## Topic 2 Cybercrime

Relatively recent issue with public use of internet because widespread in 1991 with the World Wide Web in 1993. Use of computers to commit crime developed in parallel with the legitimate uses and new varieties of criminal activity develop as rapidly as technology develops.

* Many businesses consider computer crime more costly than conventional crime
* Cost to UK business -£10 billion in 2006/£27 billion 2010
* Computer crime operates on different levels – individual hacker to organised crime
  + Russian bot nets. Google site reliability engineers in Dublin.
* Utilises variety of tools and methods – constantly evolving
  + Old school Trojans
  + Phishing/Pharming
  + Doxing

Even crimes which at first sight to not appear to be ‘computer crimes’ will often involve computer based evidence e.g. Graham Dwyer Case where the court was able to convict based on evidence on mobile phones and covering his tracks by creating multiple accounts on home pc.

Technology impacts on both substantive criminal law and criminal procedure

It is argued that the Law has struggled to keep pace with developments in technology

## Difficulties in Prosecution

* Difficulties of Investigation
* Difficulties of Proof
* Reluctance of Victims to report incidents
  + Many victims
* Viewed as a ‘white collar crime’
* [Article 1](http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/)
* [Article 2](http://www.rte.ie/news/business/2014/0403/606405-cybercrime-costs-irish-economy-630m-per-year/)
* [Article 3](http://businessetc.thejournal.ie/cyber-crime-ireland-firms-1428315-Apr2014/)
* [Article 4](https://www.theguardian.com/technology/2016/aug/27/london-police-chief-cybercrime-russia-ukraine-online-fraud-google-microsoft)

## Relevant Irish Law

* Criminal Law
* Guilt must be established beyond all reasonable doubt
* Serious Offences – trial by jury in Circuit Court
* Minor offences – trial in District Court – judge only
* Prosecution must prove both the Actus Reus and the Mens Rea

Operation of criminal law where there is a technology element to a crime. When the crime is committed with a computer.

Fraud and other crimes that are exclusive to computers like hacking.

How up until now, we have dealt with cybercrime.

TJ McIntyre on blackboard. Old but still relevant because nothing has happened in the last 15 years. Very critical of how we dealt with cybercrime in Ireland, wherever possible we have stuck the cybercrime in with traditional criminal offence, hacking basically the same as criminal damage (same as if you set fire to your neighbours car) .

In Britain, they have a separate cybercrime act, criminal misuse act.

## 2 issues to focus on

Orioctas is now considering a major change, which might take on board a lot of the criticisms TJ has which Is to pass specific legislations on cybercrime. There is a bill in oireoctas now which is not yet a law but will make a significant change as to how we deal with cybercrime.

## Computer Crime in Ireland by TJ McIntyre

Irish cybercrime law is an afterthought. The principle offences in this area are contained in the criminal damage act 1991 and the Criminal Justice Act 2001. In both cases the offences have been tacked onto an Act whos primary focus is not cybercrime and the specification of these offences is aging rapidly so some reform of the law is necessary if Ireland is to implement the Council of Europe Convention on Cybercrime.

Traditional crimes committed using computers raise few new issues for criminal law for example, a death threat is still a death threat regardless of the medium used to convey it.

Difficulties arise, however, when courts begin to encounter situations unique to computers, particularly evident in early hacking cases. In these, prosecutors struggled to fit the crime into existing context.

Following this, some success was gain by classifying hacking as a form of criminal damage as seen in Cox Riley and R v Whitely where prosecutors in England succeed in arguing that changes to programs or data should be considered as criminal damage to the physical medium on which the data is stored.

The limitations of this approach were exposed in Whitely where it was noted that in order for criminal damage to be made, the changes would have to result in “an impaired value of usefulness of the disc” so merely snooping around a disc would not quality. In whitely however, the necessary impairment was found as the hacker’s actions led to network issues and ultimately a crash.

In R V Gold, another approach was used by treating the use of false usernames and passwords as forgery. In R V gold two journalists accessed a computer network using the credentials of authorised users which they used to access information and make changes to data. They had the intention of exposition security flaws in the Prestel system.

Ultimately, they were charged under the Forgery and Counterfeiting Act 1981, a ruling which was later overruled by the House of Lords as the user credentials were not recorded or stored but merely checked for validity.

## Criminal Damages Act 1991

Was intended to deal with malicious damage and not focused on computer crime.

“A person who without lawful excuse damages any

property belonging to another intending to damage

any such property or being reckless as to whether

any such property would be damaged shall be guilty

of an offence.”

## NB: How we investigate cybercrime, criminal justice act 2011

The Criminal Justice Act 2011 (the “2011 Act”) came into effect on 9th August 2011 and was enacted with the aim of granting An Garda Síochána (the Irish national police service) more extensive powers to investigate “serious and complex offences”.

The main areas which the 2011 Act deals with are the supply of information at investigation, detention, questioning and the summoning of witnesses.

This article focuses on the 2011 Act as a tool in the fight against cybercrime, a specific sub-species of white collar crime. While cybercrime may not pose the same threat to national economic well-being as some of the criminal acts, the investigation and accordingly the prosecution of which the 2011 Act was intended to assist, with reference to the financial services sector, cybercrime is a material and ever increasing area of criminal activity.

The 2011 Act introduces a wide arsenal of powers aimed at aiding the investigation of serious offences which in the context of cybercrime are generally long overdue and are to be welcomed. The quite serious tariffs applicable under Section19 have been less welcomed by those likely to suffer cybercrime as well as the IT forensics sector, who may be ones who discover the crime.   
  
While the 2011 Act incorporates approximately 130 offences into its remit, one significant omission is reference to Section 5 of the 1991 Act, which relates to unauthorised use of a computer with intent to access data, which was intended to deal with hacking. The reason for this omission is assumed to be attributed to the same logic which associates the offence under the 1991 Act with damage to property and applies comparatively small tariffs. Under the 1991 Act a general offence relating to damage to property is stated, with property defined to include data. This is thus a fairly basic cybercrime related offence. Notwithstanding, the relative merits of Section 5 of the 1991 Act, by omitting reference to it the 2011 Act has disregarded one of the main types of cybercrime offence, namely hacking (albeit a particular type of hacking) that the new broad powers of investigation would seem to have been intended to tackle.   
  
The 2011 Act has taken significant steps to make inroads on issues which hamper the effective investigation of complex and technical crimes. This is welcome. However, overall the law applicable to substantive cybercrime offences, as set out in the 1991 Act and 2001 Act, requires significant revision, to update what are by now elderly offences. Without a more focused and sophisticated legislative framework cybercrime will remain an area where the law lags the crime.

## Key Provisions

Under Section 15 of the 2011 Act a member of the Garda Síochána may apply to a judge of the District Court for an order to make available documents or described documents available.

Investigation of cybercrime offences can clearly be substantially frustrated by the lack of access to encrypted documents, as demonstrated, for example, in recent Garda investigations at Anglo Irish Bank. This section provides the Gardai with considerable additional leverage. The 2001 Act only allowed for penalty of IR£500 or 6 months for failure to disclose passwords and as far as we are aware these penalties were never imposed.

Section 16 deals with the assertion of privilege over documents which fall subject to an application under Section 15 and allows for the Garda Síochána to apply for a determination as to whether privilege can be claimed, which application may be made in camera.

Section 18 of the 2011 Act allows for certain reasonable presumptions to be made in the context of the Criminal Evidence Act 1992 in relation to the authorship or exchange of documents by virtue of the circumstances in which the document is found or purports to be exchanged.

Under Section 19(1) of the 2011 Act it is an offence for a person to withhold information which they believe might be of material assistance in preventing the commission by another person of a relevant offence or securing the apprehension, prosecution, or conviction of any person for a relevant offence and the person fails without reasonable excuse to disclose the information to the Gardaí. This offence attracts a penalty of a class A fine (maximum €5,000) and/or 12 months imprisonment on summary conviction and an unlimited fine and/or imprisonment not exceeding a period of five years on conviction on indictment. The Gardaí may arrest and detain, for up to 24 hours, an individual without a warrant if they are suspected of withholding information.

Section 19 is the provision of the 2011 Act which has attracted most attention within the public and private sectors.

## Malware

* Maliciously developed software
* Designed to alter operation of computer usually to the users disadvantage
* Transmitted and installed without the users informed consent
* In some cases there is no particular objective – a form of cyber vandalism
* Increasingly used for commercial purposes
* Also used for criminal activity
* Adware,Spyware,Viruses,Worms

### Legal Responses

* Criminal offence – Criminal Damage
* Trojan Horse Defence – R v [Caffrey](http://news.bbc.co.uk/2/hi/technology/3202116.stm)
* Civil law – action for negligence

## Denial of Service

* Compromises victim’s internet connection
* Distributed denial of service attack
* Purpose – vandalism, political or extortion
* Examples – [here](http://www.thejournal.ie/government-websites-taken-offline-in-anonymous-opireland-attack-336623-Jan2012/) and [here](http://www.irishtimes.com/business/technology/us-coding-site-github-hit-by-denial-of-service-attack-1.2158505)
* Criminal Law – DPP v Lennon (2006)
* Civil Law – action in negligence by users against the victim of the attack

Unauthorised Access – Hacking

* Methods
* Website attacks
* Purpose
* Criminal Law
* S5 Criminal Damage Act [1991](http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print)
* S2 Criminal Damage Act 1991
* [Case 1](http://www.irishtimes.com/news/crime-and-law/ryanair-falls-victim-to-4-6m-hacking-scam-via-chinese-bank-1.2192444)
* [Case 2](http://www.irishtimes.com/news/crime-and-law/online-cheating-site-ashleymadison-hacked-1.2291065)
* [Case 3](http://www.independent.ie/irish-news/top-model-glenda-tells-of-her-terror-at-stalker-nightmare-26353336.html)
* [Case 4](http://www.breakingnews.ie/ireland/celebritys-file-accessed-80-times-on-garda-database-out-of-curiosity-594999.html)
* R v Bow Street Magistrates (Ojomo) (1999)
* DPP v Bignall

Social Engineering Offences

* Combination of old fashioned confidence trick and technology
* Phishing
* Vishing
* Pharming
* Criminal Law – Theft, Deception, Dishonest use of Computer – definitions [here](http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/pdf)

## Electronic Commerce Act 2000

* Criminalises the misuse of signature creation devises
* S25 (a) deals with accessing, copying or otherwise obtaining the signature creation device of someone else
* S25(b) deals with altering, disclosing or using the signature creation device of someone else
* S25 (c) deals with creating, altering or using an electronic signature for a fraudulent purpose
* Punishment

## Cyberbullying

* Not a distinct offence in Irish Law
* S10 Non-Fatal Offences against the Person Act 1997
* S5 Non-Fatal Offences against the Person Act 1997
* S13 Post Office Amendment Act 1951
* Prohibition of Incitement to Hatred Act 1989
* Harmful and Malicious Communications Bill 2015
* Law Reform [Commission](http://www.mhc.ie/latest/blog/tackling-cyber-bullying-the-law-reform-commission-calls-for-discussion)

## Recent Developments – Criminal Justice Act 2011

* Provides more extensive powers for Gardai in relation to ‘serious and complex’ offences
* S3(1) identifies relevant offences
* S15 – Application to District Court of order to make documents available
* Failure to provide passwords can be punished by a fine or prison term up to 12 months/2 years
* S18 – Reasonable presumption in relation to authorship or exchange of documents
* S19 – Offence to withhold information – max sentence – fine or 12 months/5 Years in prison (old offence of ‘Misprision’)
* No increase in resources for Gardai envisaged under the 2011 Act

## The Cybercrime Convention

* Signed by Ireland 2002
* Not yet implemented – recent [article](http://www.thejournal.ie/ireland-ratify-cybercrime-convention-734969-Dec2012/)
* Requirements of the Convention
* Access to computer system without right
* Illegal Interception
* Other Offences
* Procedural Law
* International Co-operation
* Extradition