WHAT CONSTITUTES CYBERCRIME?

Cybercrime = criminal activity involving an information technology structure (computers, networks, or the internet as a tool or target).[1]

Clough draws on a three-stage classification, as summarised by the US Department of Justice:

1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attacks.
2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.
3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence but is more a repository for evidence.

In the above, we see a **tripartite classification of computer crimes**, computer-facilitated crimes and computer-supported crimes. This classification has been adopted in Australia.[2]

The Internet is now used to merely facilitate traditional crimes e.g., hacking, fraud, theft, pornography, gambling, piracy, incitement, counterfeiting, gullibility scams, phishing, information warfare and terrorism. There are also crimes and opportunities unique to the Internet and computers e.g., services theft, manipulation of the stock market (through ramping up of stock prices and 'pump and dump' schemes using the Internet), software piracy, and other thefts of IP.

The complexities of cybercrime, intrinsic to the technology itself and to the vagaries of human nature, are exacerbated by the inadequacies of current law. Going forward, we need to find a way to balance regulation and innovation while ensuring safety in the digital space.[3]

THE PROBLEM OF JURISDICTION

TERRITORIALITY

A feature of the criminal justice system which affects the ability to tackle computer misuse is the **territoriality** of the criminal law. Each jurisdiction has its own separate criminal law. The international nature of many computer crimes further aggravates the problem, with international jurisdictions causing massive headaches for regulators. The key response to this challenge has been an international attempt to obtain consistent laws across the world, but it still doesn't deal with many of the challenges in prosecuting offshore perpetrators.

[1] R Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets.'
[2] Jonathan Clough, 'Principles of Cybercrime' (Cambridge University Press, 2012).
[3] R Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets.'

If laws are not kept up to date, global information is under threat. The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in other national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Cybercrime is drastically different from normal crime for a number of reasons:

- Easy to learn how to commit;
- Requires minute resources proportionate to damage they can cause;
- Can be committed in a jurisdiction without being physically present in it; and
- Not always clearly illegal.

Issues with investigation

1. Anonymity;
2. Global reach (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimization);
3. The speed at which crimes can be committed;
4. The potential for deliberate exploitation of sovereignty issues and cross-jurisdictional differences by criminals and organised crime;
5. The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints or DNA; and
6. The high costs of investigations.

Clough identifies key factors inhibiting investigation of cybercrimes:

- **Scale**: unlike more traditional forms of communication, the Internet allows users to communicate with many people, cheaply and easily. The amount of people on the Internet provides an unprecedented pool of potential offenders and victims. This acts as a force multiplier, allowing offending to be committed on a scale that couldn't be achieved in the offline environment. The ability to automate certain processes further amplifies this effect.
- **Accessibility**: technology is now ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims. Offenders who might otherwise be isolated in their offending, can now find the minds, forming virtual communities to further their offending.
- **Anonymity**: an obvious advantage for the offender, and digital technology has facilitated in numerous ways. Offenders may deliberately conceal their identity online. Simply opening an email account which doesn't require identity verification provides a false identity. Confidentiality may be protected by the use of readily available encryption technology, while traces of digital evidence may be removed using commercially available software.
- **Portability** and **transferability**: central to the power of technology is the ability to store enormous amounts of data in a small space, and to replicate it with no appreciable diminution of quality. The convergence of computing and communication technologies has made this process a seamless one, with the ability to take a digital image with a phone and then upload it within seconds.
- **Global reach**: modern computer networks have challenged the traditional criminal law paradigms existing in various jurisdictions. This presents issues for law enforcement and harmonisation.
- **Absence of capable guardians**: perceived risk of detection and prosecution may affect offending behaviour. The volatile nature of electronic data requires sophisticated forensic techniques to ensure its retrieval, preservation, and validity for

use in a criminal trial. The networked nature of modern communications makes surveillance extremely difficult. Much of infrastructure is privately owned. Communications will routinely be routed through multiple jurisdictions. Data retention may be limited or non-existent.[4]

TRANSIENT NATURE

The trans-national character of computer crimes creates new challenges for the law. More than any other international crime, the **speed, mobility, flexibility, significance, and value of transactions** in and for which cybercrimes are committed profoundly challenge the existing rules of international criminal law. Hackers can physically operate in one country, move electronically across the world from one network to another, and easily access databases on different continents. Thus, different sovereignties, jurisdictions, laws, and rules will come into play.

So, there are a number of complex issues to confront when a cybercrime is committed.

CENSORSHIP AND ONLINE CONTROLS

Governments have introduced various regulations aimed at controlling internet content, such as censorship and gambling laws. In Australia, the Federal Government implemented censorship schemes and controls over online gambling (*Interactive Gambling Act 2011* (Cth)), highlighting a symbolic role rather than achieving effective regulation. These laws are politically motivated, aiming to show the public that governments are addressing concerns related to online content and gambling.[5]

The French case of *Yahoo! Inc v La Ligue Contre Le Racisme,* 169 F. Supp. 2D 1181 (N.D. CAL. 2001) highlights the global impact of local censorship laws. In that case, a French court ordered Yahoo to block access to Nazi memorabilia auctions, and although the US agreed with this ruling, it represented the first major attempt to impose international censorship on the Internet.[6]

While governments attempt to regulate internet content, issues like cross-border enforcement become significant challenges. The *Interactive Gambling Act 2011* (Cth) aimed to block interactive gambling services, but inadvertently led to the offshoring of gambling activities, raising concerns about the effectiveness of local laws when dealing with global platforms.[7]

USING EXISTING OFFENCES (IF THERE WAS NO LEGISLATION)

FRAUD

Kennison v Daire (1986) HCA	
Facts	The accused was convicted of larceny of funds received from an auto-bank when he used the machine to successfully withdraw $200 from an account

[4] Jonathan Clough, 'Principles of Cybercrime' (Cambridge University Press, 2012).
[5] R Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets.'
[6] R Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets.'
[7] R Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets.'