CYBERSECURITY

- EXAM PERIOD SS 2020 -

Lecturer: Athina Sachoulidou, Assistant Professor, NOVA School of Law

July 6, 2020

Section A: Multiple-Choice & Short Open Questions

(10 out of 20 points | 0,5 point per question)

Justify all your answers with up to three sentences. Mere reference to the CoE Cybercrime Convention 's provisions or to other respective legal provisions is not considered a fully justified answer.

1. The CoE Cybercrime Convention distinctly regulates jurisdiction for satellites registered in a country's name.

a. True

b. False

False. The CoE Cybercrime Convention does not explicitly regulate jurisdiction for satellites, in its article 22 (1) that pertains to the prescriptive jurisdiction in the convention, it only encompasses the territoriality principle a), the Flag principle (itself a sub-principle of territoriality) applicable to only ships (art.22(1)(b), and aircraft (art.22(1)c) and nationality principle (art. 22(1)(d). Still, article 22(4) does not limit the member states to extend jurisdiction on other basis, and under international public law, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, in its article VII and VIII extends the states' jurisdiction to all objects that they place in outer space that are registered accordingly.

2. Extradition rules apply irrespective of the so-called dual-criminality

a. True

b. False

False. Extradition is a very complex topic in international public law and is mostly regulated in bilateral treaties between states that stipulate the requirement of dual-criminality to be effective – this raises a lot of problems concerning the international law principle Aut Dedere Aut judicare, as a state cannot be forced to extradite if it doesn't prosecute, with the basis of not being a crime under its legislation. The recent push of multilateral agreements that lift the dual-criminality requirement is notable, but it's a very limited phenomena, mostly pertaining to EU Law.

3. The company 'Blue Apple' is a web hosting firm providing bulletproof hosting services allowing its customers to upload videos of sexual-abusive character. 'Blue apple' can be considered as:

a. facilitator

b. money mule

c. perpetrator of online image-based sexual abuse

The company Blue Apple can be considered a facilitator - their role is to help bridge the gap between the underworld (those that commit the primary crime) and the upperworld (those less savvy, that act more as "consumers" of the unlawfull acquired material) cybercriminal network. Hosting bulletproof web-storage where its customers may upload and share illegal content is considered to be one of the exemplary possible role of a facilitator.

4. Bitcoin as a criminal tool is not absolutely safe.

a. True

b. False

True. While it helps to mask one's identity and avoid using the traditional banking services which are frequently monitored for money laundering and terrorism financing, Bitcoin, just like many other public permission-less cryptocurriencies has many flaws that make it not safe even for cybercriminals. The Bitcoin protocol is immutable and stores all the information pertaining the transfers of funds between wallets, so it is still possible to track the origin and destination of currency transfers. Plus, many of the cruptocurrencies exchange sites are very untrustworthy, as some have even been shutdown in the past leading to millions of dollars in cryptocurrencies to be lost.

5. The study of online criminal groups' structure is solely of criminological interest.

a. True

b. False

False, it is very useful to apply these studies' findings in the real world context, both for online and offline crimes, in law enforcement and to better regulate cybercrime.

6. Hackers often consider laws governing online activity as unfair. Which neutralisation technique is to find behind such a claim?

The techniques of neutralisation, as proposed by Matza and Sykes in 1957, have as an objective to explain the reasons used by individuals to avoid moral culpability for their criminal actions and thus avoid the negative sanctions of society if they can prove that criminal intent was lacking. When hackers refer that the laws governing online activity are unfair and shouldn't be followed nor enforced, they are motivated by cynicism towards what they view as the "system". It's the Condemnation of condemners Technique, as they are distrustful of authorities, justified by the unlawful activities carried out by the law enforcement agencies themselves and the persecution of whistleblowers.

7. Limiting the availability of someone's computer resources by sending lots of packets pertains to the field of cybercrime.

a. True

b. False

A DDOS attack is indeed a cybercrime, and under the Cybercrime Convention could be considered a system interference attack, article 5, as it is the massive transmission and inputting of large amounts of data with the objective of seriously hinder the function of a computer system that is unable to process those large amounts of data.

8. Mike is a former bank employee and, since he was fired, he has been providing stolen bank data of his former clients online. His behaviour can be classified as:

a. online fraud

b. data interference

c. misuse of devices

Under the Cybercrime Convention, the behaviour carried out by Mike is a misuse of devices – he had authorisation for the access of those systems that was revoked when he was fired and thus was unlawfully accessing personal data of his former clients and he was distributing that data online – it fits with article 6(1)(a)ii) "(…)when committed intentionally and without right", (1)(a) "the production, sale, procurement for use, import, distribution or otherwise making available of:" (ii) "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,".

9. General Strain Theory better describes phenomena of cyberviolence.

a. True

b. False

True. GST as many flaws in describing many financial motivated crimes, but when the subject is the phenomena of cyberviolence - hate crimes, cyberbullying, cyberdating abuse and sexual harassment and assault, it is a better theory to explain the motivations of the offender than the Routine Activity Theory. As explained by Agnew, the GST has an unique focus on the mediating role of negative emotions, so it leads to more expressive crimes in which the individual's feeling of frustration and rage motivated him/her to enact harm as a valued end in and of itself against another person.

10. Esel is a politician of Turkish origin based in Germany. Following some diplomatic incidents between the two countries, anonymous citizens formed online groups to attack and abuse Esel online. She is threatened to be viciously killed together with all her Turkish muslim family members. Some of these individuals claim that Esel has been transferring confidential information to the country of her origin since she was elected as MP in Germany. What cybercrime is committed?

Esel seems to be the target of online hate speech and hate crimes, motivated by her nationality, ethnicity and religion – she is a politician of Turkish origin, her family is muslim and she is accused of typical far-right conspiracies of not being actually a german citizen serving the public office of MP, but serving a foreign state. Interestingly, it seems that even thou she is a woman, she is not being the target of sexual harassment. This is not an instance of cyberbullying because she isn't being targeted as an individual, but because she is a member of a different origin, ethnicity and religion than the offenders.

11. Member States are obliged to introduce criminal sanctions to deal with serious breaches of the GDPR.

a. True

b. False

False, the GDPR as only administrative fines (that are very heavy) for its non-compliance, and doesn't have any provision which obliges the Member States to introduce criminal sanctions for its violation. Still,

member states are free to introduce those criminal sanctions in some instances - Recital 152 and article 84 of the GDPR established that Member States have the power to, where necessary due to lacking harmonisation rules, implement a system providing for effective, proportionate and dissuasive penalties – and so they can determine the nature of those sanctions as either criminal or administrative in their domestic law.

12. CoE Convention codifies computer-supported crimes.

a. True

b. False

False, the convention only codifies some offences: offenses against the confidentiality, integrity and availability of computer data and systems; Computer related offences (has in all offences – in case of which the computer is used to facilitate their commission); Content related offences (Child pornography); and Offences relating to copyright infringement and related rights; There are still many more criminal offences that are computer-supported offences, because computer-supported offences aren't crimes themselves, it's a concept used to describe offences where the use of computer is an incident aspect of the commission of crime, possibly affording evidence of said crime.

13. The so-called upskirting can be classified as:

a. sexploitation

b. harassment

c. sexual voyeurism

Upskirting is usually classified as sexual voyeurism, being criminalised in several jurisdictions already. It fits with the definition usually used for this typology "cases in which individuals who create/share/distribute intimate images have no intention that the victim will discover that their images have been shared", and the main motivations of the offenders is usually sexual gratification or a crude sense of humor. It's usually not meant to force another into the commission of sexual acts (sexploitation) or to harass and inflict harm in the victim

14. Happy Gardeners is a website, on which you can find instructions about how to take good care of your plants at home. The respective online publications contain hyperlinks leading to other websites containing nude photos of 16-year old girls. What cybercrime is committed?

Nude photos of 16 year old girls is considered child pornography in most jurisdictions, and its possession in a computer system or on a computer data system is considered a crime – possession of child pornography art. 9(1)(e) of the Cybercrime Convention.

Still, there are many variables at play here that could lead to not constituting a crime at all. First, some jurisdictions have an age of consent as low as 16, which could lower the threshold to constituting child pornography – article 9(3). Second, are the photos sexual in nature (art. 9(2) (a to c) "a) minor engaged in sexually explicit conduct;" "b) a person appearing to be a minor engaged in sexually explicit conduct;" "c) realistic images representing a minor engaged in sexually explicit conduct") ? If not, if it is for example, educational material in medical school for example, the representation of minors will probably not be sexual in nature and it isn't Child Pornography. Third, the happy Gardeners is a website and it isn't actually in possession of said nude photos, it has hyperlinks to other websites with said content. In some jurisdictions, this isn't possession and could be considered distribution of child

pornography. In some jurisdictions, having hyperlinks is not an act of distribution or transmission, but this is an extremely controversial topic – it varies a lot depending of the domestic law. Forth, these hyperlinks could have been published in the HG's website without their consent and their knowledge. It could be a user posting, infringing on the terms of service, or it could have been a hacker that published those hyperlinks in the website.

15. Online sexual abuses are not any different compared to the offline ones in terms of their phenomenology.

a. True

b. False

False

16. Mere hacking is punishable under the CoE Cybercrime Convention

a. True

b. False

True, under article 2 of the Cybercrime Convention, illegal access, even mere hacking is punishable. As it is explained in the Cybercrime Convention Explanatory Report, paragraphs 44 to 47, the mere act of intentional hacking is itself illegal access.

17. Policeman X taps the computer of his colleague Y to prove that his is involved in a bribery network. Is X committing a cybercrime?

a. Yes

b. No

Yes. Unless Policeman X is carrying out a lawful investigation, according to procedural law and it has met all legal requirements, that could demand a warrant signed by a judge – policeman X could be committing illegal interception, article 3 of the Cybercrime convention, and maybe, depending on how he installed the tapping on his colleague's computer, he could also have committed illegal access, art. 2.

18. Jon owns ZYY graphic-design software company. His competitor, XXP graphic-design software company, has recently launched a new programme, which was selected to be installed across all the urban design authorities of the country. Jon, who cannot understand how this product is any different from the one designed by his company, has a good friend working at XXP. While having a beer with him, he finds a chance to steal his professional credentials. Two days after this encounter, Jon 'breaks in' the XXP using his friends' credentials to both unlock the door of the building and to log in one of the desktops there. He checks the details of the programme, and he leaves the building being deeply disappointed, since XXP's product was actually of superior quality compared to the one designed by him. He did not copy any data as initially planned. Are Jon's actions relevant in terms of the CoE Cybercrime Convention?

a. Yes

b. No

Yes. By accessing the computer in XXP, Jon's actions can be classified as Illegal access of a computer system, article 2 of the Cybercrime convention, as he didn't have the authorisation to have access to the whole or any part of said computer, and used stolen credentials for it. The fact that he did not copy any

data as initially planned could be irrelevant, because even if the domestic law applicable to Jon is of one of the member states of the Cybercrime Convention that added the requirements of 1) infringing security measures and 2) intent to obtain computer data or other dishonest intent; his actions would still be considered illegal access, since he stole credentials to have access and he had that intention to copy data when he committed the crime – the fact that he regretted his actions once confronted with the data does not clear him of the fact that he indeed had that intention at the time of the illegal access – in the end, it could be considered as a mitigating factor on his sentence, but does not clear him of the crime.

19. Cybercrimes are exhaustively regulated at EU level.

a. True

b. False

False, there are a lot of matters related to cybercrime already regulated by EU law through directives and regulations, but there is still a lot of room for improvement and there are several proposals from the commission that haven't been approved yet. These EU law is mostly complimented by the European Convention on Cybercrime, from the Council of Europe, which is a different international organisation that also has as members, the EU member states.

20. The cybercrime of sextortion can be only committed by perpetrators known to the victim.

a. True

b. False

False. Complete strangers to the victim can and have committed the cybercrime of sextortion after illegally obtaining material to use to force their victims into compliance.

Section B: Open questions (10 out of 20 points)

Question 1: Explain in what ways can cybercrime interfere with territorial jurisdiction (2.5 points).

Territorial jurisdiction is the classic and most traditional form of jurisdiction by states recognised in international customary law, but even with such a long history, it still has cases in the physical world where it is challenging to correctly assert and determine.

The Territorial jurisdiction is derived from the simple idea that a state should have the exclusive and absolute criminal jurisdiction over the persons, things and events that occur within its territory – its "*logical that a state in whose territory a crime is committed should assume jurisdiction over it*"[1]. When discussing pluri-localized incidents, where the crime isn't practiced wholly in one state's territory, a conflict of jurisdiction arises, over who's state is actually competent to resolved it. To solve this issue, a concise formulation was constructed in the first half of the 20th century, the doctrine of constructive presence. This doctrine, presented in the 1935 Harvard Draft Convention, allows more than one state to exercise criminal jurisdiction by postulating that when a crime is committed in whole or in part within a territory or a said state, it may exercise his jurisdiction.

[1] Gbenga Oduntan, Sovereignty and Jurisdiction in the Airspace and Outer Space Legal Criteria for Spacial Delimitation, Routledge 2012, page 42 para. 1

This formulation gave rise to two sub-principles: the subjective territorial (the state in which the offender started committing the offense has jurisdiction) and the objective territorial principle (the state where the offence was completed or had its effects will have jurisdiction over the conduct, the offender will be considered has if he had been present there, when all the constituents' elements of the crime are put together). In the hallmark Lotus Case, the Permanent Court of International Justice referred that to invoke the objective territorial principle to extend its jurisdiction, a State may only need to assure that the alleged criminal offense produced some effects in its the territory.[2]

With the rise of the Internet and Computers, and the subsequent emersion of cybercrime, the idea of applying territorial jurisdiction onto these criminal offences was challenged due to the pluri-localization of many actions part of the same criminal conduct. In the 1990s, some scholars even defended that cyberspace should be regulated has its own space, that it was a mistake to apply the domestic law of several states to this reality where distance does not actually exist. The plurilocation nature of these crimes could be seen has it follows, A and B and accomplices, A is in state y, and B is in State x, and they are attacking the servers of company U, registered in state O, but the servers are in the States L and K, and their attacks were actually rerouted by several other servers and proxys localized in many more states. The effects of the hacking occurred in all states where company U has offices. Where did criminal action began and its affects occurred? And there are several other states that could potentially claim that effects occurred in their territories.

Trying to stablish a link between the actions and a place where they occurred became very difficult, not just because of the subject matter – many jurisdictions will classify the same action differently ontologically, some as different criminal offences, others not – but also poses a major hurdle on the procedural side of law enforcement.

For a single action, using the 2 sub-principles that I explained above, subjective and objective territoriality, many states are capable claiming adjudicative jurisdiction on the basis of previously stablished prescriptive jurisdiction, which can lead to conflicts over which state will prosecute the offender, if there is the need to extradite the offender trials in absentia in criminal matters are usually prohibited), and after the trial, where he/she will serve the sentence.

And this is only referring to the territorial jurisdiction, leaving out the other 4 principles according to Jan Klabbers: Nationality Principle; Protective (or security) Principle; Passive Personality Principle and Universality Principle. Cybercrime poses many challenges to jurisdiction.

Question 2: Provide two examples indicating that the international approach to cybercrime challenges the so-called fragmentary character of criminal law (2.5 points).

The fragmentary character of criminal law is an undeniable reality, but there still are many instruments that have been created to harmonise the legislation and action of different states to increase international cooperation in law enforcement. The first example is the Cybercrime Convention of 2001, which harmonised the legislation on cybercrime (codifying several cybercrimes and tacking even child pornography), the procedural norms to combat, investigate and prosecute cybercrime and other crimes (evidence), more than 60 different states. The second example is the European Arrest Warrant, a framework decision in the EU - 2002/584/JHA Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States –

[2] Gbenga Oduntan, Sovereignty and Jurisdiction in the Airspace and Outer Space Legal Criteria for Spacial Delimitation, Routledge 2012, page 43 para. 6

that lead to a faster a better system for the cooperation, capture and extradition of criminals among the EU member states. There is also the European Cybercrime Centre, created by the Europol, to combat cybercrime.

Question 3: Many scholars define cyberterrorism as a distinct category of cybercrime referring to the variety of actions pertaining to it. Elaborating on this opinion by taking into account the EU reaction to the so-called terrorism threat (2.5 points).

The EU as acted to combat Cyberterrorim in multiple fronts: through harmonisation of the member states legislation on criminalising terrorism and related offences; through this harmonisation, criminalise not just terrorism acts and its direction, but also the recruitment and training (the mere providing of instruction for the making explosives, guns or hazardous substances,…) ; the preparatory acts such as travelling to commit crimes; the public provocation to commit terror attacks; combating online propaganda and networking; stricter rules on banking and money transfer services to fight money laundering and terrorism financing,.. There was a shift towards the criminal repression of terrorism in the stages prior to any objective risk against people, cities and other legally protected interests. See Council Decision 2008/615/JHA that incorporated the PRUM Convention into EU Law, Directive (EU) 2018/843, Directive (EU) 2017/541, as some examples in EU Law.

There were also the EU agreements with 3rd countries on the exchange of information on terrorism, with Canada, the USA, and negation of Mexico

Question 4: Why does the codification of online hate speech in terms of a cybercrime pose significant regulatory difficulties (2.5 points)?

The codification of online hate speech raises a lot of concerns from different sides of the political spectrum, religious and non-religious backgrounds and different cultures due to one very fundamental concern: the codification of online hate speech is defining a limit to freedom of speech, of expression, itself a fundamental right recognised in many instruments of international law and the constitutions of many states.

What is considered hate speech varies a lot depending on the culture of a person and the context of a situation. Even the most agreed upon definitions lack substantial clarity – they need to be broad enough to encompass the many realities and forms in which hate speech manifests, but the use of (mostly) undefined concepts pose to met this end also poses a problem to its applicability to specific cases.

Then, there are a lot of justified fears that regulating hate speech could lead to censorship that strangles freedom of expression – weaponised for ill purposes, supressing minorities, satirical artists and political adversaries. Even in the European Court of Human Rights there were cases of hate speech that were deemed as actually being within freedom of expression (judgment of 7 December 1976 'Handyside v the United Kingdom').

Still, even with all these challenges, regulating hate speech must be a priority, since it's a major problem online, which has been growing exponentially and further radicalising many people into the far-right, especially in Europe.

It's necessary to establish a fair and independent authority with means to investigate and sanction hate speech online, and its major tool – disinformation. Hate Speech is difficult to define in many cases, but is consequences and harms are very visible.

The Framework Decision 2008/913/JHA of 28.11.2008 on combating certain forms and expression of racism and xenophobia by means of criminal law is step in a good direction, just like self-regulation of many companies and

social networking sites, that have either committed (or been pressured by the public at large and advertisers into committing) to combat hate speech. Still, should we trust the billionaires in Silicon Valley to take the role of defining what is or not hate speech? It also seems very problematic.

Good luck!