College of Informatics and Virtual Education (CIVE)

IA 418: Cyber Criminology and Techniques

International Cybercrime Issues

1

International Cybercrime Issues

- International dimension of cybercrime
  - ✓ Cyberterrorism
  - ✓ Cyberwarfare
  - ✓ Human Trafficking

Cyberterrorism

- What is terrorism?
  - ✓ It is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.
- **Cyberterrorism** is the convergence of **cyberspace** and **terrorism.**
  - ✓ It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to **intimidate** or **coerce** a government or its people in furtherance of political or social objectives.

Cyberterrorism

- To qualify as Cyberterrorism, an attack should result in **violence** against persons or property, or at least cause enough harm to **generate fear**.
  - ✓ Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples.
- Serious attacks against critical infrastructures could be acts of Cyberterrorism, depending on their impact.
  - ✓ Attacks that disrupt nonessential services or that are mainly a costly **nuisance** would not.

Cyberterrorism

- It is important to distinguish between Cyberterrorism and "**hacktivism**".
  - ✓ Hacktivism, a blend of the words "**hacking**" and "**activism**".
  - ✓ Hacktivism uses hacking techniques for **political** or **social causes**.
  - ✓ It's a form of civil disobedience, leveraging digital tools to **protest** or take direct action.
- Hacktivism work to promote issues related to **freedom of speech**, **human rights**, or **information ethics**.

Cyberterrorism

- Hacktivism, although politically motivated, does not amount to Cyberterrorism.
  - ✓ Hacktivists do want to protest and **disrupt**; they do not want to **kill** or **maim** or **terrify**.
- Hacktivists have four main weapons at their disposal:
  - ✓ Virtual blockades
  - ✓ E-mail attacks
  - ✓ Hacking and computer break-ins
  - ✓ Computer Malware

Cyberterrorism

- **Virtual Blockades:**
  - ✓ It is the virtual version of a physical sit-in or blockade
  - ✓ Political activists visit a website and attempt to generate so much traffic toward the site that other users cannot reach it.
  - ✓ Aims at disrupting normal operations while winning publicity.
- **Email Attacks**
  - ✓ E-mail bombing campaigns (bombarding targets with thousands of messages at once, also known as "ping attacks").

Cyberterrorism

- Hacking and computer break-ins:
  - ✓ Web hacking and computer break-ins (hacking into computers to access stored information, communication facilities, financial information, and so forth).
- Computer Malware:
  - ✓ Different forms of malicious code that can infect computers and propagate over computer networks.
  - ✓ During the NATO operation to evict Serbian forces from Kosovo, businesses, public entities, and academic institutes in NATO member-states received virus-laden e-mails from a range of Eastern European countries.

Cyberterrorism

- The cyberspace can be used to:
  - ✓ **Facilitate** the commission of terrorist-related offences-a form of cyber-dependent terrorism.
  - ✓ Can also be the **target** of terrorists-a form of cyber-dependent terrorism.
- Specifically, ICT can be used to **promote**, **support**, **facilitate**, and/or **engage** in acts of terrorism.
- The cyberspace can be used for the following purposes:
  - ✓ Spreading of "**propaganda**"-including recruitment, radicalization and incitement to terrorism.
    - Enables terrorists to spread their rhetoric and recruit members from a global community.

Cyberterrorism

- The cyberspace can be used for the following purposes:
  - ✓ **Training**: web-based learning may include bomb-making, use of surface-to-air missiles, border jumping, and creation of fraudulent identification.
  - ✓ **Communication**: use of technology is making terrorist networks resilient to law enforcement.
    - Communicating via cyberspace reduces the risk of physical vulnerability.
    - Online dialogue is cheaper, international in scope, more widely accessible, and poses far less risk than traditional methods.

Cyberterrorism

- The cyberspace can be used for the following purposes:
  - ✓ **Research and planning**:
    - The cyberspace may also be utilized to gain knowledge or information.
    - Critical information on satellites, military deployments, engineering schematics, and the like is readily available.
  - ✓ **Attack mechanism**:
    - The cyberspace provides numerous benefits to people.
    - Its disruption can have far reaching consequences to people, for example, stuxnet.

Cyberterrorism

- Motivation for cyberterrorism:
  - ✓ **Cheaper** than traditional terrorist methods:
    - The terrorist only needs is a personal computer and an online connection.
    - Terrorists do not need to buy weapons such as guns and explosives
    - They can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.
  - ✓ Cyberterrorism is more **anonymous** than traditional terrorist methods:
    - In cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

Cyberterrorism

- Motivation for cyberterrorism:
  - ✓ The **variety** and number of **targets** are enormous.
    - The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, etc.
    - The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit.
    - Critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attacks.

Cyberterrorism

- Motivation for cyberterrorism:
  - ✓ Cyberterrorism can be **conducted remotely**, a feature that is especially appealing to terrorists.
    - Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism.
    - It is easier for terrorist organizations to recruit and retain followers.
  - ✓ Cyberterrorism has the potential to affect directly a larger number of people than traditional terrorist methods.
    - This is likely to generate greater media coverage, which is ultimately what terrorists want.

Cyberwarfare

- **Cyberwarfare** describes cyber acts that compromise and disrupt **critical infrastructure systems**, which amount to an **armed attack**.
  - ✓ Makes use of the cyberspace as a war fighting domain, just like land, sea, and air.
  - ✓ An armed attack intentionally causes destructive effects such as death and/or physical injury to living beings and/or destruction of property.
- Only governments, organs of the state, or state-directed or state-sponsored individuals or groups can engage in cyberwarfare.

Cyberwarfare

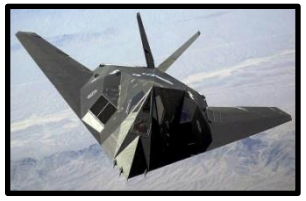
- **Cyberwarfare** describes cyber acts that compromise and disrupt **critical infrastructure systems**, which amount to an **armed attack**.



Cyberwarfare



What does a stealth bomber cost? **$1.5 to $2 billion**



What does a stealth fighter cost? **$80 to $120 million**



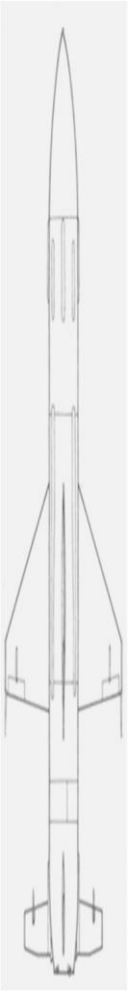
What does an cruise missile cost? **$1 to $2 million**



What does a cyber weapon cost? **$300 to $50,000**

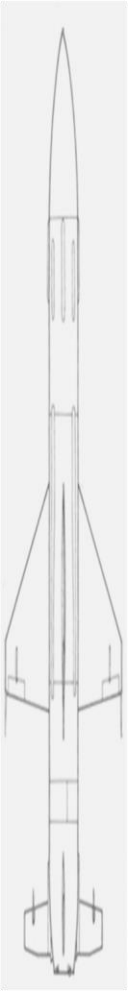
Cyberwarfare

- Cyber weapon architecture:
  - ✓ A missile is comprised of three basic elements.
    - The first is a **delivery vehicle** (rocket engine)
    - Followed by a **navigations system** (tells it how to get to the target)
    - Finally the **payload** (the component that causes harm).
  - ✓ As it turns out, the same three elements now appear in the design of **cyber weapons**.



Cyberwarfare

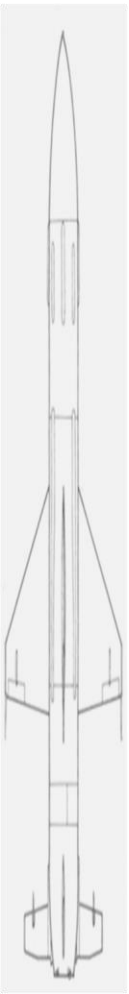
- Cyber Weapon – Delivery Vehicle



  - ✓ There are numerous methods of delivering cyber weapons to their targets.
    - Emails with malicious code embedded or attached is one mechanism of delivery.
    - Another delivery vehicle is web sites that can have malicious links and downloads.
    - Hacking is a manually delivery vehicle that allows a cyber soldier to place the malicious payload on a target computer, system or network.
    - Counterfeit hardware, software and electronic components can also be used as delivery vehicles for cyber weapons.

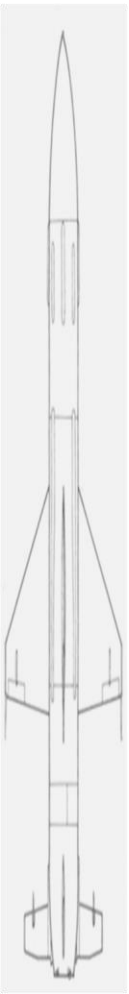
Cyberwarfare

- Cyber Weapon – Navigation System
  - ✓ Just as a navigation system guides a missile, it allows the malicious payload to reach a specific point inside a computer, system or network.
  - ✓ System vulnerabilities are the primary navigation systems used in cyber weapons.
  - ✓ Vulnerabilities in software and computer system configurations provide entry points for the payload of a cyber weapon.
  - ✓ These security exposures in operating systems or other software or applications allow for exploitation and compromise.
  - ✓ Exploitation of these vulnerabilities may allow unauthorized remote access and control over the system.



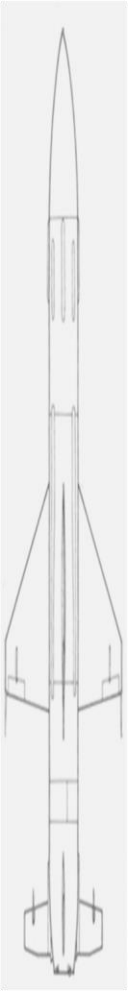
Cyberwarfare

- Cyber Weapon – Navigation System
  - ✓ Just as a navigation system guides a missile, it allows the malicious payload to reach a specific point inside a computer, system or network.
  - ✓ System vulnerabilities are the primary navigation systems used in cyber weapons.
  - ✓ Vulnerabilities in software and computer system configurations provide entry points for the payload of a cyber weapon.
  - ✓ These security exposures in operating systems or other software or applications allow for exploitation and compromise.
  - ✓ Exploitation of these vulnerabilities may allow unauthorized remote access and control over the system.



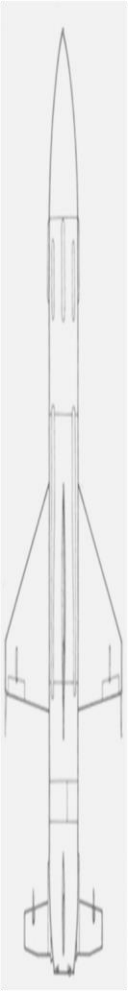
Cyberwarfare

- Cyber Weapon – Payload
  - ✓ The payload of a missile is sometimes called a warhead and is packed with some type of explosive.
  - ✓ In a cyber weapon the payload could be a program that copies information off of the computer and sends it to an external source.
  - ✓ It can also be a program that begins to ease or alter information stored on the system.
  - ✓ Finally, it can allow remote access so that the computer can be controlled or directed over the internet.
    - A "bot" (a component of a botnet) is a great example of a payload that allows remote use of the computer by an unauthorized individual or organization.



Cyberwarfare

- Cyber Weapon – Payload
  - ✓ The payload of a missile is sometimes called a warhead and is packed with some type of explosive.
  - ✓ In a cyber weapon the payload could be a program that copies information off of the computer and sends it to an external source.
  - ✓ It can also be a program that begins to ease or alter information stored on the system.
  - ✓ Finally, it can allow remote access so that the computer can be controlled or directed over the internet.
    - A "bot" (a component of a botnet) is a great example of a payload that allows remote use of the computer by an unauthorized individual or organization.



Cyberwarfare

- Types of Cyber Attacks constituting a cyberwarfare:
  - ✓ **Sabotage:** cyber-attack is directed towards sabotaging a critical infrastructure such as a nuclear reactor, it can be considered an **act of war.**
  - ✓ **Espionage:** a malware can be developed to steal sensitive government and military information as in traditional **spying**.
  - ✓ **Subversion:** an attack that create confusion by cutting communication bridge between government, public and International community.

Cyberwarfare

- Existing legal rules and norms on warfare have been applied to cyberwarfare.
  - ✓ The **right to use force** (jus ad bellum)
  - ✓ The **right conduct during war** (jus in bello)
- Before engaging in cyberwarfare, the right to use force needs to be established.
  - ✓ The reasons for using any form of force must be legitimate and sanctioned by law.
    - One such justified reason is **self-defence**.
    - The UN Charter of 1945 allows armed attacks among member states for self-defence.

Cyberwarfare

- When engaging in cyberwarfare, the **right conduct during war** is required.
  - ✓ The cyber acts that amount to a use of force must be: **proportionate**.
    - This applies both to the threat that justified this response and in light of the potential collateral damage.
  - ✓ It is aimed at minimizing casualties through the adoption of certain precautionary measures.
  - ✓ **Discriminating in its targets**-only the actual target should be subjected to the cyber act.
  - ✓ Should be used only as a last resort, after lesser invasive means have been exhausted and/or ruled out as unfeasible options.

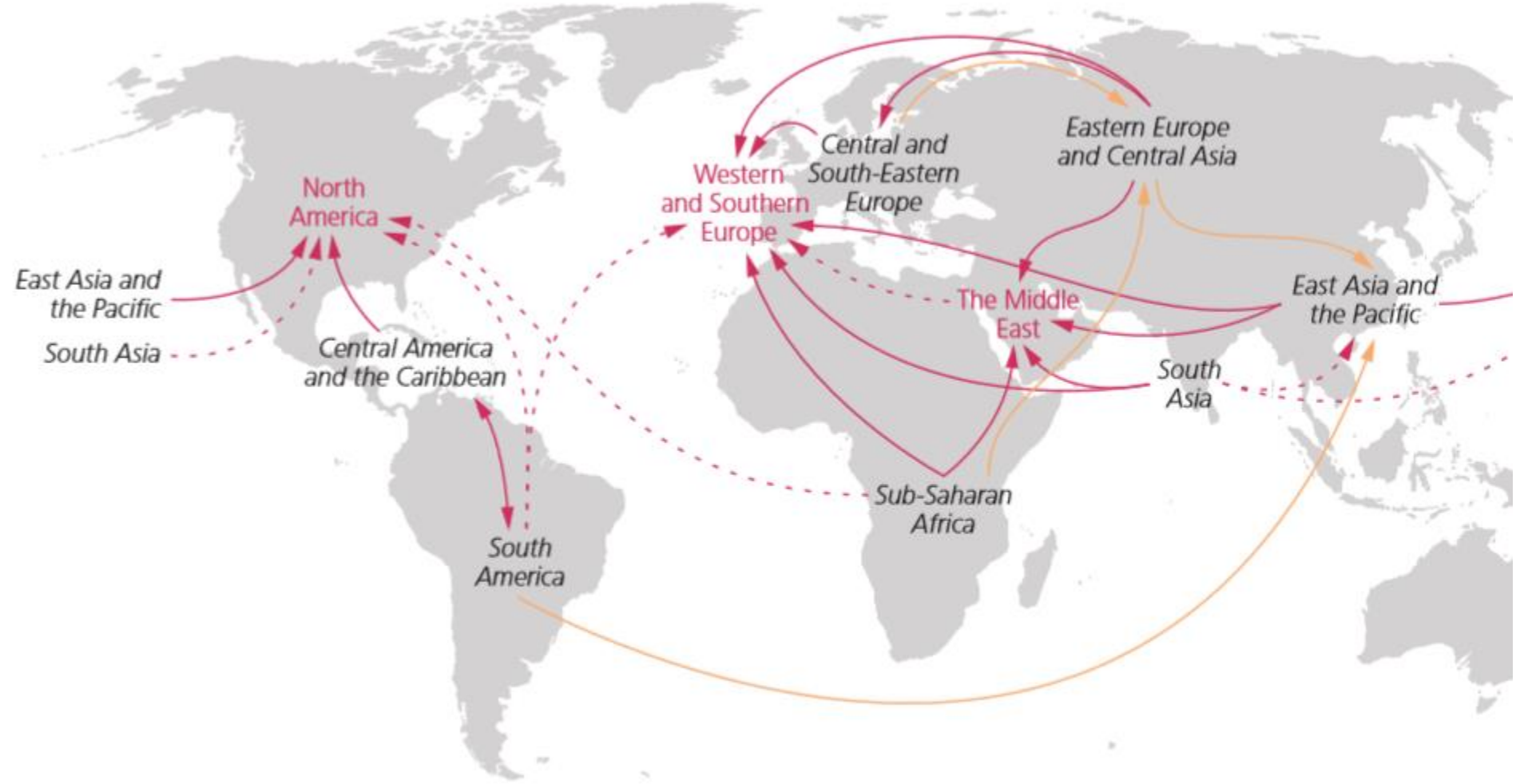
Human Trafficking

- Human trafficking is a group of crimes involving the exploitation of **men**, **women** and **children** for financial gains which is violation of fundamental human rights.
- Human trafficking is the 3rd largest international crime.
  - ✓ Over **one million** people **trafficked annually**.
  - ✓ Millions of men, women and children are victims of human trafficking.
  - ✓ Human trafficking is a part of the larger problem of **slavery**

Human Trafficking

- Human trafficking is when people are **transported**, by **force** or **deception**, or other ways, to become enslaved.
  - ✓ Traffickers use blackmail, abuse, and threats to force victims to comply with their wishes in the destination country.
  - ✓ Usually caused by poverty/lack of economic opportunities, especially for women and children, and a demand for certain services in the destination country.

Human Trafficking



Human Trafficking

- Causes of human trafficking:
  - ✓ Unemployment.
  - ✓ Poverty.
  - ✓ Absence of a social safety.
  - ✓ Political instability.
  - ✓ Status of violence against women & children.
  - ✓ The low risk, high-profit.

Human Trafficking

- Who are trafficked?
  - ✓ Women and children are the key target
  - ✓ People of low income.
  - ✓ People with low level of education.
  - ✓ Young girls running away from home
  - ✓ People who lack awareness of their legal rights.
  - ✓ Women and children of varying ages

Human Trafficking

- People are being trafficked for what? A large percentage for:
  - ✓ Forced labour e.g. in prostitution
  - ✓ The entertainment industry
  - ✓ **Sweatshops**: is a shop or factory in which employees work for long hours at low wages and under unhealthy conditions.
  - ✓ Illegal adoption of children
  - ✓ Organ transplants
  - ✓ Forced marriages

Human Trafficking

- People are being trafficked for what? A large percentage for:
  - ✓ Mail-order bride: is a woman who lists herself in catalogs and is selected by a man for marriage.
  - ✓ Domestic work construction
  - ✓ Drug trafficking
  - ✓ Begging
  - ✓ Other exploitative forms of work

Human Trafficking

- Throughout the entire human trafficking process there are 4 parties involved:
  - ✓ The recruiter
  - ✓ The trafficker
  - ✓ The victim
  - ✓ The human trafficking industry

Human Trafficking

- How Are Victims Trafficked?
  - ✓ **Force**, **fraud** and **coercion** are methods used by traffickers to press victims into lives of servitude, & abuse.
  - ✓ **Force**: Rape, beatings, confinement.
  - ✓ **Fraud**: Includes false and deceptive offers of employment, marriage, better life.
  - ✓ **Coercion**: Threats of serious harm to, or physical restraint of, any person; any scheme, plan or pattern intended to cause victims to believe that failure to perform an act would result in restraint against them; or the abuse or threatened abuse of the legal process

Human Trafficking

- How technology facilitates trafficking in persons
  - ✓ Technology increases the ease with which traffickers can **locate**, **recruit**, **coerce** and **control** their victims.
  - ✓ The internet with cybercrime tools can be used throughout the trafficking chain.
  - ✓ The tools can be used for:
    - Identification and recruitment of potential victims.
    - Coercion and control.
    - Advertising and selling goods and services produced from their exploitation.
    - Laundering of profits

Human Trafficking

- Elements of crime in human trafficking:
  - ✓ **Recruitment**
  - ✓ **Transportation**
  - ✓ **Transfer**
  - ✓ **Harbouring**
  - ✓ **Receipt**
- The crimes are committed using: threat, use of force, coercion, abduction, fraud, deception, abuse of power, abuse of vulnerability, payments or benefits from controlling parties.

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ The Internet provides traffickers with access to a greater number of potential victims through:
    - **Phones**
    - **Emails**
    - **Instant messaging**
    - **Websites**
    - **Phone applications (or apps).**

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ The recruitment tactics of traffickers include (but are not limited to):
    - **Preying on emotional or psychological vulnerabilities**
    - **Promises or threats**
    - **Theft of ID documents.**
    - **Kidnapping**

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ At the recruitment stage, traffickers are far more likely to use '**clearnet**' websites to establish initial contact with victims.
    - Clearnet websites are surface websites or visible websites that are indexed by search engines, like Google or Bing.
  - ✓ Clearnet websites allows traffickers to engage with a wider pool of Internet users, who are less likely to have a **sophisticated understanding of technology**.

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ Clearnet forums can facilitate **text** and **video chat**, **image exchange**, **dating** and other interpersonal activities.
    - Provide traffickers with unprecedented access to potential victims.
    - Provide the traffickers with information that can be used to identify victims' vulnerabilities that can be leveraged to gain victims' **trust** and **confidence** (for example, online grooming)

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ Social networking websites enables traffickers to **research** their **victim** and readily **monitor** their **likes** and **dislikes**.
    - Traffickers are able to **tailor their approach** to each victim, improving the effectiveness of their manipulations.
  - ✓ Online platforms provide traffickers with:
    - Location data
    - Identity details and information about lifestyle, routines and habits.

Human Trafficking

- Use of technology in **recruiting** victims of human trafficking:
  - ✓ Online platforms provide traffickers with:
    - Images
    - Contacts
  - ✓ Examples of commonly used sites
    - **View and comment sites**: Instagram and Facebook.
    - **Conversational sites**: Tinder, Blendr
    - **Webcam sites**: Chat roulette, Omegle
    - **Advertising and sales sites**: City guide, Skipthegames

Human Trafficking

- Use of technology in **control** victims of human trafficking:
  - ✓ Control can take several forms, among them:
    - Coercing
    - Physically luring and transporting the victims away from their home
    - Controlling finances
    - Blackmail.
  - ✓ Technology allows traffickers to avoid **physical** and **face-to-face** contact with victims, which makes **investigation** of trafficking in persons even more difficult.

Human Trafficking

- Use of technology in **control** victims of human trafficking:
  - ✓ Control may include **monitoring** victims through manual examination of **phone records**.
  - ✓ Accessing phone applications through **cloud-based applications** or by deploying **spyware**.
  - ✓ Traffickers can also send **threatening communications** to victims who manage to escape, in an attempt to **maintain** or **regain control**.

Human Trafficking

- Use of technology in **control** victims of human trafficking:
  - ✓ **Fraud**, **threats** and **deception** may be used by traffickers who obtain **compromising information** about the victim (such as images or videos) as a means to gain control.
    - For example, by promising modelling work and asking for **nude photographs** from the models, followed by **making threats**.

Human Trafficking

- Use of technology in **control** victims of human trafficking:
  - ✓ **Hijacking the social media** of victims and adding content suggestive of consent to exploitation.
    - Sexually graphic content can be posted to damage the victim's reputation and credibility as a complainant.
    - Posting explicit content may lead to the account being closed by the service provider.
    - Account closure means isolation and loss of digital identity and a loss of contact with family and the community

Human Trafficking

- Use of technology in **exploitation** victims of human trafficking:
  - ✓ Human beings are considered a **commodity** offline and online.
  - ✓ Traffickers **advertise** human beings and services they can provide, seeking clients to purchase the services.
  - ✓ Traffickers advertise on **clearnet** (the visible web) and the **deep web**.
  - ✓ The deep or "dark" web is part of the World Wide Web that is not discoverable by open search engines.
    - Content is often **password protected** and **encrypted**.

Human Trafficking

- Use of technology in **exploitation** victims of human trafficking:
  - ✓ Encryption and rerouting of traffic on the dark web makes investigation difficult.
  - ✓ Victims' services are also sold on clearnet websites so as to reach the wider audience who are not technology savvy.
    - Websites such as Craigslist , Reddit, adultsearch.com, meet4fun.com, and backpage.com have all been used by traffickers to advertise victims.
    - Traffickers advertise their victims' services under the **guise of legitimate work** (e.g. massage service).

Human Trafficking

- Use of technology in **exploitation** victims of human trafficking:
  - ✓ The advertisements on these sites hide the fact that human beings are being sold by using certain code words:
    - "girlfriend experience“ meaning sex is for sale.
    - "I have a younger friend“ meaning minor is being advertised.
    - “Fresh” or emojis such as a cherry and cherry blossom meaning identify the victim as a virgin.
  - ✓ Child exploitation can also occur through the use of **live-streaming** child sexual abuse.

Human Trafficking

- Use of technology in **profiting** from victims of human trafficking:
  - ✓ Cryptocurrencies are far **more volatile** than **physical currencies**, as they are **neither regulated nor backed** by banks.
    - Have created a means by which criminals can **receive payment** and **hide** or **move proceeds** of crime.
  - ✓ There are several advantages to using digital currencies over cash:
    - Digital currencies **remove the need to launder cash**, which is more difficult in most countries due to increasingly strict cash reporting and money-laundering compliance regulations.

Human Trafficking

- Use of technology in **profiting** from victims of human trafficking:
  - ✓ There are several advantages to using digital currencies over cash:
    - Funds in digital form can be **moved across international borders** with ease, thereby circumventing limits on cash transfers across jurisdictions.
    - Using **multiple digital "wallets"** (a separate wallet for each transaction) creates additional challenges for police and anti-money laundering authorities to track transactions and monitor patterns.

Human Trafficking

- Use of technology in **profiting** from victims of human trafficking:
  - ✓ There are several advantages to using digital currencies over cash:
    - Digital currencies provide **relative anonymity**.
    - There is a **reduced risk** of a counterparty reneging on a transaction relative to more mainstream financial based transactions. Many digital currency transactions are irreversible and can only be refunded by the receiving party

Human Trafficking

- **Class Activity**: Write a brief essay about the profile of human traffickers, taking into account the following:
  - ✓ What sort of people do you imagine become traffickers?
  - ✓ What life experiences are they likely to have had to lose their empathy and respect for other people?
  - ✓ In your view, is it more likely that victims will be trafficked by people of the same or different nationality, ethnicity or religion?
  - ✓ Do you believe it is possible to discourage traffickers from continuing their criminal activities by education or awareness-raising/media campaigns?