Module 2 Notes: Theoretical Perspectives in the Study of Cybercrime

**Learning Objectives:**

1. Describe each of the various theoretical perspectives used in cybercrime research.
2. Contrast the strengths and weaknesses of each perspective noted in class readings.
3. Apply a theoretical perspective to a fictional depiction of cybercrime.
4. Explain how the actions depicted in the film align with the selected theoretical perspective.
5. Compare your selected perspective with your classmates to aid in your understanding.
6. Examine the available research on a type of cybercrime.
7. Apply a theoretical perspective to actual forms of cybercrime.
8. Explain why the selected form of cybercrime continues to be a social problem using the noted theoretical perspective.

**Key Words and Concepts:**

1. **Deterrence Theory**: Asserts that individuals will not engage in crime if the consequences outweigh the benefits. The consequences must be swift, certain, and severe.
2. **Low Self-Control Theory**: Asserts that individuals engage in crime as a result of low-self control largely stemming from ineffective parental management during childhood/adolescence.
3. **Rational Choice Theory**: Asserts that individuals are rational creatures oriented toward specific goals. Individuals will make calculations (benefits versus costs) regarding specific actions and then decide the best way to maximize their time.
4. **Routine Activities Theory**: Asserts that crime comes down to three basic components: (1) a motivated or potential offender, (2) a suitable or vulnerable target, and (3) the lack of a capable guardian. When those three factors converge in time/space, a crime is likely to occur. For example, a motivated offender observes you post to your social networking site that you are going on vacation. Your place of residence now becomes a suitable and vulnerable target because no one is there watching it. The lack of capable guardian is therefore a given unless you have some form of guardianship at your residence (e.g., alarm, dog, other roommates, etc.). A guardian is anyone or thing that can minimize the chance of the crime occurring.
5. **Social Control Theory**: Asserts that individuals do not engage in crime due to their level of (1) attachment to others/community (e.g., family, friends), (2) commitment to a pro-social society, (3) involvement in conventional activities (e.g., church, extracurricular activities), and (4) belief in society. In other words, instead of explaining why people engage in crime, Social Control Theory explains why people do NOT engage in criminal activity. For example, think about the ramifications to your personal life if you were arrested for a serious crime. What would others think of you in your family and friendship circles? What kind of connections to the community could you stand to lose?
6. **Social Learning Theory**: Asserts that individuals engage in crime by first learning the behavior and then modeling that behavior. The key components of this perspective are: differential association (e.g., association with deviant peers or association with other cybercriminals), definitions (e.g., deviant beliefs or believing that certain types of cybercrime should not be criminalized), reinforcement (e.g., desirable events = such as earning money from identity theft) outweighs punishment (e.g., undesirable events = such as going to prison), and imitation (e.g., replicating the behavior).
7. **Strain Theory**: Asserts that individuals will act out when they become stressed and frustrated with the inability to achieve certain goals. Individuals could act out by (1) engaging in crime, (2) escaping from the source of strain, or (3) escaping from society in general. The three sources of strain later identified are: (1) the failure to achieve a positively valued goal (e.g., money, status, respect), (2) the loss of positively valued stimuli (e.g., a relationship that falls apart), and (3) presentation of negative stimuli (e.g., child abuse).

**Social Learning Theory Analysis Notes:**

* Demonstrates that measures of differential association, differential reinforcement and punishment, definitions, and sources of imitation are significantly related to **Computer** **Crime**.
* Estimates of damage done/money stolen are **$145 million - $5 billion** annually in the United States.
* During a 15-week semester, 10 percent of **Hollinger’s college-based sample** reported being involved in software piracy, and 3.3 percent had gained unauthorized access to another computer account.
* One of the **first statistical studies on unknown perpetrators** of computer crime was by Hollinger at the University of Florida. (See above Note)
* **His study indicated that Students who were**: Male, 22 years of age or older, seniors and graduate students, Asian or Hispanic, cohabitating with someone of the opposite sex, and enrolled in majors dealing with forestry, engineering, liberal arts, and science.
* **Two Variables** that were strongly correlated with computer crime were friends’ involvement and perceived certainty of being caught.
* **Social Learning Theory** has been empirically verified across numerous studies. It claims to be a general theory that applies to all types of deviant behavior. Therefore, is applicable to Computer Crime.
* It is organized around **Four Major Concepts:** Differential association, differential reinforcement/punishment, definitions, and imitation.
* **Differential Association** refers to the process by which individuals, operating in different social contexts, become exposed to, and ultimately learn, normative definitions favorable and unfavorable to criminal and legal behaviors.
* **Definitions** are attitudes about certain behavior learned through the process of differential association, imitation, and general interaction or expose to various sources of learning located in one’s social environment.
* **Differential Reinforcement/Punishment** is a concept that captures the diversity of anticipated and actual consequences of engaging in certain behavior.
* **Imitation** refers to the modeling of certain behavior through the observation of others.
* We can infer that the more college students associate with peers who are engaging in illegal computer activity, **the greater the frequency of the behavior.**
* **Students** begin to rationalize Computer Crime such as piracy and unauthorized access because “Everyone is doing it.”
* **Hypothesis** – The greater the perceived deterrent effect of being caught and severely punished, the less likely college students will engage in illegal computer activities.
* **In this study,** 13 departments chosen within the college of arts and sciences were limited to the social sciences and natural sciences. All five within the college of business and economics and all eight in the college of engineering were incorporated. 🡪 Random Classes were chosen after.