Criminology Online

Matthew Edwards

Focus: Cybercriminology

November 3, 2020

Three questions of criminology

1. Why are certain things crimes?
2. Why do people commit crime?[1]
3. How can we prevent crime?

[1] Or: ‘why does crime happen?’, which is not always exactly the same question.

Cyberlaw

Question (1) is one of legal philosophy. Answers vary, but tend to tackle concepts of **harm** and **intent**, with perhaps other considerations of *norms* of behaviour and goals such as public welfare and societal cohesion.

Specific to cybercrime:

- Troubles with *jurisdiction*.
- Sometimes **harm** is difficult to locate.
- The **intent** can be difficult to prove.
- Lawmakers don't always understand technology.

Why do (some) people commit (cyber)crime?

. . . and what can we do about it?

Four criminological theories applied to cybercrime[2]:

1. Neutralisation theory
2. Routine activity theory
3. Self-control theory
4. Social learning theory

But first. . .

[2] Attempts to explain evidence

Issue 1: Cybercriminals are different

Traditional criminals	Cybercriminals
Poorly educated	Well-educated
Poor job prospects	Often employed
Financial difficulty	No financial difficulty
Substance abuse	Not especially
Male	Male

(Remember these are common profiles, not universal truths)

Issue 2: How can I possibly know that?

In traditional criminology, you study the outputs of the criminal justice system.

- crime reports
- investigations
- arrests
- convictions

This is *all* substantially more difficult for cybercrime. Confirmed evidence is hard to get, and all observation mechanisms have biases.

Back to theory...

Neutralisation theory

Core concept: people alter their perception of the justification for (their) cybercrime, to make themselves happier with their own actions.

Reasoning

The ideal

a) Hacking is unethical.

b) I just hacked someone.

∴ I did something unethical.

In reality

a) I'm not a bad person.

b) I just hacked someone.

∴ Hacking is sometimes okay.

Techniques of neutralisation

Denial of responsibility (“I had no choice”)

Denial of injury (“It doesn’t hurt anyone”)

Denial of victim (“They deserve it because they’re. . . ”)

Condemnation of condemners (“You’re just as bad!”)

Appeal to higher loyalty For a cause/principle.

Routine activity theory

Core concept: Three things must align for crime to occur:

1. The presence of a **suitable target**
2. The presence of a **motivated offender**
3. The absence of a **capable guardian**

RAT implications

Anything that leads to more interactions without guardians will tend to increase crime. All else held constant, more interactions between people will probably cause more crime.

To intervene:

- Create guardians
- Remove (or demotivate) offenders
- Decrease visibility and access to targets

Self-control theory

Self-control is a psychological trait linked to an individual's ability to resist temptation or impulses.

Self-control (even in childhood) predicts life outcomes like:

- wealth
- health
- parenting ability
- crime

(Cyber)crime as short-term reward

General thesis: people with high levels of self-control are less likely to commit crime.

Interventions? Self-control *does* have a genetic component, but early environmental changes (mostly family, education) can have a big impact on self-control.

Otherwise, focus is on reducing short-term attractiveness of self-control.

Social learning theory

Core concept: most of our behaviour is learnt from those around us.

Two major influences on learning (cybercrime):

1. Role models (even fictional ones)
2. Perception of normality.

A cybercrime prevention campaign based on social cognitive theory should aim to communicate not just that cybercrime is *bad*, but that it is *abnormal*.

Talk to me about crime!