COMP 20333 - Social and Professional Issues in IT

Midterm Departmental Exams Reviewer

Credits to Mrs. Cecilia V. Marbella

Chapter 1 - Global Digital Environment

GLOBALIZATION

- It is a process of interaction and integration among the people, companies, and governments of different nations, a process driven by international trade and investment and aided by information technology.
- A term used to describe how trade and technology have made the world into a more connected and interdependent place.
- It means the speedup of movements and exchanges (of human beings, goods, and services, capital, technologies or cultural practices) all over the planet. One of the effects of globalization is that it promotes and increases interactions between different regions and populations around the globe. – youmatter.com

DIGITAL DIVIDE

- The digital divide describes the problem we are faced with. It is the unequal access of information and communication technology between different groups of society, and the knowledge of the skills required to use the technology.
- In Africa, only 3% of the population has the internet. In Asia, 1% of the population in Cambodia, Laos and Bangladesh has the internet. The Middle East accounts for 0.9% of global Internet users.

INFORMATION SYSTEMS TRENDS

1. **Cloud Computing**
    - The typical definition for cloud computing says that it is the use of a network that is composed of remotely connected servers.
    - This computer infrastructure, despite the various locations, can store, manage, and process data through the Internet.
    - Instead of local storage on computer hard drives, companies will be freeing their space and conserving funds.

2. **Mobile Computing and Applications**
    - Mobile phones, tablets, and other devices have taken both the business world and the personal realm by storm. Mobile usage and the number of applications generated have both skyrocketed in recent years.

3. **Big Data Analytics**
    - Mobile Big data is a trend that allows businesses to analyze extensive sets of information to achieve variety in increasing volumes and growth of velocity.
    - **Big data** has a high return on investment that boosts the productivity of marketing campaigns, due to its ability to enable high-functioning processing.
    - **Data mining** is a way companies can predict growth opportunities and achieve future success. Examination of data to understand markets and strategies is becoming more manageable with advances in data analytic programs.

4. **Automation**
    - Another current trend in the IT industry is automated processes. **Automated processes** can collect information from vendors, customers, and other documentation.

Chapter 2 - Emerging and Converging Information Communication Technologies

EMERGING SOFTWARE TECHNOLOGIES

1. **Artificial Intelligence and Smart Machines**

- It harnesses algorithms and machine learning to predict useful patterns humans normally identify.
- Smart machines take human decision-making out of the equation so intelligent machines can instigate changes and bring forward solutions to basic problems.
- Companies are embracing artificial intelligence in the workplace because it enables workers to focus their skills on the most important projects and manages these intelligent devices for a more effective system.
- Five out of six Americans use AI services in one form or another every day, including navigation apps, streaming services, smartphone personal assistants, ride-sharing apps, home personal assistants, and smart home devices.
- In addition to consumer use, AI is used to schedule trains, assess business risk, predict maintenance, and improve energy efficiency, among many other money-saving tasks.
- AI face recognition is beginning to help with missing people reports, and it even helps identify individuals for criminal investigations when cameras have captured their images.
- According to the *National Institute of Standards and Technology*, face recognition is most effective when AI systems and forensic facial recognition experts' team up.
- AI will continue to promote safety for citizens in the future as software improvements shape these applications.

2. **Virtual Reality (VR)**
   - It is a term used to describe three-dimensional computer-generated environments that replace the normal reality in which our everyday lives play out.
   - VR environments are often described as "immersive" because they engage a user's vision — and in some instances touch — to provide a seemingly three-dimensional simulated world to interact with or explore.
   - Many people have already experienced virtual reality games, and VR is of growing importance for training and education in fields like medicine, engineering, and the sciences.
   - The illusion of "being there" (**telepresence**) is affected by motion sensors that pick up the user's movements and adjust the view on the screen accordingly, usually in real time (the instant the user's movement takes place).
   - Thus, a user can tour a simulated suite of rooms, experiencing changing viewpoints and perspectives that are convincingly related to his own head turnings and steps.
   - Virtual Reality's most immediately recognizable component is the **head-mounted display (HMD)**.
   - Wearing data gloves equipped with force-feedback devices that provide the sensation of touch, the user can even pick up and manipulate objects that he sees in the virtual environment.

3. **Augmented Reality**
   - It is a more versatile and practical version of virtual reality, as it does not fully immerse individuals in an experience.
   - Augmented reality features interactive scenarios that enhance the real world with images and sounds that create an altered experience.
   - The most common current applications of this overlay of digital images on the surrounding environment include the recent Pokémon Go fad or the additions on televised football in the U.S.

- It can impact many industries in useful ways:
    - **Airports** are implementing augmented-reality guides to help people get through their checks and terminals as quickly and efficiently as possible.
    - **Retail and cosmetics** are also using augmented reality to let customers test products, and furniture stores are using this mode to lay out new interior design options.
- The possibilities for augmented reality in the future revolve around mobile applications and health care solutions.
- Careers in mobile app development and design will be abundant, and information technology professionals can put their expertise to use in these interactive experiences.

4. **Blockchain Data**
    - Blockchain data, like the new cryptocurrency Bitcoin, is a secure method that will continue to grow in popularity and use in 2019.
    - This system allows you to input additional data without changing, replacing, or deleting anything.
    - In the influx of shared data systems like cloud storage and resources, protecting original data without losing important information is crucial.
    - For transaction purposes, blockchain data offers a safe and straightforward way to do business with suppliers and customers.
    - Private data is particularly secure with blockchain systems, and the medical and information technology industries can benefit equally from added protection.

5. **Cyberprivacy and Security**
    - Cybersecurity or information security refers to the measures taken to protect a computer or computer system against unauthorized access from a hacker.
    - On its most basic level, **data privacy** is a consumer's understanding of their rights as to how their personal information is collected, used, stored and shared.
    - **Cybersecurity** is a concentration of IT that will help secure clouds and improve the trust between businesses and their vendors.

6. **Internet of Things (IoT)**
    - It describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
    - These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025.
    - Use of IoT allows people to turn on music hands-free with a simple command, or lock and unlock their doors even from a distance.

MINIATURIZATION

- Miniaturization in electronic devices involves fitting more transistor nodes on a smaller integrated circuit (IC). The IC is then interfaced within its intended system or device so that, once assembled, the system can carry out the desired function. The technology is made tinier yet mightier.

Examples: mobile phones, computers, and vehicle engine downsizing.

- Furthermore, device miniaturization aligns with Gordon Moore's 1965 prediction that cramming more components onto integrated circuits [would] lead to such wonders as home computers, automatic controls for automobiles and personal portable communications equipment.
    - His prediction proved true, ushering in an era of technology that would vary from portable computers, smartphones, and new medical devices to the Internet of Things and 5G wireless devices, as well as AR/VR and AI, all enabled by smaller yet more powerful computing systems.

MULTIFUNCTIONAL MACHINES

MFP (Multi-Function Product/ Printer/ Peripheral), multi-functional, all-in-one (AIO), or Multi-Function Device (MFD), is an office machine which incorporates the functionality of multiple devices in one.

THE RISE OF ROBOTICS

- Robotics is a branch of engineering that involves the conception, design, manufacture, and operation of robots. This field overlaps with electronics, computer science, artificial intelligence, mechatronics, nanotechnology, and bioengineering.
- Science-fiction author Isaac Asimov is often given credit for being the first person to use the term robotics in a short story composed in the 1940s. In the story, Asimov suggested three principles to guide the behavior of robots and smart machines.

Asimov's Three Laws of Robotics, as they are called, have survived to the present:

1. Robots must never harm *human beings*.
2. Robots must follow *instructions from humans* without violating rule 1.
3. Robots must *protect themselves* without violating other rules.

Chapter 3 - ICT-enabled Industry

BUSINESS PROCESS OUTSOURCING (BPO)

- **Business process outsourcing (BPO)** is the contracting of a specific business task, such as payroll, human resources (HR) or accounting, to a third-party service provider. Usually, BPO is implemented as a cost-saving measure for tasks that a company requires but does not depend upon to maintain their position in the marketplace.
- One of the most dynamic and fastest growing sectors in the Philippines is the **Information Technology - Business Process Outsourcing (IT-BPO) Industry**. The IT-BPO industry plays a major role in the country's growth and development. This is composed of eight sub-sectors:
    1. Knowledge process
    2. Outsourcing and back offices
    3. Animation
    4. Call centers
    5. Software development
    6. Game development
    7. Engineering design
    8. Medical transcription

BPO SETUPS (CAPTIVE MARKETS AND OFFSHORING/THIRD PARTY OUTSOURCING)

THIRD PARTY OUTSOURCING

1. **Project Based Outsourcing -** primarily used for business activities with irregular frequencies or one-off projects. The usual costing method makes use of time and material costs as variable costs and the fixed costs.
2. **Dedicated Development Center** - primarily used in business cases when there are hanging requirements. In this specific model it could be used for some long-term goals for developing technology or software. This is preferred when resource requirements are lower in the outsourced country than the home

country, hence developing a comparative advantage.

CAPTIVE MARKETS

This is preferred when core or crucial business activities are needed to be run at cheaper costs. The rationale for employing such a setup is to cater to long term strategic plans involving high managerial control. In this case there are two major ways of setting up a captive market and these are the:

1. **DIY or 'Start from Scratch' model**
   - The usual flow is for the company to develop all its resources in the newly designated area or country of operations.
   - This is preferred by the companies that have high levels of market knowledge and analytics.

2. **Build Operate Transfer model**
   - The practice is to contact a 3rd party vendor in order to develop a contract in which the vendor is the one who develops the property, sources the employees and manages the BPO center for the first designated period or amount of time.
   - This is preferred by companies that do not have any specialized expertise in the new country of operations hence needing a local partner or vendor to assist with market entry strategies.

TRENDS IN THE INDUSTRY

- Better Information security
- Strategic balanced-shore outsourcing
- Booming Blogging and Social Media Outsourcing
- Popularity of cloud-based software

ISSUES CONCERNING THE INDUSTRY IN THE PHILIPPINES

1. **Health Issues**: employees experience back and shoulder pains, due to the workstation setups and monitor levels, several have complained about experiencing throat irritations due to dealing with multiple calls a day coupled with a high stress work environment and concerns regarding the employees' hearing being damaged due to most of these workers being exposed to higher noise levels.

2. **Political Issues**:
   - Revision of **Republic Act 7916** to include floors in buildings where BPO companies operate to be considered as special economic zones, exempting the companies from national and local taxes, and only having to pay 5% of their gross income as tax.
   - Approval of RA 7916, the establishment of the **Philippine Economic Zone Authority (PEZA)** which considered IT Parks as special economic zones, encouraged foreign investment in the industry by providing subsidies for infrastructure development and tax exemptions.

3. **Economic Issues**:
   - The BPO industry is the fastest growing sector in the country and is expected to overtake OFW remittances in 2017.
   - The growth in the BPO industry has barely trickled down to most of the Philippine population.
   - The development of the country mainly because of the high unemployment and underemployment rates; the **BPO industry** was the **fastest growing sector** from 2005-2012 but only took in 1% of the labor force.

MOBILE-BASED SERVICE INDUSTRY

Defined as those companies, which together enable the provision of telecommunication, information and entertainment services including voice, internet, SMS, text, and other data services:

- Mobile banking
- Economic development
- Delivery of health services

- Citizen empowerment
- Greater access to media and education

E-SERVICES / E-GOVERNMENT

E-Government in the Philippines is envisioned to create “a digitally empowered and integrated government that provides responsive and transparent online citizen-centered services for a globally competitive Filipino nation.”

- Efficient delivery of public services (**Citizens**)
- Places a premium on value-added, shared services, interoperability, and the maximization of public resources (**Government**)
- Provides spaces for participation and fosters synergy in governance (**Civil Society Organizations**)
- Identifies policy and advocacy areas that need to be addressed in creating an environment necessary for fostering an integrated, interoperable, and harmonized system of e-Governance (**Policymakers**)

Chapter 4 - Internet Censorship and Freedom of Expression

INTERNET CENSORSHIP

- **Internet censorship** is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative.
- Individuals and organizations may engage in self-censorship for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequences.
    - It also occurs in response to or in anticipation of events such as elections, protests, and riots.
    - Other areas of censorship include copyrights, defamation, harassment, and obscene material.
- The extent of internet censorship varies on a country-to-country basis.

  Examples:
    - Increased censorship due to the events of the Arab Spring.
    - Internet censorship in China known for having the most incredibly censored internet in the world.

INTERNET CENSORSHIP IN PHILIPPINES

The Cybercrime Prevention Act of 2012, officially recorded as **Republic Act No. 10175**, is a law in the Philippines approved on September 12, 2012.

It aims to address legal issues concerning online interactions and the Internet in the Philippines. Among the cybercrime offenses included in the bill are cybersquatting, cybersex, child pornography, identity theft, illegal access to data and libel.

INTERNET FILTERING

It normally refers to the technical approaches to control access to information on the Internet, as embodied in the first two of the four approaches described below:

1. **Technical Blocking** - there are three commonly used techniques to block access to Internet sites: **IP blocking, DNS tampering, and URL blocking** using a proxy.
    - These techniques are used to block access to specific Web Pages, domains, or IP addresses. These methods are most frequently used where direct jurisdiction or control over websites are beyond the reach of authorities.
    - **Keyword blocking** which blocks access to websites based on the words found in URLs or blocks searches involving blacklisted terms, is a more advanced technique that a growing number of countries are employing.

2. **Search Result Removals** - in several instances, companies that provide Internet search services cooperate with governments to omit illegal or undesirable websites from search results. Rather than blocking access to

the targeted sites, this strategy makes finding the sites more difficult.

3. **Take-down -** where regulators have direct access to and legal jurisdiction over web content hosts, the simplest strategy is to demand the removal of websites with inappropriate or illegal content.
    - In several countries, **a cease and desist notice** sent from one private party to another, with the threat of subsequent legal action, is enough to convince web hosts to take down websites with sensitive content.
    - Where authorities have control of domain name servers, officials can **deregister a domain** that is hosting restricted content, making the website invisible to the browsers of users seeking to access the site.

4. **Induced Self-Censorship**
    - Another common and effective strategy to limit exposure to Internet content is by encouraging self-censorship both in browsing habits and in choosing content to post online.
    - This may take place through the threat of legal action, the promotion of social norms, or informal methods of intimidation.
    - **Arrest and detention** related to Internet offenses, or on unrelated charges, have been used in many instances to induce compliance with Internet content restrictions.
    - In many cases, the content restrictions are **neither spoken nor written**.
    - The perception that the government is engaged in the surveillance and monitoring of Internet activity, whether accurate or not, provides another strong incentive to **avoid posting material or visiting sites** that might draw the attention of authorities.

<u>Advantage</u>: content which is violent, obscene, or dangerous can be immediately blocked. This protects children from inadvertently viewing content that could be scary or harmful to them, such as the murder and decapitation videos which have made their way to sites like Facebook and Twitter in recent years.

<u>Disadvantage</u>: a restriction on a person's ability to view the content they wish to see when they wish to see it.

PROS OF INTERNET CENSORSHIP

1. **It creates the chance to set common sense limits.**
    - There are some things that just aren't part of what a society would deem to be healthy.
    - A simple search right now on an unfiltered public search can provide anyone with access to numerous videos that purport to show real murders in progress.

2. **It limits access to harmful activities.**
    - There are dark areas of the internet where anything goes right now. Access to illicit drugs, sex trafficking, human trafficking, and child pornography can be accessed with relative ease by those who seek out such things.

3. **It could lessen the impact of identity theft.**
    - One of the fastest growing crimes in the world today is identity theft.

4. **It may provide a positive impact on national security.**
    - Although hacking will occur no matter what internet censorship laws may be in place, by creating internet censorship regulations with strict and mandatory penalties for a violation, it could become possible to reduce the number of hacking incidents that occur.

5. **It stops fake news.**
    - Claims of fake news increased dramatically in 2017.
    - Fake news websites promote false reports for money through clicks because readers think the news is real.

CONS OF INTERNET CENSORSHIP

1. **Who watches the watchers?**
    - Even if internet censorship is directly supervised and ethically maintained, someone somewhere is deciding on what is acceptable and what is not acceptable for society to see online.
    - At some level, someone does not have anyone to whom they report regarding their censorship decisions.
    - With that kind of power, one individual could influence society in whatever way they chose without consequence.

2. **It stops information.**
    - Although fake information can be restricted through internet censorship, so can real information.
    - According to the World Economic Forum, 27% of all internet users live in a country where someone has been arrested for content that they have shared, published, or simply liked on Facebook.
    - 38 different countries made arrests based solely on social media posts in 2016.

3. **It is a costly process.**
    - According to research from Darrell West, VP and Director of Governance Studies and the founding director of the Center for Technology Innovation at Brookings, internet shutdowns cost countries $2.4 billion in 2015.
    - The decision to cut connectivity in Egypt came at a cost of $90 million.
    - Censoring content is costly, and it will come at the expense of taxpayers.

FREEDOM OF EXPRESSION

- **Right to express one's ideas and opinions freely** through speech, writing, and other forms of communication but without deliberately causing harm to others' character and/or reputation by false or misleading statements.
- According to the **Universal Declaration of Human Rights**, proclaimed in 1948, Everyone has the right to freedom of opinion and expression.
- This right includes freedom to **hold opinions without interference and to seek, receive and impart information and ideas through any media** and regardless of frontiers.

At an <u>individual level</u>, freedom of expression is the key to the development and fulfillment of every person.

- o People can gain an **understanding** of their surroundings and the wider world by **exchanging** ideas and information freely with others.
- o This makes them more **confident** and more able to plan their lives and to work. Sharing ideas can enhance productivity at the workplace, not to mention that it **fosters social relationships**.

At a <u>national level</u>, freedom of expression is necessary for good government and therefore for economic and social progress.

- o **Free debate** about new legislation helps ensure that the eventual law has the support of the population, making it more likely to be respected.
- o If people can speak their minds without fear, and the media are allowed to report what is being said, the **government** can become **aware** of any concerns and **address** them.
- o Free debate about and between political parties exposes their strengths and weaknesses, as a result media scrutiny of the government and the opposition

helps **expose** corruption or other improprieties and **prevents** a culture of dishonesty.

Public authorities may restrict this right if they can show that their action is lawful, necessary and proportionate in order to:

- protect national security, territorial integrity (the borders of the state) or public safety;
- prevent disorder or crime;
- protect health or morals;
- protect the rights and reputations of other people;
- prevent the disclosure of information received in confidence;
- maintain the authority and impartiality of judges; and
- an authority may be allowed to restrict your freedom of expression if, for example, you express views that encourage racial or religious hatred.

USING DIGITAL TECHNOLOGIES FOR FREEDOM OF EXPRESSION

Technically, people can have global access to information. The amount of information available to the masses is incomprehensible. At the same time, Internet security and monopolistic structures have created new dangers to freedom of speech and access to information.

1. **Social Media** is the general term used to describe the plethora of web-based applications that allow people to create, share and exchange information, opinions and ideas in virtual communities.
    - Social media use Internet and mobile technologies to create interactive platforms where individuals and communities share, co-create, discuss and modify user generated content. However, it is necessary to be mindful of the dangers of using social media as well.
    - Social media conjures up many different types of data security and access to information issues.
    - These platforms are run by businesses after all. Media projects can use social media to reach current and new audiences.
    - They can also use it to collect and collate data, to crowdsource information and to develop platforms for discussions on certain topics.
    - Social media can also be used as advocacy and lobbying tools to raise awareness amongst the general public of a specific issue.

2. **YouTube/Soundcloud** are online websites that enable people to upload and share videos and audio for free. A variety of businesses, artists, experts and organizations use them to disseminate ideas and information to a wide audience.

3. **Mobile Phones** have been around for decades and new advancements in smartphones support a variety of additional services such as business, news, social and game applications and photography.

4. **Online Website** may not be new but the way that they are being used to reach wider demographics and new audiences can be considered innovative. Being online gives organizations and businesses a platform to represent their work to the world.

5. **Tablet/Computers** are compact mobile computers that are interactive with touchscreens and have capabilities such as inbuilt cameras and microphones that make them ideal for roving reporters and journalists who are capturing stories on the go.

ADVANTAGES OF FREEDOM OF EXPRESSION

1. Allows individuals to express their opinions
2. Less corruption
3. Freedom from hunger
4. A healthier society

5. Respect for environment
6. Respect for fundamental human rights
7. Improve national security
8. Make the political system more democratic
9. Make the government more efficient
10. Lead to better decision-making
11. Help the economy become more efficient
12. Individuals will receive better treatment from institutions

This black and white picture depicts a middle-aged man with his eyes and mouth covered. The artist creates an atmosphere of sadness, distress and pain, representative of the inability of the man to open his horizons, to follow his dreams. At the first glance we immediately realize how lucky we are: we have the power to speak, to think, to argue.

CONCLUSION

- Freedom of expression, the right to express one's ideas and opinions freely through speech, writing, and other forms of communication, has developed towards progress over the years. However, there is still a long path to tread to type it as universal.
- Some experts have been asking where our freedom stops. In my opinion, there is no freedom which is absolute and unlimited.
- The exercise of the right to freedom of expression carries with its duties and responsibilities; it may be subject to formalities, conditions, restrictions, or penalties as are prescribed by law and are necessary in a democratic society.

WEBSITE CONTENT FILTRATION

Need of Filtering

1. Safe access to the internet.
2. For business.
3. Protect children for unsuitable contents.

CONTENT FILTERING

- On the internet, is the use of a program to screen and exclude from access or availability web pages or e-mail that is deemed objectionable.
- Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out.

TYPES OF FILTERING FILTERS

1. **Browser Based Filters** - is the most lightweight solution to do content filtering and is implemented via third party extensions.
    - Blocksi is the #1 rated extension for web & Youtube filtering, time management and trend analysis for Chrome and Chromebooks.

2. **E-Mail Filters** - set on information contained in the mail headers such as sender, and subject, and e-mail attachments to classify, accept or reject messages.

3. **Search-Engine Filters** - many search engines, such as Google and Bing offer users the option of turning on a safety filter. When this safety filter is activated, it filters out the inappropriate links from all of the search results.
    - If one knows the actual URL of a website, he can access without using search engine.
    - Engines like Lycos, Yahoo, and Bing offer kid-oriented versions of their engines that permit only children-friendly websites.

PROBLEMS WITH FILTERING

It could be expected that allowed content would be blocked. If all pornographic content is to be blocked, other content with a resemblance in features will also be blocked e.g. sex education, medical information, etc.

CENSORSHIP VS. REGULATION

Television and Films

- The **Movie and Television Review and Classification Board (MTRCB)** is a Philippine government agency under the Office of the President of the Philippines that is responsible for the classification and review of television programs, movies, and home videos.
- The government agency can classify a movie or television program as an X-rating which forbids the material from being shown to the public due to issues such as excessive obscenity.

FILMS DESCRIPTION

G (General Patronage) – Viewers of all ages are admitted.
PG (Parental Guidance) – Viewers below 13 years old must be accompanied by a parent or a supervising adult.
R-13 – Only viewers who are 13 years old and above can be admitted.
R-16 – Only viewers who are 16 years old and above can be admitted.
R-18 – Only viewers who are 18 years old and above can be admitted.
X – “X – rated” films are not suitable for public execution.

Chapter 5 - Sex and Technology

Criminals often take advantage of vulnerabilities in cyber security to commit crimes through the use of computer technology. Whilst using computers as the medium, technology crime is not that much different from traditional crime.

CHILD PORNOGRAPHY

- **Child pornography** is a form of child sexual exploitation.
- The law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old).
  - Images of child pornography are also referred to as **child sexual abuse images**.
  - The law **prohibits the production, distribution, importation, reception, or possession** of any image of child pornography.
- The expansion of the Internet and advanced digital technology lies parallel to the explosion of the child pornography market.
- Child pornography images are readily available through virtually every Internet technology, including social networking websites, file-sharing sites, photo-sharing sites, gaming devices, and even mobile apps.

VIRTUAL PROSTITUTION

- **Virtual Sex** is sexual activity where two or more people OR one person and a virtual character, gather together via some form of communications equipment to arouse each other, often by the means of transmitting sexually explicit messages (Wikipedia).
- **Virtual Prostitution** is an activity in which one engages in sexual activity with another person, whom neither have ever seen/met in real life before. Usually, the two met online.

CYBER SEX

- **Cybersex** can be defined as those sexual acts that are derived from surfing electronic media sites that would titillate the sexual mind and satisfies the erotic needs of an individual.
- These sites might be on websites, chat-rooms with webcams, streaming video materials, live sex shows and/or SMS messages.

TYPES OF CYBERSEX USER

A. **Group 1: Recreational Users – Appropriate**
   - This group of cybersex users are able to occasionally explore sex on the internet without problems.
   - They might use cybersex to enhance their sexual experiences.
   - They are able to enjoy intimate sexual relationships in the real world and have a healthy attitude to sexuality.
   - So, although they are seeking sexual gratification online, it is considered appropriate and not pathological.
   - As online dating is increasingly common, they may use websites to meet potential sexual partners, but other than meeting and communicating with partners online, they are as appropriate and respectful in these relationships.

B. **Group 2: Recreational Users - Inappropriate**
   - Like appropriate recreational users, this group of cybersex users can also access internet sex without compulsive use but may use this material inappropriately.
   - This could include sexting or showing sexual images to other people for amusement or shock value.
   - Such users do not keep their activities secret and may otherwise have a healthy attitude towards sexuality and relationships.

C. **Group 3: Problematic Users – Discovery Group**
   - This group has not had any past problems with online other sexual behavior.
   - They may be using the internet as a way to explore sexuality in a way that normal life has not offered them.
   - Examples of problematic users in the discovery group are people who:
     - o Compulsively visit adult dating sites in the hope of meeting a partner, while avoiding real-life opportunities to meet people; or
     - o who uses the internet in an attempt to meet an underage partner for sex, despite no prior history of doing so.
     - o They may also be using dating sites to meet multiple partners in a manipulative or dishonest way.

D. **Group 4: Problematic Users – Predisposed Group**
   - This group includes people who may have a history of fantasizing about sexual acting out, but who have never done it until accessing internet-based sexual material.
   - They might have thought about going to strip clubs or seeing prostitutes for sex, but not taken any action to do so, perhaps for fear of recognition or other consequences.
   - Their use may be regular but not excessive, although attention is taken away from real relationships, work life may suffer, or infidelity can occur.

E. **Group 5: Problematic Users – Lifelong Sexually Compulsive Group**
   - This group includes people who may have a history of fantasizing about sexual acting out, but who have never done it until accessing internet-based sexual material. People in this group are at the extreme end of the continuum of sexual problems.
   - Their sexual acting out occurs with or without access to the internet—the online world simply adds another avenue to explore sexually inappropriate material.
   - These cybersex users may access pornography frequently, as part of an

ongoing pattern of excessive sexual behavior.

- One difficulty with the online world of sex is that while users are detached from their surroundings, sexually aroused, and surfing the net, they may be exposed to images they would never seek out normally.
- This can lead to exploring illicit sexual material in a way that was never intended, sometimes with dire legal and relationship consequences.

WHY CYBERSEX?

- Websites can be accessed anytime, anywhere with anonymity.
- If not participating in cybersex with a known partner, people can portray a new identity.
- There are no consequences like sexually transmitted diseases or pregnancy.
- Can experiment sexually without anyone knowing their true identity.
- Can portray a different version of themselves that's a different gender or age.

WHEN CAN CYBERSEX BE HARMFUL?

1. Use cybersex as a means to:
   - Cope
   - Handle boredom, anxiety, and other powerful feelings
   - Feel important, wanted, and powerful
2. Spend multiple hours away from their work and family.
3. Online at times when the household is asleep -> lack of concentration at work or school.
4. Unable to stop themselves from engaging.
5. Social relationships may decline as the person spends numerous hours engaging in cybersex.
6. May not be able to refrain from accessing the materials in the workplace. May grow anxious and restless if unable to access computer (Sexual Recovery Institute, 2014).

ONLINE RELATIONSHIPS

It is a relationship between people who have met online and, in many cases, know each other only via the Internet.

Examples of Online Dating App/Sites:

- Profoundly
- Neargroup
- Tinder
- Omegle

Advantages:

1. Can immediately focus on people with similar interests, beliefs, age, and other important criteria.
2. Meaningful dating can be done at a distance, even in other countries.
3. Allows you to expand your options outside your social circle.

Disadvantages:

1. Scammers
2. Data Shared is Permanent
3. Misleading Form of Attraction
4. Distance is a Barrier

Chapter 6 - Technology and Privacy

Most people know by now social media isn't free – it's paid for with the collection of its users' sometimes-sensitive information. Your GPS system keeps track of your movements, and your smart TV or webcam can watch you. Almost all the information these devices collect can be sold to companies or used by government and law enforcement to keep tabs or gather evidence. At the same time, we use technology so frequently as a society because it allows us to do things faster and with much less effort.

IDENTITY THEFT

- It is also known as **identity fraud**, is a crime in which an imposter obtains key pieces of personally identifiable information (PII), such as Social Security or Driver's license numbers, to impersonate someone else.
- The taken information can be used to **run up debt purchasing credit, goods, and services** in the name of the victim or to provide the thief with false credentials.

- In rare cases, an imposter might provide **false identification** to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

EXAMPLES OF IDENTITY THEFT

1. **Financial Identity Theft** - this is the most common type of identity theft. Financial identity theft seeks economic benefits by using a stolen identity.

2. **Tax-related Identity Theft** - in this type of exploit, the criminal files a false tax return with the Internal Revenue Service (IRS). Done by using a stolen Social Security number.

3. **Medical Identity Theft** - the thief steals information like health insurance member numbers, to receive medical services. The victim's health insurance provider may get the fraudulent bills. This will be reflected in the victim's account as services they received.
    - **Criminal Identity Theft** - a person under arrest gives stolen identity information to the police. Criminals sometimes back this up with a containing stolen credentials. If this type of exploit is successful, the victim is charged instead of the thief.
    - **Child Identity Theft** - a child's Social Security number is misused to apply for government benefits, opening bank accounts and other services. Children's information is often sought after by criminals because the damage may go unnoticed for a long time.
    - **Senior Identity Theft** - this type of exploitation targets people over the age of 60 because senior citizens are often identified as theft targets. It is especially important for these seniors to stay on top of the evolving methods thieves use to steal information.
    - **Identity Cloning for Concealment** - a thief impersonates someone else in order to hide from law enforcement or creditors. Because this type isn't explicitly financially motivated, it's harder to track, and there often isn't a paper trail for law enforcement to follow.
    - **Synthetic Identity Theft** - a thief partially or completely fabricates an identity by combining different pieces of PII from different sources.

IDENTITY THEFT TECHNIQUES

Although an identity thief might hack into a database to obtain personal information, experts say it's more likely the thief will obtain information by using social engineering techniques. These techniques include the following:

1. **Mail Theft** - this is stealing credit card bills and junk mail directly from a victim's mailbox or from public mailboxes on the street.

2. **Dumpster Diving**
    - Retrieving personal paperwork and discarded mail from trash dumpsters is an easy way for an identity thief to get information.
    - Recipients of preapproved credit card applications often discard them without shredding them first, which greatly increases the risk of credit card theft.

3. **Shoulder Surfing** - this happens when the thief gleans information as the victim fills out personal information on a form, enters a passcode on a keypad or provide a credit card number over the telephone.

4. **Phishing**
    - This involves using email to trick people into offering up their personal information.
    - Phishing emails may contain attachments bearing malware designed to steal personal data or links to fraudulent websites where people are prompted to enter their information.

MONITORING

- Employers are justifiably concerned about threats to and in the workplace, such as theft of property, breaches of data security, identity theft, viewing of pornography, inappropriate and/or offensive behavior, violence, drug use, and others.
- They seek to minimize these risks, and that often requires monitoring employees at work.
- Employers are also concerned about the productivity loss resulting from employees using office technology for personal matters while on the job.
- Organizations must balance the valid business interests of the company with employees' reasonable expectations of privacy.
- Magnifying ethical and legal questions in the area of privacy is the availability of new technology that lets employers track all employee Internet, e-mail, social media, and telephone use.

INTRUSION/INVASION OF PRIVACY

- Invasion of privacy is a legal term. It is used to describe a circumstance where an individual or organization knowingly intrudes upon a person.
- The intrusion occurs when the person has a reasonable expectation of privacy, such as in a bathroom or locker room.
- An invasion of privacy is considered to be a tort. A tort is a wrongful act that causes injury or loss to someone resulting in legal responsibility for the wrongful act.

TYPES OF INTRUSION/INVASION OF PRIVACY

A. **Deception**
    - This group of cybersex users are able to occasionally explore sex on the internet without problems. Deception occurs when an employer collects information, he claims is for one reason but uses it for another reason, which could result in the employee's termination.
    - An example of deception is if an employer sets up a blood drive and tells employees that donations will be used to aid a local blood bank. The blood drawn from employees is tested for drugs as part of the process.
    - The employer could be accused of deception if he uses the drug results as a reason to terminate employees if employees did not consent to being drug tested.

B. **Violation of Confidentiality**
    - Violating an Employee's Confidentiality occurs when **information given** in confidence is then given **to a third party**.
    - For example, an employee who has a wife and children decides to leave his insurance policy to an unrelated female co-worker.
    - If the human resources manager reveals this confidential information to another employee, it is considered an invasion of privacy.

C. **Intrusion & Misappropriation**
    - **Intrusion** occurs in business when an employer intrudes in an employee's private life.
    - What you do in the privacy of your own home is your business and an employer may not interfere with that because you have a reasonable expectation of privacy.

Chapter 7 - Information Warfare

Information warfare opens new avenues for the conduct of politico-military operations.

INFORMATION WARFARE (IW)

- It is defined as "action as taken to **achieve information superiority** by affecting an adversary information, information-based processes, information systems and computer-based networks **while defending one's own**

information, information-based processes, information systems and computer-based networks.

- It is a concept involving the **battlespace use and management of information and communication technology (ICT)** in pursuit of a competitive advantage over an opponent.
- IW is **the manipulation of information trusted by a target without the target's awareness**, so that the target will make decisions against their interest but in the interest of the one conducting information warfare.
- Information Warfare can take many forms:
  - Television, internet and radio transmission(s) can be jammed.
  - Television, internet and radio transmission(s) can be hijacked for a disinformation campaign.
  - Logistics networks can be disabled.
  - Enemy communications networks can be disabled or spoofed, especially online social community in modern days.
  - Stock exchange transactions can be sabotaged, either with electronic intervention, by leaking sensitive information or by placing disinformation.
  - The use of drones and other surveillance robots or webcams.
  - Communication management.

WEAPONS OF INFORMATION WARFARE

A. Information Collection

- This is included as part of information warfare because "*[t]he information revolution implies the rise of a mode of warfare in which… the side that knows more… will enjoy decisive advantages*."
- The idea is that the **more information one has, the higher his/her situational awareness**, which leads to better battle plans and, hopefully, better outcomes.
- According to Singh, "*[t]ill recently, knowing your position and that of the friendly forces was itself a huge task. Precision position locating technologies such as navigation based on the Global Positioning System (GPS) has eased those problems to a large extent. Knowing the position of the enemy has also been made possible to a degree through employment of renaissance and surveillance technologies*."

B. Information Transport

- Collecting a large amount of comprehensive information is certainly good practice, but collection is of little value if the information sits in a storage facility, unused.
- As such, the **ability to transport information into the hands of those who need it, in a timely manner**, is another essential aspect of information warfare.
- The tools used in this domain are not exactly weapons, but rather civilian technologies put to use in military situations.
- The most important of these tools is communication infrastructure, composed of networks of computers, router, telephone lines, fiber optic cable, telephones, televisions, radios, and other data transport technologies and protocols.

C. Information Protection

- One of the most broadly agreed upon aspects of information warfare is the need to **minimize the amount of information to which your opponent has access**.
- The weapons used to protect the security of our information fall in two classes.
  - **First** are those technologies that physically protect our vital data storage facilities, computers, and transport mechanisms.
  - **Second**, and perhaps more important, are technologies that

prevent bits from being seen and intercepted by the enemy.

- This certainly includes basic computer security technologies such as **passwords**, as well as more sophisticated technologies like **encryption**.

D. **Information Manipulation**

- Information manipulation in the context of information warfare is **the alteration of information with intent to distort the opponent's picture of reality**.
- This can be done using a number of technologies, including computer software for editing text, graphics, video, audio, and other information transport forms.
- Design of the manipulated data is usually done manually so those in command have control over what picture is being presented to the enemy.

E. **Information Disturbance, Degradation and Denial**

- The final aspects of information warfare, according to our earlier definition, are disturbance, degradation, and denial.
- All three techniques are means to the same general end – **preventing the enemy from getting complete, correct information**.
- Because of their similarity, many of the same weapons are used to achieve one or more of the goals.
- Some of the more popular weapons used to wage these types of information warfare are **spoofing, noise introduction, jamming, and overloading**.

TYPES OF INFORMATION WARFARE

1. **Command and Control Warfare -** the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, **to deny information to influence, degrade, or destroy adversary command and control capabilities**, while protecting friendly command and control capabilities against such actions.

2. **Intelligence-Based Warfare** - is a unique concept, you wouldn't know what parts of the network to destroy in order to disrupt decision making if you didn't have good intelligence.

3. **Electronic Warfare** - are those techniques that enhance, degrade or intercept the flow of information electronically.

4. **Psychological Warfare**
   - The term used "to denote any action which is practiced mainly by psychological methods with the aim of **evoking a planned psychological reaction in other people**".
   - Psychological Warfare are **planned operations to convey selected information and indicators to audiences** to influence their emotions, motives, objective reasoning and ultimately the behavior of organizations, groups, and individuals.

5. **Hacker Warfare**
   - Probably the most familiar portion of Information Warfare for most of us.
   - This type of warfare is also known as **Computer Network Operations (CNO)** and is often portrayed in movies and headlines.
   - One of the biggest areas of IW where the military and civilian lines get mixed up and you start to see military attacks on civilian companies to gain a desired effect on an enemy.

6. **Economic Information**
   - It is defined as **channeling or blocking information** to pursue economic dominance.
   - EIW can be defined as the economic impact of Information Warfare on country or company.
   - There are two areas of EIW: **information blockade and information imperialism**.
   - A nation or company would cut-off the targeted countries access to outside information. This blockade would cripple the economy of the targeted nation.

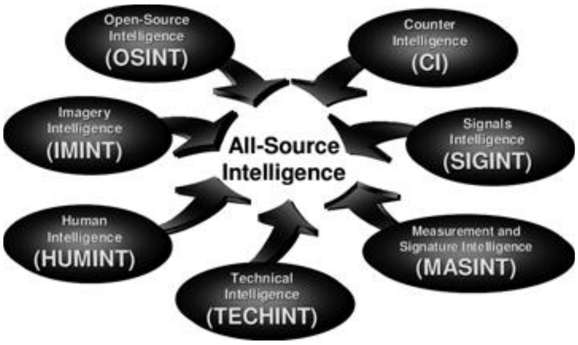
7. **Cyberwarfare**
   - It is the **use of information systems against the virtual personas of individuals or groups**.
   - It is the use of computer technology to **disrupt the activities of a state or organization**, especially the deliberate attacking of information systems for strategic or military purposes.

CYBER ESPIONAGE

- Espionage, according to Merriam-Webster, is "*the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company*."
- Cyberespionage involves the **use of information and communication technology (ICT)** by individuals, groups, or businesses for some **economic benefit or personal gain.**

INTELLIGENCE GATHERING

Collecting of information about a particular entity for the benefit of another through the use of more than one, inter-related source. Below are the IG Discipline:


Open-Source Intelligence (OSINT)
Counter Intelligence (CI)
Imagery Intelligence (IMINT)
All-Source Intelligence
Signals Intelligence (SIGINT)
Human Intelligence (HUMINT)
Measurement and Signature Intelligence (MASINT)
Technical Intelligence (TECHINT)

1. **Human Intelligence (HUMINT) -** is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines.
   - It can provide several kinds of information.
   - It can provide observations during travel or other events from travelers, refugees, escaped friendly POWs, etc.
   - It can provide date on things about which the subject has specific knowledge, which can be another human subject or, in the case of defectors and spies, sensitive information to which they had access.
   - Finally, it **can provide information on interpersonal relationship and network of internet**.

2. **Geospatial Intelligence (GEOINT) -** is **intelligence about human activity on earth** derived from the exploitation and analysis of imagery and geospatial information that describes, assess and visually depicts physical features and geographically referenced activities on the earth.

3. **Measurement and Signature Intelligence (MASINT) -** is a technical branch of intelligence gathering which serves to **detect, track, identify or describe the signature (distinctive characteristics) of fixed or dynamic target sources**.
   - It can provide several kinds of information. This often includes radar intelligence, acoustic intelligence, nuclear intelligence and chemical and biological intelligence.

- MASINT is defined as scientific and technical intelligence derived from the analysis of data from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter, or sender, to facilitate the latter's measurement and identification.

4. **Open-source Intelligence (OSINT) -** is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence.

5. **Signals Intelligence (SIGINT)** - is **intelligence-gathering by interception of signals**, whether communications between people (communication intelligence – abbreviate to COMINT) or from electronic signals not directly used in communications (electronic intelligence – abbreviated to ELINT) Signals intelligence is a subset of intelligence collection management.
   - As sensitive information is often encrypted, signals intelligence in turn involves the use of cryptanalysis to decipher the messages. Traffic analysis – the study of who is signaling whom and in what quantity - is also used to derive information.

6. **Technical Intelligence (TECHINT)** - is **intelligence about weapons and equipment** used by the armed forces of foreign nations (often referred to as foreign material). The related term, scientific and technical intelligence, addresses information collected on the strategic (i.e. national) level.
   - Technical intelligence is intended primarily to allow the armed forces to avoid technological surprise.

7. **Cyber Intelligence/ Digital Network Intelligence (CYBINT/DNINT)** - is gathered from cyberspace or interconnected technology.

8. **Financial Intelligence (FININT)** - is the **gathering of information about the financial affairs of entities of interest**, to understand their nature and capabilities, and predict their intentions.
   - Generally, the term applies in the context of law enforcement and related activities.
   - One of the main purposes of financial intelligence is to **identify financial transaction**s that may involve tax evasion, money laundering or some other criminal activity.
   - FININT may also be involved in **identifying financing of criminal and terrorist organizations**.