COMS30038 — SECURITY BEHAVIOURS

CYBERCRIMINOLOGY: UNDERSTANDING CYBERCRIMINALS

*Matthew Edwards**

---

1 CYBERCRIMES: A SURVEY

So far we have looked at some of the methods used by malicious actors, and models for understanding their attacks. What we have yet to focus on is the study of the cybercriminals themselves, the different individual backgrounds they have, and the different forms of cybercrime. As engineers, we will often be primarily interested in building things—like defences that stop crime from happening—but an important precursor to doing this effectively is to *understand* and *measure* the criminal activity. There is a purely academic motive for this, for studying and documenting the rich and varied nature of criminality as a subject in its own right, but beyond that there is also the hope that by understanding the causes and the methods of crime, we can more effectively prevent it from taking place.

As with any subject, there are a number of typologies and categorisations that can be applied to cybercrime. One binary categorisation that you may hear of is the distinction between *cyber-enabled* and *cyber-dependent* crime. Broadly speaking, the former is meant to capture traditional forms of crime which have moved online, while the latter refers to entirely new types of crime that would not be possible without computers and communication networks. As we shall see, it is not always possible to definitively place an activity within one or the other category.

Another system for organising cybercrimes is by motive, with the major division here lying between those crimes that are financially motivated and those that are not. This understanding can be critical for the construction of your countermeasures—a criminal actor motivated by money can be stopped entirely by increasing their costs to the point where it is more profitable for them to go elsewhere, but a criminal motivated by personal animosity or political goals may be at best discouraged and at worst indifferent to such interventions. The division between interpersonal and politically-motivated crime is finer, but still important when it comes to understanding targeting.

*matthew.john.edwards@bristol.ac.uk

Interpersonal crime is aimed at a specific person, often due to a pre-existing animosity, while ideologically-motivated cybercrimes more often have the goal of spreading awareness or impacting rival ideologies, and so might be countered effectively with measures that limit visibility.

Categories are best explored with examples, so let us consider a few different cybercrimes:

Advance-fee fraud is a classic scam in which the victim is promised a (usually financial) reward, but at some point during the process is asked to pay a small fee to the fraudster in order to smooth the transaction – usually this is presented as a legal fee, or a nominal amount to set up a special bank account in order to receive funds. The most well-known examples are the Nigerian prince emails promising the recipient a share of a large sum of money just for helping transfer it out of a country, but the fraud can appear in a variety of other forms as e.g., attractive online rental listings [1]. These scam letters are old in nature[1], but were heavily enabled by moving online to bulk email systems, making them a good example of cyber-enabled crime. Unlike phishing victims, advance-fee fraud victims can be active participants in the crime, working with the offender to find a way to send them money.

Child sexual abuse can be facilitated by the Internet in a number of ways, and is again a core example of cyber-enabled crime. The two major elements of this are online grooming and the sharing of child pornography. The former takes place in a number of online venues like chatrooms, games and social media sites, with offenders approaching young adolescents, often disguising themselves as children, and coaxing them into sexual acts either in person or online [2]. Child pornographers record in-person child abuse and disseminate it online via peer-to-peer platforms or anonymous forums, posing a number of technical challenges for law enforcement attempting to take down child pornography and identify its creators [3]. This category of crime falls outside of other motive-based categories, being neither financially nor ideologically beneficial to the offender, and not usually personal in the ordinary sense of the word, but instead rooted in pathology.

Click fraud takes advantage of the advertisement model through which the Web is monetised. Typically, a website hosts advertisements on their pages, and receives a small payment whenever visitors view or click on them. Click fraud occurs when the website owners generate fraudulent clicks for adverts hosted on their websites, by deploying bots or 'click farming' low-paid workers. The crime is clearly financially motivated, and can involve a great deal of technical sophistication – primarily because of advertising exchanges deploying ever more sophisticated countermeasures [4].

[1] Recall Vidoqc's letter.

Cyberbullying is an interpersonal offence, often (but not always) directed at child victims who are known to the perpetrator offline. Bullying that used to take place only during school hours has been extended into various online venues and, worse, can be scaled up more effectively by the disinhibition effect of interacting via a detached and often textual medium. Cyberbullying is thus a cyber-enabled crime causing not financial but emotional harm [5]. The varieties of its expression make cyberbullying a concern for any online platform that enables communication between potentially school-aged users.

Data leakage can be an accident caused by misconfiguration, but it is also increasingly common for attackers—especially 'hacktivists'—to release documents to the public that were stolen as part of an intrusion. Such acts might often be ideologically motivated, where the documents released relate to a social cause or issue, but can also be personally-targeted ('doxxing' an individual to enable or encourage online harassment) or financially-motivated (as part of a public relations campaign against a business competitor).

Denial of service is again more of a broadly-used method than a specific category of crime. There are a number of specific mechanisms for implementing a denial of service attack, but the most popular and widespread is the distributed denial of service (DDoS), in which large numbers of internet users (or their machines, as part of a botnet) target a site or service to exhaust its bandwidth and prevent it from operating. The most attention-grabbing DDoS attacks are ideologically-motivated protests, but the technique is also used in interpersonal conflict, to 'boot' individuals from online games [6]. While in some sense analogous to an in-person protest[2], DDoS is typically considered a cyber-dependent crime, as it exploits the technical nature of service delivery.

Drug dealing has seen new online horizons since around 2012, with the use of Tor hidden services and cryptocurrencies enabling the creation of online marketplaces where illicit substances can be purchased and delivered without any in-person interaction with a drug dealer. The transition online for this 'last mile' of the drug trade [7] has been popular due to making buying illegal substances a much safer experience for customers, even if online fraud and law enforcement takedowns remain a concern. This is a core example of a cyber-enabled and financially-motivated crime, but lacks something you would usually expect to see: an unambiguous victim.

Email spam will be familiar to anyone with a public email address, and exists as a natural outgrowth of ordinary advertisement practices. Just as the printing press enabling cheap replication of publications led inevitably

[2]Early DDoS attacks were called 'netstrikes', referencing labour union activities.

to the junk mail you get through your door, so too did the invention of practically-free electronic messaging lead to shady[3] businesses advertising their products or services via bulk unsolicited email. In particular, online pharmacies selling cheap generic pharmaceuticals were a major contributor to spam. As low conversion rates didn't matter[4], this was a successful, financially-motivated[5] activity that became criminal largely because it was so annoying – wasting the time and resources of email users and internet service providers with large volumes of unwanted advertising[6].

Financial malware is malware installed on victim machines with the dedicated purpose of stealing financial credentials such as credit card numbers or username/password combinations for online banking sites. Sophisticated botnet operations like Zeus [8] and Torpig [9] were predicated on this kind of activity, and the operators commonly sell on their credentials rather than use them themselves. This is a key example of financially-motivated, cyber-dependent crime.

Ransomware is malware that deploys blackmail tactics. Typically, he malware encrypts a victim's personal files, and the criminal holds the encryption key hostage until a cryptocurrency payment is made. As these files are rarely properly backed-up, and can be important for business or other reasons, the leverage is substantial. Despite having been described as far back as 1996 [10], this is currently one of the 'hottest' forms of cybercrime, with recent research finding a minimum of 12 million USD traceable as payments [11]. Once again, the financial motives and dependency on computerisation make categorisation simple.

Romance scams are a form of online fraud in some ways similar to advance-fee fraud. Victims are attracted via profiles on e.g., online dating sites [12] and then 'groomed' into starting an online relationship with the criminal. This relationship is then used as emotional blackmail, to extort money out of the victim under false pretences – they might claim they need money to get a flight to come see the victim, or to repair their laptop so they can continue talking online. The vast reach and anonymity of internet dating is a significant enabler for what would otherwise be a rather niche form of fraud.

Sextortion is a term for the use of compromising images, often obtained through deceit or technical exploits, as blackmail. There are many variants, including offline [13] but a major current form relies on the use of

[3]Though not always malicious – most spammers sell products that are at worst unregulated and of low quality, rather than actively fraudulent or harmful.

[4]Customers, once reached, often came back directly to the supplier repeatedly.

[5]Usually. There are still some people who use spam networks for religious or political messaging.

[6]Note how in click fraud, advertisers are victims, but in spam, they are the perpetrators.

> controllable, scripted video feeds that appear to show attractive young women. These are used to lure young men into performing sex acts on camera, and the recording is then used blackmail them – with threats to send the video to their friends and family on social media. Motives are in many cases financial, but can depend on the target – sometimes similar threats are used by abusive partners to trap people in a relationship, and sometimes sextortion is used to extract further videos of sex acts[7].

The above is by no means a complete enumeration, but hopefully gives you some idea of the range of cybercrimes, and the corresponding range of issues that you may have to face if you take up a career in cybersecurity. Cybercrime can strike at both technical vulnerabilities and human weaknesses of many forms, with a range of motives and methods. The flexibility of crime is a problem for security in general, as shutting down one illegal activity usually forces criminals to diversify their tactics and even innovate, leading to a new set of security concerns.

The variety above should also convince you of an important point: cybercriminals are not a uniform mass. The people sending spam are not the people writing malware, who in turn are not the people capturing lewd videos on Skype, and those are not the hacktivists uploading corporate emails to Wikileaks. When you find a resource (even in this course) talking about cybercriminals as a population, beware that the authors likely mean one of these (or another) subpopulations, and their conclusions will not necessarily carry to other cases. There is something of a worrying trend among classical criminologists approaching cybercrime to ignore these differences, leading to strange narratives where the rate of "Facebook hacking"[8] amongst high-schoolers is somehow linked to malware and sophisticated cyber attacks. Don't make these mistakes – when you talk about cybercrime, talk about the relevant kind.

[7] A tactic seen in child sex abuse online.

[8] Guessing passwords, or using a logged-in device.

2 CRIMINOLOGY ONLINE

Criminology in general concerns itself with three major questions:

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

The first question is at root a question of legal philosophy – how do people and their governments end up at a decision to prohibit certain activity with the force of law? Typical answers tend to involve both the notion of harm (of some form) caused to others by an act, and the intent to carry out that act on the part of an offender – but there other factors that carry weight, like the violation of established norms of behaviour.

In cybercrime, the definition of acts as criminal is certainly a contentious topic. Quite aside from the problematic notion of which 'jurisdiction' applies to Brazilian users commenting on a British news site hosted on an American-owned hosting company's servers physically located in Ireland, many online acts are problematic for both the harm and intent clauses of criminal definition. Actions like copying a series of bytes from one storage medium to another—seemingly entirely harmless—are sometimes criminalised and sometimes not[9] while at the same time law enforcement often struggle with prosecution because proving that a person's machine was involved in crime does not necessarily carry the case that *the person* was involved in crime. The latter issue may seem dubious until you consider the possibility that a personal machine has been compromised and added to a botnet that is involved in carrying out a crime – unfortunately highly common.

The definition of cybercrime, and other related elements of the intersection between technology and law are all part of "cyberlaw", one of the newest and quickest-growing areas of law. A problem historically for legislation in this area has been that many legislators, judges and other legal minds had a poor grasp of how computers and networks actually worked, sometimes leading to bizarre decisions like people being prosecuted for "unauthorised access" of material served up openly by improperly-authenticated services[10], or confusing the email header "From" line with the "Mail From" part of the SMTP envelope when defining what can be captured in a wiretap [14]. These sorts of "series of tubes" issues are becoming less common, but various parts of internet law are still outdated, and constantly need reform to keep place with developments online[11].

[9] For example, in the US, it is illegal (or at least legally contested) to watch a DVD on Linux, because doing so breaches copy-protection mechanisms.

[10] United States vs. Andrew Auernheimer.

[11] An important note for those of you interested in security research is that the Computer Misuse Act 1990—the main piece of UK legislation regarding cybercrime—criminalises "unauthorised access" in a manner that can be leveraged against security researchers discovering

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

This is a fundamental question for criminology in general, with a number of competing and sometimes complementary theories that attempt to explain the evidence about what it is in human behaviour that leads to people committing crime. Below, we dip briefly into a few of these theories and how they might apply to cybercrime, including its prevention. However, it's worth first acknowledging a few things.

Firstly, cybercrime is in many respects different from other crime[12], being by and large carried out by different kinds of people. In most traditional crimes—a vague category that tends to be dominated by variants of theft and interpersonal violence—the profile of offenders is that they are predominantly male, are poorly educated or have poor job prospects, often being in financial difficulty and/or involved in substance abuse, and they usually already have a criminal record. Of those properties, the only one that also seems to hold for cybercrime is that offenders are predominantly male[13]. Cybercriminals are generally well-educated, employed, not in financial difficulty, and, excluding those specifically involved in the online drug trade, not especially likely to have a substance abuse problem or a criminal record. While there are other consistencies—for example, there seems to be evidence that one good predictor of offending for both cybercriminals and traditional criminals is having previously been a *victim* of a corresponding crime [17]—by and large cybercriminals seem nothing like traditional criminals.

Secondly: how do we know any of that? Can we trust our evidence? In traditional criminology, the general approach to studying criminals is to make use of the products of the criminal justice system – crime reports, investigations, arrests and convictions. Trying to apply the same procedures to cybercrime, however, we encounter substantial obstacles. Cybercrime is in general heavily under-reported, law enforcement are often poorly-equipped to investigate it, and arrests and convictions are even rarer than these issues would account for, since many cybercriminals can act internationally and obfuscate their identity to a degree not typically possible for traditional criminals.

There is a longstanding truism of criminology: you only know about the criminals that get caught – by implication, these are people who may somehow be different from a more skilled subpopulation of offenders[14]. The bind is that you don't know how these offenders are different because they don't get caught, so you don't have anything to compare against. In ways, this hurdle is even higher for cybercriminology – already low rates of arrest lead to the

and reporting vulnerabilities. This is one of several flaws with the law as written which have led to calls for its reform [15].

[12]Just a page ago I was telling you to watch out for people lumping different cybercrimes together under one label, but now I'm not only doing that, but lumping all of 'crime' together as one undifferentiated mass! I plead only that sometimes generalities are useful for getting a point across.

[13]This consistency is explained in part by the fact that males are on average far more prone to risk-taking behaviour [16].

[14]Or a population the police are more willing or able to prosecute.

suspicion that arrest data mostly reflects only the *worst* cybercriminals. However, cybercriminologists also have some interesting opportunities: due to the online, pseudonymous nature of cybercrime, it is possible to safely reach offender populations for interviews, questionnaires and surveys. These methods aren't entirely novel—traditional criminologists often survey convicted offenders—but the access to a potentially *uncaught* population of offenders is an exciting possibility. Unfortunately, this avenue of research has its own drawbacks. In many cases, researchers are essentially asking strangers on internet forums to report how successful they are at cybercrime, with no way to objectively verify these claims. This leads to rather suspect results, like the most common response on a 10-point rating scale for hacking ability being 10, the maximum [18], or more than a quarter of self-reported offenders claiming to have hacked secret government agencies [19].

These prefaces aside, let's look at some of the theories that have been used for understanding cybercrime, and what we might take away from them. There is a breadth of academic literature on this topic, with many other theories from different disciplines sometimes being applied, but I'm going to focus on a brief overview of four of the most commonly-referenced.

2.1.1 Neutralisation theory

The 'Techniques of Neutralisation' are a sociological explanation for law-breaking first developed in the context of juvenile delinquency [20]. The core concept of the theory is that criminals are always aware of their moral obligation to follow the law[15], and so to resolve the dissonance between this and their own actions when they commit crime, they invent justifications for why their criminality is morally permissible.

Or, in other words, rather than follow the syllogism:

- Hacking is unethical.
- I just hacked someone.
- Therefore, I did something unethical.

As that leads to an unwelcome conclusion, criminals instead reason:

- I'm not a bad person.
- I just hacked someone.
- Therefore, hacking is sometimes okay.

The first assumption of that last set is pretty much universal, but really the interesting part of this theory is what the justifications are – the means criminals use to persuade themselves that they are not immoral for their actions. The original authors identified five key methods:

[15] Rather than, e.g., having completely rejected the idea of such moral obligations.

Denial of responsibility ("I had no choice") – the criminal claims they had no other reasonable option but to commit the crime, they were victims of circumstance.

Denial of injury ("It doesn't hurt anyone") – the criminal claims no harm was caused[16].

Denial of victim ("They deserve it because they're…") – the crime is justified by reference to some action or other failing on the part of the victim.

Condemnation of condemners ("You're just as bad!") – the criminal questions the moral authority of those accusing them, to undercut their ability to hold them to account.

Appeal to higher loyalty – the criminal suggests that their action was for the greater good, a cause or principle more worthy of following than obeying the law.

These techniques seem to have descriptive validity for a lot of misbehaviour, including many forms of cybercrime. Consider, for example, the popular rhetoric around digital piracy, or the entire scope of activities covered under 'hacktivism'. The implications of the theory in terms of concrete preventative action are perhaps less clear, but do seem to suggest particular messaging strategies for cybercrime prevention campaigns. If you can preempt these self-justifications, it may be possible to neutralise the neutralisation and dissuade individuals from engaging in crime. By stressing that individuals have other choices, demonstrating how their crime harms worthy victims[17], identifying lawmakers and law enforcement bodies as having moral authority, and setting out the argument that higher principles are best served by acting within the law, it may be possible to close-off the neutralisation methods of criminals so that they cannot by their own conscience carry out the crime. However, just as with the applications of other theories to come, whether this approach has real validity is yet to be properly determined – a critical question is whether neutralisation occurs in the lead-up to a crime, or only as a post-hoc justification.

2.1.2 Routine activity theory

Routine activity theory [22] views crime as being a predictable result of certain conditions that offer the *opportunity* for crime to happen. In particular, it posits three conditions that are necessary for creating crime, and predicts that when these three conditions are met, crime is likely to occur. These conditions are:

[16] Note how these first two mirror the common 'harm' and 'intent' components of why we consider certain actions to be crimes.

[17] That is, victims which people are predisposed to feel sympathy for as a matter of psychology – I'm not suggesting other victims did deserve it, just that some examples are more compelling [21].

1. **Presence of a motivated offender**: straightforwardly, crime doesn't happen without criminals. The concept of a 'motivated offender' captures a number of important properties – they are not just *capable* of a crime (that is, they have the required tools and abilities to commit the crime), but *willing* to do so. Routine activity theory, in a deliberate gap, does not take a particular position on what it is that motivates people to commit crime, just that motivated offenders do exist.

2. **Presence of a suitable target**: the target of a crime is another necessary component. The concept of a 'suitable target' encompasses both property and individuals, as appropriate for the crime in question. Four basic elements are considered to make the target more or less 'suitable' for crime:

   - The value of the target (expressed financially or subjectively);
   - The obstacles inherent to the target's properties (e.g., if the crime is theft, is it too much gold to carry? If it is assault, is the target a seven-foot-tall boxer?)
   - The visibility of the target – can the offender observe that the target exists?
   - The access to the target – can the offender *reach* the target easily?

3. **Absence of a capable guardian**: even if you have a highly-motivated child murderer in a room with a small child wearing a 'please murder me' t-shirt, a crime will still be unlikely to occur if the child's father is also standing there with a shotgun. This is the crux of the 'capable guardian' requirement. Even where targets and offenders coincide, the 'guardian' that might prevent crime has to be missing for crime to become likely. This guardian might be a person, like a police officer, who would intervene to prevent the crime or apprehend the offender. However, a capable guardian can also be an 'object', like an alarm that warns of shoplifting attempts, or—in the case of cybercrime—tools like intrusion prevention systems, antivirus, and many other automated controls.

The implications of routine activity theory are that anything that leads to these conditions arising more frequently at the same time and in the same 'space'[18] will tend to increase rates of crime. A result of this is, other things being held constant, just having more people interact in spaces without a guardian is likely to increase crime, as you create opportunities for offenders and targets in the population to come together.

[18] Routine activity theory was developed against the sort of crime that took place at particular physical locations, like a bank or a shop. However, it translates about as well as anything to our notion of 'cyberspace', in which we think of 'places' like an online banking site or e-commerce platform. The notion of 'proximity' between these places still requires more thought, though.

The increased connectivity of people everywhere—often touted as a major benefit of the Internet—is from this perspective highly worrying. Routine activity theory has been supported in some results related to cybercrime. For example, spending more time online and making online purchases both have a significant relationship with your likelihood of being targeted for online fraud [23]. Greater levels of internet use are also predictive of offending in cybercrime [24]. However, even in large studies the evidence is still ambiguous about the extent of support for the theory, with some factors such as target visibility having clear effects, but others such as target value having very little impact [25].

If we consider routine activity theory to hold for at least some cybercrimes, what does it imply we should do to prevent offending? Clearly, at least one of the three conditions needs to be removed in whichever online space is relevant. The most obvious of these is perhaps the absence of a capable guardian – if guardians of some form can be introduced 'wherever' online interactions take place, then crime should be reduced. This is an attractive option for security engineers in particular, as many autonomous guardians can be imagined that make internet activities safer—phishing alert warnings, for example, or fraud classifiers. These are solutions that can scale to protect hundreds of thousands of people. The drawback is that the guardians must be *capable* – countermeasures that can be evaded easily will not act as a deterrent. More traditional guardians, like 'internet police' agencies such as the NCSC are perhaps less immediately effective, but may serve as a deterrent to cybercriminals. What of the other two conditions? Removing motivated offenders requires either removing them from spaces (e.g., banning them once you identify them, arresting them) or removing their motivation. To do the latter would require first understanding the motivation for each cybercrime and coming up with appropriate interventions. Financially-motivated cybercriminals, for example, could be enticed into working in a high-paying legitimate profession. For targets, it might be possible in some cases to remove targets from interactions by e.g., taking machines[19] that don't need to be connected to the internet offline. This is a good idea when possible, but not often practical. In other cases, the signals of target suitability can be addressed by making targets less visible, or more difficult to access, reducing the temptation for offenders.

2.1.3 Self-control theory

Self-control is a psychological trait linked to an individual's ability to resist temptation or impulses. Exercising self-control involves forgoing acts that have short-term rewards in favour of your longer-term interests. Early testing of self-control is predictive of a variety of important life outcomes such as wealth, health and parenting ability [26]. Another life outcome reliably predictable from childhood levels of self-control is involvement in (and conviction for) criminal activity [26, 27].

[19] Or indeed people.

This last association hopefully makes some intuitive sense—most crime can be characterised by some features of short-term gratification such as excitement, immediate financial gain, or retaliation against a slight [27]. The association between low-self-control and crime is so well-supported that it has been considered by some criminologists as the foundation for a "general theory of crime", with a general thesis that people with high levels of self-control are less likely to commit crime [28, p. 118].

As this association has also held up in studies of (some, self-reported) cybercriminals [29, 24], the question then arises: what can we do about it? Some psychological traits (e.g., IQ) are resistant to attempts to affect them over the long term [30], while others are more malleable. If self-control is fixed, then self-control theory would suggest that certain individuals are just predisposed towards (cyber-)crime, and effective countermeasures would need to focus on decreasing the short-term 'situational' attractiveness of cybercrime for these people – a difficult proposition, as this amounts to preventing or degrading cybercriminals' ability to extract rewards from their activities[20].

Thankfully, while behavioural-genetic evidence suggests that self control does have a significant genetic component [31], there also appears to be evidence that environmental interventions in childhood can have a big impact on levels of self-control [26]. This means that changes to a population's childhood environment can increase their level of self-control, and thus both avert future crime and improve the general life outcomes of those children.

2.1.4 Social cognitive theory

Social cognitive theory, or social learning theory[21] has as its core concept that much—perhaps most—of our behaviour is learned from the examples of people around us [32]. That is, rather than being entirely governed by operant responses to rewards, we observe the behaviour of people and imitate it, and this shapes how we process a lot of reality, as well as the skills we learn.

When it comes to crime in particular, there are two major influences to be aware of: the examples of role models, and the impression of what is 'normal' behaviour. Social cognitive theory predicts that if criminal behaviour is engaged in by role models, or there is a widespread view that certain criminal behaviour is 'normal', then it is much more likely to happen[22].

This theory appears to be supported in at least some areas of cybercrime. For example, willingness to engage in digital piracy has been linked to predictors like association with peers who engage in it, parental support for the activity, and similar associations [33, 34]. Intuitively, there are a number of cybercrimes like cyberbullying that have social origins [35].

[20] This is perhaps a short treatment, there is more nuance that could be applied in reducing the attractiveness of particular forms of cyberoffending, or the attraction to particular targets.

[21] If there is a distinction it is fine.

[22] Social cognitive theory also has implications for promoting *secure* behaviour amongst members of an organisation – can you see how?

According to this theory, cybercrimes are just a set of behaviours that can be picked up socially when the conditions for social learning are in place. Preventing cybercrime is made possible by removing these conditions. This would involve avoiding creating role models[23] who engage in cybercrime, and preventing the spread of the message that certain cybercrimes are 'normal', or engaged in by groups an individual might identify with[24]. In essence, a campaign based on social cognitive theory should aim to communicate not just that cybercrime is *bad*, but that it is *abnormal* – a perhaps paradoxical message to implement at scale.

3 OPTIONAL EXERCISES

These are suggestions for students who are particularly interested in the topic of cybercriminology. They are not assessed in any way. You don't need to complete the below to do well on the course.

3.1 *Further Reading*

If you're interested in a particular form of cybercrime, the references from the first section are good starting points for finding literature – but also feel free to email me for additional resources, including about crimes not covered here. There is a broad literature from computer scientists, criminologists and psychologists studying many of these offences. If you are more interested in the criminological theories discussed above, the references from the second section are again a good starting point, though I may be able to guide you to something specific if you like.

3.2 *In Practice*

Cybercriminology isn't generally something you would do outside of academia and a rather niche area of security research or journalism. It is of course possible to integrate yourself into online criminal communities in order to observe and study them, but this carries a number of risks – not least, the possibility that you would be drawn into committing cybercrime yourself. However, as CS students you are in a much better position to contribute to this area than many criminologists. Much of my own research overlaps with areas discussed in this lecture on the basis of data mining and machine learning applications in cybercrime data. If you wanted to take on a project on one of these or similar topics—particularly in the area of data-driven investigations of cybercriminal behaviour—then please do contact me to discuss it.

[23] Even fictional ones.

[24] This is a shortened version, for a fuller breakdown of conditions for social learning see [32].

REFERENCES

References

[1] Y. Park, D. McCoy, and E. Shi, "Understanding Craigslist rental scams," in *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 3–21.

[2] H. Whittle, C. Hamilton-Giachritsis, A. Beech, and G. Collings, "A review of online grooming: Characteristics and concerns," *Aggression and Violent Behavior*, vol. 18, no. 1, pp. 62–70, 2013.

[3] C. Peersman, C. Schulze, A. Rashid, M. Brennan, and C. Fischer, "iCOP: Live forensics to reveal previously unknown criminal media on P2P networks," *Digital Investigation*, vol. 18, pp. 50–64, 2016.

[4] P. Pearce, V. Dave, C. Grier, K. Levchenko, S. Guha, D. McCoy, V. Paxson, S. Savage, and G. M. Voelker, "Characterizing large-scale click fraud in ZeroAccess," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 141–152.

[5] J. W. Patchin and S. Hinduja, "Cyberbullying and self-esteem," *Journal of School Health*, vol. 80, no. 12, pp. 614–621, 2010.

[6] A. Hutchings and R. Clayton, "Exploring the provision of online booter services," *Deviant Behavior*, vol. 37, no. 10, pp. 1163–1178, 2016.

[7] M. Dittus, J. Wright, and M. Graham, "Platform criminalism: The 'last-mile' geography of the darknet market supply chain," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 277–286.

[8] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, "On the analysis of the Zeus botnet crimeware toolkit," in *Proceedings of the Eighth International Conference on Privacy, Security and Trust*. IEEE, 2010, pp. 31–38.

[9] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009, pp. 635–647.

[10] A. L. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Communications of the ACM*, vol. 60, no. 7, pp. 24–26, 2017.

[11] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the Bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1–11, 2019.

[12] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "Automatically dismantling online dating fraud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1128–1137, 2019.

[13] R. L. O'Malley and K. M. Holt, "Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime," *Journal of Interpersonal Violence*, pp. 1–26, 2020.

[14] S. M. Bellovin, M. Blaze, S. Landau, and S. K. Pell, "It's too complicated: How the internet upends Katz, Smith, and electronic surveillance law," *Harvard Journal of Law & Technology*, vol. 30, p. 1, 2016.

[15] Criminal Law Reform Now Network, "Reforming the Computer Misuse Act 1990," Report, 2020.

[16] J. P. Byrnes, D. C. Miller, and W. D. Schafer, "Gender differences in risk taking: a meta-analysis." *Psychological Bulletin*, vol. 125, no. 3, p. 367, 1999.

[17] M. Weulen Kranenbarg, T. J. Holt, and J.-L. Van Gelder, "Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap," *Deviant Behavior*, vol. 40, no. 1, pp. 40–55, 2019.

[18] T. Hyslip and T. Holt, "Defining the profile of potential cybercriminals," *Homeland Defence & Security Information Analysis Center (HDIAC) Journal*, vol. 5, pp. 25–30, 2018.

[19] H.-J. Woo, "The hacker mentality: exploring the relationship between psychological variables and hacking activities," Ph.D. dissertation, University of Georgia, 2003.

[20] G. M. Sykes and D. Matza, "Techniques of neutralization: A theory of delinquency," *American Sociological Review*, vol. 22, no. 6, pp. 664–670, 1957.

[21] S. E. Sundby, "The capital jury and empathy: The problem of worthy and unworthy victims," *Cornell Law Review*, vol. 88, p. 343, 2002.

[22] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," *American Sociological Review*, pp. 588–608, 1979.

[23] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *Journal of Research in Crime and Delinquency*, vol. 47, no. 3, pp. 267–296, 2010.

[24] C. M. Donner, C. D. Marcum, W. G. Jennings, G. E. Higgins, and J. Banfield, "Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy," *Computers in Human Behavior*, vol. 34, pp. 165–172, 2014.

[25] E. R. Leukfeldt and M. Yar, "Applying routine activity theory to cybercrime: A theoretical and empirical analysis," *Deviant Behavior*, vol. 37, no. 3, pp. 263–280, 2016.

[26] T. E. Moffitt, R. Poulton, and A. Caspi, "Lifelong impact of early self-control," *American Scientist*, vol. 101, no. 5, pp. 352–359, 2013.

[27] T. D. Evans, F. T. Cullen, V. S. Burton Jr, R. G. Dunaway, and M. L. Benson, "The social consequences of self-control: Testing the general theory of crime," *Criminology*, vol. 35, no. 3, pp. 475–504, 1997.

[28] M. R. Gottfredson and T. Hirschi, *A general theory of crime*. Stanford University Press, 1990.

[29] A. M. Bossler and G. W. Burruss, "The general theory of crime and computer hacking: Low self-control hackers?" in *Cyber Crime: Concepts, Methodologies, Tools and Applications*. IGI Global, 2012, pp. 1499–1527.

[30] U. Neisser, G. Boodoo, T. J. Bouchard Jr, A. W. Boykin, N. Brody, S. J. Ceci, D. F. Halpern, J. C. Loehlin, R. Perloff, R. J. Sternberg *et al.*, "Intelligence: knowns and unknowns." *American Psychologist*, vol. 51, no. 2, p. 77, 1996.

[31] K. M. Beaver, J. Eagle Schutt, B. B. Boutwell, M. Ratchford, K. Roberts, and J. Barnes, "Genetic and environmental influences on levels of self-control and delinquent peer affiliation: Results from a longitudinal sample of adolescent twins," *Criminal Justice and Behavior*, vol. 36, no. 1, pp. 41–60, 2009.

[32] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ, 1986.

[33] W. F. Skinner and A. M. Fream, "A social learning theory analysis of computer crime among college students," *Journal of research in crime and delinquency*, vol. 34, no. 4, pp. 495–518, 1997.

[34] W. D. Gunter, "Piracy on the high speeds: A test of social learning theory on digital piracy among college students," *International Journal of Criminal Justice Sciences*, vol. 3, no. 1, p. 54, 2008.

[35] P. B. Lowry, J. Zhang, C. Wang, and M. Siponen, "Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model," *Information Systems Research*, vol. 27, no. 4, pp. 962–986, 2016.