College of Informatics and Virtual Education (CIVE)

IA 418: Cyber Criminology and Techniques

Legal Composition of Cybercrime

Cybercrime: Definition

- **Cybercrime** is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either **target networks**, **systems**, **data**, **websites** and/or **technology** or **facilitate** a **crime.**

- ✓ It is a fast-growing area of crime.
- ✓ Criminals are exploiting the **speed**, **convenience** and **anonymity** of the Internet to commit a diverse range of criminal activities that **know no borders**, either **physical** or **virtual**.

Cybercrime: Characteristics

- **People with specialized knowledge.**
  - ✓ To commit this kind of crime one has to be **very skilled** in internet and computers and internet to commit such a crime.
  - ✓ The people who commit cybercrime are well educated and have **deep understanding** of the usability of internet.
  - ✓ This has made work of police machinery very difficult to tackle the perpetrators of cyber crime.

Cybercrime: Characteristics..

- **Geographical challenges**
  - ✓ In cyberspace the geographical boundaries reduced to zero.
  - ✓ A cyber criminal in no time sitting in any part of the world commit crime in other corner of world.
  - ✓ For example a hacker sitting in Tanzania hack in the system placed in Kenya.

Cybercrime: Characteristics..

- **Virtual World**
  - ✓ The act of cyber crime takes place in the cyber space and the criminal who is committing this act is **physically outside the cyber space.**
  - ✓ Every activity of the criminal while committing that crime is done over the **virtual world**.

Cybercrime: Characteristics..

- **Collection of Evidence**
  - ✓ It is very difficult to **collect evidence** of cyber crime and **prove them in court** of law due to the nature of cyber crime.
  - ✓ The criminal in cyber crime invoke **jurisdiction** of several countries while committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.

Cybercrime: Characteristics..

- **Magnitude of crime unimaginable**
  - ✓ The cyber crime has the potential of causing **injury** and **loss of life** to an extent which cannot be imagined.
  - ✓ The offences like **cyber terrorism**, **cyber pornography** etc has wide reach and it can destroy the websites, steal data of the companies in no time.

Cybercrime: Classifications

- Cybercrimes can be classified into two major categories:
  - ✓ Cyber-dependent crimes
  - ✓ Cyber-enabled crimes
- **Cyber-dependent crimes:** any crime that **can only be committed** using computers, computer networks or other forms of information communication technology.
- **Cyber-enabled crimes**: traditional crimes facilitated by the Internet and digital technologies.

Cybercrime: Classifications

- The key distinction between these categories of cybercrime is the **role** of ICT in the offence
  - ✓ whether it is the **target** of the offence or
  - ✓ part of the **modus operandi** (or M.O.; i.e., method of operation) of the offender.
- Targeting ICT infrastructures affect **confidentiality**, **integrity** and/or **availability** of computer data or systems.
  - ✓ Private information should stay private
  - ✓ It should not be changed without permission from the owner, and data, services,
  - ✓ Systems should be accessible to the owner at all times.

Cybercrime: Classifications

- **Cyber-dependent** crimes include:
  - ✓ Hacking;
  - ✓ Malware creation, possession, and distribution;
  - ✓ Denial of service (DoS) attacks;
  - ✓ Distributed denial of service (DDoS) attacks;
  - ✓ Website defacement (i.e., a form of online vandalism targeting the content of websites).
- **Cyber-enabled** crimes include:
  - ✓ Fraud
  - ✓ Theft
  - ✓ Stalking

Computer-related Offences

- Computer-related offences include cyber-enabled crimes committed "for personal or financial gain or harm".
  - ✓ Computer system is inherent to the modus operandi.
- The offences can be broadly categorized as follows:
  - ✓ Computer-related **fraud or forgery**
  - ✓ Computer-related **identity** offences
  - ✓ Sending or controlling sending of **spam**
  - ✓ Computer-related **copyright** or **trademark** offences
  - ✓ Computer-related acts causing **personal harm**
  - ✓ Computer-related **solicitation** or "**grooming**" of children

Computer-related Fraud or Forgery

- Computer-related **forgery** involves **impersonation** of **legitimate** individuals, authorities, agencies, and other entities online for fraudulent purposes.
- Cybercriminals trick unsuspecting victims into revealing **personal information** and providing the offenders with **money**, **goods** and/or **services**.
  - ✓ A common trick is to spoof email addresses (domain names)-**phishing**.
  - ✓ Spoofed website looks like the organization's and prompts the user to enter login credentials.
  - ✓ The contents of the email provides different prompts to elicit **fear**, **panic** and/or **sense of urgency**.

Computer-related Fraud or Forgery

- Computer-related **fraud** involves false or misleading promises of:
  - ✓ Love and companionship (**catphishing**)
  - ✓ Property (through inheritance scams)
  - ✓ Money and wealth (through lottery scams, investment fraud, inheritance scams, etc.)
- **Social engineering** is employed to trick the victim to divulge personal information or send funds.
  - ✓ Manipulating, deceiving, influencing, or tricking individuals into divulging confidential information or performing acts that will benefit the perpetrator.

Computer-related Fraud or Forgery

- The ultimate goal of the fraud is to get personal information or funds.
  - ✓ The most well-known computer-related fraud involves a request for an **advance fee** to complete a transfer, deposit or other transaction in exchange for a larger sum of money.
  - ✓ While the story behind the fraud may change, the same tactic is used
    - ❑ a request for a **small amount** of money, in exchange for a large amount of money.

Computer-related Identity Offences and Spam

- Identity-related crime:
  - ✓ The perpetrator **unlawfully assumes** and/or misappropriates the identity of the victim and/or uses the identity and/or information associated with the identity for illicit purposes.
  - ✓ The identity is created from data collected for various purposes:
    - ❑ Identification numbers (NIDA-TZ, SSN-USA)
    - ❑ Identity documents (Passports, driver's licenses, birth certificates)
    - ❑ Online credentials (username and passwords)

Computer-related Identity Offences and Spam

- Identity-related crimes:
  - ✓ According to Tanzania's **Cybercrimes Act of 2015**:
    - ❑ A person shall not, by using a computer system impersonate another person.
    - ❑ An impersonator commits an offence and is liable on conviction, to a fine of **not less than five million shillings** or **three times the value of undue advantage received by that person**, whichever is greater, or to **imprisonment for a term of not less than seven years** or to **both**.

Computer-related Identity Offences and Spam

- Identity-related crime may or may not be financially motivated, examples:
  - ✓ Credit card fraud
  - ✓ Travel from one country to another using fake passport.
- Identity-related crimes are facilitated through the sending of unsolicited
  - ✓ Emails (spam),
  - ✓ Newsletters,
  - ✓ Messages with links to websites

Computer-related Identity Offences and Spam

- The unsolicited emails are designed to trick users into opening or clicking on links, which may contain malware or be designed to send them to pharmed websites.
- Tanzania's Cybercrimes Act 2015:
  - ✓ A person shall not initiate, relay or falsify unsolicited messages.
  - ✓ A person who commits an offence and is liable on conviction to a **fine of not less than three million shillings** or **three times the value of undue advantage received**, whichever is greater or to imprisonment for a term of **not less than one year or to both.**

Computer-related Copyright or Trademark Offences

- Various criminological, sociological, psychological, and economic theories have been proposed as possible explanations for cyber-enabled **intellectual property crime.**
- Social-cultural norms and group behaviour and dynamics influence rates of digital piracy.
- There are various sites on the internet that aid infringement of intellectual property rights:
  - ✓ Software piracy sites
  - ✓ Books/Journal Article piracy sites

Computer-related acts causing Personal Harm

- Involve the use of a computer system to **harass**, **bully**, **threaten**, **stalk** or to cause **fear** or **intimidation** of an individual.
  - ✓ Examples of these types of cybercrimes are **cyberstalking**, **cyberharassment**, and **cyberbullying**.
- **Cyberstalking**
  - ✓ The use of ICT to commit a series of acts over a period of time designed to **harass**, **annoy**, **attack**, **threaten**, **frighten**, and/or **verbally abuse** an individual (or individuals).

Computer-related acts causing Personal Harm

- **Cyberharassment**
  - ✓ The use of ICT to intentionally **humiliate**, **annoy**, **attack**, **threaten**, **alarm**, **offend** and/or **verbally abuse** an individual (or individuals).
- **Cyberbullying**
  - ✓ The use of ICT **by children** to **annoy**, **humiliate**, **insult**, **offend**, **harass**, **alarm**, **stalk**, **abuse** or otherwise **attack** another child or other children.
- These three kinds of cybercrimes differ in terms of
  - ✓ Age of perpetrators (only kids engage in cyberbullying)
  - ✓ Intensity and prevalence (cyberstalking vs cyberharassment).

Computer-related acts causing Personal Harm

- Tanzania's Cybercrimes Act 2015:
  - ✓ "A person shall not initiate or send any electronic communication using a computer system to another person with intent to **coerce**, **intimidate**, **harass** or **cause emotional distress**".
  - ✓ A person who contravenes this commits an offence and is liable on conviction to a fine of **not less than five million shillings** or to imprisonment for a term of **not less than three years or to both**.

Solicitation or "grooming" of Children

- **95%** of U.S. teens aged **13–17** years report owning a smartphone or having access to one, and 45% state that they are online on a **near-constant** basis.
- Children and adolescents are at risk for a variety of negative and potentially dangerous exposures.
  - ✓ Example: online **sexual solicitations** and **interactions** with older adolescents, peers, and adults.
- **Child grooming** is the process of fostering **rapport** and **trust** through the development of an emotional relationship with the victim.

Solicitation or "grooming" of Children

- The offender may manipulate the victim using a variety of power and control tactics, including (but not limited to):
  - ✓ **Adulation**, **gifts**, **isolation**, **intimidation**, **threats**, and/or force as well as **feigning shared interests**, or building trust by mimicking a child's apparent sense of isolation.
- Child grooming can occur on **social media platforms**, over **email**, in **chat rooms**, through **instant messaging** services, and via apps, among other areas.
  - ✓ Predators may make sexual comments or ask kids to remove their clothes.

Content-related Offences

- This kind of cybercrime involve **illegal content.**
  - ✓ Example of illegal content is **child sexual abuse material** (aka child pornography).
  - ✓ **visual depictions** of 'a **minor** engaged in sexually explicit conduct … [,] a person appearing to be a minor engaged in sexually explicit conduct … [, and/or] **realistic images** representing a minor engaged in sexually explicit conduct.
- Some countries consider only realistic images while others additionally consider non-realistic images of child pornography, such as cartoons and drawings.

Content-related Offences

- **Child pornography:**
  - ✓ "intentionally and without right … **produc[es]** child pornography for the purpose of its **distribution** through a computer system [,] … **offer[s]** or **mak[es] available** child pornography through a computer system [,] … distribut[es] or **transmit[s]** child pornography through a computer system [,] … **procur[es]** child pornography through a computer system for oneself or for another person [, and/or] … **possesses** child pornography in a computer system or on a computer-data storage medium.

Content-related Offences

- **Child pornography:**
  - ✓ Tanzania's Cybercrimes Act 2015:
    - A person shall not- (a) **publish** child pornography, through a computer system; or (b) **make available** or **facilitate** the access of child pornography through a computer system.
    - A person who contravenes these commits an offence and is liable on conviction, to a fine of **not less than fifty million shillings** or **three times the value of undue advantage received**, whichever is greater, or to imprisonment for a term of **not less than seven years or to both.**

Content-related Offences

- **Racist or xenophobic material**
  - ✓ any **written material**, any **image** or any other **representation** of **ideas** or **theories**, which **advocates**, **promotes** or **incites** hatred, discrimination or violence, against any individual or group of individuals, based on **race**, **colour**, **descent** or **national** or **ethnic origin**, as well as **religion** if used as a pretext for any of these factors.
  - ✓ Tanzania's Cybercrime Act 2015:
    - ❑ A person shall not insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion.

Content-related Offences

- **Racist or xenophobic material**
  - ✓ Tanzania's Cybercrimes Act 2015:
    - A person shall not insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion.
    - A person who contravenes this commits an offence and is liable on conviction to a fine of **not less than three million shillings** or to imprisonment for a term of **not less than one year or to both**.

Content-related Offences

- **Publication of False or Misleading Material**
  - ✓ The publication of **false information** is also considered a crime in various countries.
  - ✓ According to Tanzania's 2015 Cybercrimes Act, it is an offense to publish information or data presented in a **picture**, **text**, **symbol** or any other form in a computer system **knowing** that such information or data is **false**, **deceptive**, **misleading** or **inaccurate**, and with **intent** to defame, **threaten**, **abuse**, **insult**, or otherwise **deceive** or **mislead** the public or counselling commission of an offence.
    - ❑ On conviction be liable to a fine of **not less than five million shillings** or to imprisonment for a term of **not less than three years** or to **both**.

Cybercrime: Challenges

- **Technical challenges**:
  - ✓ Spoofing of IP/Hardware addresses
  - ✓ Software vulnerabilities
  - ✓ Cloud computing
    - ❑ Shifts part of the security responsibilities to the provider
    - ❑ Investigation of incidences requires cooperation between victim and provider, with potential technical and legal challenges emerging.
- **Legal challenges**
  - ✓ Cybercrime is a **transnational** crime and perpetrators and victims can be located anywhere in the world with an Internet connection.

Cybercrime: Challenges

- **Legal challenges**
  - ✓ Cybercrime is a **transnational** crime and perpetrators and victims can be located anywhere in the world with an Internet connection.
  - ✓ Investigators often require access to and the sharing of **data** across borders.
  - ✓ Investigation and prosecution is difficult because of:
    - The **different legal systems** between countries
    - Variations in national **cybercrime laws**
    - Differences in the **rules of evidence and criminal procedure** (e.g. search warrant)

Cybercrime: Challenges

- **Legal challenges**
  - ✓ Investigation and prosecution is difficult because of:
    - The **different legal systems** between countries
    - Variations in national **cybercrime laws**
    - Differences in the **rules of evidence and criminal procedure** (e.g. search warrant)
    - Variations in the **scope** and **geographic** applicability of regional and multilateral cybercrime **treaties**;
    - Differences in approaches to **data protection** and **respect for human rights**.

Cybercrime: Challenges

- **Ethical challenges**
  - ✓ Cybercrime should be **legally** and **ethically** investigated
  - ✓ Ethical conduct in using ICT involves refraining from harming others, systems, and data, and respecting the rule of law and human rights.
    - ❑ Collection, sharing and selling of data from social networks.
- **Operational challenges**
  - ✓ Requests for international support **can take a long time**, and may not produce usable results, such as preventing the crime or **producing evidence** for use in court.
  - ✓ Deficit in **national capacity** (especially from a developing country perspective) to deal with cybercrime.

Cybercrime: Prevention

- Cybercriminals often use both **technical** and **social** approaches to commit crime.
- Some types of cybercrime are difficult to prevent, however, technology users can take certain actions to protect themselves (to an extent) from cybercrime.
- Some tips:
  - ✓ Keep your operating system and installed software up-to-date
  - ✓ Regularly uninstall software that you no longer use
  - ✓ Use an anti-virus programme from a reputable company
  - ✓ Do not download software, movies or music from sharing sites - these very often have malware

Cybercrime: Prevention

- Cybercriminals often use both **technical** and **social** approaches to commit crime.
- Some types of cybercrime are difficult to prevent, however, technology users can take certain actions to protect themselves (to an extent) from cybercrime.
- Some tips:
  - ✓ Do not download attachments or click on links from senders you do not recognize
  - ✓ Do not enter personal information in unknown websites
  - ✓ Confirm the correct website when entering financial information

Cybercrime Prevalence in Tanzania and Beyond

- Financial sector (Banks and Mobile Financial Services)
  - ✓ Mobile Financial Services: attacks are mainly based on Social Engineering
  - ✓ Banks: Identity theft, Social Engineering, etc
- Watch live cyber attacks:
  - ✓ https://threatmap.checkpoint.com/
  - ✓ https://cybermap.kaspersky.com/
  - ✓ https://www.imperva.com/cyber-threat-attack-map/?
  - ✓ https://www.digitalattackmap.com/