COMS30038 — SECURITY BEHAVIOURS

CYBERCRIMINOLOGY: ORGANISED CYBERCRIME

Matthew Edwards[*]

---

1 ORGANISED CYBERCRIME

While some elements of cybercrime have remained remarkably constant, like some of the universal tactics used in social engineering, or methods of finding vulnerabilities in software, there have been some significant changes in what cybercrime looks like over the past couple of decades. In particular, we have seen a rise in the *complexity and sophistication* of attacks, a significant drift towards greater *commercialisation* of cybercrime, and alongside both of these a rise in the level of *organisation* involved in carrying out cybercriminal acts [1].

The increasing complexity of cybercrime is evident across a range of different dimensions. Technologically, cybercriminals have been innovating in response to the defences created by cybersecurity experts. Where once a botnet could be relied upon to dial a central, possibly hard-coded command server for instruction, now compromised hosts serve as a P2P overlay network for their communications with their controllers. Manually-constructed indirection, where an attacker would painstakingly set up a series of shells, has been replaced with readily-deployable anonymised routing in the form of TOR. Malware that would once have had a reliable binary signature is now obfuscated with mutation engines that alter the form of the binary without changing its operation [2].

Outside of technology, methods of social engineering have also clearly become more polished and sophisticated. Scams that were once almost always broad-spectrum attacks landing in nearly everyone's inbox have given way to highly-targeted spear-phishing attacks that make use of personal details, or impersonate friends and colleagues. Targets are also better-chosen. Whereas previous attempts at cyber-espionage were somewhat clumsy, poking around poorly-secured university and lab computer systems, modern spies exfiltrate terabytes of sensitive documents from commercial organisations across industry [3].

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

The increasing sophistication of method is in part a reaction to improved defences, and in part enabled by a heightened level of commercialisation in cybercrime. In the early years, many cybercriminals were not motivated by financial concerns, but by the challenge of breaking into systems, playing pranks, and demonstrating their skills to other hackers. While there are still elements of this subculture that linger on[1], modern cybercrime has a much more businesslike and acquisition-focused bent to it. Many cybercriminal operations run like businesses, with salaried employees who care little about technical innovation, and a lot more about meeting performance targets in terms of machines reached, details harvested and funds extracted.

Even outside of the 'corporate' forms of cybercrime, money has become significantly more important. There are nowadays many more "hackers for hire", and toolkits designed explicitly for cybercriminal purposes which can be rented or bought. There is an entire industry of "cybercrime as a service" which lowers costs for potential criminals, and makes them into customers of each other. If you want to launch a DDoS attack nowadays, you do not need to convince people around the world to take part, or even build your own botnet – you can just go to an existing botnet owner, pay them a fee, and rent the use of their stolen machines for a while.

The increasing value of things stored on computers has also played its part in commercialising cybercrime. Vulnerabilities in software that might once have been exploited or reported directly by their discovers are now subject to market pressures. Both private and state actors are interested in amassing previously-undiscovered exploits they can use to breach systems, and they will pay big money for exclusive information. Details on some flaws in systems can sell for hundreds of thousands of dollars.

There are, to be sure, still some cybercriminals who work mostly alone. They can be viewed as more typically being 'hobbyist' hackers, who don't usually depend on cybercrime for their living. Even though they work alone, they likely have contacts and social support groups online – chatrooms where they will brag about exploits, or get support from other peers that they trust. However, the image of the 'lone hacker' is often overplayed in the media. Much of cybercrime is actually the work of organisations, and it is these organisations that enable increasingly sophisticated cybercrime, and support its commercialisation.

It is worth a sidebar here to talk about what we mean by an organisation. The concept can be remarkably flexible, and especially when it describes online and pseudonymous organisations. There are two basic forms you can think of: *swarms* of loosely-cooperating agents, and *hubs* that coordinate actors. Neither are necessarily what we would typically think of as 'organisations' like a corporation or a university. Swarms are 'disorganised organisations' with minimalist chains of command, operating somewhat organically. To use a contentious example, Antifa would be a swarm organisation – there is no

[1] e.g., groups affiliated with Anonymous.

'Antifa HQ', or readily-identifiable leader, but there is a common purpose (or set of purposes), a means of group identification, and lines of communication that enable the sharing of resources and collective action by otherwise disconnected group members. Another typical example is Anonymous, the self-declared 'leaderless organisation'. *Hubs* on the other hand tend to consist of a core of more formally-connected and identifiable criminals who form the centre for a lot of more loosely-connected individuals who drop in and out of participation. Many groups involved in piracy operate like this, with a core crew that is dedicated to obtaining and releasing clean pirated copies of media, who are supported on a case-by-case basis by individuals who can bring them materials or otherwise contribute to the crime. Similar structures exist for botnet operators and online child abusers [4].

The above relates to prototypically online cybercriminal network structures. However, there are also offline group structures that now play a role in cybercrime. In particular, traditional organised crime groups, who have their own hierarchical structures much like many large businesses. It should not be particularly surprising that organised crime families have moved into cybercrime – they have traditionally been quite adaptive in their interests, and follow different sources of illegal funding. In many cases, their reach into cybercrime merely extends their existing interests. The traditional interest in prostitution now extends to pornography websites, and traditional control of illegal gambling is extended to online gambling sites. Fake goods and extortion are other typical areas of organised crime expertise that are being enabled or expanded by moving online [5]. What is interesting, however, is how this expansion is forcing these traditional organised crime groups to alter their means of doing business at a more fundamental level. Traditionally, pre-existing offline social ties were a requirement for involvement in the activities of organised crime groups, to raise barriers for law enforcement penetration. This is now changing as organised crime moves online, and merges with online crime's norms around anonymous online social ties. This carries some risks—criminals who were used to knowing their business partners intimately now have to trust in anonymous forum members—but also brings a lot of benefits for both parties, as complementary capabilities are brought together. For example, online criminals tend to be better at providing exploits and digital services that extract funds from a target, while offline criminals have much more capacity to recruit money mules and use businesses to launder funds.

Quite aside from the structure of the organisations involved in carrying out crime, one of the main sources of sophistication is *specialisation*. Rather than a single individual having to learn how to carry out every stage of an attack, the moden cybercrime *economy*[2] allows individuals to focus on specific areas of expertise, which they can excell at, and then sell this expertise to others. A major fraud operation in the current climate might involve the

[2]Foreshadowing – we'll look at cybercriminal economies in more detail later.

work of various coders, technicians, vendors, fraudsters, hosts, cashiers and money mules, not to mention the individuals finding and selecting targets. This both requires more organisation, pushes commercialisation of each stage, and leads to sophisticated attacks as workers at each stage seek to differentiate themselves from their competitors.

So, cybercrime is increasingly a business sector, operated for profit. There is however one area in which cybercrime has become more ideological in motivation, and that is where the involvement of state actors comes to the fore. It is no longer a controversial point to say that state actors are involved in cybercrime – we have seen numerous examples of state-led attacks over recent years. There are however a range of different *levels* of state involvement in cybercrime, from crime carried out almost entirely by the state[3] to crime that is merely permitted by the state[4]. This is an area in which cybercrime has become more organised in a different manner – there are now government agencies in many countries around the world involved in carrying out cyber-attacks on targets in other nations, buying exploits from criminals, and protecting potentially criminal assets. The question quickly arises as to whether this is *crime* as we traditionally understand it, or something more akin to *warfare* – and how can we draw the distinction?

2 Countermeasures & Consequences

So, how do we fight cybercrime? In earlier lectures we have already approached this question from a few perspectives. Last week we looked at security operations centres, and how they manage the detection of technical intrusions through system monitoring and the integration of knowledge from outside sources. We also discussed criminological theories earlier this week, and what they seem to suggest as broad strategies for effective intervention. Here we narrow this further, and look at some more specific examples of human-focused countermeasures that might be deployed to prevent cybercrime – and then how they might go horribly wrong.

2.1 *Cybercrime Prevention*

We have already covered some of the high-level strategies you might take to fighting cybercrime in a technical or semi-automated manner. If you recall the lecture on the cyber-killchain, you will remember that defences can be put in place to in some manner *detect*, *deny*, *disrupt*, *degrade* or *deceive* attackers. The same categories can often be applied to cybercriminal acts of a kind other than the prototypical computer intrusion. Consider for example the idea of a fake online persona that engages with scammers to waste their time – the

[3] For example, attacks coming out of North Korea are almost certainly being run by the state, there are no significant private actors.

[4] For example, Russia traditionally turns a blind eye to cybercrime committed by local hackers against targets in the West, in a relationship governed by mutual recognition of common interests.

application of deception is hopefully clear, with the persona acting somewhat like a honeypot computer system. If we want to go further than this, one immediate tool we might reach for is the criminal justice system – arrest the cybercriminals. This certainly has its place alongside defensive tactics, but there are other slightly 'softer' methods that are also worth considering.

2.1.1 Situational Warning Messages

A surprisingly straightforward approach to stopping cybercriminals from committing crime is to ask them to stop committing crime. We have previously mentioned honeypot systems – systems that are left deliberately insecure so that security professionals can observe them and learn about what attackers do when they get in. In a study using such honeypot machines, researchers investigated the effect of showing a warning to a computer trespasser [6]. The warning, phrased in general terms, reminded the attacker of the criminal nature of unauthorised access and indicated that the system was monitored. The effect they found was interesting – attackers on systems that displayed warnings were far quicker to end their sessions, but not detectably less likely to return for another session in the future [6], suggesting that warnings might not prevent cybercrime, but they have an effect on criminal behaviour. Further research in the same vein appears to show that if instead of a legalistic warning message, attackers are shown a message signed from the 'overworked admin' asking them not to negatively impact the system, the number of attackers who manipulated or exfiltrated data was significantly lower – suggesting that the important part is asking *politely* [7]. Variants of this scheme where law enforcement have identified a real individual involved in cybercrime can include police cautions, which may be more effective than simple server messages.

2.1.2 Mass Media Messaging

A more broad-spectrum version of the above strategy is the mass-media campaign. Instead of targeting offenders directly in the act—a difficult target to reach—you instead create a message that can be spread broadly in the population, with the aim of directly or indirectly reaching the offenders whose behaviour you want to change. This approach has been used often for behaviour like drunk-driving and illegal drug use. Two general approaches can be taken in such a campaign:

1. *Change the perception of offending risk* – increase the perception of the severity and likelihood of being punished for the crime.

2. *Promote alternative, positive behaviour* – associate the preferred alternatives to offending with rewards.

Examples in the context of cybercrime have so far most heavily focused

on digital piracy[5], but agencies like the National Crime Agency have started designing new campaigns in this vein for other forms of offending [8, p. 35–44].

2.1.3 Educational Workshops & Positive Diversions

Two tools sometimes used in traditional crime prevention are educational workshops and positive diversions, targeted at groups considered to be at risk of offending. Workshops in schools have been used to combat drug use, gang membership and similar problems, while interventions like sports programmes, wilderness camps and arts education have seen similar effects by diverting possible (or early) offenders into more positive pursuits.

When it comes to cybercrime, these tools may be somewhat under-deployed at the moment. There is some evidence that educational workshops have an effect on some behaviour like cyberbullying [9], but similar interventions are scant for others. When it comes to positive diversions, there is some evidence that diversions might work best when the activity diverted to is very similar to the criminal activity—when youths involved in graffiti can be diverted to 'urban art' projects, for example [8, p. 100]—which raises an interesting possibility when it comes to cybercriminals. As the example of criminals like Mitnick shows, there is a possible path from cybercrime to cybersecurity that could, if addressed properly, divert potentially skilled criminals and bolster the ranks of cybersecurity as a profession.

2.2 *Unintended Consequences*

With any intervention that you plan to make to a complex system[6] you must always pay some attention to the predictable possible outcomes. While you may make changes with the best of intentions, there are a number of ways these intentions can be perverted, and it is possible that something you do to try and prevent harm can actually create *more* harm. Here are seven broad categories of such unintended consequences[7]:

Displacement Cybercrime displacement occurs when cybercrime moves to other targets, places or methods as the result of cybercrime prevention initiatives. While crime is successfully prevented at one site, the benefit is at best local and perhaps illusory, as the crime 'moves' to another target or location. Examples include the surge of new online drug markets following the takedown of the first Silk Road [11], or phishing sites moving to domains and hosts which are more resistant to takedown efforts [12].

Insecure norms Sometimes a countermeasure's existence can lead to the creation of insecure norms of user behaviour – behaviours that are enabled

[5] "You wouldn't steal a car..."

[6] Such as pretty much any system involving humans.

[7] These are drawn from a paper I coauthored [10]

or encouraged by the existence of a particular countermeasure, but establish a pattern that is dangerous without that countermeasure's support. As an analogy, imagine a door which automatically locks itself as you leave – a helpful countermeasure when it protects against occasional lapses, but it enables users who never develop a habit of checking the door is locked, *reducing* the security of those users when the auto-locking fails, or when they are in a different building. For cybercrime, the door lock can be technical controls [13], or even certain industrial standards of behaviour, like how normal it has become to give websites your personal information for identity verification purposes, and the way this opens people up to attacks.

Additional costs Countermeasures and interventions will almost always involve additional costs to particular parties in terms of time or resources. Ideally, these costs are justified by the harm prevented. However, if a cost-benefit analysis has not been performed, the costs to some stakeholders may outweigh the original harm. Examples include reporting systems for social media abuse which pose a large burden of manual review for social media companies and their employees [14], and cases where there is a reliance on anti-phishing training which places the burden of responsibility for phishing detection on low-level employees. This issue is particularly a problem when costs 'move' to individuals or groups least able to bear them.

Misuse A countermeasure developed to prevent harm may be intentionally misused by a variety of actors in order to create new harms [15]. Examples include reporting systems being used maliciously as a result of personal grievances [16] or competitive business interests, or details provided by users for identity verification purposes being sold to advertisers. Even seemingly innocuous countermeasures like advice for victims may be misused by perpetrators as training materials.

Misclassification Technological or administrative systems that create good/bad or allowed/disallowed distinctions will occasionally classify non-malicious content or individuals as malicious. The harm that those affected by misclassification will suffer can be significant if it is not anticipated. A child mistakenly flagged as a cyberbully could become a scapegoat for the misbehaviour of others, and individuals labelled as malicious may even end up identifying with the label. Whatever their accuracy, classification systems may need to be augmented with some means of appeal if their application could cause harm.

Amplification Interventions can backfire, causing an increase in the behaviour targeted for prevention. Examples include abusers escalating violence when made aware of attempts at disconnecting them from their victims [17], and the 'Streisand effect', where an attempt to suppress news or online content causes increased interest in preserving and

sharing it [18]. This can apply to a range of interventions. For example, media coverage of police crackdowns on drug markets, intended to deter offenders by sending a message about enforcement, was actually found to *increase* trade on the markets [19].

Disrupting other countermeasures Novel countermeasures and interventions can interrupt the operation of other, potentially more effective, countermeasures. Examples include devices used in partner abuse being discarded, or abusive online content being taken down, destroying evidence that would have been crucial for criminal prosecution [20]. Identity verification schemes intended to protect against sock-puppet accounts can prevent users from protecting themselves from online abuse with anonymity and pseudonymity, and security and safety advice provided for a number of issues can contradict other advice, leading to confusion and mistakes among users [21]. In general, for new interventions, we should consider which *old* interventions they might break or clash with, and whether the net effect is still positive.

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*

While relatively academic in tone, two books that give a good overview of work in cybercriminology – from a variety of disciplinary perspectives – are *Cybercrime through an Interdisciplinary Lens* [22] and *Cybercrime Prevention: Theory and Applications* [8]. This lecture drew heavily on them both as sources, but there is more in them both that would be worth pursuing if you like this as a research area. You may also find it useful to read The Grugq's article on the cybercriminal group FIN7[8].

REFERENCES

References

[1] P. Grabosky, "The evolution of cybercrime, 2006-2016," in *Cybercrime through an interdisciplinary lens*, 2016, pp. 15–36.

[2] I. Stipovic, "Antiforensic techniques deployed by custom developed malware in evading anti-virus detection," *arXiv preprint arXiv:1906.10625*, 2019.

[8] https://sec.okta.com/articles/2020/08/crimeops-operational-art-cybercrime/

[3] Mandiant Intelligence Center, "APT1: Exposing one of china's cyber espionage units," Mandiant.com, Tech. Rep., 2013.

[4] M. McGuire, "Organised crime in the digital age," *London: John Grieve Centre for Policing and Security*, 2012.

[5] K.-K. R. Choo and P. Grabosky, "Cyber crime," in *Oxford Handbook of Organized Crime*, L. Paoli, Ed. Oxford University Press, 2013.

[6] D. Maimon, M. Alper, B. Sobesto, and M. Cukier, "Restrictive deterrent effects of a warning banner in an attacked computer system," *Criminology*, vol. 52, no. 1, pp. 33–59, 2014.

[7] H. Jones, D. Maimon, and W. Ren, "Sanction threat and friendly persuasion effects on system trespassers' behaviors during a system trespassing event," in *Cybercrime through an interdisciplinary lens*, 2016, pp. 150–166.

[8] R. Brewer, M. De Vel-Palumbo, A. Hutchings, T. Holt, A. Goldsmith, and D. Maimon, *Cybercrime prevention: Theory and applications*. Springer, 2019.

[9] N. Pearce, D. Cross, H. Monks, S. Waters, and S. Falconer, "Current evidence of best practice in whole-school bullying intervention and its potential to inform cyberbullying interventions," *Journal of Psychologists and Counsellors in Schools*, vol. 21, no. 1, pp. 1–21, 2011.

[10] Y. T. Chua, S. Parkin, M. Edwards, D. Oliveira, S. Schiffner, G. Tyson, and A. Hutchings, "Identifying unintended harms of cybersecurity countermeasures," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2019, pp. 1–15.

[11] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX Security Symposium*, 2015, pp. 33–48.

[12] A. Hutchings, R. Clayton, and R. Anderson, "Taking down websites to prevent crime," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2016, pp. 1–10.

[13] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

[14] S. T. Roberts, "Behind the screen: The hidden digital labor of commercial content moderation," Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2014.

[15] M. Silic, "Dual-use open source security software in organizations–dilemma: help or hinder?" *Computers & Security*, vol. 39, pp. 386–395, 2013.

[16] J. Anderson, M. Stender, S. M. West, and J. C. York, "Unfriending censorship," Onlinecensorship.org, Tech. Rep., 2016.

[17] C. Southworth, S. Dawson, C. Fraser, and S. Tucker, "A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy," *Violence Against Women Online Resources*, 2005.

[18] S. C. Jansen and B. Martin, "The streisand effect and censorship backfire," *International Journal of Communication*, vol. 9, pp. 656–671, 2018.

[19] I. Ladegaard, "We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets," *The British Journal of Criminology*, vol. 58, no. 2, pp. 414–433, 2018.

[20] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, ""a stalker's paradise" how intimate partner abusers exploit technology," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[21] S. Tye-Williams and K. J. Krone, "Identifying and re-imagining the paradox of workplace bullying advice," *Journal of Applied Communication Research*, vol. 45, no. 2, pp. 218–235, 2017.

[22] T. J. Holt, *Cybercrime through an Interdisciplinary Lens*. Routledge, 2017.