Information and Communication Technology Law

Lecture Title: Implications of IT on legal processes (I)

Diploma in Law (Malta)

Lecturer: Alexia Valenzia

Date: 30 April 2025

Legal Considerations

- **Data Privacy & Cybersecurity**
  - Biometrics
  - Big Data
  - Wearable computers
  - ‘Internet of Things’
- **Intellectual Property**
  - Copyright
  - Database rights
  - Trade secrets
  - Open-source software
- **Net Neutrality**

BOV goes dark after hackers go after €13m

Bank of Valletta says clients' funds are safe

- Hackers broke into its systems and moved €13 million into foreign accounts
- Hackers sought to make international transfers to banks in the UK, US, Czech Republic and Hong Kong. The transfers were blocked within 30 minutes and the banks alerted.
- Reversing such transactions is no easy feat.

https://www.youtube.com/watch?v=IoaPIu5uSl0

Cybercrime Statistics

"Globally, 323,972 internet users fell victim to phishing attacks in 2021. This means half of the users who were a victim of cyber crime fell for a phishing attack. This is despite Google's cyber security measures blocking 99.9% of phishing attempts from reaching users." AAG, The Latest 2025 Cyber Crime Statistics (Updated April 2025)

"*With an average of $136 lost per phishing attack, this amounts to $44.2 million stolen by cyber criminals through phishing attacks in 2021*". AAG, The Latest 2025 Cyber Crime Statistics (Updated April s2025)

Europol's Internet Organised Crime Threat Assessment (IOCTA) (14 September 2023) - Cybercrime is becoming more aggressive and confrontational
https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Cybercrime Prevalence

- Network and information security (NIS) policy making and investment have evolved rapidly, especially since 1999:
  - The ‘Millenium Bug’ or Y2K which led to a complete inventory of computing inside large organisations, often for the first time since the deployment of PCs in the mid-1980s
  - DoS attacks beginning in 2001 against Yahoo! and eBay
  - Business continuity planning in the wake of the 9/11 attacks

Legal Frameworks Surrounding Cyber Security

Malta does not have a specific law which regulates cybersecurity. Accordingly, several laws govern different aspects of cybersecurity, and such laws include both primary and secondary legislation.

EU:

- NIS Directive – NIS II
- EECC
- GDPR
- DORA
- Cyber Resilience Act

NIS 2 Directive

- Adopted by the European Parliament and the Council on 14 December 2022.
- The review of the NIS Directive was carried out in response to the increased cybersecurity threats resulting from the ever-accelerating digitalisation (especially in the context of the COVID-19 pandemic).
- The NIS 2 Directive is intended to address the limitations of the previous NIS Directive and to make it suitable for current and future needs.
- Among the changes introduced by means of the NIS 2 Directive is the expansion of the scope of application to include new sectors based on their importance in terms of societal and economic activities within the internal market. The added sectors include, but are not limited to, entities operating in the sectors of health, public administration, manufacturing, and social media platforms
- The NIS 2 Directive entered into force on 16 January 2023. As with other Member States, Malta had until 17 October 2024 to transpose the provisions of the NIS 2 Directive into Maltese law. SL 460.41 was published on 8 March 2025

EECC

- The purpose of the European Electronic Communications Code (EECC) Directive was to revise and consolidate the directives forming part of the EU telecommunications regulatory framework, on which the domestic legal system for telecommunications is based.

- Among the objectives of the EECC is to promote the interests of EU citizens by maintaining the security of networks and services. As defined in the EECC itself, 'security of networks and services' refers to the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of those networks and services themselves, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those networks or services.

EECC

- The ECNS Regulations deal with security under Part VII. In particular, the ECNS Regulations are concerned with security incidents and require undertakings providing public electronic communications networks or publicly available electronic communications services, or gateway operators, to take certain measures to appropriately manage the risk involved and to ensure a level of security appropriate to that risk, so that the incidence of security incidents is prevented or minimised. The ECNS Regulations also state that an undertaking providing publicly available electronic communications services over public electronic communications networks must undertake all necessary measures to ensure the maximum availability of such services in the event of a catastrophic network breakdown or circumstances of force majeure.

DORA

- DORA consolidates and upgrades the regulatory framework on digital operational resilience for financial entities with a view to ensure that financial entities have the capability to withstand, respond to, and recover from cyber and other ICT risks and disruptions, which would help preserve the stability and integrity of the EU financial market. DORA lays down requirements concerning the security of network and information systems supporting the business processes of financial entities, including requirements on:

    - ICT risk management;
    - reporting of major ICT-related incidents;
    - testing of ICT systems, controls, and processes;
    - information and intelligence sharing between financial entities; and
    - contracts concluded with ICT third-party service providers.

- DORA has a broad coverage to include nearly all financial entities (with the exception of those listed in Article 2(2) thereof), but the application of certain rules depends on the size and overall risk profile of the financial entity, and the nature, scale, and complexity of its services, activities, and operations. DORA shall become applicable on 17 January 2025.

The Cyber Resilience Act

Scope:

- products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules

Requirements

- Security requirements
- Vulnerability handling requirements

Free movement

- Only if compliance with requirements

High risk AI systems

- Conformity with CRA → Deemed in compliance with accuracy and robustness requirement of AI Act

Critical Products

Obligations

Manufacturers

- Ensuring compliance with requirements
- Cybersecurity risk assessment
- Documenting relevant cybersecurity aspects
- Reporting

Importers

- Placing on market only if conformity with regulation
- Corrective measures if product is not in conformity

Distributors

- not placing on the market if reason to believe that conformity is not achieved
- Ensuring that corrective measures are taken if necessary

Cyber Resilience Act: Assessment and Enforcement

Conformity

- In specific cases presumed
- Technical documentation
- Conformity assessment

Market Surveillance

- Evaluation if believed that product carries risk

Penalties

- non-compliance with essential requirements: up to 15.000.000€ or 2.5% of annual worldwide turnover
- Non-compliance with other measures: up to 10.000.000€ or 2% of annual worldwide turnover

What Constitutes 'Cybercrime'?

- There is no official definition of 'cybercrime' however, it is widely understood as being the facilitation of traditional criminal activity (be it organised or otherwise) through the use of computer systems.

- More novel means of computer crime may only be committed through digital means (such as DDoS attacks), which only came about as computer systems became more advanced, facilitating the scale and speed at which such crimes may be carried out.

- Malta is a signatory to the Budapest Convention on Cybercrime (Council of Europe Cybercrime Convention) and has therefore implemented the provisions therein within our Criminal Code (Chapter 9, Laws of Malta).

Types of Cybercrime

- using botnets—networks of devices infected with malware without their users' knowledge—to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection
- creating "back doors" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets
- creating online fora to trade hacking expertise
- bulletproof hosting and creating counter-anti-virus services
- laundering traditional and virtual currencies
- committing online fraud, such as through online payment systems, carding and social engineering
- various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse
- the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.

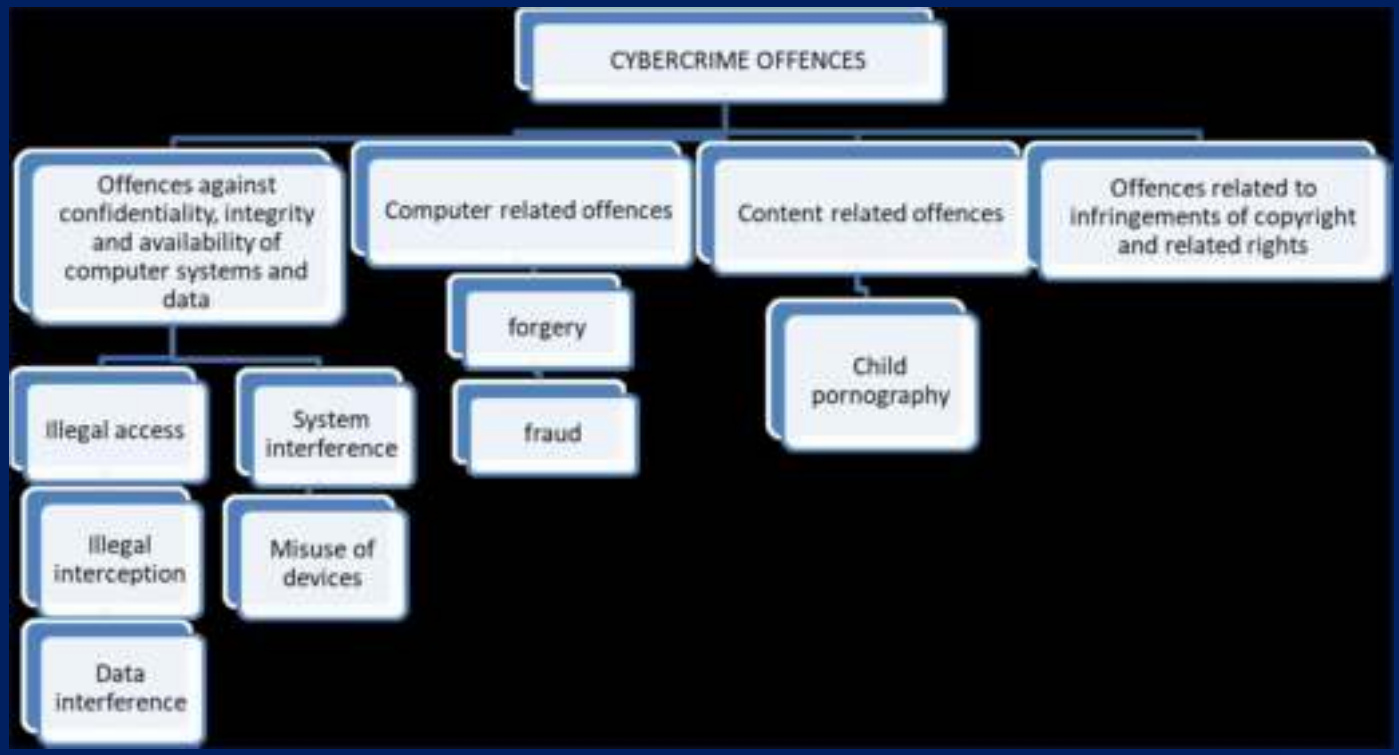
https://www.youtube.com/watch?v=P6x4GhjDVHY

What is Cybercrime from a legal perspective?

- The Budapest Convention classifies cybercrime into 4 categories:

1. Offences against confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offences
4. Offences related to infringements of copyright

The Budapest Convention on Cybercrime



European Commission – Legal Aspects of Digital Forensics

Criminal Offences Under Maltese Law

- The old legal maxim “actus non facit reum, nisi mens sit rea” means that the criminal act alone does not amount to guilt, it must also be accompanied by a ‘guilty mind’.

- The general principle within the field of Criminal Law is that **three** distinct elements must co-exist for there to be a crime:

1. The Legal Element
2. The Material Element
3. The Mental Element

The Legal Element

- *"Nullum crimen sine lege"* means that an action may only be deemed as a criminal offence if it is prohibited by a specific law.

- Prior to the amendments relating to computer misuse & extreme/child pornography within our Criminal Code, attributing a particular crime to an offence was tedious and challenging as our law did not cater for (now) illegal activity conducted through digital means.

- Previously, there was a valid (legal) argument to be made that an offence could not be committed as Maltese Law did not define an action (such as hacking) as a criminal offence.

The Material & Mental Elements

- The Material element is the *"actus reus",* which means the commission of an offence by the person to be held liable.

- In certain cases, a purposeful omission could also give rise to criminal liability, provided that the other formalities are present.

- The Mental element is the *"mens rea"* or the 'guilty mind' with which the act is done. This is a procedural necessity and cases are dismissed typically on this basis, as it is particularly difficult to prove a persons' malintent.

Various Forms of Cybercrime

- Computer Fraud
- Phishing
- Hacking
- DDoS
- Malware
- Trojans and other viruses
- Ransomware
- Sexploitation
- Cyberterrorism
- Child Pornography
- Infringement of intellectual property rights

Computer Misuse

- Malta's Criminal Code (Chapter 9, Laws of Malta) regulates computer misuse through Articles 337B-337H
- Based on the UK Computer Misuse Act and the Budapest Cybercrime Convention
- Drafted and defined broadly to account for 'all' scenarios

Computer Misuse

- Definitions
- Unlawful access to, or use of, information
- Misuse of hardware
- Commission of an offence outside Malta
- Offences and Penalties
- Search and Seizure

Interpretation – Art. 337B(1)

- "**computer**" means an **electronic device** that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, **software** and communication facilities that are connected or related to a computer in a **computer system** or **computer network**;

- "**computer network**" means the interconnection of communication lines and circuits with a computer through a **remote device** or a **complex** consisting of two or more **interconnected** computers;

- "**computer output** " or "**output**" means a statement or a **representation of data** whether in written, printed, pictorial, screen display, photographic or other film, graphical, acoustic or other form produced by a computer

Interpretation – Art. 337B(1)

- **“computer software**" or "**software**" means a computer **program, procedure or associated documentation** used in the **operation** of a computer system

- "**computer supplies**" means punched cards, paper tape, magnetic tape, disk packs, diskettes, CD-roms, computer output, including paper and microform and any storage media, electronic or otherwise

- "**computer system**" means a **set of related computer equipment, hardware or software**

Interpretation – Art. 337B(1)

- "**function**" includes logic, control, arithmetic, deletion, storage, retrieval and communication of data or telecommunication to, from or within a computer;

- "**supporting documentation**" means any documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

Unlawful access to, or use of, information – Art. 337C

A person who without authorisation does any of the following acts shall be guilty of an offence

a) **uses** a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

b) **outputs** any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

c) **copies** any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

d) **prevents** or **hinders access** to any data, software or supporting documentation;

e) **hinders or impairs** the operation of any system, software or the integrity or reliability of any data.

Unlawful access to, or use of, information – Art. 337C

f) **hinders or interrupts** the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data in accessible;

g) **takes possession** of or makes use of any data, software or supporting documentation;

h) **installs**, **moves**, **alters**, **erases**, **destroys**, varies or adds to any data, software or supporting documentation;

i) **discloses** a password or any other means of access, access code or other access information to any unauthorised person;

j) **uses another person's** access code, password, user name, electronic mail address or other means of access or identification information in a computer;

k) **discloses** any data, software or supporting documentation unless this is required in the course of his duties or by any other law;

Unlawful access to, or use of, information – Art. 337C

l) **intercepts** by technical means, non-public transmissions of data, to, from or within an information system or a computer system, including electromagnetic emissions from an information system or a computer system carrying such computer data;

m) **produces, sells, procures for use, imports, distributes, possesses or otherwise makes available** a device, including a computer program, designed or adapted primarily for the purpose of committing any of the acts in paragraphs (a) to (k) or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

What does acting without authorisation mean? Article 33C(2)

A person is deemed to be acting without authorisation if he is not duly authorised by an entitled person.

… but what is an entitled person?

A person is deemed to be entitled if the person himself is entitled to control the activities defined in (a) – (k) or in article 4(a) or 4(b) of this Sub-Title.

Misuse of Hardware – Art. 337D

Any person who, **without authorisation**, does any of the following acts shall be guilty of an offence:

a) **modifies** computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

b) **takes possession** of, damages or destroys a computer, computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairs the operation of any of the aforesaid.

Commission of an offence outside Malta – Art. 337E

- If any act is committed outside Malta which, had it been committed in Malta, would have constituted an offence against the provisions of this Sub-title, it shall, if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta, be deemed to have been committed in Malta.
- Notwithstanding sub-article (1), if the offence is committed partially outside Malta and which had it been committed in Malta constituted an offence contrary to the provisions of this Sub-title, said offence shall be deemed to have been committed in Malta.

Offences and Penalties – Art. 337F

1. Fine not exceeding €23,293.73, or imprisonment not exceeding four years, or both such fine and imprisonment.

2. When such offence is directed towards the Government or a public authority or hinders/hampers any public service or utility, the penalty shall be a fine ranging from €500 to €150,000 or imprisonment ranging from three months to ten years, or both such fine and imprisonment.

Subsequent offences shall be fined at a minimum of €5,000.

Offences and Penalties – Art. 337F

3. The increased penalty range shall also apply when committed by an employee to the prejudice of their employer.

4. If a person produces any material or acts in preparation or furtherance of an offence, the same punishment for that offence shall be awarded.

5. Accomplices or any person who aids or abets the commission of an offence shall be equally liable.

6. The burden of proof lies on the party alleging authorisation and this burden shall not be considered to have been discharged with the mere uncorroborated testimony of the person charged (hence further proof is required).

Search, Seizure & Retention – Arts. 337G & 355P

- **337G**: The Minister may, for the purposes of this Sub-title, by regulations prescribe:

a) the manner in which the Police may search computers, computer systems or computer supplies and seize data or software stored therein;

b) procedures and methods for handling evidence that is in an electronic form.

355P: The Police, when **lawfully** on any premises, may seize anything which is on the premises if they have **reasonable grounds** for believing that it has been obtained in consequence of the commission of an offence or that it is evidence in relation to an offence…and that it is necessary to seize it to prevent it being concealed, lost, damaged, altered or destroyed.

Computer Data & Retention – Arts. 355Q & 355S

- 355Q: The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.

- 355S: (1) Anything which has been lawfully seized by the Police may be retained so long as is necessary in all the circumstances.

- (2) Without prejudice to the generality of the aforesaid, anything lawfully seized by the Police under this Code may be retained for use as evidence at the trial or for forensic examination or any other aspect of the investigation, or in order to establish the thing's lawful owner.

- (3) The Commissioner shall provide for the proper custody of anything seized.


Break

Extreme Pornographic Content

- Amendments to the Criminal Code following UK's promulgation of new laws regulating extreme pornographic content.

- Article 208D prohibits the distribution, display in a public place, manufacturing, printing, or otherwise making or introducing in Malta any 'extreme' pornographic images. The penalty for any of these offences is imprisonment for a term between **18** months to **3** years or to a fine between €**3,000** and **€6,000**, or to both imprisonment and a fine.

- This also applies to any person who "keeps" or "acquires" such images. Therefore, the downloading and storage of such images is an offence under Maltese Law.

What is Considered ‘Extreme’?

- S.L 9.05 states that a pornographic image will be deemed ‘extreme’ if it portrays, in an explicit and realistic way:
  - an act which takes or threatens a person’s life.
  - an act which results, or is likely to result, in a person’s severe injury.
  - rape or other non-consensual penetrative sexual activity.
  - sexual activity involving, directly or indirectly, a human corpse.
  - an act which involves sexual activity between a person and an animal or the carcass of an animal.

Pornographic Content Depicting Minors

- Articles 204D(c) and (d) of the Criminal Code impose a term of imprisonment between **five** and **ten** years upon whosever:

  (c) knowingly causes, for sexual purposes, a person underage to participate in real **or simulated** sexually explicit conduct or exhibition of sexual organs, **including through information and communication technologies**, or

  (d) knowingly **attends a pornographic performance** involving the participation of a person under age.

- The inclusion of 'simulated' sexually explicit content covers scenarios involving deepfakes or pseudo-images which depict minors.

- For the purposes of the Code, visiting websites containing pornographic material constitutes viewing of a 'pornographic performance'.

What about Viewing?

- Downloading and storing explicit material on one's device is a clear case of possession. However, there is a divide between scholars on whether 'viewing' constitutes simple 'possession' for the purposes of the Criminal Code.

- Every time a new web page is viewed, many of its images and videos are downloaded to a folder on the hard drive. These temporary internet files or **cache files** are used by the computer to load web pages more quickly in the future.

- Depending on the amount of internet use and the space allocated for these files, these images and videos can remain on a hard drive for months or years.

What about Viewing?

- Courts will likely adopt the ‘intent-based approach’. This means that factors such as search history, numerous website visits and the duration thereof play a key role in determining the accused’s intent to view the indecent material.

- The UK previously utilised a ‘classification system’ ranging from 1 to 5, to determine the severity of the explicit image ([2003] EWCA Crim 2766 ‘Regina V. Oliver & ORS’).

- In the case of [2004] EWCA Crim 449 ‘Regina V. Beaney’, multiple files depicting sexual activities with minors were retrieved from one of the computer’s directories, having been automatically stored by the browser.

What about Viewing?

- The previously mentioned system has been replaced by a categorisation system, as pictured below (UK Sexual Offences Sentencing Guidelines). This has been implemented to streamline the complexities of overlapping levels.

	Possession	Distribution*	Production**
Category A (previously levels 4 and 5)	Possession of images involving penetrative sexual activity	Sharing images involving penetrative sexual activity	Creating images involving penetrative sexual activity
	Possession of images involving sexual activity with an animal or sadism	Sharing images involving sexual activity with an animal or sadism	Creating images involving sexual activity with an animal or sadism
Category B (previously levels 2 and 3)	Possession of images involving non-penetrative sexual activity	Sharing of images involving non-penetrative sexual activity	Creating images involving non-penetrative sexual activity
Category C (previously level 1)	Possession of images of erotic posing	Sharing of images of erotic posing	Creating images of erotic posing

* Distribution includes possession with a view to distributing or sharing images
** Production includes the taking or making of any image at source, i.e. the original image
Making an image by simple downloading should be treated as possession for the purposes of sentencing

What about Viewing?

- The UK Sexual Offences Sentencing Guidelines were amended in 2022 to address child sexual offences in cases where no sexual activity takes place or the targeted child does not exist.

- Where no sexual activity takes place, the court should identify the category of harm on the basis of the sexual activity intended by the offender and then adjust the starting point downwards to reflect what actually happened.

What about Accidental Viewing/Downloading?

- Using certain software, computer forensics experts may retrace the steps that led to a file being downloaded. Often, a link can be found between innocent search terms and the name of the illegal file. If the file was acquired through a peer-to-peer (P2P) network, an expert can survey the shared folder and find that the contents are otherwise legal.

- Certain file properties will indicate when the file was created (or downloaded), when it was last changed, and when it was last accessed. If an expert finds that the file was created and last accessed at the same time, it is quite possible the user was unaware of the file because it was never accessed after the initial download. If the file was last accessed within an hour of the creation timestamp, this suggests the user deleted it shortly after download.

- The retrieval of internet browsing history can also establish a user's online habits **(digital fingerprint)** and create a timeline of events leading up to an accidental download.

Grooming

- Article 208AA of the Criminal Code imposes imprisonment not exceeding **six** years on any person over eighteen years who "meets or communicates on one or more occasions" with a person under the age of **sixteen** years, intending to do anything to or in respect of the said person which would constitute one of the offences prohibited under Articles 204, 204A-D or 208A.

- The above includes scenarios where the offender proposes to meet or arranges to meet the victim.

- The formal requirement is that the alleged offender should not "reasonably believe" that the person they are meeting is over the age of sixteen.

Questions

1. What is the most common expression used in literature to describe crimes committed using technology? (**Computer crime**/ **Cybercrime**/ **Online crime**/ **Digital crime**)
2. Is there a precise definition for the above that is agreed upon in the international law? Mention 5 different forms of such.
3. Which of the following is a requirement for establishing a criminal offence under the principle of legality? **(Customs**/ **Written Rules**/ **Habit**/ **None)**?
4. What are the elements which need to be proven for an act to be considered as a criminal offence?
5. What are the legal terms for the abovementioned elements?
6. How are these elements linked? Are there any procedural pitfalls?

The Role of Local and Inter-state IT Crime Authorities

The Maltese Cybercrime Unit

- The Cyber Crime Unit is a specialised section within the Malta Police Force set up in 2003. It primarily provides technical assistance in the detection and investigations of crime where the computer is either the target or the means used.
- Not limited to criminal acts associated with technology, but extends to investigations of more traditional offences such as fraud, threats and other serious crimes.
- Also assists in the ansalysis of digital evidence seized in connection with investigations as well as in identifying persons who are committing crimes over the internet.
- Works closely with a number of international organisations and law enforcement agencies.

EUROPOL and EC3

- The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU.

- At operational level, EC3 focuses on the following types of cybercrimes: **cyber-dependent crime, child sexual exploitation** and **payment fraud.**

- The support provided also extends to tackling criminality on the dark web and alternative platforms.

J-CAT

- The Joint Cybercrime Action Taskforce (J-CAT) was launched in September 2014. Located at Europol's European Cybercrime Centre (EC3), it helps fight cybercrime within and outside the EU.

- Intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint **identification**, **prioritisation**, **preparation**, **initiation** and **execution** of **cross-border investigations** and operations by its partners.

- J-CAT Members include EU and Non-EU States, and their tasks includes:
  selecting the most relevant proposals;
  sharing, collecting and enriching data on the cases in question;
  developing an action plan, which is led by the country that submitted the selected proposal;
  going through all the necessary steps to ensure the case is ready to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification of the required resources, and the allocation of responsibilities.

Combatting Cybercrime

- Legislation enacted as a deterrent to commit the offence with proportionate punishments depending on the severity of the crime. The issue with this is that laws merely act as a deterrent and defendant may use certain procedural technicalities to delay the judgment or have it dismissed.

- There is also the principle of 'innocent until proven guilty' within criminal law, which means that all elements of the criminal offence must be proven by the alleging party. This causes delays to any sentence being adjudicated upon, particularly due to the compilation of 'best evidence'.

- Legislation imposing industry standard certification (particularly for cybersecurity) is one way of combatting the 'hands-on' attacks such as hacking, which relates to the physical and virtual infrastructure implemented by organisations.

- Educating the public to safeguard their digital identity and minimise their digital fingerprint could combat against cybercrime such as ransomware, malware, fraud and identity theft, as attackers typically target older or less educated individuals who would not be as tech-savvy.

Combatting Cybercrime

- Increased collaboration and information sharing between supervisory authorities may dampen the effect and longevity of any crimes as assailants will be found more effectively.

- Jurisdictional issues may be remedied through multi-lateral agreements between contracting states, setting a definite jurisdictional framework and defining which Court will have jurisdiction, so as to speed up the litigation process in cross-border situations.

Legal Challenges

- Identifying which activities can be considered illegal ("*Nullum crimen sine lege*").
- Enacting criminal law relating to computers and the Internet.
- Identifying the offenders and victims of the crimes.
- Enforcement, particularly focused on **preservation of evidence**, **jurisdiction** and the **international aspect** of the crimes.
- Concept of "adequate punishment" and how to quantify damages in the digital age.

Any Questions?

Diploma in Law (Malta)