Chapter 15

Legal Aspects of Cyberwarfare and Cyberwarfare Crimes: Criminal Law Analysis and Dilemmas in the Legal System of the European Union

Miha Šepec

Abstract

The goal of this chapter is to analyse the substantive legal content regarding cyberwarfare attacks and crimes, present procedural measures of cooperation in criminal matters for the purpose of prosecuting such crimes, and examine European Union's (EU) institutions for cooperation in such criminal matters. It should be emphasised that cyberwarfare does not have a single, clearly established legal definition. In most cases, cyberwarfare attacks refer to forms of cyberattacks that are already known, and which most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are, thus, that it is connected with the army of an individual country, which then configures a military operation; and that the range and scope of the offence are significantly wider, as cyberwarfare attacks focuses on more important targets with significantly more repulsive motives, such as paralysing a country's national security via attacks on its infrastructure and technological centres. The focus of the legal analysis is placed on the EU legislation and United Nations (UN) conventions, with particular interest on the legal definitions of terms connected to cyberwarfare (e.g. cyberattack, cyber espionage, and cyber-spying), understanding in which legal documents these terms are defined, and if these documents are legally binding to EU Member States. The study proves that cyberwarfare attacks are treated

Miha Šepec (2024) 'Legal Aspects of Cyberwarfare and Cyberwarfare Crimes: Criminal Law Analysis and Dilemmas in the Legal System of the European Union'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 663–697. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_15

in the EU as crimes with a cross-border dimension of such nature and impact that they need special treatment, that is, they require a harmonising legislation at the EU level to prosecute such crimes more efficiently.

Keywords: Cyberwarfare, Cyberattack, Defence Policy, Legal framework, Criminal Law, European Union

1. Introduction

We currently live in the digital age, where humanity is becoming increasingly dependent on electronic information systems that regulate and control most of the tasks we perform. Computer systems are increasingly penetrating society and replacing human work. In the future, information technology is likely to completely change the views we have on law and legal doctrines regarding the functioning of society. Specifically, the invention that may bring about a drastic change in society and law may be the speculated development of a self-aware artificial intelligence (AI). The term AI was developed in 1956 by the American scientist John McCarthy When describing the science of engineering of intelligent machines.[1]

Computer information systems, similar to any major human invention, also have disadvantages, the most noticeable of which is its excessive dependence on information technology. Along with such invention also came new forms of criminal acts committed with the help of these information systems. Criminal acts have existed in the cyberspace since the beginning of its development, and despite being initially relatively simple, they have been becoming increasingly complex and multifaceted. Today, we discuss topics related to a new form of crime that connects information systems, the cyberspace, and digital technology, and is called cybercrime. This type of crime includes all emergent forms of criminal acts studied within the framework of criminal law theory.

Cybercrime is considered the fastest growing criminal phenomenon in the current world. Therefore, criminal law must follow its rapid development and adapt to the specifics of prosecuting cybercrime offences. To define the new acts associated with cybercrime, we must first have detailed and accurate knowledge of the trends and forms of criminal behaviour in information systems. In general, criminal acts of cybercrime are divided into three large groups:

1. *integrity-related crimes*, where the information system is the target of the attack;
2. *computer-related crimes,* where the information system is used as a tool or accessory to commit a crime (e.g. computer fraud);

1 McCarthy, 1990, pp. 226–236.

3. *content-related crimes*, where crime is linked to a certain digital content (e.g. child pornography).[2]

The term cyberspace was first used in 1984 by Gibson in his book Neuromancer.[3] He used the term to refer to a space in which computer hackers engage in "war" to obtain confidential data that does not exist in the physical world. Thus, the cyberspace looks like the real world, but is actually a computer-generated construct of abstract data. In 2001, with the introduction of the Council of Europe's Convention on Cybercrime,[4] the term cybercrime was finally established internationally as a term that refers to all forms of criminal acts committed in the cyberspace, and it is a term commonly used today in established literature.[5]

For as long as the human race has existed, we have known war, and it is an undeniable part of our history. In fact, if we consider our historical past, there is space for arguing that it has often been the first, or sometimes the sole, way to resolve intercultural, interracial, and interstate conflicts. Furthermore, ever since its advent, the military industry has constantly developed new warfare methods using the latest technologies and means available to humans, and digital information technologies are no exception to this rule. Actually, the accelerated development of these technologies is often a reflection of the development of the war industry. It is also clear that the dimensions that new information technologies bring to the military industry are unimaginable. Today, cyberwars and/or information wars are major threats to countries worldwide, and in terms of definition, information warfare represents actions aimed at achieving information superiority by attacking a country's information centres thereby weakening it. Barrett explained that we can speak of information warfare only when actions are carried out within the framework of a national military strategy, and when both offensive and defensive actions are involved.[6] In 1997, the author predicted that, in the future, information armament in wars would reach the same status as the strength and number of classic military units.[7] Today, we can affirm that his predictions have proven almost entirely true. It is practically impossible to imagine a modern army without a strong information department, and a prime example is featured in the US Army and its special unit for this purpose, named the Cyber Command. This Command is dedicated exclusively to information warfare and defence.[8]

Digital warfare can be carried out between states, paramilitary units, or when states participate only indirectly (e.g. providing financial, legal, or moral support

2 Wall, 2005, pp. 77–98.
3 Gibson, 1984.
4 Council of Europe, 2001, CETS No. 185.
5 Clough, 2010, p. 9.
6 For example, the actions of a group of hackers who attack and weaken an important information centre of the country cannot be called an information war if the hackers are not operating under the auspices of the state or the military.
7 Barrett, 1997, p. 168.
8 Available at: https://www.arcyber.army.mil/ (Accessed: 30 August 2023).

to perpetrators who attack the basic infrastructure of a rival state). Barrett further distinguished between information warfare (i.e. involving attacks on military and operationally important targets) and full information warfare (i.e. involving attacks on strategically important state targets coordinated by top military and state officials).[9]

Cyberterrorism is relevant in today's era, as it involves the use of information networks to damage or destroy critical state infrastructures (e.g. energy structures, transportation systems, and state leadership establishments). In cyberterrorism, this is done for political, religious, or ideological reasons, and with the aim of instilling fear in the public and influencing the actions of state authorities.[10] Cybercrime and cyberterrorism are not synonymous, as attacks in the cyberspace must have a terrorist component to be considered cyberterrorism. Specifically, the attack must inspire fear and terror, which may result in death or destruction on a larger scale, and must have political motives. Terrorists also use computer systems as means for their activities, such as propaganda, recruitment, data collection, and communication.[11]

There is no single definition of cyberwarfare, but at its core, it means using computer technology to disrupt or destroy an adversary's information systems and networks. These are actions in cyberspace that threaten key state infrastructure systems in the form of armed conflicts with destructive effects. Attacks on state infrastructure can threaten or destroy the country's fundamental processes, paralyse the economy, and tarnish the country's reputation; the consequences are manifested in monetary damages as well as bodily harm or death of victims. Attacks on military networks threaten classified information and communication systems, as well as military operations. Moreover, espionage undermines national security during peacetime and wartime, while also enabling the theft of sensitive information.[12]

Today, cyberwarfare is present in practically every military operation, and classic military operations now customarily overlap with cyber operations. The enemy infrastructure can be destroyed with conventional weapons, but it can also be crippled or destroyed by cyberattacks. An example of such a cyberattack was the Stuxnet worm attack in 2010, which was directed against Iran's nuclear facilities, particularly its uranium enrichment centrifuges.[13] Stuxnet caused physical damage to Iran's nuclear infrastructure by manipulating its industrial control systems. In 2015 and 2016, Ukraine's power grids were also targets of cyberattacks,[14] causing widespread power outages, demonstrating that cyberwarfare can paralyse or at least disrupt critical services and infrastructure, and can have devastating consequences for countries and civilians.

9 Barrett, 1997, p. 170.
10 Clough, 2010, p. 12.
11 Wimann, 2005, p. 132.
12 Digmelashvili, 2023, pp. 12–19.
13 *Struxnet*, no date.
14 *Cyber-Attack Against Ukrainian Critical Infrastructure*, 2021.

Considering that technology is constantly developing, and that an ever-increasing part of the world depends on modern technologies, the potential for cyberwarfare is extremely large. In the future, European Union (EU) Member States will have to invest heavily in information technology, in addition to standard military equipment, and traditional soldiers will begin to be supplemented by information-aware soldiers, whose profiles will be completely different. Physical fitness and training will not play as much of a role as intelligence, computing and hacking skills, computer awareness, and the ability to manage advanced cyber operations. Thus, as the world changes, so do the methods of warfare, and the law must follow these changes and legally cover the new forms of warfare.

As expressed by Karim A. A. Khan, Prosecutor of the International Criminal Court:

> Cyber operations are sometimes employed as part of a so-called "hybrid" or "grey zone" strategy. Such strategies aim to exploit ambiguity and operate in the area between war and peace, legal and illegal, with the perpetrators often hidden behind proxy actors. This calls for a whole-of-society response, drawing together distinct functions and capabilities to act in a coordinated way.[15]

In this chapter, we provide a legal introduction to cyberwarfare and related crimes, presenting the definitions and legal meanings of cyberwarfare. We also list the legal acts at the EU and United Nations (UN) levels that deal with cyberwarfare and its crimes. Moreover, this section delves into the criminal law aspects of cyberwarfare, considering that cyberwarfare attacks performed during war or even at peacetime are considered criminal offences by all EU countries. Furthermore, the EU procedural mechanisms for prosecuting cyberwarfare crimes and the EU institutions responsible for cooperation in criminal matters are all presented.

2. Substantive law on cyberwarfare and cyberwarfare crimes

The goal of this chapter is to analyse the substantive legal content regarding cyberwarfare crimes, delving into both EU legislation and UN conventions. We present legal definitions of terms connected to cyberwarfare, such as cyberattacks, cyber espionage, and cyber spying. The main research question is whether these acts are defined as criminal acts in the EU and in the criminal legislation of EU Member States. Here, we must point out the diversity of criminal legislation in EU Member States and the question of whether some offences should be legalised at the EU level.

15 Khan, no date.

The EU has already compiled a list of so-called EU crimes in numerous legal acts; however, the question remains whether as to whether cyberwarfare crimes are included in these catalogues. The dilemma also remains regarding EU criminal law and whether there is a need for a new European Criminal Code that includes cyber offences and cyberwarfare crimes.

At the outset, it should be emphasised that cyberwarfare has neither a single nor a clearly established legal definition. In most cases where the topic is approached, there is reference to well-known forms of cyberattacks that most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are that it is, first, connected with the army of an individual country (i.e. it is a military operation), and, second associated to a significantly wide range and scope of offence, as it attacks more important targets with significantly more repulsive motives – such as paralysing a country's national security via attacks on its infrastructure and technological centres. Therefore, for the purpose of this chapter, the term *cyberwarfare* will be used to describe cyber acts that compromise and disrupt critical infrastructure systems and which amount to armed attacks,[16] referring to attacks that intentionally cause destructive effects (i.e. death, physical injury to living beings, and/or the destruction of property). Only governments, state organs, and state-directed or state-sponsored individuals or groups can engage in cyberwarfare.[17]

The types of cyberwarfare attacks also vary according to the definition. For the purpose of this chapter, we categorise these attacks into the following: espionage (i.e. monitoring other countries to steal secrets), sabotage (i.e. harming state organisations or institutions), denial of service (also known as DoS) attacks to disrupt critical operations and systems, attacks that disable critical systems and infrastructure, propaganda attacks, economic disruption by targeting economic establishments, and surprise attacks in the context of hybrid warfare.[18] Importantly, no legal documents in the EU or UN directly address cyberwarfare, as the term has no clear legal definition. However, numerous legal documents can be used to address the topics of cyberwarfare and cyberwarfare attacks.

2.1. The UN Charter

Before a state engages in cyberwarfare, *jus ad bellum* (the right to use force) must be established, meaning that any kind of force must be legitimate and sanctioned by law. The rule of prohibition against the use of force is codified in Art 2 (4) of the United Nations Charter,[19] which states that a UN member state cannot threaten or use force against the territorial integrity or political independence of another state or in any way that diverges from the UN's purposes. Although Art.

16 Maras, 2016, pp. 10–20.
17 Ibid.
18 *Cyber Warfare*, no date.
19 *Charter of the United Nations and Statute of the International Court of Justice*, 1945.

2(4) does not use "armed" or a similar word, the question remains as to whether the article only prohibits military force and excludes non-military forms of coercion, such as economic sanctions or cyberattacks.[20] Given that the article is written in extremely general terms and that cyberwarfare attacks today represent a modern form of warfare, insisting on a position that completely rejects the possibility of cyberwarfare attacks being covered by Art. 2(4) is pointless. At the same time, it should be emphasised that force in the sense of Art. 2(4) in the context of cyberwarfare attacks can only be understood when the territorial integrity or political independence of a state is threatened by such attacks. Therefore, only serious military attacks that attack the very existence of the country are covered, and it is quite unlikely that the UN will condone only a cyberattack as a use of force according to Art. 2(4) of the UN Charter.

Meanwhile, according to Art. 51 of the UN Charter, countries can use self-defence as an exception to the prohibition against the use of force. This provision explicitly allows one state to use force in response to an armed attack by another state. It should be emphasised that cyberwarfare attacks can represent a form of self-defence against an attacker, and that such a defence must be necessary and proportional to the aggression. Another interesting feature of Article 51 is that it provides for the self-defence of a state only when the state is actually attacked by military forces – that is, when it is an armed attack, not when the state is attacked only by cyberwarfare attacks. However, denying the possibility of defending against cyberwarfare attacks would also be completely contrary to the UN ideology and the idea of a just war. There are thus two possible solutions, the first of which is we deny that cyberwarfare attacks are a form of modern armed warfare, do not regard them as a use of force in the sense of Art. 2(4), and it is not possible to use force to defend against such attacks according to Art. 51 of the UN Charter. Alternatively, and also a more modern solution, cyberwarfare attacks, when targeted at the territorial integrity or political independence of a state, can be considered a use of force according to Art. 2(4), and self-defence is possible against such a force according to Art. 51 of the UN Charter. According to the first solution, everything remains in a grey zone, and countries fight against these forms of attacks independently. According to the second solution, such attacks must be reported to the UN, where a solution is then sought within the framework of the UN Charter.

2.2. International Humanitarian Law: the Geneva conventions and Hague conventions

International humanitarian law is covered by the Hague[21] and Geneva Conventions,[22] which determine the fundamental rules of warfare and conduct prohibited in

20 *Use of force under international law*, 2024.
21 *The Hague Conventions*, 1890, 1907, 1954.
22 *The Geneva Conventions*, 1949.

every international armed conflict. The Hague Conventions deal primarily with the means and methods of warfare, the conduct of hostilities, and occupation, whereas the Geneva Conventions primarily govern the protection of war victims. The conventions, of course, do not mention cyberwarfare because it did not exist at the time these conventions were written. However, this does not mean that the general provisions of the conventions cannot apply to modern warfare. We believe that the conventions limit all forms of attacks towards civilians or civilian facilities, medical facilities, and other forms of war crimes if these attacks are conducted through classic military operations or cyberattacks.

A more complex question is whether cyber operations can trigger the application of international humanitarian law. International armed conflict 'exists whenever there is a resort to armed force between States'.[23] However, when is this point reached in situations involving cyber operations that do not physically destroy nor damage military or civilian infrastructure? This remains unclear. A potential solution would be the proposed hybrid model, which is derived from the established term for hybrid warfare,[24] and according to which cyberattacks can constitute a violation of Hague and Geneva laws when they are committed together with traditional war crimes, but not by themselves.

2.3. Rome Statute of the International Criminal Court

The International Criminal Court (also known as ICC or ICCt) is an intergovernmental organisation and international tribunal seated in The Hague, the Netherlands. It is the first and only permanent international court with jurisdiction to prosecute individuals for the most serious war crimes and crimes against humanity, as well as for crimes of genocide and aggression. It was established in 2002 with the multilateral Rome Statute,[25] which affords the legal basis for the functioning of the Court. The Court has its own problems, the main one being that most of the world's military superpowers (e.g. the USA, Israel, Russia, and China) have not signed the statute, so they do not recognise the jurisdiction of the International Criminal Court. However, almost all European countries are signatories.

The Rome Statute, in its Article 5, limits the jurisdiction of the Court to the most serious crimes against the international community. The Court has jurisdiction over the following crimes: (a) crimes of genocide, (b) crimes against humanity, (c) war crimes, (d) crimes of aggression.[26] Art. 6 of the Rome Statute defines the crime of genocide as acts committed with the intent of destroying a national, ethnic, racial, or religious group. Although killing a group with cyberattacks seems highly unlikely, deliberately inflicting on the group conditions of life calculated to bring about its

23 *Cyber Warfare: does International Humanitarian Law apply?*, 2021.
24 Weissmann et al., 2021.
25 *Rome Status of the International Criminal Court*, 1998.
26 *Rome Statute of the International Criminal Court*, 2002.

physical destruction, be it in whole or in part, is imaginable through attacks on basic life sustaining infrastructure (e.g. water and electricity). Cyberattacks can also be used in combination with traditional war crimes (i.e. hybrid model).

Crimes against humanity, after Art. 7 of the Rome Statute, refer to acts committed as part of a widespread or systematic attack directed at any civilian population. Most of the crimes against humanity are "physical" in nature (e.g. rape, murder, and enslavement); notwithstanding, if targeted at critical infrastructure for a population and thereby intentionally causing great suffering or injury to people, even cyberattacks could be a method of execution. It is important to note that such attacks must be part of a widespread or systematic attack on the population, and not just a singular attack against the national security of a country. Generally, cyberattacks are not defined as crimes against humanity. However, in combination with traditional war crimes (hybrid model), this would be possible.

Cyberattacks, when considering war crimes as defined in Art. 8 of the Rome Statute, are similar to crimes against humanity. Typically, cyberattacks on their own will not be defined as war crimes, but their combination with traditional war crimes (hybrid model) make their categorisation as such a possibility. War crimes must be committed as part of a plan or policy, or as part of a large-scale commission of, such crimes, and are grave breaches of the Geneva Conventions and of the laws and customs applicable in international armed conflict within the established framework of international law.[27]

The crime of aggression, as defined in Article 8 (bis) of the Rome Statute, refers to planning, preparation, initiation, or execution, by a person in a position where one can exercise effective control over or direct the political or military action of a state, of an act of aggression which, by its character, gravity, and scale, constitutes a manifest violation of the UN Charter. According to this definition, it is highly unlikely that a cyberattack by itself can be perceived as an act of aggression. This is because, first, it must be performed by a person in a specific position (military or state), and not by an ordinary individual or a hacker group. Second, because the act must be considered a violation of the UN Charter (para. 4 of Art. 2), where the standards are very high, in that the violation must be obvious in terms of its weight and scope. In light of these descriptions, it is very unlikely that the UN would regard cyberattacks as acts of aggression when they are conducted in isolation of other acts. However, it is possible that a cyberattack would accompany traditional war crimes, such as an unlawful war attack by one state on the integrity and sovereignty of another.

No provision of the Rome Statute specifically refers to cyberattacks or cyberwarfare, as this form of warfare was not yet present at the time the statute was drafted. However, it is entirely possible that cyberwarfare attacks will be covered in one of the already defined forms when the nature and scope of these attacks reach the level of intensity otherwise achieved by classic international crimes. A similar

27 Art. 8 of the Rome Statute, 1998.

point of view was shared by Khan, the prosecutor of the International Criminal Court, who described that:

> the tools used to commit serious international crimes constantly evolve – from bullets and bombs to social media, the internet, and perhaps now even artificial intelligence. As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another.[28]

He further expresses that international criminal justice must adapt to this new landscape, as follows:

> While no provision of the Rome Statute is dedicated to cybercrime, such conduct may potentially fulfil the elements of many core international crimes, as already defined. In particular, the International Committee of the Red Cross has reiterated that cyber-attacks must comply with the cardinal principles of distinction and proportionality, and should only be directed against military objectives.[29]

The cyberspace is, therefore, not a special domain free from regulation, but rather a domain where international law has a clear role to play. Importantly, in modern warfare, the frontlines are no longer just physical, and digital frontlines can give rise to damage and suffering comparable to what the founders of the International Criminal Court sought to prevent.[30]

2.4. Convention on Cybercrime

Cybercrime is predominantly an international phenomenon, as new forms of criminal acts related to computer systems can spread worldwide very quickly. Accordingly, it is necessary to harmonise the international criminal legislation on cybercrime, especially owing to the processes involved in prosecuting cybercrime offences. Such prosecution requires not only clear definitions of related criminal acts in domestic criminal legislation, but also effective international cooperation between countries. Therefore, the purpose of the Convention on Cybercrime[31] is to unify measures at the criminal, material, and procedural levels and contribute to better prosecution of cybercrimes.

The Convention on Cybercrime contains a basic list of crimes that the signatories must accept, and at the time the Convention was adopted in 2001, this list was

28 Khan, no date.
29 Ibid.
30 Ibid.
31 *Convention of Cybercrime*, 2001; Council of Europe, 2001, CETS No. 185.

considered extremely advanced and elaborate, containing practically all the most important forms of criminal acts in information systems. However, the last 20 years since its adoption saw the rise of numerous new forms of cybercrime. This renders the Convention a representative of minimum standards that should be followed by practically every advanced criminal legislation in the world.

The Convention on Cybercrime was adopted by the Council of Europe on 23 November 2001, in Budapest, and had already been ratified in most European countries[32] and countries outside Europe, such as the United States of America, Canada, Japan, Israel, and Australia. The Convention is the main, fundamental document for harmonising the cybercrime-related regulations of EU countries and those of other countries that have ratified the Convention. The Convention also places strong emphasis on international cooperation in the prosecution of cybercrime. It is also necessary to emphasise the efforts of the Committee of Experts on Crime in Cyberspace, which is responsible for the effective implementation of the Convention's measures in the legislation of the signatory countries. The Committee's goal is to get as many countries as possible to sign and ratify the Convention.[33]

Prior to the adoption of the Convention, the basic document in this area was Recommendation No. R(95) 13 of the Council of Ministers of the Council of Europe[34] on criminal procedure problems related to information technology. After the creation of the Convention, the Council of Europe soon realised that it was necessary to add special racist and xenophobic crimes committed through information systems to the basic catalogue of crimes. For this purpose, the Council of Europe adopted the Additional Protocol to the Convention on Cybercrime, which deals with the criminalisation of racist and xenophobic acts committed in computer systems (CETS 189). The Protocol is an addendum to the Convention and is open to ratification by countries that have already ratified the Convention. The Additional Protocol was adopted and opened for ratification on 28 January 2003, but its adoption was slightly more restrained than that of the Convention, as only 42 countries signed the Protocol, while the Convention had 68 parties and 23 other signatories.

The title of the Additional Protocol already tells us how it deals with the various types of racist and xenophobic acts that can be carried out in computer systems or on the Internet. Unfortunately, some of the consequences of globalisation include the spread and dissemination of racism, discrimination, xenophobia, and other forms of intolerance, and the development of electronic communication and networks can contribute to racism and other xenophobic acts. In light of this, the Additional Protocol was adopted following two main purposes; the first is to harmonise criminal law in the field of combating racism and xenophobic acts committed on the Internet, and the second is to improve international cooperation in this area.[35] The legal in-

32 Ireland only signed the Convention, but did not accede to it.
33 *Explanatory report on the Convention on Cybercrime*, 2001, p. 4.
34 Council of Europe, R 95 13, 1995.
35 *Explanatory report on the Convention on Cybercrime*, 2001, p. 42.

terests protected by the Protocol are the equality of all people and equal protection of human rights against discrimination and racism. However, another legal interest stands in opposition to these rights, which is the freedom of expression, which led the Additional Protocol to be established as an attempt to strike a balance between the two interests and enable their protection.

In 2022, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) was put forward. While cybercrime proliferates in the context of increasingly complex ways of obtaining electronic evidence, mostly owing to these pieces of evidence being stored in foreign, multiple, shifting, and/or unknown jurisdictions, the powers of law enforcement remain limited by territorial boundaries. As a result, only a very small share of cybercrimes reported to criminal justice authorities leads to court decisions. In response, the Second Additional Protocol to the Convention on Cybercrime (CETS No. 185) provides a legal basis for the disclosure of domain name registration information, direct cooperation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate cooperation in emergencies, mutual assistance tools, and personal data protection safeguards.[36]

The Convention on Cybercrime comprises four chapters:

4. Use of terms
5. Measures to be taken at the national level (substantive criminal law and procedural law)
6. International co-operation
7. Final provisions

The most important part of the Convention for cyberattacks is on Chapter 2 on measures that must be taken at the national level. The substantive criminal law in it defines the criminal acts that must be outlined in the criminal codes of the signatory countries, whereas the procedural part defines the procedural provisions and guidelines that must be adopted in the procedural mechanisms of the signatory countries. The substantive criminal law part is represented by the following provisions in the Convention:

Art. 2 – Illegal access
Art. 3 – Illegal interception
Art. 4 – Data interference
Art. 5 – System interference
Art. 6 – Misuse of devices
Art. 7 – Computer-related forgery
Art. 8 – Computer-related fraud

36 *Details of Treaty No. 224*, no date.

Art. 9 – Offences related to child pornography
Art. 10 – Offences related to infringements of copyright and related rights

The Convention also defines international cooperation, in which provisions on a 24/7 network are at the forefront. This is an international information network that is supposed to be accessible 24 hours a day and seven days a week, through which signatory countries are supposed to exchange information and data related to cybercrime.

Regarding cyberwarfare attacks, the most relevant articles in the Convention are as follows: the notion of illegal interception under Art. 3, which can be used in cases of cyber-spying and espionage; the description on data interference under Art. 4; the description on system interference under Art. 5. These articles tackle issues that are present in any kind of cyberattack targeting an information system in the context of cyberwarfare, be it a denial of service attack, attacks to disrupt critical operations and systems, attacking and disabling critical systems and infrastructure, economic disruption by targeting economic establishments, surprise attacks in the context of hybrid warfare, or even sabotage. The difference between the offences in Arts. 4 and 5 is that data interference comprises damage, deletion, deterioration, alteration, or suppression of only computer data, whereas system interference disrupts the functioning of an information system as a whole, even if it is performed by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Computer-related forgery (Art. 7) and fraud (Art. 8) are connected to cyber-spying and espionage. Moreover, Art. 6 on the misuse of devices could be associated to all types of cyberwarfare attacks because it criminalises any kind of production, sale, procurement for use, import, distribution or otherwise making available of devices, programs, or codes that enable the perpetrator to perform one of the criminal offences listed in the Convention. This means that all those who aid in cyberwarfare attacks by providing software or hardware to attackers will be criminally liable together with the perpetrators.

It should be emphasised that the Convention on Cybercrime, with its Additional Protocols, is not the only regulation governing the field of cybercrime worldwide. Since it was written more than two decades ago, it has become relatively outdated in some respects. During this period, the EU has taken over legislative initiatives in Europe, with the largest shift in the field of European legislation being associated with the Treaty of Lisbon (i.e. the Treaty on European Union and the Treaty on the Functioning of the European Union, TFEU) in 2009. This Treaty gave the EU a legal basis for the adoption of criminal law directives to ensure the effective implementation of EU policies. Before the adoption of the Treaty of Lisbon, the EU intervened in criminal law mainly through framework decisions and conventions.[37] Interven-

37 *The 1995 Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions.*

tions by the EU were mainly focused in the area of the EU's financial interests, but they also spread to other criminal areas (e.g. child pornography).[38] According to the Treaty of Lisbon, instead of just being a provider of framework decisions and conventions, the EU can now adopt normal community instruments (regulations, directives, and decisions) with direct effect on the territory of EU Member States.[39]

2.5. Directive EU 2013/40/EU on attacks against information systems

Directive EU 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA continues the unifying work of the Convention on Cybercrime. The main objective of the Directive is to approximate the criminal law of Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and relevant sanctions. It is also aimed at improving cooperation between competent authorities, including the police and other specialised law enforcement services of EU Member States, competent specialised EU agencies and bodies (e.g. European Union Agency for Criminal Justice Cooperation [Eurojust], European Union Agency for Law Enforcement [Europol], and its European Cyber Crime Centre, and the European Network and Information Security Agency, ENISA).[40]

The Directive sets out substantive measures and contains articles on improved cooperation at the procedural level. Some of the material measures are on the following topics: illegal access to information systems (Art. 3); illegal system interference (Art. 4); illegal data interference (Art. 5); illegal interception (Art. 6); tools used for committing offences (Art. 7); incitement, aiding, abetting, and attempt (Art. 8). The definitions are quite similar to those of the Convention on Cybercrime; therefore, states that have signed the Convention are already familiar with these offences. A novelty that the new Directive brings is the demanded penalties from EU Member States, which now vary from at least two years of imprisonment for less serious offences to at least five years for more serious offences. The Directive also adds the criminal liability of and sanctions for legal persons that must be implemented in the national law of EU Member states. Still on a procedural perspective, the Directive also defines the jurisdiction for the prosecution of cyberattacks (Art. 12) and demands the exchange of information relating to the offences described in the

38 *Council Framework Decision 2004/68/PNZ of 22 December 2003 on combating the sexual exploitation of children and child pornography.*

39 This applies especially to the so-called "European crimes", which include terrorism, human trafficking, sexual exploitation of women and children, illicit traffic of illegal drugs and weapons, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. The Council can only establish additional "European crimes" unanimously and with the consent of the European Parliament.

40 Preamble of the Directive, 2013, p. 1.

Directive (Art. 13). The EU Member states must also monitor and prepare statistics on cybercrime (Art. 14).

With regard to cyberwarfare attacks, the Directive does not bring about drastic changes. Attacks that could already be prosecuted based on the definitions in the Convention on Cybercrime can also be prosecuted based on this Directive. The central definition of a cyberwarfare attack is the illegal interference in systems and data (Arts. 4 and 5 of the Directive, respectively). It is important to note that this is a mandatory Directive with which all EU Member States must comply, and even the United Kingdom and Ireland have notified their wish to take part in the adoption and application of this Directive. Although the Directive does not include as broad a spectrum of cyber offences as the Convention does, it still mostly covers all offences related to cyberwarfare attacks by sanctioning illegal interception, data interference, and system interference, and aiding and abetting these offences.

2.6. Directive EU 2022/2555 on measures for a high common level of cybersecurity

The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), is aimed at building the cybersecurity capabilities of the EU. It also focuses on mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing incidents, thus contributing to the EU's security and to the effective functioning of its economy and society.[41] The EU emphasises that during the war in Ukraine, cyberattacks went hand in hand with conventional military tactics, and their main purposes were destroying and disrupting the functioning of government agencies and organisations that managed critical infrastructure, as well as undermining confidence in the country's leadership. Basic services, such as transport, healthcare, and finance, are increasingly dependent on digital technologies and are therefore extremely susceptible to cyberattacks.[42] This is the main reason why the new Directive was adopted at the EU level, namely, so as to ensure the greatest possible information and cyber security in the EU.

In December 2020, the European Commission and the European External Action Service (also known as EEAS) presented a new EU cybersecurity strategy, aimed at making the EU more resilient to cyber threats and securing that all citizens and businesses can enjoy the full benefits of trusted and reliable services and digital tools. Part of the new EU cybersecurity strategy was adopted by the EU Cybersecurity Act, which focused on strengthening the ENISA and establishing a cybersecurity certification framework for products and services. Meanwhile, the ENISA plays a key role

41 Preamble to the Directive, 2022, p. 1.

42 *Cybersecurity: why reducing the cost of cyberattacks matters*, 2021.

in setting up and maintaining the EU's cybersecurity certification framework by preparing the technical grounds for specific certification schemes.[43]

Part of this new EU cybersecurity strategy also involves the new NIS 2 Directive.[44] This Directive lays down measures aimed at achieving a high level of cybersecurity across the EU and improving the functioning of the internal market. It defines that EU Member States must adopt national cybersecurity strategies and designate/establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and computer security incident response teams (also known as CSIRTs). Specifically, Chapter III of the NIS 2 Directive is dedicated to cooperation at the EU and international levels. The Directive also establishes a Cooperation Group composed of representatives of EU Member States, the Commission, and ENISA (Art. 14). Furthermore, it describes a network of national computer security incident response teams to promote swift and effective operational cooperation among EU Member States (Art. 15), and the European Cyber Crisis Liaison Organization Network (also known as EU-CyCLONe), which should support the coordinated management of large-scale cybersecurity incidents at the operational level and ensure the regular exchange of relevant information among EU Member States and EU institutions, bodies, offices, and agencies (Art. 16). Chapter IV of the Directive deals with cybersecurity risk-management measures and reporting obligations, while Chapter II deals with coordinated cybersecurity frameworks, including national cybersecurity strategy (Art. 7), competent authorities and single points of contact (Art. 8), national cyber crisis management frameworks (Art. 9), and computer security incident response teams (Art. 10).

Although the new NIS 2 Directive does not include new definitions of criminal offences and, therefore, does not directly address definitions of cyberwarfare crimes, the goal of the Directive is to prepare a defence strategy against such attacks for the information systems of EU Member States. The new Directive also imposes stricter requirements (vs. prior similar documents) and obligations for EU Member States regarding cybersecurity, especially in terms of supervision. Moreover, the Directive improves the enforcement of these obligations through the harmonisation of sanctions across all EU Member States. In fact, the major purpose of the Directive is to improve cooperation between EU Member States, especially in the event of major cyber incidents. Therefore, while the Directive in question does not define criminal acts under which individual forms of behaviour in the context of cybercrime could be placed, nor specifically refers to cyberwarfare, it does generally apply to all cyberattacks and cybercrimes.

43 *The EU Cybersecurity Act*, no date.

44 *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

2.7. Criminal Law of the European Union

One question that can arise here, based on the expositions in the prior sections, is the following: is there a European criminal law? That is, in the sense that the EU acts as a sovereign state, formulates criminal acts, carries out criminal prosecution, and sanctions the perpetrators of criminal acts? The answer is a resounding no. However, we can speak of European criminal law when the EU protects its financial interests through legislation enforced on its Member States, but only in this sense. Regardless of this situation, the EU still depends on its Member States to enforce the regulations, as the EU itself has no means physically coerce individuals. As Ambos writes,

> the designation European criminal law is a kind of umbrella term covering all those norms and practices of criminal and criminal procedural law based on the law and activities of the EU and the Council of Europe and leading to widespread harmonisation of national criminal law.[45]

Therefore, there is no comprehensive, self-contained European criminal law or justice system, but more of an umbrella-like system that connects different entities, organs, and legislations in the EU towards the investigation and prosecution of transnational crimes.[46] This is especially for those crimes connected to the financial interests of the EU.

There are debates on whether the EU should have its own criminal code, which would in turn represent the next level of harmonisation and unification of criminal offences in the EU. However, an initial problem with such a venture is the sovereignty of Member States. The criminal code of a country presents the ultimate expression of its legal authority, in that each state declares conduct that is unacceptable to such a degree that it will use its physical coercion capabilities to enforce its rules. By renouncing its own criminal code and leaving it in the hands of another authority, the sovereignty of the state becomes questionable; in such a scenario, someone who does not follow the elected legitimate rule of the state becomes able to enforce criminally prohibited conduct, or conduct that would otherwise be seen as prohibited. It seems that EU Member States are not (yet) ready to take such a step, and is questionable if they ever will. Unlike other federations, the EU was primarily established as an economically-unifying union of completely different sovereign states, which in turn have different languages, established nationalities, long histories, and different origins. Another problem regarding the potential of the EU having a criminal code would be the different interpretations of the law in different jurisdictions; this problem could be solved by establishing a common European High Court, whose precedents should be binding on inferior courts throughout Europe.[47] A final problem, at least for the

45 Ambos, 2018, p. 14.
46 Ambos, 2018, p. 15.
47 Cadoppi, 1996, pp. 2–17.

purposes of this study, is that the TFEU does not include an authorisation for the EU to create codes of law. A criminal code should include more than a compilation of European Directives and Framework Decisions. Still, in the TFEU, its Art. 83/1 gives the EU the option to adopt directives that establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crimes with a cross-border dimension and that are of such nature or impact that there is a special need to combat them at the EU level.[48]

Therefore, no independent supranational European criminal law has been created beyond the EU's competence. However, the national criminal law of EU Member States is influenced by EU law through its Directives, Framework decisions, and other normative guidelines, as well as by the principle of mutual recognition. This Europeanised criminal law is complemented by the creation of different European institutions in the area of criminal law, which in turn have their own goals and authorisations.[49]

As defined in Art. 83/1 of the TFEU, the European Parliament and Council may adopt directives to combat cross-border crimes that threaten the (economic) interests of the EU. The areas in which criminal unification is possible are also defined in this article, and are the following: terrorism, human trafficking, sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. The EU, therefore, has some power to harmonise the criminal law of its Member States. This harmonisation takes place through an assimilation obligation on the part of EU Member States, and the harmonisation of substantive criminal law by means of the EU's competence to approximate and annex criminal law pursuant to Art. 83(1) and (2) TFEU. Indeed, making use of these competences, the EU has issued several directives[50] aimed at harmonising national criminal law.[51] The list of crimes described in Art. 83/1 of the TFEU was included in the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) and the jurisdiction of Europol and Eurojust in Art. 4.1 of the Council Decision establishing the European Police Office (Europol) (2009/371/JHA) and its Annex, and later in Annex D of the Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters.

The 32 offences related to this article can be grouped into crimes defined in EU law, typical crimes in national laws, and crimes within the jurisdiction of the International Criminal Court. The list of offences ranges from crimes such as terrorism to swindling and arson, and there is no guiding system or principle on how the list was

48 Long, 2011, pp. 49–52.

49 Ambos, 2018, p. 15.

50 For example, *Directive (EU) of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.*

51 Šepec and Schalk-Unger, 2023, pp. 203–224.

made. More specifically, it includes cross-border crimes (e.g. terrorism and drug trafficking), crimes that relate specifically to the EU (e.g. protection of its financial interests), and ordinary offences such as fraud, arson, and extortion. Some offences are formulated in a vague, broad manner (e.g. corruption, organised or armed robbery), while others only capture a criminal phenomenon (racism and xenophobia), raising doubts as to whether such phenomena can be referred to as offences.[52]

This list also includes computer-related crimes, which in turn feature probably one of the vaguest definitions on the entire list. Computers and information systems have become essential tools for the functioning of modern society and are commonly used when committing criminal offences. Accordingly, a unified and comprehensive list of crimes performed against or with the help of computer systems has been compiled under the Convention on Cybercrime, which lists the following offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to infringement of copyright and related rights. However, only computer-related forgery and fraud are defined under the chapter Computer-related offences (others are defined under the chapters named Offences against the confidentiality, integrity and availability of computer data and systems; Content-related offences; and Offences related to infringements of copyright and related rights). The offence list of the Convention was later expanded with the Additional Protocol, which criminalises acts of a racist and xenophobic nature committed through computer systems. Therefore, it is quite evident that the term "computer-related crimes" could include a vast list of different offences, the problem being here that such wideness of the term opposes the principle of legality, as it is not clear which offences are really meant with the term. This dilemma was at least partly solved by the Directive 2013/40/EU,[53] which includes five different offences: illegal access to information systems, illegal system interference, illegal data interference, illegal interception, and tools used for committing offences. This entails that only these offences should be covered by the category "computer-related crime" in the Annex D of the EIO Directive. That is, cyberwarfare attacks, which are included illegal system interference, illegal data interference, and illegal interception, are covered in the lists of EU crimes after Art. 83/1 of the TFEU. Cyberwarfare attacks are therefore treated by the EU as crimes with a cross-border dimension of such nature and impact that they need special treatment, and require the harmonising of legislation at the EU level to prosecute such crimes more efficiently. The proof of this is the adopted Directive 2013/40/EU on attacks against information systems.

Therefore, for the purpose of prosecuting cyberwarfare attacks within the EU, there is no need to amend EU legislation or adopt new EU Directives on the criminal material level, as the adopted legislation already covers the main offences. However,

52 Ambos, 2018, p. 435.

53 *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing council framework decision (2005/222/JHA).*

current EU legislation is written mainly for the purpose of normal cyberattacks (by hacker groups or individuals), and does not contemplate cyberwarfare attacks or operations against EU Member States. If the EU develops a system of joint military defence, legislation that provides further protection to the EU against cyberwarfare attacks could be a viable option in the future.

3. EU procedural measures of cooperation in criminal matters for prosecuting cyberwarfare crimes

The judicial cooperation in the EU is based on the principle of mutual recognition. In accordance with Art. 82 of the TFEU, this includes rules and procedures for ensuring recognition throughout the EU of all forms of judgments and judicial decisions, preventing and settling conflicts of jurisdiction between EU Member States, training of the judiciary and judicial staff, and cooperation between judicial or equivalent authorities of EU Member States in relation to proceedings in criminal matters and the enforcement of decisions. This means that the EU has a legal basis for implementing procedural measures that can be used to prosecute cyberwarfare crimes internationally. When prosecuting cross-border crimes, EU Member States are not alone nor isolated from each other, but rather can and should rely on joint mechanisms of cooperation at the EU level to facilitate criminal prosecution. This means that EU Member States can help each other in the cross-border prosecution of cyberwarfare crimes not only politically but also legally; what this means is that the EU Member State does not decide on cooperation politically, but rather is legally bound to such cooperation by EU legislation.

With the Treaty of Lisbon, police and judicial cooperation was transferred to the area of justice and home affairs. Consequently, mutual legal assistance in the EU has developed from classic treaty-based assistance to a system of executive assistance based on mutual recognition. The European Parliament and the Council can jointly establish minimum rules for the approximation of law in ordinary legislative procedures.[54]

Indeed, the approximation of procedural law is possible according to Art. 82 of the TFEU. Minimum rules can be established through directives in the fields of the admissibility of evidence, rights of individuals, and rights of crime victims. Furthermore, legal assistance in the EU includes areas of extradition and other mutual assistance in criminal matters (e.g. questioning witnesses, gathering evidence, searching, and confiscating) and enforcement (e.g. the execution of foreign judgments and decisions).[55]

54 Ambos, 2018, pp. 411–412.
55 Ibid., pp. 414–415.

On this premise, the EU has adopted numerous conventions, directives, and framework decisions to facilitate mutual cooperation and recognition among its Member States. This means that the Member State is never alone in gathering evidence or prosecuting a criminal offence when the offence was committed internationally or in the territory of other EU Member States. For the purposes of prosecuting cyberwarfare crimes, the most relevant procedural measure of the EU may be the European Investigation Order.

3.1. European Investigation Order

Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO-Directive) established a single comprehensive framework, based on the principle of mutual recognition, that allows EU Member States to obtain evidence from other Member States. This Directive replaced existing frameworks for the gathering of evidence, namely the 2000 EU Mutual Legal Assistance Convention, Framework Decision 2008/978/JHA on the European evidence warrant, and Framework Decision 2003/577/JHA on the freezing of evidence. The EIO-Directive was adopted in April 2014, giving EU Member States (except Ireland and Denmark) three years for its transposition. After its implementation, the EIO-Directive soon became the leading legal instrument for gathering evidence in the EU, revolutionising EU cooperation in criminal matters. By providing deadlines for execution and introducing a practical form in Annex A that was soon adopted in practice, the EIO did not remain a theoretical concept but a commonly used and useful tool for legal practitioners dealing with offences that have a cross-border element in the EU.

The EIO-Directive also introduced rules relating to the types of procedures in which it can be used, conditions for its usage, rules of recognition and execution, and legal safeguards for refusal of execution, thereby safeguarding the basic rights of the defendants and preventing serious infringements to the criminal procedures of EU Member States (e.g. demanding an execution of an investigative measure that is not legally implemented in the executing state). The overall objective of introducing a standard EIO form, available in all official languages of member States, was to simplify formalities, improve quality, and reduce translation costs. Despite the fact that the form itself could be improved, research shows that practitioners consider the EIO form usable in their current formulations, and regularly use it.[56] In this form, the issuing authority describes the criminal offence being investigated, the applicable criminal law, and the types of measures requested. If there are no grounds for refusing the EIO, the executing authority of the EU Member State shall execute the demanded EIO. However, the executing authority shall have some margin to check the proportionality of the EIO when the latter is not in conformity with the

56 Šepec, Dugar and Stajnko, 2023, p. 123.

constitutional standards of the executing state. There is also the possibility of replacing the requested measure with a similar one providing the same results.[57]

Of course, it would be utopian to expect such a commonly used legal instrument to be completely absent of any theoretical or practical shortcoming. In light of this reality, an international project called EIO-LAPD was funded by the European Commission, which aimed to identify these difficulties and find solutions. The thorough analysis of the legal framework and practical dilemmas conducted by the project highlighted possible solutions for various shortcomings of the EIO form, including the following: dilemmas on accepted languages in urgent cases; transmission of EIOs and electronic evidence via insecure communication channels; video conference tool use; requests for non-existent measures; the *ne bis in idem* non-recognition ground; coercive measures; speciality rule; requests for issuing EIOs by the defence.[58] Despite its shortcomings, the EIO remains the main cooperative measure at the EU level for gathering and exchanging evidence in criminal prosecutions and trials, including those pertaining to cyber warfare attacks.

In the near future, we can expect facilitations in the development of the e-Evidence Digital Exchange System (also known as eEDES), and a push for its implementation in all EU Member States, as digital evidence is ever more prevalent in criminal law and new problems regarding securing such data are constantly emerging. We expect this to be the next stage of the EU development on the topic of evidence exchange in criminal matters. However, this push to regulate the exchange of digital evidence should not come at the cost of amending other pressing issues in the EIO-Directive, such as rethinking the existing legal framework from the perspective of the rights of the accused and the *ne bis in idem* principle.[59]

EU Institutions for cooperation in criminal matters

This section presents the main EU Institutions that cooperate in criminal matters. We are interested in understanding the roles of these institutions, whether they are of a political nature, and whether they have legal authority. One question that can be proposed here would be the following: what are the capabilities and jurisdictions of EU institutions regarding cyber and cyberwarfare crimes? Can EU Member States refuse the authority of EU institutions, or do they have to submit and cooperate with them? What is the legal basis of EU institutions, what are their main goals, and how effective are they in prosecuting international crimes?

To respond to these questions, the following subsections explore the main EU institutions connected to criminal offences.

57 Bachmaier-Winter, 2023, p. 295.
58 Ibid., pp. 127–137.
59 Šepec, Dugar and Stajnko, 2023, p. 136.

Europol

The Europol is the most important agency for police cooperation in the EU, having the main goal of supporting and strengthening EU Member States' law enforcement agencies, especially the police. Importantly, the Europol does not have executive power and cannot arrest people or conduct investigations independently. This is evident from Art. 88 of the Treaty on the Functioning of the European Union, which states that the application of coercive measures should be the exclusive responsibility of competent national authorities.

The Europol was established in 1998 in the context of the Third pillar of the Europol Convention.[60] In 2009, the Council of Europe repealed the primary Convention and adopted the Europol Council Decision, which was later repealed by Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol). The Europol is based on The Hague, in the Netherlands, and serves as the central hub for coordinating criminal intelligence and supporting the EU's Member States in their efforts to combat various forms of serious and organised crime, as well as terrorism.

The Europol facilitates the exchange of information and intelligence, provides analytical support, and offers specialised training and expertise. Some of the key areas of focus of the Europol, as listed in the Annex I to the Europol Regulation, include drug trafficking, human trafficking, cybercrime, money laundering, and counterterrorism. This list is quite similar to that of crimes for which the Council Framework Decision 2002/584/JHA on the European Arrest Warrant and other EU instruments of mutual recognition do not require a double criminality standard.[61] This poses questions about the exact authorities of the Europol, as these offences are defined vaguely and without a system behind the seemingly random list of offences; this contradicts the principle of legality as the core criminal law principle of national legal systems. The principle of legality in relation to the categories of offences listed in Annex I to the Europol Regulation can be fully respected only when a clear legal definition of each listed offence can be found in EU legislation. If there is no clear normative content provided by the EU, then the differences between the legal definitions of certain offences can vary across EU Member States to such an extent that there is no clear legal definition of the offence at all.[62]

As Europol is competent to support and strengthen national authorities in preventing and combating computer-related crimes (Art. 3 and Annex I to the Europol Regulation (EU) 2016/794), the principle of legality can once more be questioned, as "computer crimes" is a very vague definition that includes numerous offences, and it is not clear which offences are really meant with the title "computer-related offences".

60 *Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office* (Europol Convention). See also Ligeti and Giuffrida, 2023, p. 362.
61 Ligeti and Giuffrida, 2023, p. 367.
62 Šepec and Schalk-Unger, 2023, p. 207.

This dilemma was at least partly solved by the Directive 2013/40/EU,[63] which includes five different offences, as follows: illegal access to information systems, illegal system interference, illegal data interference, illegal interception, and tools used for committing offences. Therefore, only these offences should be covered by the category "computer-related crime" in Annex I to the Europol Regulation.

Regarding computer crimes, which cover cyberwarfare attacks, Europol has important data processing tasks that include gathering and processing information, incorporating criminal intelligence, and performing strategic and operational analyses. Although the Europol does not have coercive powers, the institution's information gathering generates knowledge that can lead to evidence useful in national court procedures.[64] The Europol is, therefore, an essential partner of national authorities when discovering cybercrime offences with international elements. This becomes especially evident when Europol coordinates the organisation and execution of investigations together with Member States, or within the framework of joint investigative teams.

For this purpose, Art. 4(l) of the Europol Regulation (EU) 2016/794 stipulates that the body shall develop Union centres of specialised expertise to combat certain types of crime falling within the scope of Europol's objectives, particularly the European Cybercrime Centre. To prevent and combat cybercrime, which are associated with network and information security incidents, Europol lays down measures to ensure a high level of network and information security across the EI, and cooperates and exchanges information with national authorities competent on the security of network and information systems. Member States should also supply Europol with information about any alleged cyberattacks affecting EU bodies located in their territory.[65] Furthermore, when coordinated action among several EU Member States is necessary, the Europol may recommend the establishment of Joint Investigative Teams (also known as JITs), and Europol can participate in and support these teams through the collection and analysis of intelligence data.[66] As Europol is an agency of the EU, judicial control of its concrete measures is exercised by the Court of Justice of the European Union **(**CJEU).

Eurojust

The Eurojust was established in 2002 and is located in The Hague, in the Netherlands. The main goal of the agency is to improve cooperation among EU Member States on the investigation and prosecution of serious cross-border and organised crime. Eurojust started functioning as a provisional unit (Pro-Eurojust),[67] and was

63 *Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing council framework decision* (2005/222/JHA).
64 Ligeti and Giuffrida, 2023, p. 385.
65 Preamble of the Europol Regulation (EU) 2016/794, paras. 13 and 30.
66 Ambos, 2018, p. 565.
67 *Council Decision 2000/799/JHA*.

later established by Council Decision 2002/187/JHA. Its legal basis was amended thrice, specifically by Council Decisions 2003/659/JHA and 2009/426/JHA, which broadened its original powers,[68] and finally by Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust). The latter is the current legal basis for Eurojust's authority, and was adopted because of the need for enhanced cooperation among EU Member States for establishing the European Public Prosecutor's Office (EPPO).

Eurojust was established to address the need for centrally coordinated cross-border prosecution of the most serious crimes committed in the EU. This can only be achieved using a decentralised network of national contact points, which in turn made necessary to the creation of an additional central body in which representatives of the judicial authorities of all Member States are located.[69]

Furthermore, the Eurojust was conceptualised as an independent, collegial judicial institution of the EU that should have its own legal personality. Eurojust's main tasks are the initiation of criminal investigations and prosecutions, the coordination of investigations and prosecutions in EU Member States, and the strengthening of the judicial cooperation of EU Member States.[70] Still, Eurojust lacks any real formal investigative power, as the decision to investigate or prosecute a crime in a EU Member State falls under national authorities. The right of initiative shows only the Lisbon Contracting Parties' willingness to grant Eurojust this right.[71]

The Eurojust's jurisdiction covers crimes listed in Annex 1 of the Regulation (EU) 2018/1727, which encompasses the familiar list of EU crimes, including "computer-related crimes". Therefore, according to the principle of legality, Eurojust has jurisdiction over the computer-related crimes listed in the Directive 2013/40/EU, which includes the five different offences mentioned before in this paper. Although the list is slightly more detailed than the first one proposed in the European Arrest Warrant framework decision (e.g. the new list specifies fraud affecting the financial interests of the European Communities, while the first list only included fraud and swindling), there has been no change in computer crimes. This means that Eurojust has competencies over cybercrime and cyberwarfare offences when committed against or in EU Member States. An exception here is Denmark, which owes to the special regime foreseen in Protocol no. 22 of the Lisbon Treaty.

It should be emphasised that when the EPPO starts its investigative and prosecutorial functions, Eurojust should not exercise any competencies. The exception to this rule, meaning that Eurojust would maintain its competence, is when a request is made by the authorities of EU Member States, or a request is issued by the EPPO itself. The same can be said for crimes on which EPPO has no competence, or on

68 Hernandez Lopez and Jimenez-Villarejo Fernandez, 2023, p. 387.
69 Ambos, 2018, p. 569.
70 Ibid., p. 570.
71 Ibid.

which it has decided not to exercise such competence.[72] Still, even as the EPPO takes over the investigation, Eurojust still keeps the obligation to mutually consult and cooperate with the EPPO. Furthermore, Eurojust can assist EU Member States even in crimes not listed in Annex 1 of the Regulation (EU) 2018/1727, meaning that it could offer assistance even in computer-related crimes not defined in Directive 2013/40/EU. Finally, Eurojust can support EU Member States in investigating or prosecuting a crime that only affects that Member State (i.e. without an international element) if the case could have an impact at the EU level.[73]

Today, Eurojust, together with the EPPO, represents the peak of investigative and judicial cooperation in the EU. Eurojust was designed to allow EU Member States to perform their investigative tasks more effectively while preserving their national and operational independence.

The CJEU

The CJEU was established in 1952 and represents the judicial branch of the EU. It comprises two separate courts, the Court of Justice and the General Court; however, it also includes specialised courts. The CJEU is thus a supranational institution, meaning that it is empowered to exercise powers and functions otherwise reserved to states.

Accordingly, the CJEU is the EU's chief judicial authority and oversees the uniform application and interpretation of EU law. The CJEU interprets the EU law to ensure that it is applied in the same manner to all EU Member States. The Court also settles legal disputes between national governments and EU institutions, and can sometimes be used, under specific circumstances, by individuals, companies, or organisations to act against an EU institution if the party states that the institution somehow infringed upon their rights.[74] Through the communisation of the former third pillar, the CJEU's jurisdiction has been extended to the area of police and judicial cooperation, and is now part of "justice and home affairs".[75]

The CJEU performs the following functions. Interpreting the law: the national courts of EU countries are required to ensure that EU law is properly applied; however, courts may interpret EU law differently. If a national court doubts the interpretation or validity of EU law, it can ask the Court for clarification. The same mechanism can be used to determine whether a national law or practice is compatible with EU law. The Treaty of Lisbon further strengthened the role of the CJEU as the sole interpreter and enforcer of EU law.[76] Enforcing the law: when a national government fails to comply with EU law, a procedure can be initiated by the European Commission or by

72 Hernandez Lopez and Jimenez-Villarejo Fernandez, 2023, pp. 390–391.
73 Ibid.
74 *Court of Justice of the European Union (CJEU)*, no date.
75 Ambos, 2018, p. 573.
76 Ambos, 2018, p. 573.

another EU country to request the CJEU to enforce EU law. Annulling EU legal acts: when an EU act is believed to violate EU treaties or fundamental rights, the CJEU can be asked to annul it. In fact, private people can ask the Court to annul an EU act that directly affects them, including criminal law and procedures. This ensures that the EU takes actions when the Parliament, Council and Commission must make certain decisions, and choose to do not. In such cases, a complaint can be issued to the CJEU. Sanctioning EU institutions: any person or company who has had their interests harmed as a result of the action or inaction of the EU or its staff can initiate this procedure in the CJEU.[77]

In the past, the CJEU has generally adopted a pro-EU, integrationist stance, and advocated the principle of mutual recognition, assuming mutual trust, although there is no solid basis for this in national law and practice. This has led the Court to be often characterised as a driving force of EU integration.[78] Although the CJEU has no direct function regarding cyberwarfare offences, it will play an important role in interpreting EU legislation and enforcing it on EU Member States. For example, the actual use of Directive EU 2013/40/EU on attacks against information systems, and/or of directives that provide cybersecurity protection (e.g. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union), depends on the interpretation of this legislation by the CJEU. However, it is worth noting that the CJEU is not in charge of conducting criminal trials against defendants of cyberwarfare offences, and this task instead falls to the national courts of EU Member States. Regardless, in the case of a misunderstanding pertaining to the legal regulations of the EU, the CJEU could get involved to interpret EU law. This, of course, does not mean that the CJEU will pass a judgment, as this task always falls under the national court of EU Member States.

The EPPO

The EPPO is the EU's first independent prosecuting office. It has the power to investigate, prosecute, and bring to judgment crimes against the EU budget, such as fraud, corruption, and serious cross-border value added tax fraud.[79] The EPPO was established out of the need for an independent, decentralised prosecutorial body to combat crimes affecting the financial interests of the EU. More specifically, it was introduced with Regulation 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (RegEPPO), and started to function on 1 June 2021. It was approved after two decades of political and doctrinal debate, specifically thanks to the enhanced cooperation mechanism of the Treaty of Lisbon under Art. 86 of the TFEU. Still, the investigative and prosecutorial powers

77 *Court of Justice of the European Union (CJEU)*, no date.
78 Ambos, 2018, p. 573.
79 *European Public Prosecutor's Office*, no date.

of the EPPO throughout the territory of EU Member States are limited to crimes affecting EU financial interests, as defined by Directive 2017/1371.[80]

The EPPO is based on the separation of prosecutorial and adjudicatory powers. The first is in the hands of the EPPO, while the latter is in the hands of national authorities. This was a political compromise, since EU Member States were not willing to submit to a full-fledged EU criminal justice system, which in turn implied the need for a EU criminal justice system.[81] As things stand now, EU Member States still control the judging process and overall judicial control over criminal proceedings; therefore, the judicial process is still in the hands of national authorities.

The EPPO is accountable only to the European Parliament, Council, and Commission. It comprises its Central Office at The Hague, in the Netherlands, and European Delegated Prosecutors coming from and located in EU Member States. The Central Office consists of the College, Permanent Chambers, European Chief Prosecutors, Deputy European Chief Prosecutors, European Prosecutors (each Member State has one), and the Administrative Director. There exists a hierarchy between delegated prosecutors at the central level and at the Member State level, which may often lead to tension and conflict, as delegated prosecutors at the national level must follow the instructions of the European prosecutor.[82]

At a given point in time, there was a raging debate as to what would be the material and territorial competence of the EPPO. Regulation 2017/1939 defined in Art. 22 that the EPPO shall be competent in respect of the criminal offences affecting the financial interests of the EU that are provided for in Directive (EU) 2017/1371, as implemented by national law, irrespective of whether the same criminal conduct could be classified as another type of offence under national law. This implies that the principle of dual criminality does not apply. The EPPO shall also be competent for offences regarding participation in a criminal organisation, as defined in Framework Decision 2008/841/JHA, if the focus of the criminal activity of such a criminal organisation is to commit any of the offences referred to in Directive (EU) 2017/1371. Furthermore, the EPPO shall also be competent for any other criminal offence inextricably linked to criminal conduct affecting the financial interests of the EU that are provided for in Directive (EU) 2017/1371. The material competence of the EPPO is, therefore, quite broad and could include cyberwarfare attacks; however, it would include so only when the attack is inextricably linked to criminal conduct affecting the financial interests of the EU, as the Directive (EU) 2017/1371 does not directly include computer crimes or cyberwarfare crimes. Therefore, the EPPO will not be the main protagonist when prosecuting cyberwarfare crimes on the EU territory. This task will instead fall to the national prosecutors of the EU Member State that was the target of the cyberwarfare attack. As aforementioned, the exception here would be

80 Allegrezza, 2023, p. 413.
81 Ibid., p. 414.
82 Ambos, 2018, p. 575.

attacks inextricably linked to criminal conduct affecting the financial interests of the EU, where the EPPO would maintain its material competence.

Additionally, Art. 23 of Regulation 2017/1939 defines the territorial competence of the EPPO, describing that it is competent if the offences were committed in whole or in part within the territory of one or several EU Member States, or committed by a national of a EU Member State. Importantly, the EPPO regulation follows the model of shared competence, where the EPPO only intervenes if the national authority is unable or not in a position to sufficiently protect the EU's financial interests itself. Thus, the decision whether to initiate an investigation right away or not falls to the EPPO. It remains, notwithstanding, that disagreements lend the final decision to fall to the EU Member State.[83] This means that the EPPO cannot overrule the decision of a Member State if the latter decides that it can protect the EU's financial interests.

If the EPPO decides to prosecute a crime under its jurisdiction, prosecution at the national level is executed by the European delegated prosecutor under the procedural law of the EU Member State where the trial will be held. This of course leads to abnormalities, as while the substantive law under which the EPPO functions is at least partly harmonised in Directive (EU) 2017/1371, the procedural law always varies depending on the EU Member State where the trial takes place.

Office de Lutte anti-fraude

The Office de Lutte anti-fraude (OLAF) was established on 28 April 1999, by Commission Decision 1999/352/EC and Regulations 1073/99 (EC) and 1074/99 (Euratom), as an independent investigative Commission agency. The OLAF's legislation was amended numerous times, the latter being Regulation NO 883/2013 (OLAF Regulation) and Regulation No. 2020/2223.[84] The main goal of the OLAF is to detect fraud against the EU budget, acts of corruption, and serious misconduct against EU institutions. It conducts independent investigations into fraud and corruption involving EU funds, as well as other serious illegal activities against the financial interests of the EU.[85] Furthermore, the OLAF investigates corruption in EU institutions and proposes anti-fraud legislation and EU policies.

It performs both external and internal investigations. External investigations are performed at the EU Member State level, where the OLAF depends on the competent national investigative authority and is not permitted to adopt any coercive measures.[86] Internal investigations refer to irregularities within the EU's institutions, offices, and agencies, whereby the OLAF has a much broader authority, can carry out investigations, examine and confiscate documents and data media, and gather

83 Ibid., p. 576.
84 Cahn, 2023, p. 330.
85 Ibid., p. 331.
86 Ambos, 2018, p. 561.

information from EU officials.[87] Nonetheless, the OLAF is obliged to surrender its investigation to national authorities in the case of criminal proceedings, as it cannot prosecute suspects by itself.

Although the OLAF is an important EU institution regarding financial frauds against the interests of the EU, when the topic is cyberwarfare attacks or even ordinary cyber offences, it does not play an important part, having practically no competencies or authority for investigating such offences. Furthermore, the OLAF is not a law enforcement agency; therefore, even if it had any jurisdiction over cyberwarfare or cyber offences, it would not be the institution coordinating the gathering of evidence and criminal prosecution of such offences. Some even question the nature of the OLAF and the task of its staff; are they investigators, prosecutors, or something in between?[88]

5. Conclusion

Cyberwarfare has neither a single definition nor a clearly established legal definition, but at its core, it means using computer technologies to disrupt or destroy an adversary's information systems and networks. In most cases, these are already known forms of cyberattacks, and which most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are thus that it is connected with the army of an individual country, which configures a military operation, and that the range and scope of related offences are significantly wider, as cyberwarfare involves attacks to more important targets with significantly more repulsive motives, such as paralysing a country's national security via damages to its infrastructure, and technological centres.

No legal documents in the EU or UN directly address cyberwarfare, as the term has not yet a clear legal definition. However, we can use numerous legal documents that indirectly address the topic of cyberwarfare and related attacks, such as the UN Charter, International humanitarian law, the Rome Statute of the International Criminal Court, Convention on Cybercrime, Directive 2013/40/EU, and Directive EU 2022/2555.

There is no European criminal law, such that the EU does not act as a sovereign state, formulate criminal acts, carry out criminal prosecution, nor can sanction perpetrators of criminal acts. Instead, the EU can only protect its financial interests through the legislation enforced by its Member States, hence depending on EU Member States to enforce its regulations; that is, in itself, the EU has no means of physical coercion.

87 Ibid., p. 562.
88 Xanthaki, 2016.

To prosecute cyberwarfare attacks within the EU, there is no essential need to amend EU legislation or adopt new EU Directives on the criminal material level, as the adopted legislation already covers the main offences. However, current EU legislation is written mainly for the purposes of normal cyberattacks (e.g. by hacker groups or individuals), and not specific for the purpose of war attacks or war operations against EU member states. If the EU develops a system of joint military defence in the future, legislation that provides further protection to the EU against cyberwarfare attacks could turn out valuable.

At the procedural level, the EU has a legal basis (Treaty on the Functioning of the European Union) for implementing procedural measures that can be used to prosecute cyberwarfare crimes at the international level. When prosecuting such cross-border crimes, EU Member States are not alone or isolated from each other, but rather can rely on joint mechanisms of cooperation (the most important being the European Investigation Order) at the EU level, which can be used to facilitate criminal prosecution. This means that EU Member States can help each other in the cross-border prosecution of cyberwarfare crimes. This cooperation is not political but of a legal nature, meaning that the EU Member State does not decide on cooperation politically, but is legally bound by EU legislation to cooperate. For this purpose, the EU can use its institutions for cooperation in criminal matters, including the Europol, Eurojust, OLAF, CJEU, and EPPO.

References

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003) Council of Europe, CETS No. 189, Strasbourg, 28 January 2003.

Allegrezza, S. (2023) 'The European Public Prosecutor's Office (EPPO)' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 413–438.

Ambos, K. (2018*) European Criminal Law.* Cambridge: Cambridge University press; https://doi.org/10.1017/9781316348628.

Bachmaier-Winter, L. (2023) 'Further Mutual Legal Assistance' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 283–305; https://doi.org/10.1017/9781108891875.017.

Barrett, N. (1997) *Digital crime, Policing the Cybernation*. London: Kogan Page.

Cadoppi, A. (1996) 'Towards a European Criminal Code', *European Journal of Crime, Criminal Law and Criminal Justice,* 4(1), pp. 2–17; https://doi.org/10.1163/157181796X00104.

Cahn, O. (2023) 'EU Anti-Fraud Policy – Administrative Investigations – EPPO' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 229–360.

Charter of the United Nations and Statue of the International Court of Justice (1945) United Nations.

Clough, J. (2010) *Principles of cybercrime*. Cambridge: Cambridge University press; https://doi.org/10.1017/CBO9780511845123.

Consolidated version of the Treaty on the Functioning of the European Union (2012) OJ C 326, 26 October 2012.

Consolidated version of the Treaty on the Functioning of the European Union PROTOCOLS – Protocol (No 22) on the position of Denmark (2012) OJ C 326, 26 October 2012.

Convention of Cybercrime (2001) Council of Europe, CETS No. 185, Budapest, 23 November 2001.

Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) (1995) OJ C 316, 27 November 1995.

Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions (1995) OJ L 312, 23 December 1995.

Council of Europe (2001) 'Explanatory report on the Convention on Cybercrime' Budapest, 23 November 2001.

Council Framework Decision 2004/68/PNZ of 22 December 2003 on combating the sexual exploitation of children and child pornography (2004) OJ L 013, 20 January 2004.

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002) 2002/584/JHA, OJ L 190, 18 July 2002.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (2009) OJ L 121, 15 May 2009.

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002) OJ L 063, 6 March 2002.

Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2003) OJ L 245, 29 September 2003.

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2009) OJ L 138, 4 June 2009.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (2017) OJ L 283, 31 October 2017.

Digmelashvili, T. (2023) 'The Impact of Cyberwarfare on the National Security', *Future Human Image*, 2023/19, pp. 12–19; https://doi.org/10.29202/fhi/19/2.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013) OJ L 218, 14 August 2013.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (2014) OJ L 130, 1 May 2014.

Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (2017) OJ L 198, 28 July 2017.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) OJ L 333, 27 December 2022.

Directive (EU) of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (2018) OJ L 156, 19 June 2018.

The Geneva Conventions (1949) Geneva, 12 August 1949.

Gibson, W. (1984) *Neuromancer*. London: Voyager.

The Hague Convention (II) on the Laws and Customs of War on Land (1899).

The Hague Convention III – XII (1907).

The Hague Convention for the Protection of Cultural Property (1954).

Hernandez Lopez, A., Jimenez-Villarejo Fernandez, F. (2023) 'Eurojust' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law*. Cambridge: Cambridge University Press, pp. 361–386; https://doi.org/10.1017/9781108891875.022.

Khan, K.A.A. (no date) 'Technology Will Not Exceed Our Humanity', *Digital Front Lines*. [Online]. Available at: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/ (Accessed: 15 August 2023).

Ligeti, K., Giuffrida, F. (2023) 'Europol' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law*. Cambridge: Cambridge University Press, pp. 361–386; https://doi.org/10.1017/9781108891875.021.

Long, N. (2011) 'Towards a European Criminal Law Code?', *EIPAScope*, 2011/1, pp. 49–52.

Maras, M.H. (2016) *Cybercriminology*. Oxford: Oxford University Press.

McCarthy, J. (1990) 'Generality in artificial intelligence' in Lifschitz, V. (ed.) *Formalizing Common Sense*. Norwood: Ablex Publishing Corporation, pp. 226–236.

Recommendation no. R(95) 13 of the Council of Ministers of the Council of Europe (1995) Council of Europe R (95) 13, 11 September 1995.

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (2018) OJ L 295, 21 November 2018.

Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations (2000) OJ L 437, 28 December 2020.

Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-fraud Office (OLAF) and repealing Regulation (EURATOM) No 1074/1999 (2011) European Commission, Brussels, 17 March 2011.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (2016) OJ L 135, 24 May 2016.

Rome Status of the International Criminal Court (1998) UN Security Council.

Šepec, M., Schalk-Unger, L. (2023) 'Special part of EU criminal law: the level of harmonization of the categories of offences listed in annex D in EU legislation and across selected member states' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation*. Berlin: Duncker & Humblot, pp. 203–224.

Šepec, M., Dugar, T., Stajnko, J. (2023) 'European Investigation Order – A Comparative Analysis of Practical and Legal Dilemmas' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation.* Berlin: Duncker & Humblot, pp. 123–137.

Wimann, G. (2005) 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict and Terrorism,* 28(2), pp. 129–149; https://doi.org/10.1080/10576100590905110.

Wall, D.S. (2005) 'The Internet as a Conduit for Criminal Activity' in Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. Lowell: Sage Publications, pp. 77–98; https://doi.org/10.4135/9781452225708.

Weissmann, M., Nilsson, M., Palmertz, B., Thunholm, P. (eds.) (2021) *Hybrid Warfare, Security and Asymmetric Conflict in International Relations*. London: I.B. TAURIS; https://doi.org/10.5040/9781788317795.

Xanthaki, H. (2016) 'The Kessler case should lead to a reform of OLAF', *Euractiv*, 20 June 2016. [Online]. Available at: https://www.euractiv.com/section/justice-home-affairs/opinion/the-kessler-case-should-lead-to-a-reform-of-olaf/ (Accessed: 10 November 2023).

Court of Justice of the European Union (CJEU) (no date). [Online]. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en (Accessed: 20 October 2023).

Cyber-Attack Against Ukrainian Critical Infrastructure (2021) *America's Cyber Defense Agency*, 20 July 2021. [Online]. Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (Accessed: 30 August 2023).

Cybersecurity: why reducing the cost of cyberattacks matters (2021) *European Parliament*, 12 October 2021. [Online]. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters (Accessed: 10 October 2023).

Cyber Warfare: does International Humanitarian Law apply? (2021) *ICRC, International Committee of the Red Cross*, 25 February 2021. [Online]. Available at: https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law (Accessed: 30 August 2023).

Cyber Warfare (no date) *Imperva*. [Online]. Available at: https://www.imperva.com/learn/application-security/cyber-warfare/ (Accessed: 25 August 2023).

Details of Treaty No.224 (no date) *Council of Europe*. [Online]. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (Accessed: 25 September 2023).

The EU Cybersecurity Act (no date) *European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (Accessed: 10 October 2023).

European Public Prosecutor's Office (no date) *European Anti-Fraud Office*. [Online]. Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-public-prosecutors-office_en (Accessed: 20 December 2023).

Struxnet (no date) *ScienceDirect*. [Online]. Available at: https://www.sciencedirect.com/topics/computer-science/stuxnet (Accessed: 30 August 2023).

Use of force under international law (2024) *Justia*, June 2024. [Online]. Available at: https://www.justia.com/international-law/use-of-force-under-international-law/ (Accessed: 25 August 2023).