also pose far greater challenges for law enforcement. Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.[7]

Cyber crimes pose unique legal and political issues because it is usually international in nature. The issues to be so addressed are as follows :

i. There is no single international entity that can investigate and prosecute international cyber crimes.
ii. There is also no clear definition of cyber crime at the international level, so countries have different standards for defining various forms of cyber crimes such as violation of intellectual property rights, right to privacy and child pornography.
iii. There are different requirements for record keeping among various countries such as how long traffic logs need to be kept and legal ability maintained to monitor the perpetrator.
iv. The victim and perpetrator are found often in different countries complicating where the case should be prosecuted.
v. The evidence can also remain in multiple countries making its collection very difficult.

---

6. Cyber Crime and Punishment, Archaic Laws Threaten Global Information, Mcconnell International, Dec, 2000. Available at http :// www.mcconnellinternational /service/ cybercrime.htm.(accessed 3 April 2015)
7. ibid.

After analyzing the above issues it can be said that, the cyber crime is one kind of digital crime which occur by using computer, internet, mobile phones etc. It is a criminal activity or a crime that involves the internet, a computer system, or computer technology.

3. Brief History of Using Internet in Bangladesh

In late 1995, the Government of Bangladesh invited applications to subscribe the Very Small Aperture Terminal (VSAT)[8] data circuits and on June 4, 1996 the VSAT connection was commissioned and the internet was launched in Bangladesh for the first time. The first usage of internet was the publication of the National Polls Result in 1996.[9] But this introduction could not create a good market at the very initial stage. After the year 1996, there were only two Internet Service Providers[10] (ISPs) and about one thousand of users in the country. But the year 1997 is a landmark in this field as it recorded a tremendous advancement in internet using. The number of ISPs increased into twelve and users into ten thousand. Afterwards some new ISPs started their service which fuels the proportional advancement of this sector. However, the Government adopted more liberal national policies for a sustainable and rapid growth of this industry and as a result 180 ISPs were working by 2005. In 2006 Bangladesh got connected with Submarine Cable which afforded big bandwidth and low cost than ever before. After this, over the years Bangladesh Telecommunications Company Ltd. (BTCL), presently 'Bangladesh Telecommunication Regulatory Commission' (BTRC)[11], reduced the bandwidth price at regular intervals which

---

8. The term Very Small Aperture Terminal may be mentioned as VSAT throughout the study.
9. Hamidur Rashid, Internet History of Bangladesh, http ://ezinearticles.com/ ?Internet-Historyof-Bangladesh&id=2327010 (accessed 1 January 2015).
10. An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.
11. The Bangladesh Telecommunication Regulatory Commission (BTRC) is an independent commission founded under the Bangladesh Telecommunication Act, 2001 (Act no 18 of 2001). The BTRC is responsible for regulating all matters related to telecommunications (wire, cellular, satellite and cable) of Bangladesh.

6. Cyber Crimes Characterised

Founding fathers of internet hardly had any idea, at the time when internet was developed, that internet could also be misused for criminal activities. Presently it is a real fact that it is happening roughly and largely all over the world. Now the question is how these offences could be treated by conventional or extraordinary methods. It is proved that apparently there is no great difference between conventional crimes and cyber crimes. The first demarcating line between the two is the medium of committing a particular crime. Conventional crimes are *prima facie* territorial and occurred in physical world, but cyber crimes are not limited to territorial boundaries as they occur in the world which is an electronic or virtual one. A major question may arise regarding the nature of the cyber crimes that whether they are criminal offences or civil wrongs or a tort. The answer would depend on the nature of the incident. Under the Information and Communication Technology Act, 2006 all the aforesaid computer-based crimes are treated as criminal offences.

7. Remedies Available and their Lacking

'Prevention is better than cure' is a wise saying. For the prevention of numerous cyber crimes it is better to initiate advanced technological actions or technological precautionary measures. But as the time runs along with computer-civilization, an attempt may be taken to cure the alleged cyber crimes, for which legal and other remedies and their lacking available in Bangladesh are to be found out. A cyber victim in Bangladesh has a better opportunity to get proper remedy under the ICT Act, 2006. The statute is the first of the kind in Bangladesh and the only door open for lawful remedy against various cyber crimes in the country. Through this statute it is being tried to locate all the probable grounds of cyber crime frequently occurring at present and which might occur in future as well like damaging any computer or computer system, hacking, spreading viruses and false information, causing defamation through internet, changing source code, stealing or damaging any text, audio, video

documents etc. Provisions for special Cyber Tribunals[28] having both original and appellate jurisdictions and punishments of lighter or severe form have been fixed. Mass people are not much aware about such types of crimes and the procedure of remedies against them. Under the provisions of the ICT Act a number of other procedural and structural hurdles are found to exist which are as follows :

Firstly; Under the ICT Act of 2006 a Sessions Judge or an Additional Session Judge is to preside over the Cyber Tribunal.[29] A Tribunal[30] which includes a Chairman, who may be an ex or acting judge or a competent person to be a judge of the Supreme Court, and two members one of whom should be an ex or acting District Judge and the other an ICT expert. Like other criminal cases Public Prosecutors are to prosecute on behalf of the State. The problem that may arise here is that judges and the lawyers are the experts of laws, not of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the oppórtunity to be assisted by the ICT expert. But is it possible to give verdict on the basis of another's knowledge? The reality in our country is that so long as no initiative is taken by the Government to train up the judges of the Tribunals for acquiring proper technological knowledge no justice can, in this respect, be ensured.

Secondly; A police officer not below the rank of a Sub-Inspector can be an Investigation Officer (IO)[31] regarding cyber crimes. Like the judges, police officers also under the law may have no opportunity to gather required technological knowledge due to lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. Is it, then, possible for such a police officer to make proper investigation

---

28. The Information and Communication Technology Act, 2006, Sec : 68, 82.
29. Ibid, Sec 68(2)
30. Ibid Sec 82(2)(3)
31. Ibid Sec 69(1)

into the matters in dispute? Moreover, it may result in a snag to justice.

Thirdly; The Government bears the responsibility not only of forming the cyber tribunals but also of formulating terms and conditions of the service of the Judges of the proposed tribunals.[32] Regrettably, neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the State. Proper execution of statutes ensures rule of law. But present circumstances say that inadequate execution of the ICT Act, 2006 is one of the root causes for the increasing cyber crimes in Bangladesh. The solution of the aforementioned problems demands that the State must take nippy steps along with logistic and financial assistance.

8. Some New Dimensions as Remedies against Cyber Crimes

No doubt technological defense is better than legal remedy in preventing hi-tech crimes, but there is always a chance of destruction of such defenses as these are not of perpetual nature. People who are more advanced in technology can smash the security wall anytime. So, legal and other related remedies are a must for fighting the war against the said evils. In addition to the present remedies the State can commence some new course of actions which are being trailed by some developed hi-tech state of the world. Let us have a glance at their features :

i. **Constitutional Safeguard :** Bangladesh is a country of constitutional supremacy.[33] Constitution plays the mother role in preserving and ensuring the rights and duties of both the State and the people. Constitutional provisions against cyber crimes may escort the cyber warfare to a national temperament which may result in a better form than any other organizational and legal remedy. Constitutional amendment may be the introducing procedure of such provisions.

ii. Special Wing of Police : For a digital Bangladesh, we need to equip our law enforcement agencies with training and technologies

---

32. Ibid, Sec 82(4)
33. Art.7, Constitution of the People's Republic of Bangladesh.