Unit 2 Seminar

Title: Cybercrime Case Analysis

Firstly, ensure you have completed the reflections from Unit 1 and come prepared to share your work.

Now, skim through the Cyber Physical Systems (CPS) guidance 'Cybercrime – Prosecution Guidance' on the CPS website.

Choose one of the cybercrimes in the guidance.

Write a brief (200-500 words) case analysis on the crime you have chosen.

The case analysis should provide:

- Some description and explanation of the crime.
- Identify its unique characteristics.
- Evaluate the extent of which this cybercrime is different than its off-line version (if it lacks a direct comparison, assess whether this is a complete new offence or whether there could be any analogies with an even remotely similar offline offence).
- Identify and assess issues concerning laws (you can focus on one jurisdiction or provide an international overview).
- Identify and assess issues concerning burden of proof, standards of proof and admissibility.

1. Cyber-Dependent Crimes

According to the Crown Prosecution Service, cyber-dependent crimes “can be committed only through the use of Information and Communications Technology (‘ICT’) devices” (CPS, 2019), and comprise either of hacking or the disruption of networks. The sections below will focus on hacking as a crime, discussing it’s unique characteristics, analogous off-line comparisons, and some obstacles to the burden of evidence for prosecution.

2. Hacking as a Crime

At its core, hacking is the ability of a rogue actor to bypass the security measures implemented by a network, system, application, or function by manipulating weaknesses in a target’s code infrastructure. Common attacks include broken access control through cross-site scripting, cryptographic failures, and various injection attacks (OWASP, 2021). The goal of such attacks is to gain access to sensitive data and/or user information (Burruss et al., 2021), sometimes for clout but more often for profit.

Perhaps the closest off-line crime is corporate espionage, the “theft of vital business information, which may include trade secrets, to gain a financial or commercial advantage over time” (Tzenios, 2023: 13). In this instance a rogue actor is physically inside the company conducting nefarious intel gathering, but the motivation behind these actions are very similar to a hacker, for example, rummaging around an IoT system’s log files.

3. Prosecutable Evidence

One interesting aspect of hacker culture is the tendency for pseudonymous hackers to take credit for major attacks in public hacking forums (Burruss et al., 2021). One would think such disclosure leads to the easy identification and prosecution of major crimes, but this depends on how well the hacker has been able to hide thier source IP address.

If law enforcement were able to locate the source IP address of the hacker, this would reveal their physical address and could lead to the discovery and confiscation of devices used to commit cybercrime. Digital footprints, “the aggregate data derived from the digitally traceable behaviour and online presence associated with an individual” (Büchi et al., 2018: 243), are the key element to reverse engineer a hacker’s network path back to their source IP address. Any footprints left unaccounted for by the hacker could lead to identification and subsequent arrest.

Hackers are thus very diligent when obfuscating their online identity through proxies, TOR-bridging, virtual private servers, and blockchain technologies (Graham, 2021). If law enforcement has limited technological ability or budget, it is often too difficult to trace a hacker past a certain point (Bossler, 2022), especially if they use cryptocurrency to pay for a VPN or VSP. This is often why a skilled hacker will not be easily identifiable to law enforcement.

If a hacker is apprehended, and their devices impounded to evidence, robust digital forensics would need to be employed to verify any criminal evidence found on the devices (Bossler et al., 2022). But the difficulty with prosecuting hacking crimes is not so much in proving the evidence once devices are located, but rather locating the devices at all.

4. Conclusion

This post has discussed the cyber-dependent crime of hacking, defining and discussing its unique characteristics, analogous off-line crimes, and obstacles to the burden of proof required for prosecution.

5. References

Bossler, A., Holt, T., & Seigfried-Spellar, K. (2022) *Cybercrime and Digital Forensics.* New York: Routledge.

Büchi, M., Lutz, C., & Micheli, M. (2018) Digital Footprints: An Emerging Dimension of Digital Inequality. *Journal of Information, Communication and Ethics in Society*, 16 (3): 242 – 251

Burruss, G. W., Howell, C. J., & Maimon, D. (2021) Restrictive Deterrence and the Scope of Hackers' Reoffending: Findings from Two Randomized Field Trials. *Computers in Human Behavior*, 125: 1 - 15

CPS (2019) *Cybercrime – Prosecution Guidance* | Legal Guidance, Cyber / Online Crime. Crown Prosecution Service. [Available Online] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Graham, D. G. (2021) *Ethical Hacking: A Hands-On Introduction to Breaking In*. San Francisco, USA: No Starch Press.

OWASP (2021) *Top 10 Web Application Security Risks* | OWASP Top Ten. OWASP. [Available Online] https://owasp.org/www-project-top-ten/

Tzenios, N. (2023) *Corporate Espionage and the Impact of the Chinese Government, Companies, and Individuals in Increasing Corporate Espionage*. Dissertation.