Module 1 Notes: Introduction to Cybercrime

**Learning Objectives:**

1. Define what Cybercrime is.
2. Describe how Cybercrime developed as the advancement of the internet and technology occurred.
3. Describe what the public’s perception of internet crime is.
4. Explain two (2) separate problems related to the advancement of technology.
5. Describe how these problems developed with the advancement of technology.
6. Contrast how these problems occur "offline" versus "online" and the implications for law enforcement in combating these incidents.

**Key Words:**

1. **Continuum of Cybercrime:** "Cybercrime really presents a continuum ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people-related" (Gordon & Ford, 2006, pg. 3).
2. **Crimeware:** "The software used in cybercrime is sometimes referred to as 'crimeware'" (Gordon & Ford, 2006, pg. 4).
3. **Cybercrime:** "Cybercrime can be broadly defined as the destruction, theft, or unauthorized or illegal use, modification, or copying of information, programs, services, equipment, or communication networks" (Marcum, 2014, pg. 3).
4. **Transnational Cybercrime:** Cybercrimes that occur across geographically boundaries (Marcum, 2014).

**Ch. 1 Notes (Marcum):**

* The internet was birthed in 1962 by **J.C.R Licklider** of Massachusetts Institute of Technology.
* In 1964, MIT colleague, **Leonard Kleinrock** persuaded Roberts that using packets in networking would be a more efficient connection. Packets allowed multiple computers to exchange information asynchronously as peers. This was better than the traditional circuits.
* Tested this connection with a TX-2 computer in MA with a Q-32 computer in CA with low speed dial-up telephone line. The idea of these packets and connections was called **ARPANET**.
* ARPANET eventually turned into a more efficient version of protocol called **TCP/IP**. By the 1980s, vendors were using TCP/IP, and by the 1990s, internet was widespread in businesses and homes.
* The **Internet** is an intercontinental information highway that enables people of all ages to communicate with family and friends at lightning-fast speed.
* **Cybercrime** can be broadly defined as “the destruction, theft, or unauthorized or illegal use, modification, or copying of information, programs, services, equipment, or communication networks.” -> Criminality utilizing technology.
* **Types of Criminality** include: digital piracy, identity theft, financial theft, computer hacking, embezzlement, and espionage. It can also be sexual in nature, such as child pornography.
* **First Generation** of cybercrime is characterized by the illegal exploitation of mainframe computers and their operating system -> Manuals for making bombs, meth, etc. These are considered “low-end”.
* **Second Generation** of cybercrime is characterized by those utilizing networks. Hacking and cracking are common in this generation. This was in the form of breaking into private networks and collecting secured information. These crimes are classified as “hybrid” as they fall between traditional and true cybercrimes.
* **Third Generation** of cybercrime is characterized by the nature of distribution. These crimes could not exist if not for the internet. Spam, viruses, digital piracy, and malware are all forms of this. This is considered “true cybercrime”.
* The **Public’s View of Cybercrime** is pretty standard when it comes to issues such as child pornography, quick and decisive; however, while the public pushes for action, legislation is sometimes overturned due to constitutional infringement issues. For example, digitally created images of child pornography is legal because no real children were harmed in the creation.
* **Fear of Crime** is a cumulative measure of several things: personal judgements about the crime; estimations of an individual’s vulnerability to crime; media reports of statistics of crime; and hearsay. This ‘fear’ is more subjective and personal rather than hard facts.
* Newer technologies tend to be more easily embraced by younger people than older generations. **The Net** and **Hackers** were movies that heightened fears of the dangers of using the World Wide Web.
* Fear of crime and **Victimization** may lead people to not drive in certain areas or visit night clubs. Similarly, many people may not want to buy things online for fear of identity theft.
* Cybercrime is a **Transnational** issue. Often, one country will depend on another country to assist them in the investigation of cybercrimes. These crimes create two challenges for law enforcement: collection of evidence and obtaining custody of a suspect.
* A **Letter Rogatory** is a request from a court in one country to a court in another country to perform a judicial act.
* Letter Rogatory is a time-consuming act, so often requests under the **Mutual Assistance Treaty (MLAT)** are faster and used whenever possible. -> in 2009, the US had 53 MLATs with other countries
* Law enforcement can make a request for evidence under an **Executive Agreement**, which is a pact made with another country to provide evidence in criminal investigations.
* Law Enforcement usually use **Informal** **Methods** of gathering information as they are quicker and more useful. In the mid-1990s, the United States and United Kingdom worked together in the Rome Labs hacking case. All of this occurred in the United Kingdom, and the United States still issued help.
* **Arresting** suspects in transnational cybercrimes can occur in two ways: extradition or extralegal unilateral action.
* **Extradition** is the formal transfer of suspects from one country to another and requires a treaty between the two.
* **Extralegal Unilateral Action** is a trick to convince suspects to come to they country they have crimes against, and arrest them on arrival.

**Ford & Gordon Research Paper Notes:**

* This paper defines **Cybercrime** and **Crimeware**. There are two types of Cybercrime (I & II), the first is mostly technological the second is more human in nature.
* **Crimeware** is an inclusive term for many different Trojans, Viruses, Bots, Spyware and Worms, which are instrumental in facilitating certain Cybercrimes.
* **Cybercrime’s** definition differs depending on perception of both observer/protector and victim. The Council of Europe’s Cybercrime Treaty refers to offenses ranging from **criminal activity against data to content and copyright infringement**. Zeviar-Geese says Cybercrime includes **fraud, unauthorized access, child pornography, and cyberstalking**. The United Nations Manual on the Prevention and Control of Computer Related Crime includes **fraud, forgery, and unauthorized access.** In the end, we define Cybercrime as, **“any crime that is facilitated or committed using a computer, network, or hardware device.”**
* **Type I** – It is generally a singular, or discrete, event from the perspective of a victim. It often is facilitated by the introduction of crimeware programs such as key loggers, viruses, rootkits or Trojan horses into the user’s computer system. The introductions can, but may not necessarily be, facilitated by vulnerabilities.
  + The user goes online to perform a task.
  + The user takes action which then allows the criminal to access information.
  + This information is then used by the attacker.
  + The user becomes aware of the crime (This is the single event from the perspective of the user). This usually occurs much later in the lifecycle of Cybercrime.
  + The crime is investigated and resolved.
* These types of crimes are as follows: phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud based upon stolen credentials.
* **Type II** – activities such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online. It is generally facilitated by programs that do not fit under the classification crimeware. For example, Instant messaging software. There are generally repeated contacts or events from the perspective of the user.
  + User(a) foes online to see what she can find out about llama farming.
  + User(a) decides to participate in an online forum about llama farming.
  + User(b) sees User(a), watches her participation in the forum for several days, and responds to some of her comments.
  + User(b) sends a request for a private chat using a common IM client.
  + User(a), being familiar with User(b) via the online forum, responds positively and they begin to chat daily as well as participate in the forum. This period is known as instilling trust.
  + After several interactions, User(a) reveals that she is single, likes llamas, has a quarter of a million dollars for a llama farm, and that she likes to go to concerts. She tells him her real name is Jenny.
  + User(b) asks jenny to meet in person and go to a concert.
  + Jenny becomes suspicious when User(b) will not give his contact information other than online information, she refuses.
  + User(b) becomes irrational and begins to post false claims against Jenny in the online forum calling her a fraud, and of being there to pick up men, not to find others interested in llamas. He posts her home number. He goes onto other online forums posting as Jenny asking for dates and leaving her contact information.
  + Jenny tries to defend herself in the forum, and asks User(B) privately to stop, using IM. She begins to get numerous emails about the dates she requested and realizes then that someone is impersonating her online. She confronts User(b) with her suspicions.
  + User(b) becomes more irrational and begins to make hang-up and harassing phone calls to Jenny. Jenny becomes afraid for her safety.
  + The telephone company and the local police become involved.
  + Jenny files charges against User(b), who is, it is later learned, a former child-pornographer with links to organized crime, under investigation for the disappearance of three women he allegedly met on the internet.
* These two examples show that Cybercrime is a continuum of ranging from purely technological to purely people.
* The software used in Cybercrime is sometimes referred to as **Crimeware**. It is defined as:
  + Used (directly or indirectly) in the commission of the criminal act;
  + Not generally regarded as desirable software application from the perspective of the computer user;
  + Not involuntarily enabling the crime.