VOL. 7 - SPECIAL ISSUE
(2026)

Journal of International Criminal Law

Online Scientific Review

Special Issue
EU-GLOBACT HANDBOOK

EUROCRIMES

EDITED BY
Heybatollah Najandimanesh
Anna Oriolo

ISSN: 2717-1914

www.jiclonline.org

EU-GLOBACT HANDBOOK

EUROCRIMES

A Q&A Compendium and Structural Frameworks on Offences Under Article 83 TFEU

This JICL Special Issue constitutes one of the scientific products the Jean Monnet Module (2023-2026) *Transnational Crime and EU Law: Towards Global Action against Cross-Border Threats to Common Security, Rule of Law, and Human Rights* (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo).

Project funded by European Commission Erasmus + Programme – Jean Monnet Action Project number 101126599. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

TABLE OF CONTENTS
VOLUME 7 – SPECIAL ISSUE

BOARD OF EDITORS

OVERVIEW

The Journal of International Criminal Law (*JICL)* is a scientific, online, peer-reviewed journal, first edited in 2020 by Prof. Dr. Heybatollah Najandimanesh, mainly focusing on international criminal law issues.

Since 2023 JICL has been co-managed by Prof. Dr. Anna Oriolo as General Editor and published semiannually in collaboration with the International and European Criminal Law Observatory (IECLO) staff.

JICL Boards are powered by academics, scholars and higher education experts from a variety of colleges, universities, and institutions from all over the world, active in the fields of criminal law and criminal justice at the international, regional, and national level.

The aims of the JICL, *inter alia*, are as follow:

- to promote international peace and justice through scientific research and publications;
- to foster study of international criminal law in a spirit of partnership and cooperation with the researchers from different countries;
- to encourage multi-perspectives of international criminal law; and
- to support young researchers to study and disseminate international criminal law.

Due to the serious interdependence among political sciences, philosophy, criminal law, criminology, ethics and human rights, the scopes of JICL are focused on international criminal law but not limited to it. In particular, the Journal welcomes high-quality submissions of manuscripts, essays, editorial comments, current developments, and book reviews by scholars and practitioners from around the world addressing both traditional and emerging themes, topics such as

- the substantive and procedural aspects of international criminal law;
- the jurisprudence of international criminal courts/tribunals;
- mutual effects of public international law, international relations, and international criminal law;
- relevant case-law from national criminal jurisdictions;
- criminal law and international human rights;
- European Union or EU criminal law (which includes financial violations and transnational crimes);
- domestic policy that affects international criminal law and international criminal justice;
- new technologies and international criminal justice;
- different country-specific approaches toward international criminal law and international criminal justice;
- historical accounts that address the international, regional, and national levels; and
- holistic research that makes use of political science, sociology, criminology, philosophy of law, ethics, and other disciplines that can inform the knowledge basis for scholarly dialogue.

The dynamic evolution of international criminal law, as an area that intersects various branches and levels of law and other disciplines, requires careful examination and interpretation. The need to scrutinize the origins, nature, and purpose of international criminal law is also evident in the light of its interdisciplinary characteristics. International criminal law norms and practices are shaped by various factors that further challenge any claims about the law's distinctiveness. The crime vocabulary too may reflect interdisciplinary synergies that draw on domains that often have been separated from law, according to legal doctrine. Talk about "ecocide" is just one example of such a trend that necessitates a rigorous analysis of law *per se* as well as open-minded assessment informed by other sources, *e.g.*, political science, philosophy, and ethics. Yet other emerging developments concern international criminal justice, especially through innovative contributions to enforcement strategies and restorative justice.

The tensions that arise from a description of preferences and priorities made it appropriate to create, improve and disseminate the JICL as a platform for research and dialogue across different cultures, in particular, as a consequence of the United Nations push for universal imperatives, *e.g.*, the fight against impunity for crimes of global concern (core international crimes, transboundary crimes, and transnational organized crimes).

COPYRIGHT AND LICENSING

Cybercrime (Computer Crime)

by Teresa D'Aniello[*]

SUMMARY: I. What Regulatory Instruments Become Available to The EU Following the Qualification of Cybercrime as A Eurocrime? – II. When does a Simple Digital Action Cross the Boundaries of Legality and become a Cybercrime? – III. How Does the Budapest Convention Align with Domestic Penal Systems? – IV. What Main Categories of Computer Crimes Define Domestic Substantive Law? – V. How Does European Legislation Address Jurisdictional Overlaps in Computer Crimes? – VI. How Does The 2024 UN Convention Innovate the Cybersecurity Framework? – VII. How Are INTERPOL's Modern Global Strategies Structured Against Computer Crime? – VIII. What Function Does Incident Information Sharing Perform Within the Context of European Cybersecurity? – IX. What Is the Impact of The NIS 2 Directive on Critical Infrastructures? – X. How Does the Cyber Solidarity Act Improve European Cybersecurity Policies? – XI. How Does Private Sector Involvement Impact Europol's Digital Threat Prevention? – XII. What Structural Differences Exist Between the US And EU Cyber Regulatory Models? – XIII. How Does the AI Act Regulate Defensive and Offensive Cybersecurity Technologies? – XIV. How Can the Ambiguity of State-Sponsored Cyber-Attack Attribution Be Overcome?

KEY FINDINGS: Cybercrime as a complex and evolving phenomenon; Global regulatory response and the Budapest Convention; Centrality of domestic Italian criminal and procedural protection; The transition toward cyber-resilience and mandatory sharing; Essential involvement of the private sector and security agencies; Protection of digital rights, AI Act, and cyberwarfare frontiers.

I. What Regulatory Instruments Become Available to The EU Following the Qualification of Cybercrime as A Eurocrime?

Following the qualification of computer crime (*cybercrime*) as a **Eurocrime**, based on **Art. 83, para. 1 of the Treaty on the Functioning of the European Union (TFEU)**, the European Union has acquired a specific criminal competence that allows it to adopt binding regulatory instruments to harmonize the legislations of Member States regarding the definition of offenses and their related sanctions. Art. 83 TFEU constitutes the legal basis that allows the Union to intervene in particularly serious areas of crime that have a cross-border dimension and a high potential for harm, as is the case with cybercrime. The necessity for a common response is dictated by the global nature of these phenomena, which cannot be effectively tackled through isolated national measures.
The **2009 Treaty of Lisbon** formalized the inclusion of cybercrime among the Eurocrimes, recognizing that computer offenses constitute a growing threat to critical

[*] Member of the Secretariat of the International & European Criminal Law Observatory (IECLO), University of Salerno, Italy.

infrastructures and public safety. Being phenomena without geographical borders, cybercrime requires international cooperation to be countered effectively.
This qualification is justified by **three main reasons** that we must remember:

- **The cross-border nature of the phenomenon:** It allows cybercrime to be perpetrated from any point in the world and to produce effects across multiple Member States, making purely national actions entirely insufficient.
- **The systemic threat:** It represents a danger to public safety, digital infrastructures, and personal data protection, with potentially devastating impacts on the economy and social stability of the Union.
- **The need for legal uniformity:** The criminal laws of Member States varied significantly, creating severe difficulties in cross-border cooperation and in the uniform enforcement of laws against computer crime. By virtue of this, the European Union has been able to adopt binding regulatory instruments to harmonize national legislations.

REFERENCES

Directive (EU) 40, 2013
Directive 2013/40/EU of the European Parliament and of the Council represents one of the primary regulatory instruments adopted in implementation of Art. 83, para. 1, TFEU. The latter is expressly cited in the legal basis of the directive, confirming that computer crime is considered one of the particularly serious forms of transnational crime over which the Union has competence to adopt minimum rules of substantive criminal law. The directive, therefore, does not limit itself to establishing obligations for Member States in terms of criminalizing specific conducts (such as illegal access to systems, illegal data interference, use and dissemination of malicious computer tools), but also lays the foundations for a structural strengthening of European cooperation, considering the operational and strategic involvement of supranational agencies such as **Eurojust** and **Europol** (through the European Cybercrime Centre - **EC3**) to be essential.

II. When does a Simple Digital Action Cross the Boundaries of Legality and become a Cybercrime?

From a technical-legal standpoint, a digital conduct becomes cybercrime when it presents certain essential elements that determine its criminal relevance. First, it requires an active behavior, concretely realized through computer tools, that violates a criminal provision. This conduct must be capable of harming or endangering a protected legal interest – such as system security, data confidentiality, or economic assets – and must be accompanied by the awareness and will to realize it, namely **intent (*dolo*)**. Not every improper use of technology is automatically a crime, but it becomes one when it crosses the threshold of criminal wrongfulness, meaning when the action offends a legally protected interest in a serious and conscious manner.
The boundary between lawful and unlawful, in the computer domain, is rendered particularly blurred not only by the apparent neutrality of digital tools but also by the invisible or automated nature of many conducts. One can consider the simple unauthorized use of a password to access an account: an apparently trivial gesture that, in the presence of intent and an actual or potential harm, can constitute unlawful access with criminal relevance. Or the massive sending of fraudulent emails, which can configure a computer fraud or unlawful data processing.

The purposes pursued by cybercriminals are manifold:

- **Economic advantages:** As in the case of ransomware or digital fraud.
- **Political or ideological goals:** As occurs with hacktivism and attacks on state infrastructures.
- **Personal or relational motives:** As in the more subtle forms of cyberstalking, revenge porn, or coercive control.

In all these cases, digital criminality feeds on the ability to act rapidly, anonymously, and potentially cross-border, escaping classical mechanisms of control and repression. The term cybercrime identifies that set of criminally relevant conducts realized through the unlawful use of information or telecommunication technologies, or that have digital systems, networks, and data as their direct target. It is a criminal phenomenon deeply linked to the digital transformation of society and the growing centrality of information in economic, social, and institutional life.

Computer criminality not only exploits new technologies but develops precisely within the folds of the digital dimension, making the detection of the offense, its repression, and often its definition more difficult. The international legal community has not yet produced a single, universally shared definition of cybercrime, but there is a convergent orientation in recognizing that it encompasses, on the one hand, **proper computer crimes**– namely those aimed at directly hitting the digital infrastructure, such as unauthorized access to a system, data damaging, or interference with a computer system – and, on the other hand, **common crimes committed by means of digital technologies (computer-related crimes)**, such as online fraud, child pornography, or online defamation. In both cases, what characterizes cybercrime is the centrality of the digital environment in the realization of the conduct.

REFERENCES

The Council of Europe Convention on Cybercrime (Budapest Convention), 2001

At the international level, the first reference regulatory instrument is the **Budapest Convention of 2001**, adopted by the Council of Europe and ratified by numerous States, including non-European ones. The Convention does not provide an abstract definition of the phenomenon but identifies a series of behaviors deemed criminally relevant insofar as they harm the integrity, availability, or confidentiality of computer systems and data. This outlines an open model capable of adapting to continuous technological transformations.

In the European domain, **Directive 2013/40/EU** represented a decisive step for the harmonization of national criminal regulations, introducing a common discipline on main computer crimes and promoting more effective cooperation among Member States. In this context as well, the definition of cybercrime remains functional to the typification of specific behaviors, rather than structured as a general category.

In the Italian context, **Law No. 48 of March 18, 2008** transposed the contents of the Budapest Convention, intervening on the Criminal Code with the introduction and modification of various provisions. Among the most relevant offenses that we must remember are:

- **Unauthorized access to a computer or telecommunication system (Art. 615-*ter* c.c.)**
- **Damaging of computer data, programs, or systems (Art. 635-*bis et seq*. c.c.)**
- **Computer fraud (Art. 640-*ter* c.c.)**
- Offenses related to the use of digital technologies for purposes of sexual exploitation, blackmail, or unlawful dissemination of content.

The classification of cybercrime conducts is divided into two categories:

- **Proper computer crimes**: Conducts directed against hardware, software, or digital data. The goal is to violate the integrity and confidentiality of the system (e.g., DDoS attacks, hacker intrusions, malware dissemination, ransomware).

- **Crimes committed via computers (Computer-related crimes)**: Traditional crimes that find in the network and telecommunication technologies a new and powerful means of execution and dissemination (e.g., telematic fraud, phishing, cyberstalking, online child pornography, defamation on social networks, counterfeiting of non-cash means of payment).

FOCUS

Comparison with other Eurocrimes: The Link between Cybercrime and Terrorism Financing

Computer criminality increasingly serves as a predicate offense or a logistical operational tool for the commission of other very serious Eurocrimes under Art. 83 TFEU. In international investigative practice coordinated by Europol, a tight link exists with **Transnational Terrorism** and the **Counterfeiting of means of payment**. Terrorist cells exploit cybercrime techniques (such as digital identity theft and phishing) to compromise bank accounts or clone credit cards in order to accumulate clean funds. Furthermore, the proceeds of online fraud and ransomware ransoms are regularly converted into anonymous cryptocurrencies and laundered (connecting to the Eurocrime of **Money Laundering**), providing eversive networks with the financial autonomy necessary to plan attacks or finance online radicalization campaigns without passing through the monitoring of the traditional banking system.

III. How Does the Budapest Convention Align with Domestic Penal Systems?

The absence of a uniform definitional and sanctioning framework on a planetary level has historically generated deep pockets of impunity, transforming un-updated criminal systems into true legal havens for cybercriminals. The asymmetric and delocalized nature of computer criminality means that a conduct orchestrated on one continent produces systemic damage on another, making the principle of **dual criminality** a potential obstacle to extradition and mutual legal assistance in the absence of harmonized treaties.

FOCUS

The Case of the "ILOVEYOU" Worm, 2000

The case of the "ILOVEYOU" computer worm, which spread on a global scale in May 2000, highlights in an emblematic way the limits of a fragmented international legal system in the fight against cybercrime. The virus, transmitted via e-mail in the form of an apparently innocent attachment (a fake love message in text format), self-replicated using the user's contact address book and compromised the files present on the device, causing damages estimated at **over 5.5 billion dollars** and hitting strategic world infrastructure and entities such as the CIA, the Pentagon, NASA, and Microsoft.

Investigative computer traces rapidly led to the identification of the suspected author, Onel de Guzmán, a Filipino computer science student. However, the **absence of specific national legislation** regarding computer crimes in the Philippines at the time of the facts prevented any form of domestic criminal prosecution, as well as extradition to the United States of America, precisely due to the **lack of the principle of dual criminality**. This historical episode brought to light how legislative disparities between jurisdictions can offer digital criminals true "safe havens", removing them from the repressive action of States. If a common and binding regulatory framework had existed among the nations involved, based on shared standards and effective judicial cooperation, the sanctioning response would have been far more effective, timely, and symmetrical.

To fill this geo-legal vacuum, the Council of Europe launched the **Budapest Convention of 2001**, which constitutes the first global reference system for the typification of computer crimes and for establishing common procedural rules in digital forensics. The Italian system transposed this multilevel framework through **Law No. 48 of March 18, 2008**, remodeling traditional offenses within the Criminal Code to adapt them to the virtualization of harms.

In order to facilitate university study and mnemonics for the exam, a detailed analysis and comparative study between the international Budapest model and the criminal response of the Italian legislator is presented below:

- **Unauthorized Access**
  - International Model (Art. 2 Convention): Requires intent and the intrinsic unlawfulness of the action. The transnational rule does not consider the presence of a specific unlawful purpose or the material violation of security measures as essential elements for the configuration of the offense.
  - Domestic Italian Discipline (Art. 615-*ter* c.c.): Focuses as a priority on the **violation of security measures** (access keys, credentials, digital barriers) introduced by the owner of the computer space, regardless of the absolute illegitimacy of the access.
  - Main Dogmatic Differences: The Convention does not consider the bypassing of physical or digital security barriers a necessary element, whereas the Italian system does. Furthermore, **unauthorized remaining** in the computer system beyond the limits of the mandate constitutes an autonomous offense in Italy but is not explicit in the Convention.
- **Data Interference**
  - International Model (Art. 4 Convention): Encompasses in an extended and all-inclusive way all intentional conducts of alteration, deletion, deterioration, concealment, or suppression of digital data.
  - Domestic Italian Discipline (Art. 635-*bis et seq*. c.c.): Punishes the damaging of private information, data, and computer programs, but establishes that **criminal prosecution is conditional upon a formal complaint (*querela*) by**

the injured person, except in the presence of specific aggravating circumstances (e.g., public assets or strategic infrastructures).
    - Main Dogmatic Differences: In the Italian system, it is necessary for the victim to submit a formal complaint within legal deadlines to activate criminal action (except in cases prosecuted *ex officio*), whereas the international Convention does not provide for this procedural distinction.
- **System Interference**
    - International Model (Art. 5 Convention): Concerns the serious, intentional, and unjustified hindering of the proper functioning of a computer or telecommunication system through the input or damaging of data.
    - Domestic Italian Discipline (Art. 635-*quater* c.c.): Introduces incrimination for the damaging of computer or telecommunication systems. The rule closely mirrors Art. 5 of the Convention, but legal doctrine notes that it was inserted among existing rules in a sometimes confused and stratified manner.
    - Main Dogmatic Differences: The Italian provision represents a direct and literal adaptation of the Convention's article, but it suffers from a partial lack of coordination and clear systematic integration with the traditional structure of the national Criminal Code.
- **Illegal Interception**
    - International Model (Art. 3 Convention): Punishes interception carried out without right, by technical means, of "non-public" transmissions of computer data (from, toward, or within a system). Defines technical means in a partially restrictive manner.
    - Domestic Italian Discipline (Art. 617-*quater* c.c.): Sanctions the illegal interception, prevention, or interruption of computer or telematic communications, but expressly adds liability for the conduct of **revealing or disclosing to the public** the content of the intercepted information.
    - Main Dogmatic Differences: The Italian penal system provides for a severe increase in punishment (special aggravating circumstance) in case of disclosure of protected data and, unlike the Convention, anticipates criminal protection by autonomously punishing the **installation of equipment designed to intercept** under Art. 617-*quinquies* c.c.
- **Computer Fraud**
    - International Model (Art. 8 Convention): Is based on the intentional causing of economic or patrimonial damage to another through any manipulation of data or interference with the functioning of the system. The procurement of an unjust profit is considered merely an element of intent.
    - Domestic Italian Discipline (Art. 640-*ter* c.c.): Configures computer fraud by sanctioning anyone who, by altering the functioning of a system or intervening without right in data, programs, or information, procures for himself or others an **unjust profit with damage to another**.
    - Main Dogmatic Differences: In Italy, the procurement of **unjust profit is an essential constitutive element** of the material fact for the configuration of the offense, whereas in the Budapest Convention it represents exclusively a possible subjective intention of the culprit.

IV. What Main Categories of Computer Crimes Define Domestic Substantive Law?

Law No. 547 of December 23, 1993, entitled "Modifications and integrations to the provisions of the Criminal Code and the Code of Criminal Procedure on the subject of computer crime", marked the **first systematic and organic intervention** of the Italian legislator aimed at adapting the national penal system to the challenges posed by technological evolution and the growing dissemination of criminal phenomena in the digital environment. Prior to this reform, magistrates were forced to apply traditional offenses (such as theft or common damaging) to dematerialized conducts analogously, facing severe constitutional limitations. The reform introduced and typified new criminal offenses within the Criminal Code destined to safeguard the integrity, confidentiality, and security of computer systems and communications.
The main categories of computer crimes introduced by Law 547/1993 that we must remember are:

- **Unauthorized access to a computer or telecommunication system (Art. 615-*ter* c.c.):** Incriminates anyone who enters a computer or telecommunication system protected by security measures without authorization, as well as anyone who remains therein against the express or tacit will of the person entitled.
- **Possession and unlawful dissemination of access codes/damaging programs (Art. 615-*quater* and *quinquies* c.c.):** Punishes the conduct of anyone who, for the purpose of procuring a profit for himself or others or causing damage to others, procures, holds, produces, disseminates, or installs programs designed to compromise, intercept, or interrupt the functioning of computer or telecommunication systems (e.g., dissemination of malware or spyware).
- **Damaging of computer or telecommunication systems (Art. 635-*bis* c.c.):** Provides a specific hypothesis of damaging aimed at hitting the efficiency, integrity, and functionality of electronic systems, data, and programs, safeguarding public and private interests in the availability of digital services.
- **Illegal interception, prevention, or interruption of computer or telecommunication communications (Art. 617-quater c.c.):** Disciplines and punishes conducts harming the freedom and secrecy of communications carried out via computer or telecommunication means, equalizing virtual space to the private domicile.
- **Computer fraud (Art. 640-*ter* c.c.):** Punishes anyone who, by altering in any way the functioning of a computer or telecommunication system or intervening without right in any modality on data, information, or programs, procures for himself or others an unjust profit with damage to another, configuring a technologically evolved form of the crime of swindling.

The repressive system introduced by Law 547/1993 constituted the foundation of criminal discipline in the field of computer crime, subsequently integrated and updated by **Law No. 48 of March 18, 2008**, with which Italy ratified and executed the **Council of Europe Convention on Cybercrime (Budapest, 2001)**. The latter introduced further reforms on both substantive and procedural levels, strengthening the regulatory response to computer crimes and promoting more effective international judicial cooperation instruments.

REFERENCES

Italian Code of Criminal Procedure, Art. 51, 3-*quinquies*

One of the innovations of greatest relief introduced into the Italian procedural system with the transposition of the Budapest Convention via Law No. 48 of 2008 concerns the modification of Art. 51 of the code of criminal procedure, with the insertion of para. 3-*quinquies*. The provision attributes **exclusive functional competence in the matter of computer crimes** (including Articles 615-*ter*, 617-*quater*, 635-*bis*, and 640-*ter* c.c.) to the public prosecutor at the Court of the capital of the district of the Court of Appeal, establishing the so-called **District Prosecutor's Office for Computer Crimes**.

FOCUS

The *Ratio* of Judicial Centralization

This regulatory choice of the Italian legislator responds to the technical and investigative necessity of tackling in a coordinated manner criminal phenomena characterized by a strong transnational dimension, the immateriality of evidence, and the structural difficulty of identifying a territorial scope or a *locus commissi delicti* of reference, as typically occurs in cybercrimes. The centralization of investigations at District Prosecutor's Offices allows:

- Greater immediate coordination between national and international investigative authorities (through the channels of **Europol and Eurojust**).
- The development of a high **technical and computer-forensic specialization** by the magistrates and judicial police units in charge (Postal and Communications Police).
- A homogeneous and swift judicial response, suitable to overcome territorial jurisdictional conflicts linked to the fluid nature of telecommunication networks.

The historical evolution of computer criminal law in Italy has followed three major steps:

- **Pre-1993 Phase (Regulatory Vacuum):** Absence of specific offenses; judges apply common offenses (e.g., swindling or damaging of movable things), clashing with the prohibition of analogy *in malam partem*.
- **National Typification Phase (Law 547/1993):** Introduction of proper offenses (Articles 615-*ter*, 640-*ter* c.c.); protection of "computer space" as an autonomous legal interest.
- **International Harmonization Phase (Law 48/2008 - Budapest):** District centralization of investigations (Art. 51 c.c.p.); introduction of sanctions for the administrative liability of entities (Legislative Decree No. 231/2001) for computer crimes and hardening of penalties for attacks on critical infrastructures, in line with **Directive 2013/40/EU**.

V. How Does European Legislation Address Jurisdictional Overlaps in Computer Crimes?

The growing dissemination of computer criminality at a transnational level has challenged traditional criteria for attributing criminal jurisdiction, based on the principle of territoriality, according to which the State exercises its judicial authority in relation to crimes committed within its geographical borders. Cyberspace, by its nature, is devoid of physical boundaries, making the application of traditional concepts of *locus commissi delicti* inadequate. In response to this complexity, European law has sought to address the critical issues connected to the overlap of investigations and jurisdictional fragmentation through the introduction of regulatory instruments aimed at guaranteeing effective judicial and investigative cooperation among Member States.

One of the first regulatory interventions in this sense is represented by **Council Framework Decision 2005/222/JHA** on attacks against information systems. Inspired by the Budapest Convention, it constituted the first binding regulatory act at the European level in the field of computer criminality. An innovative aspect introduced by the Decision concerns the provision of criteria for resolving conflicts of jurisdiction, which can arise when multiple Member States claim competence to prosecute criminally for the same criminal fact. The ultimate purpose of these provisions is to favor a rational distribution of jurisdictional competences, avoiding the risk of multiplication of criminal proceedings, negative conflicts of competence (namely investigative inertia due to jurisdictional uncertainty), or phenomena of criminal forum shopping, as well as guaranteeing operational coordination between competent authorities, also through judicial cooperation instruments and recourse to specialized European bodies, such as **Eurojust**.
This Framework Decision was subsequently succeeded by **Directive 2013/40/EU**, which repealed its provisions, offering a more organic and detailed regulatory framework. The Directive, in addition to typifying with greater clarity criminal offenses related to attacks against information systems – such as unauthorized access, illegal data interference, and the use of computer tools for the commission of offenses – strengthened the principle of operational cooperation among national authorities, both in the investigative phase and in the trial phase, fixing rigid cross-border jurisdictional criteria that bind Member States.

REFERENCES

Directive (EU) 40, 2013, Art. 12

"1. Member States shall establish their jurisdiction with regard to the offenses referred to in Articles 3 to 8 where the offense has been committed: a) in whole or in part on their territory; or b) by one of their nationals, at least in cases where the act constitutes a criminal offense at the place where it was committed.
2. When establishing their jurisdiction in accordance with paragraph 1, letter a), a Member State shall ensure that it has jurisdiction where: a) the offender commits the offense when physically present on its territory, whether or not the offense is against an information system on its territory; or b) the offense is against an information system on its territory, whether or not the offender was physically present on its territory at the time of committing the offense.
3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offense referred to in Articles 3 to 8 committed outside its territory, including where: a) the offender has his or her habitual residence in its territory; or b) the offense is committed for the benefit of a legal person established in its territory."

To understand the effective extension of the protection of "virtual space" and the application of these jurisdictional criteria, we must consider how the domestic Italian system qualifies the material object of the conduct, namely the very notion of a computer system, overcoming old physical limits.

CASE STUDY

Italian Cassation Court, Fifth Penal Section, No. 40470, 2018

The Court of Cassation, in judgment No. 40470 of 2018, affirmed a principle of fundamental systematic relief in the matter of computer crimes, clarifying that the notion of **"computer system"** cannot be reduced solely to the presence of a connection or an interconnection in a network, but must be understood in a broad and substantial sense. According to the Supreme Court, what matters for the purposes of criminal protection (e.g., for the application of Art. 615-*ter* c.c.) is the **aptitude of the machine (hardware) to organize and process data**, based on a program (software), for the pursuit of heterogenous purposes. Beside the function of mere registration and storage of data, the activity of processing and organizing the data themselves must also be present.

The judges of legitimacy specified that it appears completely **irrelevant that the apparatus is not connected to a telecommunication network**, provided that it is structured to operate according to logics proper to computer science (offline systems). The Court clarifies that internal criminal law has not provided a rigid regulatory definition of a computer system, but that, in the absence of a legislative classification, it is the case law of legitimacy that must specify its contours, in light of the **protective function of the "*ius excludendi alios*"** that the rule intends to pursue. This orientation strengthens the idea that protection extends to all those devices whose structure allows even partially the use of digital technologies (e.g., electronic safes, automotive control units, evolved cash registers) and imposes a substantial evaluation of the device's characteristics, based on its real operational functionalities and not on its mere formal classification.

The criteria for attributing jurisdiction in cybercrimes *ex* art. 12 of Directive 2013/40/EU are:

- **Criterion of Physical Presence (Offender):** The Member State is competent if the hacker or cybercriminal carried out the telematic action while physically located on its territory, regardless of nationality or the location where the targeted server is situated.
- **Criterion of the Targeted Infrastructure (Target):** The Member State holds jurisdiction if the computer system or the server victim of the attack is located on its geographical territory, even if the perpetrator acted physically from a third or non-EU State.
- **Criterion of Nationality and Habitual Residence:** Active competence for computer crimes committed abroad by its own nationals (subject to dual criminality) or by individuals stably residing in the territory of the State.
- **Criterion of Corporate Benefit (Legal Person):** Extension of the Member State's jurisdiction where the transnational cyber-attack was perpetrated to procure an economic or strategic advantage for a company or legal person that has its registered office in the territory of the State (connecting with the **Liability of Entities under Decree 231/2001**).

VI. How Does The 2024 UN Convention Innovate the Cybersecurity Framework?

The **2024 United Nations Convention on Cybercrime** represents a regulatory evolution of historical scope compared to the 2001 Budapest Convention, redefining the architecture of judicial and police cooperation on a planetary level. While the Budapest framework was born within the Council of Europe – configuring itself as a regional treaty open to the accession of third countries – the new UN Convention rests on an **ambition**

of multilevel universality, addressing technological asymmetries between the Global North and South.

The innovativeness of the United Nations text is based on **four strategic aspects** that we must keep in mind:

- **Inclusive Global Participation:** The text overcomes Western geopolitical blocs by extensively involving **developing countries**. Broadening the baseline of participation aims to clear out digital "safe havens", harmonizing the criminal response even in those jurisdictions that historically lacked resources to update their codes.
- **Cross-Border Common Penal Policy:** The UN Convention pursues, as a priority, a common penal policy aimed at protecting society from computer crime. This objective is enacted through the typification of new offenses and common procedural powers that take into account the total virtualization of economic assets and data.
- **Obligation of Technical Assistance and Capacity Building:** Unlike previous treaties, the UN introduces a true pillar of **solidary cooperation**. Technologically advanced States have an obligation to provide forensic software, training, and structural support to countries with lower operational capacity, strengthening the global resilience of networks and the stability of digital forensics systems.
- **Institutionalization of INTERPOL's Role:** The text recognizes and codifies the essential role of **INTERPOL**, the international criminal police organization that reunites 196 States. INTERPOL is integrated as the primary nerve hub to facilitate the **rapid, secure, and encrypted exchange of information** and digital evidence among the investigative authorities of different continents.

REFERENCES

United Nations Convention against Cybercrime, 2024, Preamble and Purposes
The Convention establishes that States Parties undertake to promote and strengthen measures aimed at preventing and combating computer crime more efficiently and effectively, promoting, facilitating, and supporting international cooperation and technical assistance, including the development of technological capabilities of police forces, in full respect of the rule of law and human rights.

The 2024 UN Convention dedicates wide space to the intersection between information and communication technologies (ICT) and the most serious forms of transnational organized crime. In international application practice, an indissoluble link emerges between cybercrime and the Eurocrime of **Trafficking in human beings**. Modern criminal networks use computer techniques not only for the digital recruitment of victims (e-recruitment) but exploit the black markets of the Darknet to purchase surveillance and geolocalized tracking software for exploited migrants. Furthermore, large-scale computer frauds and banking system breaches managed by hacker cells serve to produce the liquidity necessary to finance the logistics and transport of victims across the borders of the European Union, highlighting how computer crime is by now the enabling infrastructure of all other Eurocrimes under Art. 83 TFEU.

FOCUS

Comparative Study of Conventions on Cybercrime (Budapest 2001 v. UN 2024)

Budapest Convention (2001 - Council of Europe):

- Genesis: Euro-Atlantic and regional matrix.
- Focus: Typification of classical computer crimes (unauthorized access, data interference).
- Limits: Difficult penetration in developing countries due to the lack of structured financial and technical assistance tools.

UN Convention on Cybercrime (2024):

- Genesis: Universal matrix (United Nations General Assembly).
- Focus: Multidisciplinary approach to ICT, countering the illicit use of cryptocurrencies, and timely removal of terrorist and child pornography content.
- Innovation: Obligation of international Capacity Building, 24/7 emergency cooperation, and a direct portal through the INTERPOL network.

VII. How Are INTERPOL's Modern Global Strategies Structured Against Computer Crime?

The study of computer crime and its relative defense strategies demands an in-depth analysis of its historical origins. This analysis demonstrates that the birth of modern **cybersecurity** was not the result of theoretical planning, but rather an immediate reaction to large-scale computer incidents that exposed the intrinsic fragility of early global network infrastructures.

FOCUS

The "Morris Worm" and the Birth of Cybersecurity, 1988

The **Morris Worm** was one of the most significant and disruptive events in the history of information security, marking the **first major large-scale attack on the Internet**. Released on November 2, 1988, the worm was designed and launched by Robert Tappan Morris, a graduate computer science student at *Cornell University*. The original intent, according to the defense, was purely exploratory – aimed at measuring the size of the Arpanet network (the ancestor of the Internet). However, due to a programming error in the code, the worm began to replicate uncontrollably. The algorithm rapidly infected thousands of computers connected to the network, overloading processors, causing system crashes, total service disruptions, and considerable economic and logistical damage to universities, research centers, and US military laboratories.

Under the profile of judicial prosecution and comparative criminal law, Morris was indicted under the **Computer Fraud and Abuse Act (CFAA) of 1986**, historically becoming the **first individual convicted** under this special legislation on computer crimes in the United States of America. In 1991, the federal Court sentenced him to three years of probation, a $10,050 fine, and mandatory 400 hours of community service.

The Morris Worm represented a radical **turning point in the history of information security**, drastically increasing the awareness of public and private institutions regarding structural network vulnerabilities and the risks connected to malware codes capable of self-replicating autonomously. The incident highlighted how exposed and defenseless systems were against new types of asymmetric attacks. One of the most significant institutional and procedural consequences of the event was the immediate creation of the first **Computer Emergency Response Team (CERT)**, a technical rapid-response body tasked with providing support, analysis, and central coordination during computer emergencies. The attack also pushed the scientific community to develop and deploy the first essential tools for advanced perimeter defense, such as **firewalls** and network intrusion detection systems (IDS), paving the way for modern cybersecurity. The Morris Worm case established itself as a crucial jurisprudential precedent, proving the urgent need for specific criminal regulations and security structures ready to respond to digital threats.

Having outlined the historical origins of the phenomenon, in the current technological and geopolitical scenario of **2026**, governance and the global operational response to advanced cybercrimes are entrusted to the coordination of INTERPOL, which implements multi-year action plans to support the law enforcement forces of its 196 Member Countries.

The INTERPOL Strategic Framework 2022-2025 is the multi-year planning instrument through which the Organization defines its operational, institutional, and technological priorities to strengthen the support provided to national law enforcement. Approved by the General Assembly at its 89th session (November 2021), the document adopts a global, future-oriented approach to address the emerging challenges of transnational and computer crime. The programmatic plan is articulated across **four strategic objectives** and 17 operational targets that we must remember:

- **Trusted information for action:** The aim is to thoroughly strengthen access to and interoperability of INTERPOL's information systems and databases by national police authorities, guaranteeing the secure use of data and the development of high-quality criminal and forensic analyses. Strict and binding compliance with international standards on personal data protection and fundamental rights is central and mandatory, serving as an indispensable element to consolidate mutual trust among States using the Organization's protected communication systems.

- **Partnerships for global security:** INTERPOL aims to consolidate its role as the central global platform for immediate information exchange and operational coordination in the fight against transnational organized crime. This strategic objective includes promoting diversified partnerships with the private sector (tech companies), strengthening the technical capabilities of Member States (particularly developing countries through dedicated programs), and actively contributing to United Nations regulatory processes by offering strategic recommendations in the fight against advanced computer crime, in perfect synergy with the new 2024 UN Convention.
- **Innovation in policing (Smart Policing):** Through a massive push toward digitalization and the native integration of emerging technologies (such as Artificial Intelligence applied to predictive policing and data analytics software), INTERPOL intends to improve the efficiency of its investigative processes and the quality of services offered to Member Countries. In this perspective, promoting a permanent global dialogue with public and private actors is vital to developing innovative forensic solutions to counter crime.
- **Organizational efficiency and governance:** Strengthening the Organization's operational and administrative capacity requires modern leadership, decentralized resource management, and an internal corporate culture strictly grounded in the values of ethics, total transparency, and inclusion. Particular attention is dedicated to organizational resilience in the face of geopolitical crises, integrated risk management, and the consolidation of the internal legal framework to secure the institution.

VIII. What Function Does Incident Information Sharing Perform Within the Context of European Cybersecurity?

The sharing of incident information performs a **strategic and advanced prevention function** within European cybersecurity, configuring itself as an essential tool to guarantee systemic resilience, operational continuity of the single market, and a coordinated response capacity against asymmetric transnational threats. Cyberspace renders obsolete old models of isolated defense: a ransomware or DDoS attack hitting an infrastructure in one Member State represents an immediate alarm bell for the entire Union.

The architecture of community cybersecurity has historically structured itself through **Regulation (EU) No 526/2013**, which imposed on Member States the obligation to designate competent national authorities and to establish **CSIRTs (Computer Security Incident Response Teams)**, with the aim of creating an integrated, synergistic network to mitigate threats beyond geographical borders. This obligation, formalized through provisions requiring the mutual exchange of information regarding significant digital incidents, configures itself as an indispensable mechanism for timely monitoring and coordinated crisis management, strengthening the collective protection of the Union. The community regulatory action provides for information regarding incidents to be shared in a structured, standardized, and continuous manner between designated national authorities, allowing for the alignment of operational responses on the field and guaranteeing effective emergency management. Within this multilevel ecosystem, **ENISA (The European Union Agency for Cybersecurity)** plays a central role, acting

as a coordination hub and facilitating the transfer of knowledge, predictive analyses, and best practices among Member Countries.

The regulatory framework on information security at the community level was subsequently consolidated and standardized through the **Cybersecurity Act (Regulation EU 2019/881)**, which repealed and replaced the previous Regulation 526/2013, granting ENISA a **permanent mandate** and equipping it with greater resources. This regulatory pillar introduced, among other structural measures, the first **European cybersecurity certification framework** for ICT products, processes, and services. This system aims to standardize and elevate the security level of digital devices placed on the market (from corporate software to Internet of Things – IoT – devices), guaranteeing adequate protection against the growing technological sophistication of attacks. The Cybersecurity Act also establishes and values the **Interinstitutional Cybersecurity Board (IICB)**, a special body tasked with monitoring, supporting, and supervising the implementation of cybersecurity measures specifically within European Union institutions, bodies, and agencies, favoring constant dialogue with national authorities and supporting the development of common guidelines.

In the current context of **2026**, this framework for sharing information and the resilience of critical infrastructures has found its definitive operational fulfillment through the mandatory transposition of the **NIS 2 Directive (Directive EU 2022/2555)**. This text has drastically raised security standards for essential sectors (energy, transport, banking, health, and digital infrastructures), introducing a strict obligation for **early warning notifications of significant incidents within 24 hours** to the national authority and ENISA, backed by severe administrative and financial sanctions for non-compliant corporate executives.

REFERENCES

Regulation (EU) 881, 2019, Art. 4

The Regulation establishes that ENISA shall pursue the objective of achieving a high common level of cybersecurity across the Union, supporting Member States and European institutions in developing operational capabilities and cross-border cooperation, promoting the timely sharing of information on cyber threats and incidents among all strategic network actors.

FOCUS

Eurocrime Interconnection: Computer Fraud and the Counterfeiting of Non-Cash Means of Payment

The rapid sharing of information on computer incidents coordinated by ENISA and Europol proves to be an essential safeguard to restrict the ramifications of other Eurocrimes under Art. 83 TFEU. There is a direct operational link with the **Counterfeiting of non-cash means of payment** (protected by Directive EU 2019/713). When a structured criminal group launches an advanced cyber-attack against an EU banking institution's home banking system or inoculates a malware into commercial POS terminals, the event is classified as a cybersecurity incident. The immediate sharing of technical data and "Indicators of Compromise" (IoCs) through the European CSIRT network allows other banks and Eurozone supervisory authorities to proactively shield their servers. This blocks mass credit card cloning, financial identity theft, and subsequent telematic fraud, stopping the laundering of illicit capital at its source.

The European Architecture for Cyber Incident Sharing and Management is divided into four phases:

- **Phase 1 - Detection and Early Warning (National/Corporate Level):** An operator of essential services (e.g., a hospital or power plant) suffers a cyber-attack and is obliged under the NIS 2 Directive to submit an early warning notification within 24 hours to the competent national CSIRT.
- **Phase 2 - Centralization and Forensic Analysis (ENISA):** The national CSIRT transfers the technical data to ENISA. The agency analyzes the malware, isolates its digital signature, and drafts a technical risk mitigation report.
- **Phase 3 - Cross-Border Dissemination (CSIRTs Network):** ENISA distributes the security alert to all CSIRTs across the other 26 Member States, enabling proactive blocking of servers and communication ports on a continental scale.
- **Phase 4 - Internal Institutional Monitoring (IICB):** The IICB applies the same security standards within the servers of the European Parliament, Commission, and Council, verifying the defense and impermeability of the Union's own systems against external threats.

IX. What Is the Impact of The NIS 2 Directive on Critical Infrastructures?

The adoption of **Directive (EU) 2022/2555 (known as the NIS 2 Directive)** has significantly impacted the European system for protecting critical infrastructures, moving past the limitations inherent in the previous Directive (EU) 2016/1148 (NIS 1) and radically strengthening the regulatory framework of cybersecurity.

NIS 1 represented the first historic step toward harmonized regulation at the European level regarding the security of network and information systems. It introduced minimum obligations for **Operators of Essential Services (OES)**, active in strategic fields such as energy, transport, healthcare, and finance, as well as for **Digital Service Providers (DSPs)**. Central to this was the provision of a cooperation mechanism between Member States via **CSIRTs** and the NIS Cooperation Group, aiming to strengthen the collective response to cyber incidents.

However, concrete enforcement experience highlighted significant structural weaknesses in NIS 1: fragmented and inconsistent approaches among Member States (due to excessively wide margins of discretion in national transposition), limited subjective scopes of application, an absence of common security criteria, and a lack of incisiveness in criminal and administrative sanctions. With NIS 2, the European Union intervened to build a more coherent, comprehensive, and resilient system, adapted to the new technological and geopolitical context of **2026**.

Compared to NIS 1, the new directive does not merely update but **redefines the entire regulatory architecture**, focusing on four macro-innovations that we must remember:

- **Removal of the OES/DSP Distinction and Subjective Expansion:** The old classification between operators of essential services and digital service providers has been eliminated, replaced by size-based criteria establishing two new categories: **"Essential Entities"** and **"Important Entities"**. This expansion includes public administrations, manufacturing sectors, chemicals, waste management, and postal services.
- **Supply Chain Security:** Increased attention is directed toward the security of commercial and technical relationships with external ICT partners and vendors, identified by ENISA as potential systemic **single points of failure**.

- **Direct Governance Accountability:** Specific obligations are introduced that directly involve **management bodies and board members** of the affected organizations. They face personal liability, including financial penalties, for failing to approve or supervise corporate cyber risk management measures.
- **Harmonized and Effective Sanctioning Regime:** It introduces administrative and statutory fines aligned with the GDPR model, providing for financial penalties of up to **10 million euros or 2% of the total worldwide annual turnover** for non-compliant essential entities.

REFERENCES

Directive (EU) 2555, 2022, Art. 21

Art. 21 mandates that essential and important entities take appropriate and proportionate technical, operational, and organizational measures to manage risks posed to the security of network and information systems. These measures must strictly include: risk analysis policies, incident handling, business continuity (business continuity and disaster recovery), supply chain security, cryptography, and the use of multi-factor authentication (MFA) solutions.

The structural differences between the NIS 1 and the NIS 2 Directive are the following:

- **Subjective and Objective Scope of Application**
  - NIS 1 Directive: Restricted to predefined traditional essential sectors such as energy, transport, health, and banking, leaving wide margins of discretion to States in identifying individual operators.
  - NIS 2 Directive: Extended to a wide range of strategic sectors, including digital services, cloud computing providers, e-commerce portals, electronic communication networks, and all critical and important infrastructure providers based on clear size thresholds.
- **Cyber Risk Management Obligation**
  - NIS 1 Directive: Provided a general, generic, and abstract obligation to adopt proportionate security measures for networks and information systems.
  - NIS 2 Directive: Introduces a strict focus on technical risk management, mandating specific security measures and an absolute obligation to control and audit **supply chain security**.
- **Timeframes for Incident Reporting and Notification**
  - NIS 1 Directive: Stated that a serious incident had to be reported to competent national authorities or CSIRTs without undue delay, a parameter typically quantified as within **72 hours**.
  - NIS 2 Directive: Drastically tightens reaction times, mandating that a significant incident must be reported via an initial early warning alert **within 24 hours** of becoming aware of it.
- **Sanctioning and Liability Regime**
  - NIS 1 Directive: Provided for sanctions in case of non-compliance, but these were less severe, lacked common statutory maximums, and were fragmented among individual national legislators.
  - NIS 2 Directive: Introduces much more severe, harmonized penalties based on the GDPR model, including hefty administrative-financial fines proportional to global turnover and personal civil liability for board members.
- **Cooperation and Information Exchange Between Member States**

  - NIS 1 Directive: Regulated limited cooperation and a primarily formal or voluntary coordination between different national authorities.
  - NIS 2 Directive: Mandates a radical reinforcement of mandatory cross-border cooperation, featuring active, standardized, and real-time exchange of information on cyber threats and emerging software vulnerabilities.
- **Powers of Competent National Authorities**
  - NIS 1 Directive: Established that each Member State should designate one or more responsible authorities, which were often devoid of real powers for direct inspections or corporate audits.
  - NIS 2 Directive: Requires every Member State to have centralized cybersecurity authorities that are structurally stronger and armed with **greater powers of proactive oversight, criminal, and administrative enforcement**.
- **Protection and Resilience of Critical Infrastructures**
  - NIS 1 Directive: Regulated the protection of critical infrastructures at the community level, but in a less detailed manner that lacked a synergistic link with physical security.
  - NIS 2 Directive: Places major strategic emphasis on coordinated **global resilience and protection**, working in tandem with the CER Directive (EU 2022/2557) on the physical resilience of critical entities.

X. How Does the Cyber Solidarity Act Improve European Cybersecurity Policies?

The **Cyber Solidarity Act**, formally approved by the European Union and entering fully into force in **February 2025**, represents the operational pillar of European collective cyber defense. This regulation introduces a complex set of legal, financial, and operational measures aimed at overcoming the fragmented defensive approaches of individual Member States, establishing instruments designed to strengthen capabilities to prevent, detect, and handle cyber threats with cross-border or potentially systemic impacts.
The architecture of the regulation rests on **four operational pillars** that we must keep in mind:

- **The European Cyber Shield:** An integrated, cross-border network of **national and multi-state Security Operation Centres (SOCs)**. These centers, utilizing advanced artificial intelligence and data analytics, are tasked with continuous network traffic monitoring, immediate technical information sharing on emerging threats, and defining coordinated Union-wide responses.
- **The EU Cybersecurity Reserve:** A genuine "task force" consisting of **highly specialized and accredited private security and emergency response services**. These vendors are deployable and financially covered by EU funds to offer immediate emergency interventions in the event of severe cyber-attacks against public institutions or critical infrastructures, guaranteeing rapid, structured operational support.
- **The Cyber Incident Review Mechanism:** A review process for significant incidents through which the dynamics, exploited vulnerabilities, and consequences of major attacks are analyzed. The goal is to draw lessons from systemic failures to update the Union's preventive strategies and increase operator accountability.

- **Regular Testing of Vulnerable Sectors:** Funding and planning systematic security audits of information systems in the most exposed compartments (energy, finance, transport, and healthcare) to detect structural weaknesses before threats can materialize on the field.

REFERENCES

Regulation (EU) 38, 2025, General Objectives
The legislative text establishes a Union solidarity mechanism to strengthen common detection capabilities and situational awareness of cyber threats. It sets up a cybersecurity reserve at the European level to assist Member States in the event of significant or large-scale incidents, ensuring single market continuity and internal security.

The solidarity measures and the Cyber Shield established by the Cyber Solidarity Act have become essential in the current **2026** geopolitical context to counter connections between cybercrime and other Eurocrimes under Art. 83 TFEU, particularly **Transnational organized crime**. Modern criminal syndicates and state-sponsored hacker groups coordinate cyber-attacks on port logistics or customs systems, not merely for extortion, but to temporarily paralyze security checks. The European shield of SOCs allows for the interception of these anomalous intrusions in real time, preventing system lockouts from being exploited as a diversion to facilitate the smuggling of illicit shipments connected to **Drug trafficking** or **Human trafficking**.

FOCUS

Technological Evolutions: The Quantum Security Transformation, 2025
Throughout **2025** and **2026**, the field of cybersecurity is experiencing a radical transformation driven by the adoption of quantum technologies and the definition of new digital sovereignty models for the Union. This scenario, constantly monitored by ENISA and national authorities, articulates around three technological and legal pathways:

- **Post-Quantum Cryptography (PQC):** Emerging as the mandatory foundation to protect the Union's strategic communications against decryption threats posed by future quantum computers, utilizing complex mathematical algorithms that ensure unbreakable security.
- **Quantum Key Distribution (QKD):** Advanced protocols based on quantum physics that make it virtually impossible to intercept or spy on the exchange of encryption keys, since any interception attempt alters the physical state of the particles, immediately alerting the system.
- **Predictive Models and Adaptive Defenses:** Risk assessment in critical infrastructures evolves by integrating technical tools of quantum artificial intelligence to anticipate threats and react flexibly, establishing criteria for shared responsibility and operational transparency between public and private actors.

XI. How Does Private Sector Involvement Impact Europol's Digital Threat Prevention?

In a geopolitical and technological context characterized by increasingly sophisticated, rapid, and transnational cyber threats, public-private cooperation is no longer an optional accessory, but rather a **structural necessity** to guarantee the effectiveness of the Union's cybersecurity policies and criminal law enforcement. **Europol** (the European Union Agency for Law Enforcement Cooperation) has progressively extended its mandate in

response to the digitalization of criminal activities. This institutional evolution saw a fundamental turning point with the establishment and reinforcement of the **European Cybercrime Centre (EC3)**, a highly specialized structure operating within the agency to coordinate the EU's strategic and operational response to computer crime.
The EC3 exercises its competence in computer crime by focusing on **three macro-areas of high social alarm** that we must remember:

- **Cybercrimes for profit:** Conducts managed by transnational organized crime groups aimed at producing massive illicit financial flows, such as e-commerce fraud, large-scale phishing, and ransomware attacks targeting banking institutions.
- **Cybercrimes causing serious harm:** Computer crimes directly attacking human dignity and fundamental rights, with specific reference to online child sexual exploitation and abuse (CSAM - Child Sexual Abuse Material).
- **Attacks against critical infrastructures:** Structured actions directed against information systems of strategic importance for Member States (e.g., Distributed Denial of Service – DDoS attacks against energy or health networks), aimed at paralyzing essential services.

In this framework, strategic collaboration with the private sector assumes a crucial role. Private enterprises – particularly major technology companies (Big Tech), Internet Service Providers (ISPs), cybersecurity firms, and financial institutions – are structurally the first actors to have immediate visibility over new software vulnerabilities and anomalous network traffic flows.
Their active involvement allows for a **two-way flow of information**: on one side, Europol and the EC3 benefit from timely data, advanced technical expertise, and cutting-edge forensic technologies; on the other, private companies receive directives, Indicators of Compromise (IoCs), and institutional support to prevent the escalation of threats and protect their customers. Through the EC3, Europol has institutionalized this synergy through structured partnerships aimed at exchanging operational intelligence, sharing digital investigative tools, and co-developing advanced cyber-defense technologies, raising the cyber-resilience of the European Space.

FOCUS

Investigative Practice: The EC3 Strategic Tools (The IOCTA Report and the J-Cat)
To guide the field activities of law enforcement forces and define the action priorities of the permanent **EMPACT** platform, the European Cybercrime Centre relies on two strategic operational instruments:

- **The IOCTA Report (Internet Organised Crime Threat Assessment):** An in-depth assessment that the EC3 drafts and publishes periodically. This document provides quantitative operational data, strategic intelligence, and analyses of emerging trends in cybercrime (e.g., the abuse of artificial intelligence for hostile attacks or the evolution of cryptocurrency scams), serving as a compass for European legislators and investigators.
- **The J-CAT (Joint Cybercrime Action Taskforce):** A permanent operational taskforce hosted at the headquarters of the EC3. The mission of the J-CAT is to coordinate and execute complex cross-border investigations and operations based on intelligence, aimed at countering and dismantling the primary networks of hackers and digital criminals, drawing on direct operational support from liaison officers seconded from Member Countries and international partners (e.g., the United States, United Kingdom).

XII. What Structural Differences Exist Between the US And EU Cyber Regulatory Models?

The phenomenon of cybercrime is not limited to the mere alteration of network systems, but qualifies as an asymmetric eversive tool aimed at the **exfiltration and commercialization of private, corporate, and strategic information assets**. Personal and industrial data constitute the true currency of exchange in the digital economy, turning storage servers into the primary target of targeted attacks managed by transnational cartels.

FOCUS

Crimes on Information assets (Sony Pictures 2014 & Equifax 2017)

The analysis of international practice highlights two landmark cases that illustrate the differing nature of digital offenses:

- **The attack on Sony Pictures (2014):** Represents the prototype of corporate cyber-sabotage with a geopolitical matrix. Structured hacker cells breached the multinational's servers, exfiltrating and disseminating online confidential executive emails, unreleased scripts, and protected financial data. The event caused not only devastating direct economic damage, but a **severe, permanent impact on commercial reputation** and the security of intellectual property, highlighting the vulnerability of digitalized industrial secrets.
- **The Equifax system breach (2017):** Constitutes one of the most severe and massive data breach cases in global economic history, operating as a direct attack on consumers. Cybercriminals exploited a known, unpatched *software* vulnerability to penetrate the databases of one of the main credit reporting agencies in the US. The attack **exposed the personal and sensitive data of over 140 million individuals**, including social security numbers, dates of birth, driver's licenses, and protected financial details, putting the privacy and economic security of a massive segment of the population at risk and fueling the Eurocrime of **Counterfeiting of non-cash means of payment** through subsequent financial identity theft.

Under the profile of comparative law, the Equifax case highlighted the structural weaknesses of the **United States data protection system**. The regulatory approach of the United States relies on a **sectoral, fragmented, and inconsistent framework** (*patchwork approach*), devoid of an omnibus federal privacy law, which leaves wide regulatory gaps and creates asymmetries of protection across different States.
Conversely, the European Union adopted an opposing regulatory philosophy based on the precautionary principle and the centrality of an individual's fundamental rights. Through the **GDPR (Regulation EU 2016/679)**, the Union imposed a **comprehensive, uniform, and directly applicable model** across the EU, built on the principles of *privacy by design* and *accountability*. This framework mandates *data breach* notifications within 72 hours and levies severe sanctions proportional to a company's global turnover. This rigorous protective architecture applies not only against external illicit intrusions, but serves as a preventive and sanctioning shield against emerging technologies and commercial artificial intelligence systems.

FOCUS

The Italian *Garante della Privacy*'s Injunction on ChatGPT, 2023

Particularly significant regarding future developments, including criminal ones (connected to large-scale illicit data processing), is the decision taken via **Injunction No. 112 of March 30, 2023, by the Italian Data Protection Authority (*Garante per la protezione dei dati personali*)**, which ordered a temporary limitation on data processing for national users against *OpenAI*, the US company behind well-known artificial intelligence software **ChatGPT**.

The Italian Garante identified two structural macro-violations of GDPR parameters:

- **Absence of Disclosure and Legal Basis:** ChatGPT failed to provide users with any clear disclosure regarding personal data collection. Furthermore, there was a structural **absence of any suitable legal basis** to justify the massive scraping and storage of personal information for the purpose of "training" the platform's underlying algorithms.
- **Lack of Age Verification Filters:** Despite the service being theoretically aimed at users over 13, the Authority noted a total absence of technical systems to verify a user's actual age, exposing minors to completely inappropriate software responses relative to their developmental stage and self-awareness.

This landmark intervention, which anticipated the strict criminal and administrative *compliance* requirements later introduced by the **European Artificial Intelligence Act (AI Act)**, opened a permanent debate on balancing algorithmic innovation with digital sovereignty and European citizens' core rights.

The centrality of protecting information assets within the Euro-unitarian space finds its ultimate fulfillment in civil liability paths for cyber-attack victims, extending data controllers' responsibility far beyond tangible financial loss alone.

CASE STUDY

Court of Justice of the European Union, VB v. Natsionalna agentsia za prihodite, 2023

With its judgment of December 14, 2023, in Case C-340/21, the Court of Justice of the European Union offered an important, innovative clarification regarding **recoverable non-material damage for GDPR violations** following a cyber-attack. The Luxembourg judges clarified that the **fear felt by a person** that their personal data, following a *data breach*, might be unlawfully used by third parties can, by itself, constitute a compensable non-material damage under **Art. 82 of the Regulation**.

It is therefore not necessary for the data subject to prove a concrete, already occurring abusive use of the data, or that the psychological injury has reached a statutory minimum threshold of severity. It is sufficient for the individual to prove they suffered a form of **distress, worry, or anxiety** linked to the actual risk that their personal data might be subject to misuse in the future. The Court specified that Art. 82(1) precludes a national practice that conditions compensation on a minimum gravity threshold of non-material damage, and that one cannot exclude from the very concept of non-material damage a situation where the data subject invokes the fear that their personal data will be subject to future misuse by third parties. This historic ruling raises the cyber-resilience standard for European businesses, forcing them to invest thoroughly in the security protocols mandated by the **NIS 2 Directive** to prevent class-action compensation claims by consumers.

XIII. How Does the AI Act Regulate Defensive and Offensive Cybersecurity Technologies?

The evolution of **Artificial Intelligence (AI)** has had a disruptive impact on computer crime, introducing new attack methods that pose complex technical, criminological, and legal challenges. The contemporary cyber space of **2026** is configured as an asymmetric theater of conflict where AI is utilized both as an offensive weapon and a shield of predictive defense.

On the front of offensive threats, the use of **advanced generative AI systems** allows *cyber-criminals* to design and deploy **polymorphic and adaptive malware**. These malicious codes are capable of autonomously modifying their own strings and dynamically adapting to the operational environments into which they are inoculated, evading traditional detection mechanisms based on fixed digital signatures used by ordinary *antivirus* software. Added to this is the increasingly sophisticated use of social engineering (*social engineering*), enhanced by the automated, mass analysis of large amounts of personal and economic data from open sources (*OSINT*) or compromised databases (*data breach*). This allows eversive cells to create highly personalized fraudulent communications and *phishing* emails (*spear phishing*), increasing the effectiveness of the deception. Another particularly insidious expression of AI in the criminal context concerns the use of **deepfake** technology, which allows for the high-precision biometric simulation of real subjects' vocal, phonic, and visual appearances to carry out complex identity frauds and gain unauthorized access to protected systems.

Nevertheless, AI offers extremely powerful tools to reinforce cyber defenses, turning into a strategic ally for *cybersecurity*. Through the application of **predictive algorithms and Machine Learning models**, it is possible to analyze colossal volumes of network traffic in real time, quickly identifying anomalous behaviors or statistical deviations that indicate a cyber-attack is underway. This preventive detection capability allows for immediate mitigation action by CSIRTs, which is decisive in containing damage and isolating compromised servers before data encryption takes place. In the banking sector, the integration of AI into financial monitoring systems enables the identification of suspicious transactions and atypical account accesses, facilitating the adoption of **adaptive multi-factor authentication (MFA) measures**. Finally, AI proves indispensable in post-attack digital investigations (*incident response*), supporting forensic analysis, system log correlation, and the temporal reconstruction of intrusion dynamics.

In this technologically fluid context, the European Union's intervention through the adoption of **Regulation (EU) 2024/1689 (globally known as the AI Act)** holds a central dogmatic relevance, standing as the world's first comprehensive framework on artificial intelligence.

REFERENCES

Regulation (EU) 1689, 2024, Recitals 4, 5, and 6

The European legislator, in the introductory recitals of the AI Act, establishes the dual and anthropocentric philosophy of the rule:

Systemic Benefits (Recital 4): AI represents a fast-evolving family of technologies that brings a wide range of economic, environmental, and social benefits across the entire spectrum of industries and social activities. By improving forecasting, optimizing operations and resource allocation, and personalizing digital solutions, AI can provide key competitive advantages to companies and lead to beneficial social and environmental outcomes, such as in healthcare, infrastructure management, energy, transport, security, and justice.

- **Risks and Prejudices (Recital 5):** At the same time, depending on its specific application, utilization, and technological development, AI can generate risks and harm public interests and fundamental rights protected by Union law. Such harm can be both material and non-material, including physical, psychological, social, or economic injury.
- **The Anthropocentric Approach (Recital 6):** Given the significant impact AI can have on society and the need to build trust, it is essential that AI and its regulatory framework develop in accordance with Union values (Art. 2 TEU) and fundamental rights and freedoms (Art. 6 TEU, Charter). As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

To translate these principles into binding legal obligations, the AI Act introduces a strict risk-based approach for classifying intelligent software. Systems intended to be used for the management and operation of **critical infrastructures** (such as water, gas, electricity, and transport networks), as well as those used by law enforcement for crime risk assessment or remote biometric identification, are strictly classified as **high-risk systems**. Such systems are subject to demanding technical and legal *compliance* obligations, including risk management systems, total training data traceability (*data governance*), technical robustness against external attacks (*cyber-resilience*), and mandatory **human oversight (*human-in-the-loop*)**.

The AI Act categorically prohibits AI systems presenting an unacceptable risk, such as subliminal behavioral manipulation practices or social scoring . This regulatory framework, coordinating in perfect tandem with the **NIS 2 Directive** and the **Cyber Solidarity Act**, responds to the need to ensure that European digital security is built on ethical, transparent, auditable, and legally sustainable foundations, guaranteeing that algorithmic innovation does not result in a violation of the rule of law.

FOCUS

AI in Deepfakes and the Counterfeiting of Non-Cash Means of Payment

The abuse of AI technologies and the creation of sophisticated audiovisual deepfakes constitute the operational arm for executing behaviors falling under other Eurocrimes under Art. 83 TFEU, with specific reference to the **Counterfeiting of non-cash means of payment** and **Organized crime**. In international financial fraud schemes, criminal syndicates use AI-assisted voice cloning (*voice cloning*) to simulate executives' directives over the phone (*CEO Fraud*), inducing accounting departments to transfer massive amounts of money to offshore bank accounts. The integration of intelligent monitoring systems mandated by the AI Act and banking supervision authorities (the European **AMLR** package) allows for the detection of atypical financial orders, blocking fraudulent transactions and severing the profit line of mafia organizations.

XIV. How Can the Ambiguity of State-Sponsored Cyber-Attack Attribution Be Overcome?

The increasing integration of information technologies and offensive digital tools into national military strategies (a phenomenon known as ***cyberwarfare***) raises substantial legal and dogmatic issues regarding international responsibility for state-sponsored cyber operations. The primary challenge on a global scale relates to the **identification and accountability of the sovereign State** to which the hostile cyber act should be attributed, especially when it is programmatically executed to mask its origin. State-backed hacker groups and military agencies structurally exploit network anonymity, the use of non-state actors operating as intermediaries (*proxies*), or complex technological deception and obfuscation techniques, such as *proxy servers* and false flag operations (*false flag operations*).
In the absence of a specific and binding international treaty governing military operations in cyberspace, doctrine and practice refer to the **Draft Articles on Responsibility of States for Internationally Wrongful Acts** (UN International Law Commission, 2001).

REFERENCES

International Law Commission, Draft Articles on State Responsibility, 2001, Art. 8
The text establishes that the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting **on the instructions of, or under the direction or control** of that State in carrying out the eversive conduct.
However, the standard of technical and digital evidence required to legally prove such direct or stringent control (*effective control*) before international courts is extraordinarily complex to obtain. This fuels the so-called **attribution dilemma (*attribution dilemma*)**, hindering the activation of any legal response, retaliatory countermeasure, or official diplomatic sanction.

From the standpoint of public international law and the preservation of global peace, the qualification of a cyberattack clashes with the cornerstones of the UN Charter. **Art. 2, para. 4, of the United Nations Charter** expressly prohibits the threat or use of force in international relations between States. A cyberattack that causes structural damage equivalent to that resulting from a conventional kinetic military action–such as the coordinated collapse of vital civilian critical infrastructures (nuclear plants, power grids), direct civilian casualties, or the systemic paralysis of a country's telecommunications–falls within this notion of aggression, paving the way for the application of **Art. 51 of the same Charter**, which legitimizes the inherent right to **individual or collective self-defense** against an armed attack.

FOCUS

The "Stuxnet" Malware Case, 2009

The cyberattack known as **Stuxnet**, which occurred in 2009, is universally recognized by international law doctrine as the **first documented and tangible case of cyber warfare (*cyberwarfare*)**. The *malware*, the result of a joint intelligence operation likely attributed to the United States and Israel, had the geopolitical objective of **disrupting nuclear enrichment activities in Iran**, specifically targeting the Natanz military facility, home to the centrifuges for uranium enrichment. The attack stood out for its extremely high level of technical sophistication: inoculated via an infected USB flash drive to bypass networks isolated from the Internet (*air-gapped*), the virus altered the rotation speed of the centrifuges, causing their physical destruction, while displaying completely normal operating parameters on the technicians' monitors. Stuxnet thus succeeded in achieving a **concrete destructive effect on a military critical infrastructure**, without the deployment of conventional armed forces, missiles, or troops on the ground.

Beyond its direct effects on the Iranian facility, Stuxnet had a global impact, spreading uncontrollably and infecting industrial control systems (*SCADA*) in over one hundred countries. The event exposed the **systemic vulnerabilities of digitalized critical infrastructures**, revealing the absence, until then, of adequate protection and resilience mechanisms. The incident fueled the international debate on the necessity of legally regulating state conduct in cyberspace, especially when it is capable of producing effects comparable to a kinetic armed attack, configuring hypotheses of **unlawful use of force under Art. 2, para. 4, of the United Nations Charter**.

FOCUS

Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013

The ***Tallinn Manual*** **(drafted by a group of international experts under the mandate of the NATO Cooperative Cyber Defence Centre of Excellence)**, while not a binding legal treaty, constitutes the most authoritative interpretative framework for applying the international law of armed conflict to cyberspace. The Manual affirms the principle of **equivalence of effects**: a *cyber operation* constitutes an unlawful use of force under Art. 2(4) of the UN Charter if its physical effects and destructive consequences (injuries to persons or destruction of physical property, as historically demonstrated by *Stuxnet*) are analogous to those produced by traditional military operations or kinetic bombardments. This dogmatic equivalence, however, requires a rigorous case-by-case assessment, coordinating it with absolute respect for the principles of **proportionality, necessity, and distinction** between civilians and combatants should the attacked State decide to launch a retaliatory armed or digital response.

The legal uncertainty stemming from the lack of universally shared rules, combined with the technical difficulty of definitively identifying the digital perpetrator of an attack, makes it crucial to strengthen supranational mechanisms of transparency, adopt common standards for the **forensic preservation and cross-border sharing of digital evidence**, and draft an updated public international law framework capable of definitively closing the current regulatory gaps in cyberspace.

FOCUS

The Tandem Between Cyberwarfare and Transnational Terrorism

In today's geopolitical scenario, state-sponsored cyber warfare techniques regularly intertwine with the Eurocrime of **Transnational Terrorism** under Art. 83 of the TFEU. States acting as sponsors of global eversion (*State-sponsored terrorism*) provide military-grade spyware, cyber weapons, and attack instructions to terrorist cells or structured eversive groups. The latter execute cyberattacks against European Union institutions or financial systems, acting as a shield and allowing the mandating State to invoke **plausible deniability** to avoid retaliation under Art. 51 of the UN Charter. This demonstrates that countering state-sponsored *cybercrimes* requires immediate operational coordination between **Europol (EC3 Centre)**, defense intelligence agencies, and the **Cyber Solidarity.**

The legal flow of attribution and reaction in cyberwarfare takes place into 4 phases:

- **Phase 1 - The Cyber-Offensive Event:** Inoculation of a military-grade malware (e.g., the *Stuxnet* attack). Obfuscation of digital traces through *proxy* servers located in non-cooperative jurisdictions.
- **Phase 2 - Forensic and Technological Analysis:** Intervention of CSIRTs and military laboratories to isolate the source code and identify the digital footprint of the attack (*cyber-attribution*).
- **Phase 3 - Dogmatic Review (ILC Model / Tallinn Manual):** Verification of the command link under Art. 8 of the 2001 ILC Draft. Evaluation of the attack's impact: if analogous to a kinetic military aggression, it triggers a violation of Art. 2(4) of the UN Charter.
- **Phase 4 - Multilevel International Response:** Activation of diplomatic channels or, in cases of a systemic and lethal threat to the State's vital infrastructures, legitimization of a response in self-defense under Art. 51 of the UN Charter, backed by the **European Cyber Shield** of the Cyber Solidarity Act.

XV. Key Findings

The scientific, historical, and regulatory analysis carried out within this paper leads to the outline of **six fundamental findings** that we must keep in mind for a complete understanding of the subject matter:

- **Cybercrime as a Complex and Evolving Phenomenon:** A cybercrime is configured when an active or passive digital conduct, carried out with awareness and **intent (*dolo*)**, damages or endangers legally protected assets, such as system integrity, data confidentiality, or economic property. The objectives pursued by transnational syndicates can be financial (e.g., *ransomware* ransoms), ideological (*hacktivism*), or personal (*revenge porn*), moving along a border between lawful and unlawful that is often blurred by the apparent neutrality of digital tools.
- **Global Regulatory Response and the Budapest Convention:** Historically, the lack of a unified definition and binding sanctions on an international scale favored the impunity of perpetrators, offering **"safe havens"** to cybercriminals due to the absence of the dual criminality principle, as highlighted by the *ILOVEYOU* virus of 2000. The **Budapest Convention (2001)** by the Council of Europe represented the first step toward a coordinated response and the typification of core offenses (*illegal access, data interference*), now enhanced by the adoption of the new **UN**

Convention on Cybercrime of 2024, aimed at guaranteeing universal accession and mandatory *capacity building* for developing nations.

- **Centrality of Domestic Italian Criminal and Procedural Protection:** The Italian legislator, from Law 547/1993 to Law 48/2008, transposed international standards by introducing specific offenses into the Criminal Code (Art. 615-*ter*, and Art. 640-*ter* c.c.). The jurisprudence of legitimacy (Supreme Court Judgment No. 40470/2018) extended penal protection by clarifying that the notion of a "computer system" is independent of a network connection, emphasizing the substantive functionality of the device. On a procedural level, **Art. 51, para. 3-*quinquies* of the Code of Criminal Procedure (c.c.p.)** centralizes investigative powers within District Prosecutor's Offices, ensuring high technical and digital-forensic specialization.
- **The Transition toward Cyber-Resilience and Mandatory Sharing:** European security policy supplements criminal enforcement with a structural pillar of technical prevention. The **Cybersecurity Act of 2019** granted a permanent mandate to **ENISA** and established the European certification framework for ICT products. This system is today completed by the **NIS 2 Directive (EU 2022/2555)**, which imposes strict risk management obligations along the *supply chain* and mandatory urgent notifications of significant incidents within 24 hours to secure the Union's economy and vital infrastructures against priority threats.
- **Essential Involvement of the Private Sector and Security Agencies:** Given the speed and transnational scale at which digital threats evolve, Europol and its specialized **EC3** center closely collaborate with private technology companies (*Big Tech* and *ISPs*). Through operational tools such as the strategic threat assessments of the **IOCTA** report and the operational arm of the **J-CAT** taskforce, the public-private partnership enables a two-way exchange of tactical *intelligence* and the execution of coordinated cross-border operations to dismantle malicious networks and clandestine servers.
- **Protection of Digital Rights, AI Act, and Cyberwarfare Frontiers (2026):** European cybersecurity is inextricably linked to the protection of the individual and fundamental rights. The **GDPR** guarantees concrete remedies (mandatory notifications of data breaches and the extension of compensation to **immaterial damage arising from the fear of future data abuse under CJEU Judgment C-340/21**), also acting as a shield against the commercial deployment of AI software (the Italian Privacy Guarantor's order against *OpenAI/ChatGPT* in 2023). With the entry into force of the **Cyber Solidarity Act in 2025**, the Union addresses priority threats through the *European Cyber Shield* and the transition toward post-quantum cryptography (PQC). Finally, in military contexts (*cyberwarfare*), the application of the 2001 ILC Draft Articles and the *Tallinn Manual* parameters becomes fundamental to resolve state attribution dilemmas highlighted by the *Stuxnet* case, defining the limits of the use of force and self-defense under Art. 51 of the UN Charter in cyberspace.