IT Forensics – Week 9

CyberCrime Law

Overview

- From a European Perspective
- From an Irish Perspective
- Jurisdiction

Note

- **We will focus on the Irish and EU Law.**
- There will be no exam questions on US Law, this content is just to show how they deal with legislation in their jurisdiction

From a European Perspective

- Countries in Europe have fundamentally different legal systems, unlike the United States, which at least share a common framework.
- Europe has countries with a common-law system (the United Kingdom and Ireland) as well as countries with a civil-law system (most Continental countries), which have different traditions in the sources of law.
- Several initiatives are under way to increase consistency in legal frameworks among countries in Europe and to support law enforcement involving multiple jurisdictions.
- Fundamental differences between common-law and civil-law criminal justice systems remain.
- Two supranational bodies— the European Union and the Council of Europe (CoE)—influence cybercrime law in European countries, creating unique challenges for harmonization and for dealing with this topic

European and National Legal Frameworks

- The Council of Europe(CoE) launched the most comprehensive initiative with the Convention on Cybercrime, but the EU moves beyond that in some respects in an effort to better harmonize legislation in its member states
- The CoE is a pan-European international body with 47 member states, focusing on human rights, democracy, and the rule of law. For cybercrime, the Convention on Cybercrime stands out.
- Apart from CoE member states, other countries can accede to this convention as well.
- In addition to the Cybercrime Convention, some other instruments make up the European cybercrime legal framework, such as the Additional Protocol to the Cybercrime Convention on racism through computer systems and the Lanzarote Convention on the protection of children against sexual abuse

CoE Convention on Cybercrime

- In 2001, 26 member countries convened in Budapest and signed the Council of Europe Convention on Cybercrime to create “a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international cooperation”
- The COE Convention on Cybercrime represents an aspirational policy document, a country that ratifies the Convention commits to putting in place a legislative framework that deals with cybercrime according to Convention requirements.
- Within this commitment, each country is given discretion in relation to the full scope, say, of a criminal offence, by defining its particular elements of dishonest intent or requiring that serious harm be done before an offence is deemed to have been committed.
- CoE Cybercrime: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

CoE Convention on Cybercrime

- The Convention on Cybercrime entered into force on July 1, 2004, and its status as of November 2016, is that it has been signed by 50 States and including the United States of America .
- Another 17 from all regions of the world had signed it or been invited to accede.
- Concerned by the risk of misuse or abuse of computer systems to disseminate racist and xenophobic propaganda, the member states of the CoE and other State Parties to the Convention on Cybercrime agreed on an additional protocol to the Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems on January 28, 2003.
- That protocol entered into force on March 1, 2006, and (as of Feb 2021) has 68 signatories, 65 of whom have ratified it. Source: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

CoE Convention on Cybercrime

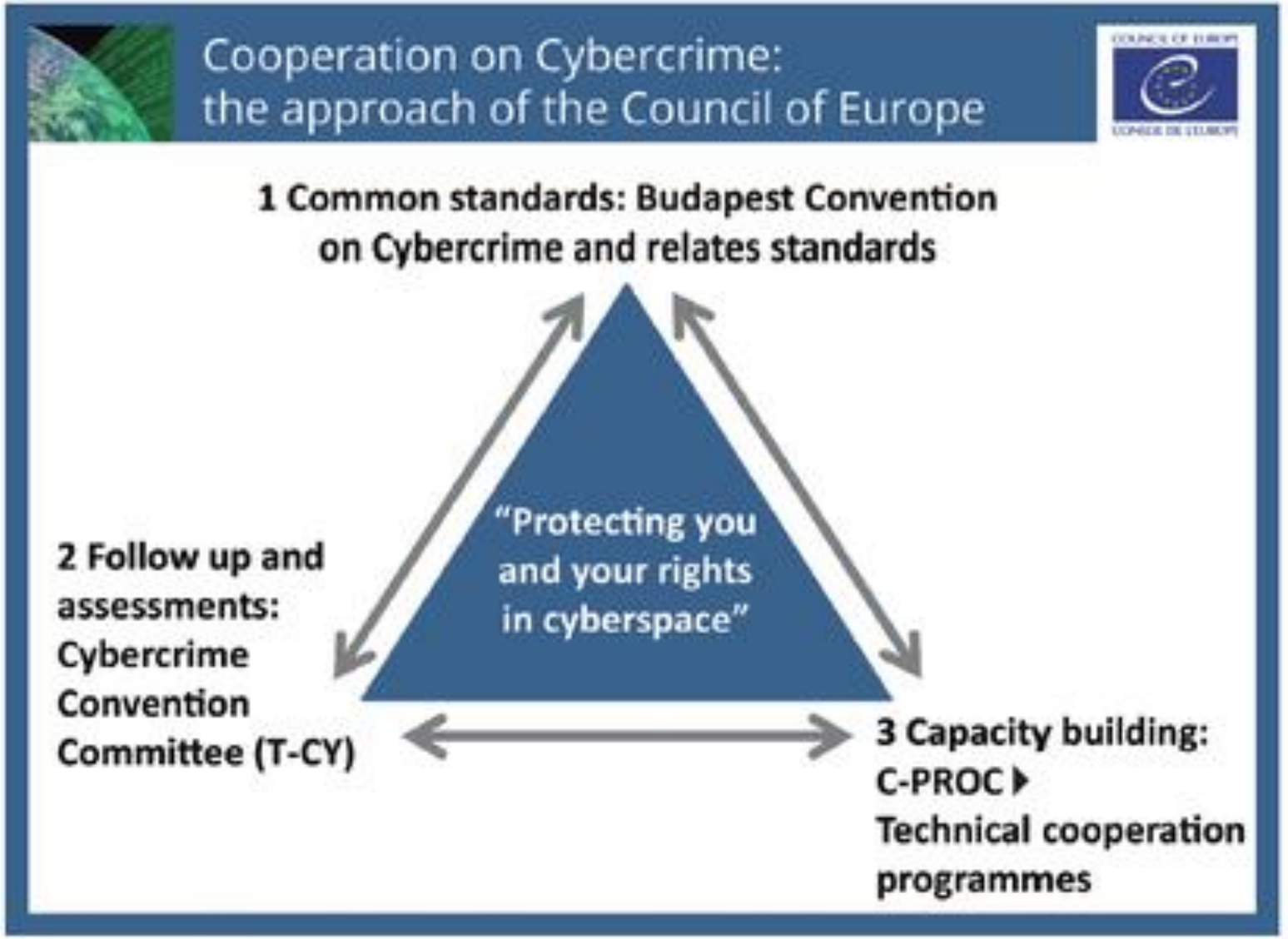
- The Budapest Convention is a criminal justice treaty that provides States with
  - (i) the criminalization of a list of attacks against and by means of computers;
  - (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and
  - (iii) international police and judicial cooperation on cybercrime and e-evidence.
- The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.
- The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.
- https://www.coe.int/en/web/cybercrime/the-budapest-convention

Coe Convention on Cybercrime

- These States that currently amount to 68, together with ten international organisations (such as the Commonwealth Secretariat, European Union, INTERPOL, the International Telecommunication Union, the Organisation of American States, the UN Office on Drugs and Crime and others), participate as members or observers in the Cybercrime Convention Committee.
- This Committee assesses implementation of the Convention by the Parties, and keeps the Convention up-to-date.
- Current efforts focus on solutions regarding law enforcement access to electronic evidence on cloud servers.

Capacity Building

- The need for a broad agreement on capacity building was stated in February 2013 by the United Nations Intergovernmental Expert Group on Cybercrime and by the European Union in its Cybersecurity Strategy.
- In October 2013, it was the focus of the Global Cyber Space Conference in Seoul, Korea.
- The European Union and the Council of Europe followed up immediately and in the very same week signed their agreement on the joint project on 'Global Action on Cybercrime' (GLACY), while at the same time, the Council of Europe decided to establish a Cybercrime Programme Office (C-PROC) for worldwide capacity building in Bucharest, Romania.
- The creation – at the subsequent Global Cyber Space Conference (Netherlands, April 2015) – of the Global Forum on Cyber Expertise was a further logical consequence.
- By August 2016, C-PROC managed a series of projects – including several joint projects with the European Union – covering the Eastern Partnership region (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) or South-Eastern Europe and Turkey (the project 'iPROCEEDS' is targeting proceeds from crime online).


Cooperation on Cybercrime:
the approach of the Council of Europe
1 Common standards: Budapest Convention on Cybercrime and relates standards
"Protecting you and your rights in cyberspace"
2 Follow up and assessments: Cybercrime Convention Committee (T-CY)
3 Capacity building: C-PROC ▸ Technical cooperation programmes

Computer Integrity Crimes

- The Council of Europe Convention on Cybercrime introduces the following five offenses against the confidentiality, integrity, and availability of computer data and systems:
  - Illegal access, that is, intentional access to the whole or any part of a computer system without right (Article 2)
  - Illegal interception, being the intentional interception without right made by technical means of nonpublic transmissions of computer data to, from, or within a computer system (Article 3)
  - Data interference, that is, the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right (Article 4)
  - System interference, being intentionally seriously hindering without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (Article 5) and
  - Misuse of devices, that is, the production, sale, procurement for use, import, distribution, or otherwise making available of a device or password or access code with the intent that it be used for the purpose of committing any of the offenses established in articles 2-5 (Article 6).

Computer Assisted Crimes

- Computer-assisted crimes are traditional crimes in which the computer is “merely” a tool.
- The EU Council Framework Decision on combating fraud and counterfeiting of noncash means of payment directs member states to take necessary measures to ensure that two types of conduct—relating to computer use—are criminal offenses when committed intentionally, they being
  - offenses related to computers (article 3): performing or causing a transfer of money or monetary value and thereby causing an unauthorized loss of property for another person, with the intention of procuring an unauthorized economic bene t for the person committing the offence or for a third party, by
  - introducing, altering, deleting, or suppressing computer data, in particular identification data without right, or
  - interfering with the functioning of a computer programme or system without right.

Computer Assisted Crimes

- Offenses related to specifically adapted devices (article 4): the fraudulent making, receiving, obtaining, selling, or transferring to another person or possession of
  - instruments, articles, computer programmes, and any other means particularly adapted for the commission of counterfeiting, or falsification of a payment instrument for it to be used fraudulently;
  - computer programmes the purpose of which is the commission of any of the offense described under Article 3.

Content Related Crimes

- Content Related Crimes are similar to the computer-assisted crimes in that they relate to traditional offenses and that computers are tools rather than targets, but they differ from them in that it is the content of data rather than the result of an action that is the core of the offence.
- The only content-related offence that the parties involved in drafting the Convention could agree upon was child pornography.
- The other major candidate—racism—was not acceptable to the United States to include in the Convention, given the thrust of the First Amendment.
- As a consequence, racism was transferred to an Additional Protocol to the Convention, which parties can decide to sign at their own discretion.

Laws affecting CyberCrime
-
Irish Perspective

Irish Legislation - History

- For several years it was noted that the Law in Ireland had limitations in dealing with computer crime.

- The main areas were:
  - Criminal Damage Act 1991
  - Criminal Justice (Theft and Fraud Offences) Act 2001
- These were not designed specifically to deal with computer crime.
- This had an impact on policing of computer crimes.

Irish Legislation – History (types of crimes)

- Unauthorised access (Criminal Damage Act 1991)
- The criminal damage act made a distinction between computer hacking (intended to cause damage) and unauthorized access. "Looking around" was not to be considered an offence as it is just a breach of confidentiality. (two exceptions: Official Secrets Act 1963 and Data protection Act 1988)
  - **5.**—(1) A person who without lawful excuse operates a computer— accessing of data.
  - (a) within the State with intent to access any data kept either within or outside the State, or
  - (b) outside the State with intent to access any data kept within the State,
  - shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.

Irish Legislation – History (types of crimes)

- Dishonest operation (Criminal Justice (Theft and Fraud Offences) Act 2001)
  - *"9.—(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence."*

Irish Legislation – History (types of crimes)

- Creating a false instrument (Criminal Justice (Theft and Fraud Offences) Act 2001)
  - *25.—(1) A person is guilty of forgery if he or she makes a false instrument with the intention that it shall be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person.*
- Eg. Username and password entered falsely into a computer system.
- Looking at misuse of verification etc.
- Closely linked to the Electronic Commerce Act 2000

Irish Legislation – History (types of crimes)

- Information Theft (Criminal Justice (Theft and Fraud Offences) Act 2001)
- Historically Irish Law did not specifically deal with any offence of the theft of Information.
  - *4.—(1) Subject to section 5, a person is guilty of theft if he or she dishonestly appropriates property without the consent of its owner and with the intention of depriving its owner of it.*
- Dependent on the interpretation of:
  - Property
  - With the intent of depriving its owner of it.

Irish Legislation – History (types of crimes)

- Official Secrets Act (Official Secrets Act 1963)
  - *"official information" means any secret official code word or password, and any sketch, plan, model, article, note, document or information which is secret or confidential or is expressed to be either and which is or has been in the possession, custody or control of a holder of a public office, or to which he has or had access, by virtue of his office, and includes information recorded by film or magnetic tape or by any other recording medium;*
- Offers protection to official information that is not available for unofficial information.

Irish Legislation – History (types of crimes)

- Data protection offences
  - Data Protection Act 1988 (Data protection act 1988)
  - Data Protection Act 2003 (2006 amendment). (2003)
- Relating to the processing of information
- Unauthorised access

Irish Legislation – History (types of crimes)

- Scams or advanced fee fraud
- Damage to data
- Extortion
- Passive hacking
- Distributed denial of service attacks
- Possessing anything with intent to damage property

Criminal Justice Act 2011

- Came into effect 9th August 2011
- Gave Gardai more extensive powers to investigate ”Serious and Complex” Offences

Scope of the 2011 Act

- Section 3(1) of the 2011 Act brings a number of relevant offences within its ambit, among them Section 9 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the “2001 Act”) and Sections 2, 3 and 4 of the Criminal Damage Act 1991 (the “1991 Act”).
- Section 3(2) provides that the Minister may, by order, specify as a relevant offence, any arrest able offence relating to criminal acts involving the use of electronic communication networks and information systems or against such networks or systems or both
- it does not solve the problem that an offence has to be rendered arrest able before it can also be designated as reportable, a problem when Irish authorities have historically had difficulty keeping up with the apparently boundless imaginations of cyber criminals when applied to developing new varieties of IT fraud and cybercrime.

Key Provisions of 2011 Act

- 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 particular documents or described documents available or to give information for the purposes of the investigation of a relevant offence.
- In the case of documents being handed over under this section which are illegible or inaccessible, the court order may also stipulate that any relevant access or passwords be given.
- Failure to provide passwords can be punished by a fine or prison term of up to 12 months on summary conviction or 2 years on indictment.

Key Provisions of 2011 Act

- Requiring passwords is a significant power, given that without the key the lock remains unopened. 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.

New Legislation

- The National Cyber Security Strategy 2015 – 2017
  - Promised new legislation
  - This is an implementation of EU Directive 2013/40
- New Act: The Criminal Justice (offences relating to information systems) Act 2017. (view)
  - Took effect 12th June 2017
  - Creates a number of very specific criminal offences
  - Strict penalties, aimed at tackling the use of ransomware and other cyber security threats

The Criminal Justice (offences relating to information systems) Act 2017

- Accessing information system without lawful authority, etc.
  - 2. A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure shall be guilty of an offence.
- Interference with information system without lawful authority so as to hinder or interrupt its functionality
- Interference with data without lawful authority
- Intercepting transmission of data without lawful authority
- Use of computer programme, password, code or data for purpose of the commission of any of the above offences

The Criminal Justice (offences relating to information systems) Act 2017

- Act strengthens the power of investigation for the Gardaí.
- District Court can issue search warrants where Gardaí have reasonable grounds to suspect a crime has occurred under this Act.
- The new cybercrime offences are reportable offences under Schedule 1 of the Criminal Justice Act 2011.

Gardaí access to passwords

- “A Garda will only have the power to require someone to provide a password in relation to devices found when carrying out a warrant to search a place for evidence of an offence. A search warrant can only be obtained where there are reasonable grounds to suspect that there is evidence of an offence at the place,”

Gardaí access to passwords

- Under the GENERAL SCHEME OF GARDA SÍOCHÁNA (POWERS) BILL we can see the exact wording:
- https://assets.gov.ie/137505/620ea206-de91-4bb3-97b1-0e0209b3ecf8.pdf
  - (search for password) then (search for encryption)

- https://www.iccl.ie/archive/a-handy-guide-to-the-phone-snooping-powers-of-the-garda-siochana-ombudsman-commission-gsoc-and-an-garda-siochana/
- https://www.thejournal.ie/gardai-phone-bill-password-5780057-Jun2022/

Gardaí access to passwords

- Paragraph (e) of the General Scheme of Garda Síochána (Powers) Bill implements the recommendations of the Law Reform Commission that a person executing a search warrant should have certain powers in relation to the persons present at the place. It also includes the power to require a person to give passwords, and to produce material in a visible and legible form.
- Without the password it would be virtually impossible to get access to a device within a reasonable time frame. Some phone devices reset to factory default if the password is entered incorrectly a number of times. eg. iphone: Erase data after 10 failed passcodes (https://support.apple.com/en-au/guide/iphone/iph14a867ae/ios)

Questions