

**CYB250 - Cybercrime, Cyberlaw and Cyber-ethics**

**Tutorial 1 (Week 1): Criminology Foundations and Cybercrime Contexts**

**Learning Objectives for this session**

By the end of the session, students understand:

1. Define criminology and explain its relevance to cybersecurity.

Ans: Criminology scientifically studies crime, criminals, and the social impact of wrongdoing. In today's cyber world, learning criminology helps us understand why people commit cyber-offenses, how offenders choose targets (say networks or systems that are poorly secure), and what actually motivates them (money, activism, or just pure disruption). By applying criminology to cybersecurity, we can enhance security mechanisms-that is, anticipate how attackers behave rather than merely responding to attacks after-the-fact.

1. Differentiate between classical, positivist, and critical schools of criminology and apply them to digital contexts.

Ans:

**Classical school:** Offenders are regarded as rational actors who consider the risks and rewards before undertaking an act. An example of a classical hacker could be one who calculates that a server with weak protection measures is an easy target that carries a high payoff.

**Positivist school:** Seeks a scientific explanation (biological, psychological) for criminal behavior. The positivist could undertake research on whether certain personality traits (impulsivity, sensation-seeking) correlate with participation in Internet hacking fora.

**Critical school:** Concerned with power structures and social inequalities. From this view, cybercrime could be seen as a form of protest or resistance-the group is targeting government websites to somehow articulate perceived injustices.

1. Analyze biological, psychological, and sociological theories of crime in relation to cyberoffenses.

Ans:

* Biological theories might look for genetic or neurochemical factors that predispose someone to risk-taking or rule-breaking online.
* Psychological theories examine personality (e.g., high narcissism leading to “bragging” hacks) or cognitive distortions (justifying theft of digital goods).
* Sociological theories explore how social environments—peer groups in darknet forums, workplace strain, or cultural attitudes toward piracy—influence individuals to commit cybercrimes.

1. Discuss the evolution and impact of cybercrime as a modern criminological issue.

Ans:

Now cybercrime has matured in sophistication. It has gone from lone script kiddies vandalizing websites in the '90s to big ransomware rings and state-sponsored espionage now-a-days. This climbortsocide-type range extends from piddling identity theft, small businessman loss, and breaches of national security. This rapid evolution presents law enforcement and businesses with the cat-and-mouse challenge of staying two steps ahead-thought on deep-fake scams and cloud-based attacks.

1. Identify how criminological theory informs cybercrime prevention and policy development.

Ans: Just as criminological frameworks leave room for prevention:

* Situational theory (ancient school of thought) would harden targets—better passwords, multi-factor authentication.
* Social learning (surpassing positivist origin) requires training users about online ethics and peer pressure.
* Critical approaches go for policy changes that promote equality in some way-cyber-education for underprivileged communities so that fewer young people take to hacking as a measure of social mobility.

1. Evaluate the criminal justice system’s response to cyber threats and digital law enforcement challenges.

Ans:

Digital law enforcement faces hurdles like cross-border jurisdiction, rapidly changing technology, and limited cyber-forensics expertise. While many countries have set up specialized cyber units and passed new legislation (e.g., data-breach notification laws), challenges remain in international cooperation, evidence preservation (volatile memory, encrypted data), and training judges and prosecutors to handle technical testimony.

# Class Discussion Questions

1. How do classical and positivist criminological theories apply to cybercriminal behavior?

Ans:

Applying Classical and Positivist Theories to Cybercriminal Behavior

**Classical Theory**

* In rational-choice schema, cybercriminals consider perceived advantages (data theft, monetary gain, or reputation), against the threats (being caught or punished). For instance, a hacker looking for unsecured IoT devices may perceive that low security means a high payoff with little chance of being caught.
* In deterrence doctrine, increasing certainty, severity, and celerity of punishment shall theoretically repel potential offenders from committing an act that they believe outweighs its disadvantage. For example, are we willing to implement mandatory sentencing guidelines for data breaches?

**Positivist Theory**

* **Individual Traits:** Positivists look for biological or psychological factors that predispose someone to cybercrime. High impulsivity or sensation-seeking, for instance, may drive an individual toward thrill-based intrusions of computer systems.
* **Environmental Influences:** Through scientific study, positivists examine how early exposure to hacking communities or online forums might “socialize” individuals into normalizing illicit activity. This blends into psychological learning theories, where repeated rewards strengthen the cyber-offending behavior.

1. In what ways has the rise of cybercrime challenged traditional criminological theories and criminal justice systems?

Ans: The Challenges Posed by Cybercrime to Traditional Theories and Justice Systems

**Blurred Lines:** Many scholars argue that traditional theories of crime developed for a street-level crime conceptualization do not consider the presence of anonymity over the Internet and its global outreach. The ease of crossing jurisdictional boundaries thus reduces the applicability of any local deterrence or rehabilitation model.

**Evolving Offense Types:** Most forms of harm-ransomware, deep-fake scams, cryptocurrency laundering-do not easily fit into traditional categories of law.

**Evidence and Investigation:** The evidence related to cybercrime is digital and often ephemeral or encrypted; this creates challenges for police procedures traditionally based on physical evidence, witnesses, and well-defined crime scenes.

1. Can sociological factors, like social disorganization or differential association, explain hacking communities or online criminal networks?

Ans:

**Social Disorganization:** In areas (online or offline) where formal controls and community bonds are weak in such case alternative norms can take hold. Dark web forums or IRC channels often provide structure and status systems that fill this void.

**Differential Association:** According to Sutherland’s theory, individuals learn criminal techniques and justifications from peers. A novice hacker may pick up coding exploits and neutralization arguments (“we’re just testing security”) by spending time in experienced hacking groups.

**Collective Identity:** Shared grievances—such as opposition to corporate surveillance—can forge strong subcultural ties, reinforce group loyalty and further embedding members in illicit networks.

1. How might labeling theory contribute to the stigmatization of individuals accused of cyber offenses?

Ans: Labeling Theory and Stigmatization of Cyber Offenders

* **Master Status:** If their name is ever publicly linked with a cyber offense, an individual will forever be relegated to the expense that professional labels like "hacker" will become more important to their identity than any other. This is pertinent for legitimate reintegration or employment.
* **Self-Fulfilling Prophecy:** Basically, treating someone like a criminal pushes them further into that in terms of deviant action, particularly when they have been alienated from conventional social circles and find acceptance among similarly stigmatized people.
* **Policy Implications:** Too broad or overly publicized labeling, for example, naming suspects before they are convicted, can prematurely single out and marginalize an individual beyond what is necessary. This may turn out to be the justice process's undoing.

# In Class Activity

**The Rise and Fall of Silk Road**

**Background:**

Silk Road was an infamous dark web marketplace that operated from 2011 until its shutdown in 2013 by the FBI. Founded by Ross Ulbricht, it facilitated anonymous transactions for illegal goods using Tor and Bitcoin, showcasing a real-world intersection of technology, crime, and regulation.

**Instructions:**

Students will work in small groups to analyze the Silk Road case using criminological frameworks. Each group will:

* Identify which criminological theory or theories best explain the behavior of Ulbricht and users of Silk Road.
* Discuss the effectiveness and ethical implications of law enforcement tactics used to dismantle Silk Road.
* Reflect on the policy and legal implications this case has had on cybersecurity governance and internet freedom.

**Discussion Points:**

* Motivation behind cybercriminal enterprises and user participation.
* Role of anonymity and encryption in enabling digital crime.
* Government surveillance and privacy trade-offs in cybercrime enforcement.

**Ans:**

Ross Ulbricht he went ahead to set up Silk Road, confident that the proceeds and level of anonymity around it, using Tor and Bitcoin, were sufficient to reward that risk. Similarly, buyers and sellers seemed to have made the same supernatural calculation: high reward, low chance of being caught.

**Differential Association:** New users learned how to use Silk Road by mingling with more experienced people on forums. They picked up the technical know-how (Tor, Bitcoin wallets) and the excuses ("it's about privacy," "it's consensual") that enabled them to feel fine about breaking the law.

**Strain Theory:** Some people felt that traditional markets and laws were prejudiced or too strict. In other words, the Silk Road was giving them a way to make money beyond those confines, so this would lessen the "strain" they felt.

**Critical Theory:** According to Ulbricht and a few users, the Silk Road was a way to resist the control of government. In their opinion, it was an ideological stand for personal freedom.

**2. How Law Enforcement Closed down Silk Road & Ethical Questions**

* Undercover Purchases: Federal agents bought proscribed goods to set up a case.
* This worked because they got direct proof.
* Ethical worry: Could be classified as entrapment if officers egged on crimes

**Traffic and Metadata Analysis: Following the Bitcoin payments and other Internet data, the FBI was able to locate the servers' positions.**

* This worked because they found a match between transaction records and IP logs.
* Ethical concern: This involved an inordinate level of surveillance over all data of Tor users.

**Server Seizure in Iceland: Reportedly, the FBI seized the principal servers of Silk Road.**

* This worked because it took the site immediately offline.
* Ethical worry: Raised jurisdictional questions and whether proper consent from Iceland was obtained.

**Public Arrest of Ulbricht: He was arrested in a library to prevent him from further destroying evidence.**

* The action worked as it prevented additional data loss.
* Ethical concern: There was a need to remain focused on the extent of such deep undercover surveillance.

**3. Policy and Legal Changes After Silk Road**

* Harder regulations on Crypto: Governments went on to hard-sell KYC and AML rules to avoid anonymous trading in Bitcoin.
* Monitoring in the Dark Web: While increasing the risk of losing privacy also for non-criminals using Tor, authorities are finding ways of tracking Tor traffic more effectively.
* Privacy vs. Security Debate: Discourses regarding how far enforcement should go into the online space and ways to balance individual rights with public safety abounded in the backdrop of Silk Road.

**4. Discussion in the Classroom**

* What made participants go to the Silk Road? For money, and especially to gain freedom from government rules.

**What did anonymity help with?**

* Tor hidden IP addresses; Bitcoin, real identities.

**What's the Con?**

* Greater efficiency in detecting crime would come from higher surveillance on the non-culprit people. There need to be clear legal limits.

**Conclusion:**

The Silk Road shows that technology can very well enable new forms of crime, thereby compelling both those enforcing the law and making it and the society at large to reflect on strategies for their prevention as well as protecting privacy possible.