Freedom of speech in cyber space in human rights protection perspective:

- Freedom of speech is a part of human rights, which freedom is manifested from the submission speech orally in any media without any obstruction from any party.
- Freedom of opinion is a part of basic human rights.
- A freedom of speech is recognized as a "basic human rights" and gets protection assurance in universal declaration of Human rights 1948.
- Constitution of the republic of Indonesia stated "Everyone has the rights to develop themselves through the fulfillment of basic needs.
- The cyber world has a major role in the stand-up for human rights.
- Restrictions are made to meet the demand of fairness in accordance with morality consideration, religion values, and security as well as needed in a democratic.

5) What is the Rights of access to cyber space?

- Article 33: Citizens have the right to freely and without discrimination enjoy access to communicate and obtain information and knowledge from cyber space.
- Article 34: Citizens have the right to enjoy the benefits of e-governance and e-commerce and user training without any discrimination.
- Article 35: Citizens have the right to enjoy the right of cyber securities, security of communication technologies and informatics of their personal data and privacy.

Right to internet access:

- The right to internet access, also known as the right to broad band (or) freedom to connect, is the view that all people must able to access internet.
- The right to internet access is fundamental right of every Indian.
- India has declared that internet access is a basic fundamental right for all Indians.
- This right cannot be curtailed and blocked at any cost.
- This is one of those watershed and blocked at any cost.
- Every Indian citizen has "the right to be informed and the right to know and the feeling of protection of expensive connectivity.

- **Network Equality:** Everyone shall have universal and open access to the internet's content.
- **Standards and regulations:** The internet's architecture, communication systems and documents and data formats shall be based on open standards.
- **Governance:** Human rights and social justice must form the legal and normative foundation upon which the internet operates and is governed.

4) Write about freedom of speech and expression in cyber space

A) Freedom of expression and Act No. 39 year 1999:

- As a member of united nations, Indonesia cannot let go off taking normal and legal responsibility.
- With regard to the freedom of expression stipulated in article 19 of the universal declaration of human rights , Act No. 39 of 1999, set in Article 14 states that:
  1. Every person has the right to communicate and obtain information needed to develop the personal and social environment.
  2. Every person has the right to seek, obtain and convey information Article 310 on deformation and Article 311 criminal law code on contempt.

Freedom of speech and information and electronic transaction Act:

- The Act No. 11, year 2008 on the information on electronic transaction Act.
- Although journalists and bloggers are now have to be cautious of the article 27 due to frequently used article by the law enforcement to prosecute them as criminals.
- In this formulation there are 3 elements that must be considered namely,
  (i) Element of intent and without right.
  (ii) Element distribute, transmit, make accessible of the information and electronic development.
  (iii) Elements of contempt and deformation.
- Measurement used in the criminal law is objectively subjective.
- Judicial review attempt on Article 27 information and electronic transaction Act.

- These rights are interrelated, interdependent, indivisible.
- In the universal declaration of human rights, there are 30 articles, describing the civil, political, economic, social and cultural rights that should be enjoyed by the human in every country.
- John Locke, Montesquieu and Rousseau or express various human rights namely:

a) Freedom for themselves.
b) Freedom of religion.
c) Freedom of assembly and association.
d) Write of Habeas Corpus Rights.
e) Freedom of thought and freedom of the press.

Freedom of Speech in Cyber Space:

- Freedom of Speech in Cyberspace is one of the human rights in being by human in the world as stated in article of Article 19 of UDHR.
- The article states that everyone has the right to freedom of opinion and speech.
- The freedom of speech rights in regard of speaking and giving opinion which associated with it is often leads to victim suspected of breaking these limits.
- Actually the freedom of speech rights itself is regulated in the article 28 of the 1945.

10 principles and human rights are :

- **Universality and Equality**: All the humans born free and equal in dignity and rights.
- **Rights and social justice**: The internet is a space for the promotion, protection and fulfillment of human rights and advancement of social justice.
- **Accessibility**: Everyone has an equal right to access and use a secure and open internet.
- **Privacy and data protection**: Everyone has a right to privacy online. Everyone also has the right to data protection, including control over personal data collection, retention, processing and disclosure.
- **Life, Liberty, and Security**: The rights to life, liberty and security must be respected, protected, and fulfilled online.
- **Diversity**: Cultural and linguistic diversity on internet must be promoted and technical and policy innovation should be encouraged to facilitate plurality of speech.

UNIT - III

CONSTITUTIONAL & HUMAN RIGHTS ISSUES IN CYBERSPACE

1) what is Constitutional case?

A) An appeal can be filed against any judgment, decree or final order of a High Court in a civil, criminal or other proceedings if the concerned High Court certifies that the case involves a substantial question of law as to the interpretation of the constitution. Where such a certificate is given any party in the case may appeal to the Supreme Court on the ground that any such question has been wrongly decided.

i) Any case can become a constitutional case if a constitutional question is involved.

ii) This can allow cases to move to higher courts such as the supreme court.

2) write about constitutional issues related to the use of administrative sanctions.

A) constitutional issues related to the use of administrative sanctions are two types

1) Delegation and separation of powers:

The first objection that was raised against the use of administrative sanctions by administrative agencies was that imposition of sanctions by the executive was contrary to the principle of separation of powers.

i) Delegation of legislative power

ii) Delegation of judicial power

2)Protection of constitutional rights: Questions have been raised as to whether the use of administrative sanctions converts an otherwise criminal matter into a civil matter. Legal implications are significant because if a sanction is considered criminal, procedural and other legal protection must then be accorded to defendants.

3) Freedom of speech in cyberspace in Human rights protection perspective

A) Human Rights:

- Human rights are rights inherent to all human beings, whatever our nationality, place of residence, national (or) origin or any other status
- We are equally entitled to our human rights without discriminations

It is expected that working through the EMC will produce tangible synergies as a result of collaboration and networking, in the traditions of the Commonwealth.

It will operate as a consultative body that:

- Provides strategic direction to the CCI programmes.
- Contributes to the resourcing and strategic planning of the implementation of CCI's work across the Commonwealth.

CCI's successes:

Ghana

- The first national CCI project;
- Launched in partnership with the Office of the President including signing a Memorandum of Understanding between CCI and Ghana.
- Appointed local project coordinator to aid implementation.

Trinidad and Tobago

- Specialist Child Online Protection needs assessment completed;
- Recruited expert to conduct review and updating of cybercrime legislation; and
- Conducting a nationwide awareness raising programme.

The Commonwealth adds:

- a strong track record in this area. The Commonwealth Model Law on Cybercrime and Harare Scheme for Mutual Assistance are recognised as international, best practice in the field and a viable alternative to the Budapest Convention on Cybercrime.
- value as a "trusted partner". No agenda beyond assisting the member state, providing unique convening power.
- endorsements by major players in the fight against cybercrime.
- an unambiguous mandate of the Commonwealth Heads of Government which provides CCI with unique political buy-in.

This comes from its simplicity – instead of each international organization working on its own delivering a narrow program; the concept utilizes the Commonwealth's convening power to build a consortium of the willing to assist member countries.

CCI coordinates and leverages the expertise of each partner by having them buy into a collective needs assessment process. This allows the development of a comprehensive program consisting of legislation, mutual assistance frameworks, prosecutorial and enforcement capabilities.

CCI governed:

• Com Sec, Rule of Law is the focal point for CCI; sits on the Executive Management Committee ('EMC') and provides secretariat functions to EMC.

• Commonwealth Executive Management Committee consists of representatives from member countries and CCOC; provides overall direction; manages CCI; coordinates activities; liaises with CCOC members to conduct scoping missions and assist with the implementation of action plans.

• CCI Operations Consortium ('CCOC') consists of approximately 40 international organizations and member countries and is the primary source of resources to conduct scoping missions and implement action plans. Members bring specific Cybercrime skills / resources to the consortium and collectively create synergies to assist member countries.

CCI staffed:

- The CCI programme is embedded within the Rule of Law Division of ComSec which provides secretariat functions.
- This falls under the responsibility of the divisional Director Katalaina Sapolu.
- The Director is supported by two legal advisors, Shadrach Haruna and Marie-Pierre Olivier. Technical advice is provided by Tony Ming of the Governance and Natural Resources Division.

EMC in detail:

The CCI EMC consists of Commonwealth states and organisations who are committed to the cause, mission and vision of CCI and can contribute expertise necessary to the CCI methodology.

7) what is the commonwealth cybercrime initiative(CCI)?

A) The Commonwealth is a "trusted partner". No agenda beyond assisting the member state, provides unique convening power. The CCI has been endorsed by major players in the cybercrime space. The unambiguous mandate of the Commonwealth Heads of Government provides the initiative with unique political buy-in.

CCI is a programmed of the Secretariat to assist member countries through multistakeholder partnership created to deliver a comprehensive program to reduce Cybercrime.

Mission :

CCI aims to provide coherent, comprehensive and sustainable assistance to member states to help build the necessary capacity to combat cybercrime.

Methodology:

Working with a range of committed international partners, the CCI is designed to extend support to member states ensuring that they have in place the appropriate legal frameworks complemented with attendant investigative, technical, enforcement and prosecutorial capabilities.

CCI get its authority:

CCI was created in 2011 under the auspices of the Commonwealth Connects program which was created by the Heads of Government during their 2005 meeting in Malta to bridge the digital divide. CCI was formally endorsed by CHOGM during their 2011 meeting in Perth.

Commonwealth Heads of Government Meeting 2013 at Colombo, mandated:

"Heads noted the Commonwealth Cybercrime Initiative and the recent endorsement of its methodology by senior officials of Commonwealth Law Ministries in September 2013 and called for the provision of assistance to developing countries on their cybercrime issues."

CCI work:

CCI is a unique and innovative multi-stakeholder partnership created to deliver a comprehensive program to reduce both cybercrime and duplication of effort.

As of November 2018 the largest recipients of world bank loans were India ($859million) in 2018 and china ($370million) in 2018 through loans from IBRD.

The World Bank is different from the World Bank group. An extended family of 5 international organizations:

1. International bank for reconstruction and development (IBRD)
2. International development association (IDA)
3. International finance corporation (IFC)
4. Multi lateral investment guaranty agency (MIGA)
5. International centre for settlement of investment disputes (ICSID)

Advantage of World Bank for India:

The advantage of borrowing from the WB is the low cost and stable financing it provides with no longer maturity periods that better match India's investment needs....when combined with IDA financing, the cost of borrowing on commercial terms from the market based IBRD also works out cheaper for India.

The World Bank is a very powerful organization. Many counties that need to build roads ,or deliver services to their people ask for help from the world bank. The bank also has many experts that know a great deal about economics and development.

Purpose and function:

The world bank provides low interest loans ,interest free credits and grants . It focuses on improving education, health and infrastructure. It also uses funds to modernize a countries financial agriculture and natural resources management.

The council guidelines:

- Having regard to the convention on the organization for economic co-operation & development of 14th December-1960, in particular article 1(b) (c) 3(a) 5 (b)
- Having regard to the declaration on trans-border data flows adopted by the governments of OECD members countries on 11th April 1985.
- Having regard to the recommendation of the council concerning guidelines for cryptography policy of 27th March-1997.
- Having regard to the ministerial declaration on the protection of privacy on global network of 7-9th December-1998.
- Having regard to the ministerial declaration on authentication or electronic commerce of 7-9th December-1998.

6) Write a short note on World Bank.

A) The World Bank is an international financial institution that provides loans to countries of the world for capital projects. It comprises two institutions: the International Bank for Reconstruction and development (IBRD), and the international development association (IDA) . The world is a component of World Bank group.

- Its headquarters is located in Washington D.C. John Maynard_Keynes and Harry Dexter white, the founding fathers of both the world bank and the IMF (international monetary fund). JIM YONG KIM is the president of the world bank group

The World Bank's most recent stated goal is the reduction of poverty. the intension behind the founding was to provide temporary loans to low income countries which were unable to obtain loans commercially.

- Security should be implemented in a manner consistent with the values recognized by domestic society.

Risk assessment:

- Participant should conduct risk assessment.
- Risk assessment identifies threats & vulnerabilities should sufficiently broad based to encompass key internal & external factors.
- Risk assessment should include consideration of the potential harm that may originate from others.

Security design & implementation:

- Participant should adopt a in corporate security as an essential element of information systems & networks
- Systems, networks & policies need to be properly designed implement & co-ordinate to optimize security.
- Security should be a fundamental elements of all products, service network.

Security Management:

- Participants should adopt a comprehensive approach to security management.
- Security management should be based on risk assessment & should be dynamic & encompassing all level of participants.
- It should include forward looking responses to emerging threats & address prevention.
- Information systems & procedures should be co-ordinated & elevated to create a coherent systems of security.

Reassessment:

- Participants should review & reassess the security of information systems & networks

- Promote co-operation and information sharing as appropriates among participants in the development.

Principles:

- The following nine principles are complementary & should be as whole.

Awareness:

- All participants are responsibilities for the security of information systems & network.
- They should be accountable in appropriate manner to their individual roles.
- Participants should review their own policies practices & process

Responsibility:

- All participants are responsibility for the security of information systems & networks.
- Participants depend upon the interconnected local & global information systems &networks should understand their responsibility for the security.

Response:

- Participants should act in a timely & co-operative manner to prevent detect & respond to security incidents.
- Recognizing the interconnectivity of information systems &networks the potential for rapid & wide spread damage.
- Participants should act in a timely & co-operative manner to address security incidents.

Ethics:

- Participants should respect the legitimate interacts of others.
- Given the pervasiveness of information systems & networks in our societies participants need to recognize their action may harm others.

Democracy:

- The security of information systems &networks should be compatible with essential values of democratic society.

- The project database contains information about all the APEC projects.

5) OECD (Organization for Economic Co-operation & Development):

A) (i)Towards a culture of society:

- These guidelines respond to an ever changing security environment by promoting the development of a culture of security.
- The guidelines signal a clear break with a time when secure design and use of networks and systems were too often system.
- Participant is becoming more dependent on information systems, network and related services.
- Only an approach that takes due account of the interests of all participants & nature of the system.
- Each participant is an important actor for ensuring security relevant security risks & preventive measures.
- Participants, as appropriate to their roles, should be aware of the relevant security risks & preventive measures.
- Promotions of a culture of security will require both leadership & extensive participation.
- Security issued should be topics of concern & responsibility at all levels of government and business for all participants.
- These propose that all participants adopt & promote a culture security as a way of thinking about, assessing and the operations of information systems & networks.

(ii)Aims:

These guidelines aim to:

- Promote a culture of security among all participants as a mean of protecting information systems & networks.
- Raise awareness about the risk to information systems& networks, the policies measures and the need for their adoption
- Faster greater confidence among all participants in information systems.

- 30the November 2013, October-2013 focused on global cyber security awareness.

APEC secretariat:

- The APEC secretariat is based in Singapore, and operates as a core support mechanisms for the APEC process.
- It provides co-operation, technical & advisory support as well as information management.
- The APEC secretariats performs a central project management roles.
- APEC's annual budget is also administrated by APEC secretariat.
- APEC operations:
- APEC-A multiple economic forum.
- APE operates as a co-operative, multilateral economic & trace forum
- APEC achieves its goals by promoting dialogue & arriving at decisions on a consensus basis, giving equal weight to the views of all members.
- APEC members economic report progress towards achieving free and open trade and investment goals through individual action (IAP)s and collective action plans.
- APEC funding
- APEC is not a donor organization
- APEC activities are centrally funded by annual contribution from PEC members economic presently totaling USDS million
- Member's economics also provide voluntary contributions to support projects that advance APEC's trade & investment.
- In generally the projects do the following:
- Relate to the priorities of APEC economic leaders & APEC ministers.
- Cover the interest of at least several APEC members economics
- Build capacity
- Improve economic efficiency
- Encourage the participation of the business sector

- To ensure maximum consensus & compliance, this instrument must necessarily be negotiated with active participation from all states.

4) Write about Asia – Pacific economic cooperation (APEC)

A)

- APEC is a forum with the primary goal to support sustainable economic growth & prosperity.
- The forum was established in 1989 & currently has 21 members.
- With APEC's structure there are several steering committee & working groups operating in different fields.
- ICT is within the mandate of the APEC telecommunications of & information working group (TEL)
- In 2002 TEL issued the APEC cyber security strategy, comprising recommendations in the area of cybercrime legislation.
- At the APEC telecommunications and improving information infrastructure advance information society meeting in 2005, the lima declaration was issued.
- Later in 2005 the APEC economic leaders adopted the APEC strategy to ensure a trusted, secure & sustainable online environment.
- This strategy expands APEC's work on promoting information & network security.
- APEC's goals & activities in the field of cyber security are enshrined is APEC telecommunications and information working group (APEC TELWG) 2016-2020, adopted on the basis of the previous APECTEL strategic action plan 2010-2015.
- Including the following key areas: enhancement of the resilience of critical domestic infrastructure, security & risk management.
- 18th May 2015, APEC's new strategic action plan for the internet shows, limited cyber security co-operation with the region.

- It is clear then that assistance facilitated by the convention relies in pre-existing co-operative agreements between the parties.
- Thus, as also stated in article-39 of the convention, the provisions only serve to supplement multilateral & bilateral treaties b/w parties.
- In addition mutual legal assistance (MLA) b/w parties where no such mutual arrangement exists.
- The convention itself doesn't committee (T-cy) was set up to represent the interests of & foresee regular consultations.
- The biannual plenaries conducted by the T-cy working group's discus development, grievances of the Budapest convention.

Significant draw backs of the convention:

- The convention on cybercrime has also come under serve criticism or both its specific provisions that fail to protect rights of individual's states.
- The 12th plenary of T-cy concluded that the mutual legal assistance facilitated by the convention was too complex & lengthy.
- Article 32 has been contentious as it allows local police to access servers located in another country's jurisdiction.
- However it is important to note that the claim that provisions infringe on sovereignty has been addressed by the T-cy in its guidance note on article 32.
- Russia's displeasure with the existing multilateral instrument was evidence by the introduction of Russia-backed proposal.
- Cybercrime was considered & rejected at 12th UN congress in crime prevention & criminal justice.
- Regardless, Brazil & China which have expressed displeasure at the primarily European treaty have refused to adopt the convention for the same reason.
- India's statement also reflects its belief that the Budapest convention in this present form is insufficient in talking cybercrimes

- It was drafted by the council of Europe with active participation from its observer states in 2001.
- Therefore it is widely recognized as a decisive document on international best practice and enjoys compliance even from non-signatory states.
- The Budapest convention is also supplemented by an additional protocol to the convention which was adopted in 2003.

Offences under the convention:

The Budapest convention broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices.

- Offences perpetrated by means of computer systems such as computer fraud, distribution & transmission of child pornography and copy right offences are addressed by provisions of conversion.

The substantive offences under the convention can broadly be classified into:

- Offences against the confidentiality & availability of computer data & system.
- Computer related offences.
- Content related offences.
- Copy right criminal in fingerprint.
- The additional protocol makes act of using computer networks.
- However, the full range of cybercrimes are not covered under the Budapest convention.

Provision of the convention:

- The treaty functions on a mutual information sharing &formal assistance model in order to facilitate better law enforcement.
- Article 23- general principal relating to international co-operation
- The parties shall co-operate with each other, in accordance with the provisions of this chapter

UNODC agreement :

- On 19th May 2011, the ITU signed an agreement with the UN office on drugs and crime.
- The organizations will collaborate in assisting ITU and UN member states mitigate the risks posed by cyber crime.

Symantec partnership:

- The ITU draws its membership from public and private sectors.
- The ITU has also signed a MOU with Symantec cooperation.
- ITU will distribute the reports the interested member states to help improve response to cyber threats.

❖ **Council of Europe**

Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

3) What is Budapest convention on crimes and council of Europe?

Budapest, 23/11/2001, Treaty Open for Signature by the member states and the non-member states which have participated in its elaboration and for accession by other non member states.

- The convention on cyber crime or Budapest convention is the only finding multilateral treaty instrument aimed at combating cyber crime.

- Development of strategies for creation of global frame work or watch, warning and incident response.
- Development of global strategies for the creation and endorsement of a generic and universal digital identity system.
- Development of global strategies to facilitate human and institution capacity building.
- Proposals on a frame work for global multi-stake holder strategy.

The child online protection initiative:

- The child online protection initiative is a first specialized GCA program.
- ITU secretary general, Dr. Toure states that the ITU launched COP to kick start the process.
- COP takes a multi-stake holder approach to defending children's interests.

COP new phase:

- On 17th November 2010, the ITU launched a new COP phase. The new phase aims to encourage the development of COP centers.

GCA partnerships:

ITU-impact alliance:

- The GCA is both a frame work for visualizing the cyber security domain and tool for national action.
- Impact activities support GCA is the following ways.
- First impact center for policy and international cooperation supports ITU's legal measures
- Second impact supports GCA for the creation of global frame work.
- Third the impact's center for security assurance.
- Fourth the impacts center for training and skill development.

Pillar 1- Legal measures:

- The pillar seeks to elaborate strategies for the development model globally applicable and interoperable cybercrime legislation.
- The overall goal of the pillar is to develop advise and internationally compatible process for handling crime committed over ICTS.

Pillar 2- Technical and procedural measures:

- The pillar focuses on measures for addressing vulnerabilities in S/W products. The pillar aims to device globally acceptable accreditation schemes, protocols and standards.

Pillar 3- Organizational structures :

- The pillar aims to create organizational structures and strategies to help, prevent, detect and respond to attacks against critical information infrastructures.

Pillar 4- Capacity Building:

- This pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cyber security on the national policy agencies.

Pillar 5- International co-operation:

- The pillar focuses on strategies for international cooperation, dialogue, coordination.

GCA (global cyber security agenda) strategic goals:

On top of the 5 pillars, the GCA contains 7 strategic goals. These are

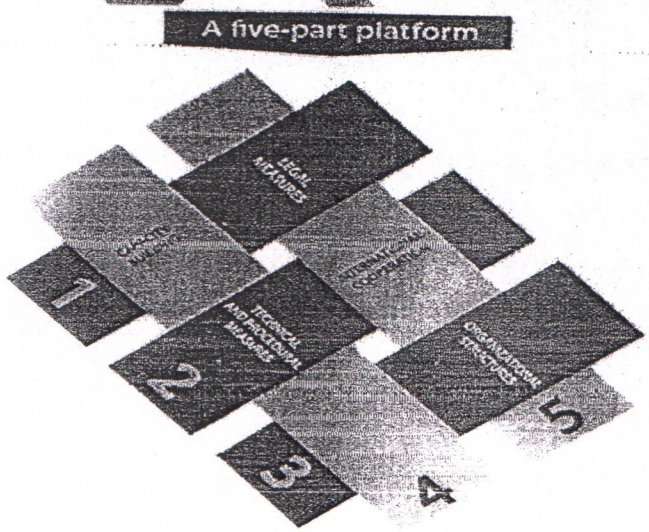
- Elaboration of strategies for the development of a model cyber crime legislation i.e., globally applicable and interoperable with existing national and regional legislative measures.
- Elaboration of global strategies for the creation of organizational structures and policies.
- Development of strategy for establishment of security criteria and accreditation schemes for h/w and s/w systems.

WSIS Action line C5:

- The WSIS Tunis agenda underlined the value of multi-stake holder action at international level.
- The two summits asked UN agencies to facilitate action lines in an of their expertise.
- Therefore, world leaders participating in WSIS cntrusted the ITU wins the role of sole moderator of action line C5, "Building confidence and secure in the use of ICT'S".
- On 17th May 2007 newly elected ITU secretary-general Dr.Hamadoun in I.Toure launched the ITU global cyber security agenda.

Global Cyber Security Agenda :(GCA)

- The GCA is a frame work for international multi-stake holder co-operation on cyber security.
- The GCA encourages collaboration with and between all relevant partners and builds on existing initiatives to avoid duplicating efforts.
- The GCA aggregates cyber security activities in the three sectors.
- Diagram below illustrates the five pillars / work areas of the GCA.



- Issued on 23rd December 2003, it notes the growing reliance information infrastructure by critical national services in areas such as energygeneratic transmission and distribution.
- Thus the resolution invites UN member states to develop strategies for reducing risks to critical information infrastructure in accordance with national laws and regulations.

5. Global culture of cyber security:

- The resolution covers similar security ground to the preceding four resolutions.
- The resolution consider the outcomes of the 2 phases of the world summit on the information society (WSIS)
- The WSIS appointed ITU as the sole moderator of action line and focusing on "Building confidence "and trust in the use of ICT's.

2) what are ITU (international telecommunication union) Cyber Security activities?

A) ITU has played an important role in global telecommunications information security and standards setting in different capacities. Since its formulation in 1865. ITU became the United Nations specialized agency in the field of telecommunications, information, and communication technologies ICT's in 1949.

World summit on the information society (WSIS):

- The UN general assembly resolution 56/183 endorsed the holding of the world summit on the information society in 2 phases.
- The first WSIS phase took place in Geneva. Switzerland from 10 to 12 December 2003.
- The second phase took place in Tunis, Tunisia from 16 to 18 November 2005.

UNIT – II

INTERNATIONAL PERSPECTIVES

1) Write about UN cyber security activities.

A) 1. Resolution of cyber security:

- Cyber security has been high on the agenda of the united nation (UN) for a number of years.
- The UN took up the subject out of recognition that building trust and confidence in the use of ICT's is crucial to the socioeconomic well being of humanity.
- As a result, the UN general assembly (UNGA) has expressed itself.

2. Combating criminal use of ICT's:

- The resolution issued on 4th December 2000 focused on combining the criminal issues of information technologies.
- It recognizes free flow of information can promote economic social development, education and democratic governs.
- Indeed the resolution warns that unless addressed, the increasing criminal misuse of information technologies may have grave impacts in all states.

3. Culture of cyber security:

- The resolution of focuses on the creation of global culture of cyber security and the protection issued on 20th December 2002.
- It notes the growing depending of governments, businesses, other organizations and individual users on information technologies.
- The resolution makes it clear that government and law enforcement cannot addresses cyber security alone without the support of all stake holders.

4. Critical infrastructure:

- The resolution is focuses on the creation of a global culture of cyber security and the protection of critical information infrastructure.

- Following this the central government passed on order dated 23rd March 2003 appointing the secretary of Department of Information Technology of each of the states or of 'union territories' of India as the adjudicating officers.
- The information technology (security procedure) rules, 2004 came in to force on 29th October 2004. They prescribed provisions relating to secure digital signatures and secure electronic records. Also relevant are the information technology (other standards) rules, 2003.
- An important order relating to blocking of websites was passed on 27th February 2003.
- Computer emergency response team (CERT-IND) can instruct department of tele communications (DOT) block a website.
- The Indian Penal Code (as amended by the IT act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.
- Digital evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT act) In case of bank records, the provisions of the bankers, books evidence act (as amended by the IT act) are relevant.
- Investigation and adjudication of cybercrimes is done in accordance with the provisions of the code of criminal procedure and the IT act. The Reserve Bank of India act was also amended by the IT act.

- The cyber regulations appellate tribunal (procedure) rules, 2000 also came in to force on 17th October 2000.
- These rules prescribe the appointment and working of the cyber regulation appellate tribunal (CRAT) whose primary role is to hear appeals against orders of the adjudication officers.
- The cyber regulations appellate tribunal (salary allowances and other terms and conditions of service of presiding officer) rules, 2003. Prescribe the salary, allowances and other terms for the presiding officer of the act.
- Information Technology (other powers of civil court vested in cyber appellate tribunal) rules 2003 provided some additional powers to the CRAT.
- On 17th March 2003, the information technology (qualification and experience of adjudicating officers and manner of holding enquiry) rules 2003 were passed these rules prescribe the qualifications required for adjudicating officer.
- Their chief responsibility under IT act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of virus, denial of service attacks, disruption of computers, computer manipulation etc.
- These rules also prescribe the manner and mode of inquiry and adjudication by these officers.
- The government had not appointed the adjudicating officers or the cyber regulations appellate tribunal for almost 2 years after the passage of the IT act.
- This prompted ASCL students to file a public interest litigation (PIL) in the Bombay high court asking for a speedy appointment of adjudicating officers.
- The Bombay high court, in its order dated 9th October 2002, directed the central government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments.
- Shah and Honble justice Ranjana Desai also ordered that the cyber regulations appellate tribunal be constituted within a reasonable time frame.

- The IT act also penalizes various cybercrimes and provide strict punishments (imprisonment terms up to 10 years and compensation up to Rs. 1 crore)
- An executive order dated 12 September 2002 contained instructions relating provisions of the act with regards to protected systems and application for the issue of a digital signature certificate.
- Minor errors in the act were rectified by the information technology (removal of difficulties) order, 2002 which was passed on 19 September 2002.
- The IT act was amended by the negotiable instruments (amendments and miscellaneous provision) act, 2002. This introduced the concept of electronic cheques and truncated cheques.
- Information technology (use of electronic records and digital signatures) rules, 2004 has provided the necessary legal framework for filling of documents with the government as well as issued of licenses by the government.
- It also provides for payment and receipt of fees in relation to the government bodies on the same day, the information technology (certifying authorities) rules 2000b also came into force.
- These rules prescribe the eligibility, appointment and working of certifying authorities (CA) these rules also lay down the technical standards, procedures and security methods to be used by CA.
- The rules were amended in 2003, 2004 and 2006. Information technology (certifying authorities) regulation, 2001 came in to force on 9 July 2001.
- They provide further technical standards and procedures to be used by a CA.
- Two important guidelines relating to CAs were issued.
- The first are the guide lines for submission of application for license to operate as a certifying authority under the IT act. These guidelines were issued on 9th July 2001
- Next were the guide lines for submission of certificates and certification revocation lists to the controller of certifying authorities of publishing in national responsibility of digital certificates. These were issued on 16th December 2002.

- Government form including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards, for shopping. Most people are using email, cell phones and sms messages for communication.
- Even in "non-cybercrime" cases, important evidence is found in computer / cell phones etc. E.g. In cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cybercrime cases such as online banking frauds, online share trading frauds, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are lost replacing conventional methods of transacting business.
- Technology per se is never a disputed issue but for whom and at what cost has been issued in the ambit of governance.
- The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technology, which had a trickledown effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic matrix.

5) Explain Jurisprudence of Indian cyber laws?

A) Cyber Jurisprudence: Cyber jurisprudence is the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law.

- Jurisprudence of Indian cyber law in cyber spaces The primary technology act. 2000 (IT Act) which came into force on 17 October 2000.
- The primary purpose of the act is provide legal recognition to electronic commerce and to facilitate filing of electronic records with the government.

CGI stands for common gateway interface. Similar to ASP and PHP CGI is used for server side processing for web applications.

ASP is an abbreviation for active server pages. ASP is a server side scripting technology that you can use to create dynamic web pages.

4) Explain Importance of Cyber law (OR) Need for Cyber law (or) Discuss ongoing Developments in law relating to IT's.

- Integrity and security of information.
- Security of government data.
- Intellectual property rights.
- Privacy and confidential of information.
- Legal status of online transactions.
- To prevent misuse of technology.
- To govern the law relating to internet, cyberspace.
- To prevent the cyber crimes.
- In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes.
- Internet was initially developed as a research and information sharing tool and was in an unregulated manner.
- As the time passed by it became more transactional with e-business, e-commerce, e-government and e-procurement etc.
- All legal issues related to internet crime are deal with through cyber laws. As the number of internet users in on the rise, the need for cyber laws and their application has also gathered great momentum.
- In today's highly digitalized world, almost everyone is affected by cyber law for example: almost all transactions in shares are in demoting form.
- Almost all companies extensively depend upon their networks and keep their valuable data in electronic form

The protocol specifies how information is transferred from a link. The protocol used for web resources is Hypertext Transfer Protocol (HTTP). Other protocols compatible with most web browsers include FTP, telnet, newsgroups, and Gopher.

The protocol is followed by a colon, two slashes, and then the domain name. The domain name is the computer on which the resource is located.

Links to particular files or subdirectories may be further specified after the domain name. The directory names are separated by single forward slashes.

- **Website:**

A collection of various pages written in HTML markup language. This is a location on the web where people can find tutorials on latest technologies. Similarly, there are millions of websites available on the web.

Each page available on the website is called a web page and first page of any website is called home page for that site.

Programming languages and technology:

Java script is an interpreted scripting language commonly used on the internet for creating w.eb pages that respond to user actions.

VB script is an interpreted scripting language that is a subset of Microsoft visual basic. As a result the structure and syntax are similar to visual basic.

PHP is an interpreted scripting language that is used as an alternative to ASP on UNIX based servers. PHP is commonly used to access database and provide server side form and e-commerce processing.

Visual Basic Net is the next generation of the visual basic programming language visual basic Net is compiled; object oriented language that leverages the net frame work for developing powerful ASP net web applications.

World Wide Web (WWW):

WWW stands for World Wide Web. A technical definition of the World Wide Web is – All the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C): The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

➢ HTTP:

HTTP stands for Hypertext Transfer Protocol. This is the protocol being used to transfer hypertext documents that makes the World Wide Web possible.

A standard web address such as is called a URL and here the prefix http indicates its protocol

➢ URL:

URL stands for Uniform Resource Locator, and is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files).

A URL will have the following format –

protocol://hostname/other_information

document in to another kind of document xml, HTML, (or) another mark-up language format.

Internet:

The Internet is essentially a global network of computing resources. You can think of the Internet as a physical collection of routers and circuits as a set of shared resources.

Some common definitions given in the past include –

- A network of networks based on the TCP/IP communications protocol
- A community of people who use and develop those networks.

Internet-Based Services

Some of the basic services available to Internet users are –

- **Email** – A fast, easy, and inexpensive way to communicate with other Internet users around the world.
- **Telnet** – Allows a user to log into a remote computer as though it were a local system.
- **FTP** – Allows a user to transfer virtually every kind of file that can be stored on a computer from one Internet-connected computer to another.
- **UseNet news** – A distributed bulletin board that offers a combination news and discussion service on thousands of topics.
- **World Wide Web (WWW)** – A hypertext interface to Internet information resources.

interconnected via a network, allowing for quick and convenient transmission of information. The processes involved in web technology are complex and diverse. Web technology has revolutionized communication methods and has made operations for more efficient.

Computers and other network devices need to communicate. A mechanism must make it possible for a computer to communicate with another computer on the same network (or) another network.

Some examples of web technologies include:

Mark – up language including HTML, CSS, XML, CGT, and HTTP.

- HTML stands for hypertext mark-up language. HTML is the primary mark-up language that is used for web pages.HTML tells the browser what to display on a page.
- CSS stands for cascading style sheets. CSS provides the ability to change the appearance of text on web pages.

Using CSS, one can also position elements on the page, make certain elements hidden, or change the appearance of the browser, such as changing the color of scroll bars in Microsoft internet explorer.

- XML stands for extensible mark-up language. Similar to HTML, XML is a mark-up language designed for the internet. However, unlike HTML, which was designed to define formatting of web pages XML, was designed to describe data.

One can use xml to develop custom mark-up languages.

- XSLT is an abbreviation for Extensible Style sheet Language transformation XSLT uses to define the appearance of an xml document (or) change on xml

Each instruction has to be given to the computer. A computer cannot take any decision on its own.

2. Dependency:

It functions as per the user's instruction, thus it is fully dependent on humans.

3. Environment:

The operating environment of the computer should be dust free and suitable.

4. Emotion less:

Computers have no feeling or emotions. It cannot make judgement based on feeling, taste, experience, and knowledge unlike humans.

Over view of web technology:

History: Sir Tim Berners-Lee (a British computer scientist) invented the **World Wide Web** in 1989. In March 1989, Tim laid out his vision for what would become the web in a document called information management. A proposal "Believe it or not", Tim's initial proposal was not immediately accepted. In fact, his boss at the time, Mike Sandals, noted the words "Vague but exciting" on the cover. The web was never an official CERN project but mike managed to give Tim time to work on it in September 1990. He began work using a next computer, one of Steve Jobs early products by October of 1990, Tim had written the three fundamental technologies that remain the foundation of today's web and the first web page was served on the open internet in 1991.

Web technology:

Web technology is the development of the mechanism that allows two or more computer devices to communicate over a network. For instance in a typical office setting, a number of computers plus additional devices such as printers may be

5. Versatility:

A computer is a very versatile machine. A computer is very flexible in performing the jobs to be done. This machine can be used to solve the problems related to various fields. At one instance, it may be solving a complex scientific problem and the very next moment it may play a card game.

6. Reliability:

A computer is a reliable machine, modern electronic components have long lives. Computers are designed to make maintenance easy.

7. Automation:

Computer is an automatic machine. Automation is the ability to perform a given task automatically. Once the computer receives a program i.e. the program is stored in the computer memory, then the program and instruction can control the program execution without human interaction.

8. Reduction in paper work and cost:

The use of computers for data processing in an organization leads to reduction in paper work and cost.

9. Results in speeding up the process:

As data in electronic file can be retrieved as and when required, the problem of maintenance of large number of paper files gets reduced.

Though the initial investment for installing a computer is high, it substantially reduces the cost of each of transaction

- Disadvantages of computers:

1. No intelligence: A computer is a machine that has no intelligence to perform any task

Step-3: processes the data and convert in to useful information.

Step-4: generates the output.

Step-5: control all the above four steps.

- **ADVANTAGES OF COMPUTER :**

1. High speed:

Computer is a very fast device. It is capable of performing calculation of very large amount of data.

The computer has units of speed in micro second, nanosecond, and even the picoseconds.

It can perform millions of calculations in a few seconds as compared to man who will spend many months to perform the same task.

2. Accuracy: In addition to being very fast, computers are very accurate. The calculations are 100% error free. Computers perform all jobs with 100% accuracy provided that the input is correct.

3. Storage capability: Memory is a very important characteristic of a computer.

A computer has much more storage capacity than human beings. It can store large amount of data. It can store any type of data such as images, videos, text, audio etc.

4. Diligence:

Unlike human beings, a computer is free from monotony, tiredness, and lack of concentration. It can work continuously without any error and boredom. It can perform repeated tasks with the same speed and accuracy.

3) Write a note on overview of computer and web technology.

A) Over view of a computer: The computer as we know it today had its beginning with a 19th century English mathematics professor name Charles Babbage. He designed the analytical engine and it was this design that the basic frame work of the today are based on.

Generally, computers can be classified in to generations. Each generation lasted for a certain period of time, and each gave us either a new and improved computer or an improvement to the existing computer. They are,,

1. First generation:

The period of first generation 1946-1959 vacuum tube based.

2. Second generation:

The period of second generation 1959-1965. Transistor based.

3. Third generation:

The period of third generation 1965-1971. integrated Circuits based.

4. Fourth generation:

The period of fourth generation 1971-1980. VLSI(Very Large Scale Integration) microprocessor based.

5. Fifth generation:

The period of fifty generation 1980-onwards. ULSI microprocessor based and Artificial Intelligence.

- **Functionalities of a computer:**

If we look at in a very broad sense, any digital computer carries out the following five functions.

Step-1: takes data as input

Step-2: stores the data / instructions in its memory and uses them as required.

They have touched every aspect of our technological civilization and have the potential to do even more.

- **Negative impact of computer in society**:

Though computer has numerous positive implications, some people show its negative impact in the following points they are

1. The computer is highly expensive and they are not affordable for general people.
2. There are some methods people can pirate data for misuse.
3. Since, a computer can do work much faster number of employees can do more work and its leads to increased unemployment.
4. Due to malfunction of the computer, huge data and information can be lost.
5. Computer technology is fast changing technology which might become difficult for small firms and schools.
6. Due to the difficulty of data transmission, we fail in providing proper services.
7. Violation of Data Integrity , data security and computer ethics.

- **Safeguarding the citizen from those above negative impacts**

1. Computerized system provides various safeguarding systems.
2. Personal data stored by the police, personal data stored by the local administrative bodies.
3. Information about the weather forecast, information about natural calamities such as earth quake, flood, etc.
4. Information about recent events of traffic, roads etc.

Social effects: (ATM, visa card and master card)

People can use automated teller machine cards for withdrawing money deposited with the help of ATM card, visa card or master card.

2) Define computer. Explain positive and negative impact of computer in society.

A) **Computer**: A computer is programmed device with a set of instructions to perform specific tasks and generate results at a very high speed.

The computer users are increasing day by day. The use of computer has surpassed manual operations and it has become an essential tool for human development. It is true that the organization with a computerized system is more efficient than the others which rely on manual operations.

➢ **Positive impact of computer in society:**

It is obvious that the computers are revolutionizing our daily life. More and more educated people are being attracted to using computers for solving their daily problems from word processing and spread sheet calculations to solve a very complex simultaneous equation.

The following are the basic reasons of increasing attraction towards the use of computers in homes and offices.

1. A tedious work can be carried out with the use of computers speeding and accurately.
2. Instead using paper files and occupying large space, more information can be stored in small space electronically that can be accessed as required.
3. Computers possess multitasking and multiprocessing capabilities with facilitate multirole operation on data.
4. Since, the data are stores in electronic devices, they can be easily accessed.
5. Computers obey the instructions and they process the data impartiality during result processing.
6. Documents can be kept secret with the special login name and password protection
7. Access to information(Google, Wikipedia Quora ...etc)

particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming.

2. (a).Digital Signature:

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

b.Electronic Signature:

An electronic signature or e-signature indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

3. **Intellectual Property:**

Intellectual Property is a broad category of law concerning the rights of the owners of intangible products of invention or creativity. For example, IPlaw grants exclusive rights to certain owners of artistic works, technological inventions, and symbols or designs.

4. Data Protection and Privacy:

The legal challenge in Indian context includes lack of privacy, data protection and cyber security legislation model so it is extremely difficult to ensure protection for same. But in absence of specific laws there are some laws or incident safeguard that the government is using for privacy purpose.

UNIT - I

INTRODUCTION TO CYBER LAW

1) What is Cyber Law? Explain it. (Or) Write about Introduction to Cyber law.

A) ***Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law has been referred to as the Law of the Internet.***

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices. (Such as hard disks, USB disks etc.), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Law encompasses the rules of conduct:

1. That has been approved by the government,
2. Which are in force over a certain territory, and
3. Which must be obeyed by all persons on that territory.

Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation. Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

1.Cybercrimes: *Cybercrimes is crime that involves a computer and a network. Issues surrounding these types of crimes have become high-profile,*

Ch Vanaja

VI Semester B.C.A.

Cyber Laws

Time: 3 Hrs

Max Marks: 75

Answer any FIVE from the following. Each question carries 15 Marks.

1. What is Cyber Law? Discuss about Need for Cyber Laws.
2. Discuss about Jurisprudence of Indian Cyber Law.
3. a) Discuss about Budapest Convention for Cyber Crime.

   b) Explain about International Cyber Laws
4. Explain about APEC.
5. Discuss about issues in Cyber Space.
6. Explain various possibilities of Cyber Crimes may appear and also discuss about rules to handle those crimes.
7. Discuss about different offense under IT Act, 2000.
8. Explain about Cyber Defamation and issues on Defamation.
9. a) Discuss about Copyright Law

   b) Explain about issues related to Doman Names.
10. Explain about Cyber Terrorism.