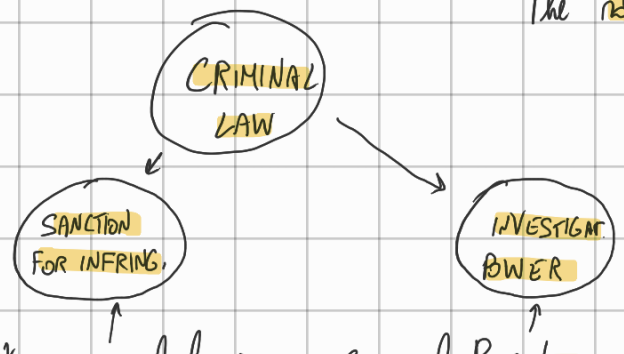
1) Both CyberCrime and CS can be seen as related to CIA of inf. and communication tech.

2) The role of criminal law in protecting comp. sys and networks



Substantive criminal law (1) vs Criminal Procedure

(1) Provides all the offenses and defines the behaviors to be punished be penalties, and is the part of criminal law that provides the fines.
(2) Determines the investigative power of criminal law actors.
(1) legislators should develop new offences designed on technological domain. On the other hand, for (2), legislators should update procedures to encompass technological aspects for cyber and regular crime. Tech. evolution calls for this.

3) Cybercrime (United national Cybercrime (2) Strategy: guidebook on how to develop a (1)). (2021)
Cybercrime and CS are both converging in the protection of tech and critical assets.
CS encompasses laws suited to protect CIA of sys. (technical and administrative dimension)
CC defines the offenses that when committed against sys can lead to punishment.
CC: offenses committed against comp. data, computer data storage media, computer sys, service providers.

4) CS has a preventive perspective. CC: reactive perspective. Only when behaviors are considered as crimes by substantive criminal law, then criminal procedures can be applied.
This gets even more problematic in case of international cooperations. Offences may be different and put an obstacle to cooperate with foreign authority.
6) As a conclusion: CC and CS share a common goal: combating CC, preventing CC and ensuring CS and Cyber Resilience. (reducing opportunities for CC, ensuring business continuity, Mitigating harmful effects of cybercrime, reducing incentive for cyber offenders, facilitating collection of evidence, enhancing legality of businesses and risk management initiatives)

7) EU CS strategy (2020): tackling CC, the EU noticed that due to dependence on online tools, attack surface for Cyber Criminal has increased, plus, investigation of nearly all types of crime has a digital component.

Tackling CC effectively is a key factor in ensuring CS; deterrence cannot be achieved through resilience alone but also requires identification and prosecution of offenders. ①,② important!
↳ Plus the def. of offences! Laws need to be effective!

INTERLUDE: The crime perspective was the first to emerge. A preventive perspective for CS came after.

8) Computer: "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution" (US Dep. of Justice '84) *

Cybercrime Typologies: • Computer as the target / tool / as a repository of evidence of a (traditional) crime

* + Internet → Cybercrime, encompassing all criminal activities perpetrated in cyberspace.
Violations related to a computer + criminal activities enabled by cyberspace (so IT connected)
Destruction of a computer for example was a computer crime. ↳ Copyright violations, for ex.

9) Distinctive features of CC: CC laws should take into account global dimensions, anonymity, real-time, new vulnerabilities, speed, de-territorial, scale.
↳ transcends physical / geographical boundaries

10) At international levels, we have bodies like Council of Europe (no part of EU):
• Council of Europe Recommendation (1989) on computer-related crime, Council of Europe Budapest Convention on Cybercrime (2001) and it's additional Protocols (Xenophobia and Racism--)
↳ This is countries coming together to share concerns. This helps facilitating cooperation. Plus it is not authority of the EU. Those are conventions to try and reach harmonization.
Draft United Nations convention against cybercrime (2024)
• EU level (limited): Directive 2013/40 on attacks against information systems. ①
Regulation 2023/1543 on EPO for electronic evidence in criminal proceedings.

• National level: L 90/2024. ②

① EU has limited competence in criminal laws. Only indirect competences like directives. But in general only for serious and cross-border matters, so computer crime (as stated in TFEU) falls under this.

Regulation of 2023 about investigation. The first time EU developed a framework for investigations involving providers too, so important step for this. [still appealing to the computer crime legal basis] [but also on principles of mutual cooperation exc.]

② Divided in CS and CC parts. *of sys and data

11) Council of Europe recomm (1989): a lot of states of the council decided to gather to tackle the challenge of comp. crime. [NEED FOR HARMONISATION AND INTERNAT. COOP]

- Legal interests to be protected: (first time they addressed the fact that we have new interests such as CIA* to be protected), including also classical legal interests.
  → Report on Computer-related crime elaborated by the European Committee on Crime Problems (90).
  In Italy, technology is seen as a way to attack some old legal interests but in old ways; not shared by IT. They tried to adapt this view in the traditional interpretative framework.

[WORKING DEFINITION: computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data] + new sources of evidence

12) (2001) Council: first international treaty on crimes committed via the internet and other computer networks.

- Strategy to pursue a common criminal policy aimed at the protection of society against cybercrime: 1. adopt of an appropriate legislation (to consider changes brought about by the digitalization); 2. fostering international co-operation (given globalisation of computer networks); 3. Need for cooperation between states and private industry in combating CC.

GOAL: deter actions directed against CIA of computer systems, networks and computer data as well as their misuse by providing for the criminalization of such conduct.

13) Chapter 3: measures to be taken at national level

Section 1: Substantive criminal law:

Title 1, 2: offenses against C/A of computer data and systems and computer-related offenses

3: Content related offences. (classical crimes).

4: Offences related to infringements of copyright and related rights.

14) For title 1: several offences: Art. 2: illegal access: (each party shall adopt measures to establish as criminal offenses under its domestic law, when intentional, the access to the whole or any part of a comp. sys without right)

15) Art. 3: Illegal interception: each party shall adopt measures to establish as criminal offences under its domestic law, the committed intentionally, the interception without right, made by technical means, of non public transmissions of computer data to, from or within a computer system.

15) Art. 4: Data interference: punishing damaging, deletion, deterioration, alteration or suppression of computer data without right. For data to be damaged, there weren't proper measures to tackle those crimes: not a physical damage.

Art. 5: Sys interference: [...] criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. [offenses are specific to avoid wide interpretation by law enforcement and judges.]

16) Art. 6 Misuse of devices: [...] when committed intentionally and without right:

1. the production, sale, procurement for use, import, distribution or otherwise making available of:
   - a device designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
   - a computer pw, access code, or similar data by which the whole or any part of a computer sys is capable of being accessed, with intent that it be used for the purpose of committing offences pre-defined.
2. the possession of an item of the ones described.

One of the most contested provisions! Critique: no direct negative effect, it shouldn't be this strict,

Exemption: member states could exclude the application of this article when not for the purpose of committing an offence, such as for the authorised testing or protection of computer systems [Not implemented by Italy]

Article 7: Computer related forgery: each party shall adopt measures to establish as criminal offences under its domestic law, when committed intentionally and without rights, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.

Article 8: Computer related fraud: each party shall adopt measures to establish as criminal offences under its domestic law, when committed intentionally and without rights, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

→ COMPUTER RELATED OFFENCES (computer-assisted crime) → the others (Title 1, computer integrity crime)

21) Article 83 TFEU states that EU parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. Those areas of crime include computer crime.

22) 2013 directive was related to attacks on IS: society is highly and increasingly dependent on such systems. Ensuring an appropriate level of protection of IS should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to CC.

IS form part of the critical structure of Member States of the Union.
It has become apparent that measures against cyber attacks should be complemented by stronger criminal penalties reflecting the gravity of such attacks.
Article 1: directive establishes minimum rules concerning definition of criminal offences and sanctions in the area of attacks against IS. Also aims to prevent offences.
Structure of the directive is very similar to the convention [Art. 3, illegal access to IS, 4: illegal system interference, 5: illegal data interference; 6, illegal interception, 7 tools used for committing offences]

↳ Illegal data interference is the offence associated to data breaches. GDPR takes into account accountability of the controller, the perpetration is investigated by looking Article 5 as a reference. [deleting, damaging, deteriorating, altering or suppressing computer data on an IS, or rendering such data inaccessible, intentionally and without right].
PART 2: Recent development: at national level (90/2024 law) was the first law in 20 years on CC that did not reference European or international agreements.

34) The general assembly of the UN in 2019 adopted a resolution, tackling how ICT could contribute to a rise in level and complexity of crime. For this, there's the need of cooperation and coordination.
Draft of 2024, after 5 years of negotiation, came to the conclusion of promote measures to prevent and combat cybercrime, cooperation, technical assistance to police authority.

36) Related to crimes, we have illegal access, interceptions exc. very similar to the ones seen before + adding on cyber-enabled crimes non consensual dissemination of intimate images, laundering of proceeds of crime (as new, also offenses related to child abuse).
38) We see also preventive measures in next chapters.

45) National law 90/2024 : divided in CS and CC approach: traditional approach* + specificities (and evolution) of cybercrime (specific provisions to incriminate ransomware; coordination between national Response and (criminal) Law Enforcement)

↳ update offences in the CC realm

* with respect to phenomena characterized by growing social alarm: increase of penalties and extension of the "emergency" procedural regime → symbolic criminal law?

↳ traditional approach by increasing penalties.

46): Basically law 90 added a new paragraph in art 629 Penal code, extension offence, to address cyber extension with penalties higher in this case.

47) Pros: explicit prohibition by law is important as a deterrent and gives investigative power to law of enforcement, and defining it as a standalone is important to make things smoother for punishment.

Cons: can be ineffective, for ex, in case of other countries and absence of cooperation.