



## A Comparative Study of the Legal Framework for Combating Cyberterrorism in Iranian and EU Law

Amir Chaman

Master of Criminal Law and Criminology, Islamic Azad University, Lahijan Branch, Gilan, Iran

### Article info

Received: 25.08.2026

Accepted: 05.10.2026

Available Online: 05.10.2026

Checked for Plagiarism: Yes

### Keywords:

cyberterrorism; Iran; European Union; comparative criminal law; critical infrastructure; NIS2

### ABSTRACT

Cyberterrorism is not synonymous with serious hacking, ideologically motivated disruption, terrorist propaganda, or state-sponsored cyber operations. This article compares how Iranian law and European Union law address digitally enabled violence and interference that may meet a terrorism threshold, while also assessing ordinary cybercrime, critical-infrastructure security, electronic evidence and procedural safeguards. Employing a qualitative doctrinal and functional comparative method, it reads Iran's Computer Crimes Act against the EU Counter-Terrorism Directive, the attacks-against-information-systems framework and the layered cybersecurity acquis, with developments through 24 September 2026. It finds a shared capacity to prosecute harmful interference with essential systems but significant differences in the express legal link between cyber interference and terrorist purpose, the distribution of preventive duties and the architecture of cross-border evidence. The comparison also demonstrates that resilience laws cannot replace criminal-law proof of intent and that cybersecurity incident datasets must not be treated as estimates of terrorist offending. The article proposes tightly defined offence criteria, interoperable evidence safeguards and risk-based infrastructure protection without conflating political expression, cybercrime and terrorism.

### Introduction

Networked energy, health, transport, finance and public-administration systems can suffer serious consequences when malicious actors obstruct their availability or corrupt operational data. The same technical technique may, however, have very different legal meanings: a profit-oriented extortion attempt, a short-lived political protest against a public website, a hostile intelligence operation and a deliberately coercive attack endangering patients are not equivalent categories. An adequate comparative legal inquiry begins by asking which legally relevant conduct occurred, what mental element and purpose can be proved, what consequences were intended or foreseeable, and which authority has jurisdiction. An operational label used by an incident-response team is not automatically a criminal-law classification. [R03-R05, R15-R16]

Iran and the European Union offer a useful comparison because their legal instruments are organized differently. The Iranian Computer Crimes Act criminalizes several attacks on data and systems and contains an aggravated provision dealing with essential public-service systems. The EU uses a two-level criminal structure: the 2013 information-systems directive establishes underlying cyber-offence categories, while the 2017 terrorism directive expressly connects specified severe cyber interferences to terrorist offences when the requisite context and purpose are established. Contemporary EU legislation adds security-management, reporting, financial-sector resilience, critical-entity preparedness, product-security and cross-border electronic-evidence rules. A comparison that treats all these rules as a single "cyberterrorism law" would mistake prevention and investigation for substantive offence definition. [R01-R09, R13-R14]

\*Corresponding Author: Amir Chaman (Amirchaman30@gmail.com)

The research question is therefore not simply which legal system punishes cyberterrorism more severely. It asks how the two frameworks distinguish terrorist cyber violence from ordinary cybercrime, coordinate punishment with prevention, facilitate the recovery of volatile electronic evidence, and constrain public power. Four subsidiary questions guide the inquiry: (1) what legal threshold marks the transition from cyber interference to terrorism; (2) how are essential services and systemic risks protected; (3) what evidence, jurisdiction and cooperation mechanisms apply; and (4) where do legal certainty and rights-based review constrain investigative or content-removal measures? The article offers a doctrinal rather than an empirical evaluation of enforcement outcomes; access to comparable prosecution datasets is outside its scope.

**Method, materials and analytical framework**

The study applies functional comparative legal analysis. First, it maps the actus reus, mental element, protected interests and jurisdictional reach of relevant provisions. Secondly, it separates ex ante organizational resilience obligations from ex post criminal liability and from procedural powers used to acquire evidence. Thirdly, it examines three constructed fact patterns using the same questions on both sides; the examples illustrate doctrinal distinctions and are not reported cases. Finally, it evaluates rights-sensitive tensions in evidence preservation, data retention, content governance and classification of ideology-related conduct. This transparent sequence avoids drawing claims about practical enforcement effectiveness from statutes alone. [R19-R21]

Primary sources comprise Iranian legislation reproduced in Persian and the accessible English translation of selected jurisdictional provisions, official EU legislative texts and authoritative agency materials. The source cut-off is 24 September 2026. Statutes enacted before September 2023 remain necessary primary law: an instruction to cite recent research cannot make the foundational 2009, 2013 and 2017 provisions disappear. Recent 2024-2026 academic work, Commission reports, ENISA threat assessments and FATF statements are used to identify new developments and contextual challenges. When the English translation of Iranian law may be incomplete, the legal proposition is tied to a specified article rather than assumed to describe every aspect of current Iranian practice. [R01-R24] The comparison concerns Iran as one national legal order and the EU as a supranational framework implemented, in material part, by individual Member States. EU directives require national transposition and do not themselves provide a complete uniform criminal code. A full assessment of national variation would require jurisdiction-specific criminal statutes, judicial decisions and enforcement records, which are not systematically compared here. This asymmetry is made explicit because a minimum-harmonization directive, directly applicable regulation and national penal statute perform different legal functions. The resulting conclusions concern legislative design and doctrinal possibilities, not an ordinal ranking of political systems or unsupported claims about enforcement performance. [R03-R09]

**Table 1.** Scope and function of the legal materials compared

| Material                               | Legal role                                           | Question addressed                                                                 |
|----------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------|
| Iranian computer-crime legislation     | National criminal and procedural law                 | Substantive cyber offences, essential-services aggravation, jurisdiction, evidence |
| EU cybercrime and terrorism directives | Minimum-harmonization criminal instruments           | Underlying system/data interference and additional terrorist-offence elements      |
| EU resilience instruments              | Regulatory duties, mainly entity- and product-facing | Risk management, notification, continuity and supervisory arrangements             |
| EU electronic-evidence instruments     | Regional criminal-procedure cooperation              | Defined preservation and production orders; no universal third-country power       |
| ENISA and FATF publications            | Institutional reporting and compliance assessments   | Contemporary context; neither a source of individual criminal culpability          |

**Defining cyberterrorism without expanding ordinary cybercrime**

**Conduct, purpose, gravity and nexus:**

A legally workable category should be narrower than “any politically motivated online attack.” This article uses cyberterrorism as an analytical term for

intentional conduct involving information systems that satisfies a relevant criminal predicate, reaches the applicable gravity and harm threshold, and is committed with a legally established terrorist aim. An additional definitional question is whether digital infrastructure is the instrument, the direct target, or

merely an incidental communication medium. A bomb attack coordinated through messages is terrorism using digital communication; it is not necessarily an illegal-system-interference offence. Conversely, malicious code that disables a hospital's life-support control system may supply an underlying cyber predicate while the terrorist qualification still requires proof of purpose and statutory conditions. [R03-R04]

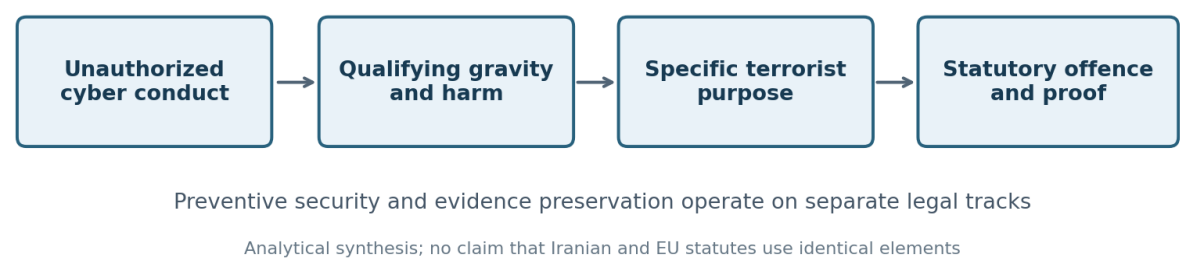
Digital attribution is probabilistic and may identify infrastructure rather than persons. Location of an IP address, choice of language, re-use of a malware family or public claims of responsibility does not on its own prove the accused's identity, direction by a group or terrorist intent. Courts should distinguish technical attribution from legal attribution, preserve alternative explanations and evaluate whether circumstantial evidence supports each element. A manifesto may assist proof of intent, but mere possession of controversial speech cannot replace evidence of participation in an offence. This distinction is relevant on both sides of the comparison and becomes especially important when investigative authorities use broad social or ideological descriptors as triage signals. [R20-R21]

**Three categories that must remain distinct:**

The first category is cyber-dependent criminal conduct, such as unlawful system access, unauthorized interference, interception, destructive

modification of data or deployment of attack tools with the relevant unlawful purpose. The second is terrorism-related conduct, which may include a sufficiently serious qualifying cyber-attack, planning or financing of terrorism, or recruitment and instructions under applicable legal conditions. The third is resilience governance: advance duties to identify risks, harden systems, notify regulators, respond to incidents and restore essential functions. A single event can activate more than one category, yet the legal bases and burdens of proof remain separate. NIS2 non-compliance is not itself evidence that a network intrusion was terrorist. [R03-R06, R11]

An important counterexample is a brief distributed-denial-of-service incident against an informational public website that has no demonstrated serious downstream consequences. It may constitute unlawful interference under the relevant national cybercrime rules, but terrorist classification cannot follow merely from the operator's political slogan. At the other extreme, an intentionally engineered cross-border blackout designed to coerce a government through serious public danger presents a different combination of act, context, severity and purpose. The distinction guards against both underinclusive law, which overlooks digitally mediated catastrophic harm, and overinclusive law, which transforms dissent or commonplace cyber offending into terrorism. [R03-R04, R20]



**Figure 1.** A sequential legal-classification model; the diagram is an original analytical schematic, not a transcription of either statute.

**Iranian legal framework**  
**Substantive computer-crime offences and the essential-services aggravation:**  
Iran's 2009 Computer Crimes Act establishes discrete offences concerning unauthorized access, illegal interception and interference with data or systems. Article 1 addresses access without authorization to protected data or systems; Article 2 addresses interception of non-public communications; Article 8 addresses deletion, destruction, impairment or making another person's data processable; and Article 9 addresses acts that disable or disrupt another person's computer or telecommunication systems. Article 10 addresses unauthorized obstruction of access by lawful users,

including conduct involving changed passwords or encryption. These provisions create a general cybercrime substrate and do not make every security incident a terrorism offence. [R01, R24]

Article 11 is especially important for the present comparison. In substance, it elevates acts described in Articles 8-10 when directed against computer or telecommunication systems used to provide essential public services, with a specified intention to endanger security, public peace or public security. Its illustrative service fields include health, water, power, gas, telecommunications, transport and banking; the statutory imprisonment range is three to ten years in the published text. The provision attaches both a sensitive target and a distinctive

culpability element to aggravated punishment. Yet Article 11 should not be casually relabeled a stand-alone “cyberterrorism definition”: the statutory wording, the intent requirement and the separate legal construction of terrorism must be respected. [R01, R24]

Target sensitivity alone does not decide culpability. An administrator’s authorized testing, an accidental outage and an intrusion that unexpectedly affects an essential-service supplier raise different questions of authorization, knowledge, intention, causation and scope. If the public-service system is one link in a subcontracted digital chain, the prosecution must also establish the relevant statutory relationship between attacked system and essential service. The Article 11 model has the practical advantage of naming vital-service contexts without requiring every incident to be categorized under a universal terrorism label; its application nevertheless turns on proof of the mental element specified by the text. [R01]

#### **Jurisdiction and electronic evidence:**

The Act contains specific jurisdictional connectors in Article 28. These include data stored on systems or carriers within Iranian territory, certain offences committed through Iranian country-code domain websites, and enumerated offshore attacks against systems used by governmental bodies or providers of public services. The statutory connectors extend adjudicative reach beyond a simple “offender physically present in Iran” model, but identifying legal jurisdiction is different from gaining lawful access to a server or witness abroad. Jurisdictional overlap can occur where the actor, victim, target service, routing infrastructure and cloud provider are located in different states. [R01-R02]

The statute also contains procedural rules on retention and preservation. Article 32 prescribes periods for access-provider traffic data and specified user information; Article 33 addresses domestic hosting providers, while Article 34 provides for orders to preserve stored data, with an emergency procedure subject to subsequent judicial notification in the statutory circumstances. These tools address volatility but raise separate questions about targeted necessity, reliability, chain of custody, access control and individual remedies. A preservation order prevents deletion; it is not conceptually identical to indefinite, generalized storage of every user’s communication or unrestricted disclosure. [R01, R24]

#### **Terrorist financing and institutional limits of this comparison:**

A computer intrusion may also be used to solicit, move, conceal or distribute resources connected to an unlawful violent operation. Such a scenario requires analysis under applicable terrorist-financing, financial and ordinary computer-fraud

rules rather than assuming the cyber predicate alone resolves the financing issue. Cross-border financial compliance is particularly sensitive because the FATF’s 19 June 2026 statement continued to identify Iran as a high-risk jurisdiction subject to a call for action and set out that body’s assessment of outstanding deficiencies and treaty-related reservations. These are attributed FATF compliance findings, not a judicial finding that a particular cyber incident, institution or individual funded terrorism. [R17]

The present inquiry does not claim that Iran lacks intelligence, incident-response or sectoral administrative rules beyond the computer-crimes statute. Rather, it restricts conclusions about enacted general obligations to the instruments verified for this paper. A finding that the listed provisions do not themselves establish an EU-style cross-sector supervisory matrix is not a claim that Iranian organizations operate without security requirements. Evaluation of ministerial rules, sector-specific norms and unpublished operational protocols would require a separate primary-source study. The comparative finding is therefore about the difference in the publicly mapped statutory architecture, not a factual claim that particular attacks were prevented or investigated more effectively in one place. [R01, R05-R07]

#### **European Union legal framework**

##### **The underlying offence: attacks against information systems:**

Directive 2013/40/EU requires Member States to criminalize specified intentional conduct without right. Article 3 concerns unlawful access by infringement of a security measure in at least non-minor cases; Article 4 concerns serious hindering or interruption of system functioning through interference with computer data; Article 5 concerns data interference; Article 6 addresses unlawful interception; and Article 7 addresses specified attack tools supplied with the requisite purpose. Article 9 establishes minimum requirements concerning maximum penalties, with more serious cases involving scale, critical infrastructure and other aggravating circumstances. The directive harmonizes offence elements and sanction floors, rather than creating a single direct-prosecution EU criminal code. [R03]

The relevant distinction between illegal access and illegal interference matters in cyberterrorism analysis. Reconnaissance or unauthorized entry may be criminal even absent service interruption, but those facts alone need not satisfy the more serious cyber-interference predicates cross-referenced by the terrorism instrument. Equally, proof of large-scale disruption does not alone prove the accused had a terrorist purpose. An investigation can properly begin under a general cybercrime predicate and develop additional evidence; legal classification

should be revised by reference to verified statutory elements rather than a dramatic initial incident description. [R03-R04]

**Terrorist aim and the explicit cybercrime cross-reference:**

Directive (EU) 2017/541 Article 3 requires qualifying intentional acts, understood in their nature or context as potentially seriously damaging a country or international organization, together with one of the specified terrorists aims. Those aims include seriously intimidating a population, unduly compelling a government or international organization to act or abstain, or seriously destabilizing or destroying fundamental political, constitutional, economic or social structures. Article 3(1)(d) refers to extensive destruction of infrastructure facilities, expressly including an information system, where the relevant endangerment or major economic loss criteria apply. Other provisions address disruption of essential resources where human life is endangered. [R04]

Crucially, Article 3(1)(i) expressly covers selected aggravated illegal system interference and illegal data interference by cross-reference to Articles 4 and 5 and the specified Article 9 circumstances of Directive 2013/40/EU. The cross-reference is deliberately qualified: not every act satisfying the general computer-crime directive automatically becomes a terrorist offence. The prosecutor must connect the precise cyber predicate, referenced aggravating circumstances, Article 3 context and the terrorist aim. This layered method supplies a more express statutory bridge between cyber harms and terrorism than is visible in the standalone wording of Iran's Article 11, while still depending on Member State implementing law and ordinary proof standards. [R03-R04]

The EU terrorism framework further regulates offences associated with terrorist groups and activities, including conduct such as recruitment, training and terrorist financing subject to the instrument's definitions and conditions. These provisions may be relevant to online planning or facilitation; however, use of an online platform is not sufficient to classify every message, donation or technical tutorial as an offence. Where material is publicly available for legitimate security research or journalism, analysis must evaluate intention, context and the particular statutory elements. A strong legal boundary is especially important when multi-purpose digital tools have substantial lawful uses. [R04, R20]

**Ex ante resilience: NIS2, CER and DORA:**

Directive (EU) 2022/2555, commonly called NIS2, addresses cybersecurity governance for defined essential and important entities. It requires risk-management arrangements, incident reporting and supervisory measures across the designated sectors

and establishes governance and cooperation structures involving competent authorities and CSIRTs. Its Article 41 set 17 October 2024 as the transposition deadline and application of national measures from 18 October 2024. Because actual national implementation and supervisory practice can differ, the existence of the EU directive should not be treated as conclusive proof that every relevant actor in every Member State has identical practical duties. [R05, R19]

Directive (EU) 2022/2557, the Critical Entities Resilience framework, addresses wider continuity and non-cyber risks for designated critical entities; it complements rather than duplicates the digital protections of NIS2. Regulation (EU) 2022/2554 (DORA), applicable from 17 January 2025, supplies a tailored operational-resilience regime for the financial sector, including ICT risk management and incident arrangements. Taken together, these measures make it possible to detect, contain and recover from serious attacks without first proving that an attacker belongs to any ideological organization. They are risk-management instruments, not shortcuts around the elements of a criminal terrorism offence. [R05-R07]

A 2024 implementing regulation further specifies technical, methodological and significant-incident rules for enumerated NIS2 digital infrastructure and service providers. Later instruments enlarge the lifecycle perspective: the Cyber Solidarity Act (Regulation (EU) 2025/38) strengthens coordinated detection and response capacities, while the Cyber Resilience Act (Regulation (EU) 2024/2847) develops product-security requirements. The latter's general obligations apply from 11 December 2027, but Article 14 reporting obligations began applying on 11 September 2026 and the notified-body chapter began applying on 11 June 2026. Accordingly, the September 2026 legal picture should not present its entire regime as already fully applicable. [R12-R14]

**Online material versus a cyber-attack:**

Regulation (EU) 2021/784 concerns dissemination of terrorist content through hosting services and includes removal-order and safeguard mechanisms. The Commission's 2024 implementation report describes a framework directed at preventing exploitation of hosting services for intimidation, recruitment or attack facilitation. This online-content track must remain separate from malware-driven interference with critical systems. The fact that extremist material appears on a platform does not demonstrate a successful infrastructure attack; equally, a serious technical intrusion does not necessarily involve publication of unlawful content. Investigative and regulatory measures should therefore be selected for the actual underlying conduct and subject to the applicable procedural and expression safeguards. [R10-R11]

Table 2. EU instruments and their distinct functions as of September 2026

| Instrument       | Primary legal function                        | Temporal / scope note                                       |
|------------------|-----------------------------------------------|-------------------------------------------------------------|
| 2013/40/EU       | Cybercrime predicates                         | 2013 instrument; transposed into national law               |
| 2017/541         | Specified terrorist offences and aims         | 2017 instrument; requires national implementation           |
| NIS2 (2022/2555) | Entity risk management and incident reporting | National measures applicable from 18 Oct 2024               |
| DORA (2022/2554) | Financial-sector ICT resilience               | Applicable since 17 Jan 2025                                |
| Reg. 2023/1543   | EU e-evidence preservation and production     | Applicable since 18 Aug 2026                                |
| Reg. 2025/38     | Coordinated cyber detection and response      | 2025 Cyber Solidarity Act                                   |
| Reg. 2024/2847   | Product lifecycle cybersecurity               | Article 14 since 11 Sep 2026; broad regime from 11 Dec 2027 |

Comparative findings by legal function  
Criminal liability and the classification threshold:

Both systems provide rules capable of reaching intentionally destructive or disruptive computer conduct. The central difference in the selected primary texts concerns the relationship of aggravated cyber interference to terrorist qualification. Iranian Article 11 focuses on identified essential public services and a security-related mental element; the EU scheme incorporates specified serious cyber-interference offences into an express terrorism definition, with further serious-damage and terrorist-aim requirements. This is a difference in doctrinal structure rather than evidence that every Iranian Article 11 conviction would, or would not, qualify as terrorism under other Iranian law. A rigorous comparison should ask which components of a hypothetical attack are established and which additional elements remain unproved. [R01, R03-R04]

Neither model should turn mere technical disruption into a categorical inference of political purpose. Where an attacker changes the operation of a water utility, proof must identify the affected system, unauthorized interference, objective severity, causal connection and the requisite intent. An ideological claim can be evidence of motivation but not a substitute for proving the underlying technical act or its connection to a given defendant. Conversely, a severe and deliberately coercive operation should not escape examination solely because its initial detection was routed through an ordinary fraud or systems-interference unit. The legal category should follow the proved facts; emergency response must proceed independently when life or essential service continuity is at risk. [R01, R03-R04]

Institutional responsibilities and private actors:

A second difference is the visibility of preventive obligations. The selected EU framework distributes ex ante tasks among operators, sector regulators, incident-response networks, financial supervisors, product manufacturers and competent national authorities. Critical-infrastructure operators may face risk management, continuity and incident-reporting duties before an offence occurs. This allocation of responsibilities is analytically distinct from substantive criminal law; the responsible company can be a victim of a terrorist attack while also facing a separate regulatory inquiry into whether it complied with applicable duties. The public text of Iran’s Computer Crimes Act principally provides offence, jurisdiction and evidence provisions, so a comprehensive comparison of business-side obligations requires additional verified Iranian sectoral instruments. [R01, R05-R07, R12-R14]

The EU’s plurality of instruments also creates overlap questions. A financial entity, its cloud provider and a connected device manufacturer may be governed by different but interacting duties. The risk is not simply a lack of law but uncertainty about the allocation of reporting, remediation and disclosure duties during a fast-moving incident. Recent legal scholarship on NIS2 and the growth of EU cybersecurity regulation illustrates this governance challenge; it does not establish that cyberterrorism itself is more or less prevalent in the Union. The sensible comparative unit is the function of a rule, its addressee and the relevant period of application. [R05-R07, R19]

A structured comparison

**Table 3.** Functional comparison of the verified statutory frameworks

| Function                      | Iran (specified materials)                                               | EU (specified materials)                                                             |
|-------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Criminal predicate            | Unauthorized data/system interference; arts. 8-10                        | Directive 2013/40/EU; Member State offences                                          |
| Serious essential-system harm | Art. 11: essential public services and specified security-related intent | Art. 3(1)(d), (i) of 2017/541 adds qualifying context, predicates and terrorist aims |
| General preventive duties     | Not comprehensively mapped by the Computer Crimes Act alone              | NIS2, CER, DORA and connected product/response rules                                 |
| Evidence and jurisdiction     | Arts. 28 and 32-34 supply connectors, retention and preservation         | National powers plus defined EU e-evidence cooperation                               |
| Rights-sensitive issue        | Precise statutory elements and review of investigative measures          | Charter/GDPR safeguards and national criminal-procedure review                       |

### Three illustrative legal scenarios

#### Hospital systems and threatened patient safety:

Assume an actor deliberately deploys code that disables a hospital's core clinical network, blocks access to urgent patient records and claims the purpose is to coerce a government into changing policy. This is a constructed hypothetical, not an allegation about any known incident. In Iran the legal inquiry would begin with whether the conduct satisfies Articles 8, 9 or 10 and whether the hospital's system falls within Article 11's essential-services context and mental element. Under the EU model investigators would assess the Directive 2013/40/EU offence and aggravation, then the Article 3(1)(d) or (i) route under the 2017 terrorism directive, the seriousness requirement and proof of the asserted coercive aim. A mere posted statement would still require authentication and attribution. [R01, R03-R04]

The operational responsibilities would not wait for those issues to be settled. Backups, segmented access, clinical continuity, forensic preservation and notification could be relevant under the applicable domestic regulatory regime. In the EU, NIS2 or sector-specific national rules and critical-entity measures may govern affected entities, subject to the actual designation and Member State implementation. Public disclosure should avoid compromising an ongoing incident response or prejudging criminal liability. The legal lesson is that prevention, victim support, digital forensics and criminal attribution operate on related but distinct tracks. [R05, R07]

#### Ideological denial-of-service and a municipal website:

Assume a self-described activist group floods a municipal information website for several hours, with no substantiated effect on emergency services or other essential functions. The conduct can be assessed under unlawful system-interference rules if the applicable statutory requirements are met. It would be analytically unsound, however, to infer

terrorist intent merely from the presence of a political slogan or the fact that a government website was involved. The EU terrorism directive additionally demands the specified serious-damage context, qualifying act and terrorist aim; Iran's Article 11 involves its essential-service target and purpose requirements. Whether other offences apply remains a separate question. [R01, R03-R04]

A useful evidentiary checklist asks whether the attack affected the website alone or a back-end system providing safety-critical services, how long the effects lasted, whether a credible threat to life or major economic damage arose, and whether the accused knowingly intended the established consequences. This checklist does not create a numerical threshold; it orders the legal inquiry and exposes missing proof. The ENISA 2025 report recorded many hacktivist-driven DDoS incidents, but its cybersecurity incident counts are not terrorism prosecutions or evidence that the doctrinal terrorism threshold was met in those events. [R15, R23]

#### Cross-border cloud intrusion and contested attribution:

Assume malicious operator accesses credentials from one state, stores tools on a server in a second state, targets an electricity-service vendor in a third state and uses a cloud provider in a fourth. In an Iranian proceeding, the connectors in Article 28 may be examined where Iranian data, domains or enumerated domestic interests are involved. For EU Member States, national jurisdictional rules and the relevant EU cooperation framework may be engaged, but neither a technical trace nor a supranational legislative text alone resolves every conflict of laws. Competent authorities must separately establish jurisdiction, lawful acquisition of evidence, admissibility, disclosure to the defence and the individual's conduct and intent. [R01-R04, R08]

The cross-border problem is time-sensitive because account content and traffic metadata can be

modified, overwritten or moved. Requests for expedited preservation should be distinguished from obtaining the protected information itself; a lawful preservation order may stabilize material pending later review. Evidence handling should document timestamps and time zones, cryptographic hashes where appropriate, system-clock uncertainty, provenance, provider declarations and transfers among investigators. These are prudent forensic requirements rather than a claim that any one cited statute mandates every listed practice. They reduce the risk of mistaking compromised infrastructure for the responsible person and allow later judicial testing. [R01-R02, R08-R09]

### **Electronic evidence, territoriality and international cooperation**

#### **Why preservation is not production:**

The volatile nature of logs and cloud accounts makes electronic evidence central to cyberattack investigations. Yet preservation, acquisition and disclosure are legally distinct acts: freezing stored data to prevent alteration need not confer authority to inspect its contents, while production or access generally requires its own applicable legal basis. Iran's Articles 32-34 provide several retention and preservation mechanisms; EU Regulation 2023/1543 creates European Production and Preservation Orders within its defined EU scope. The regulation has applied since 18 August 2026, while Directive 2023/1544 set an 18 February 2026 national transposition deadline for designated service-provider establishments and legal representatives. The new EU arrangement is not a generic warrant for directly obtaining data from Iran. [R01, R08-R09]

Evidence requests may implicate different categories of records and different jurisdictional protections. The interests of account holders, third parties, service providers, investigators and defendants do not perfectly coincide. A defensible scheme specifies competent issuing and executing authorities, offence and necessity thresholds, time-bound preservation, confidential handling where warranted, independent review, notice and effective remedies subject to carefully defined exceptions. Defendants need a meaningful opportunity to challenge reliability and legality of evidence, particularly when foreign-provider records are difficult to reproduce. These requirements also protect the prosecution against exclusion or overstatement of digital traces. [R08-R09, R20]

#### **Convention-based and ad hoc cooperation:**

The Council of Europe Convention on Cybercrime provides a prominent convention-based model for cybercrime offences, procedural measures and cooperation. It must nevertheless be distinguished from EU membership and from bilateral or other multilateral channels. The Council of Europe's

published status chart is the appropriate starting point for determining participation in that treaty at a specified date; a state's absence from its party list is not a claim that it has no mechanisms for mutual legal assistance or cannot cooperate operationally. A full bilateral-cooperation analysis would require mapping individual agreements, reservations, lawful-intercept rules and current relations with every requested state. [R18, R21]

The most achievable common technical standards concern evidence integrity and request specificity rather than wholesale harmonization of domestic terrorism definitions. An urgent request should identify the user or system with adequate precision, describe the statutory offence and factual nexus, distinguish preservation from later disclosure, provide a contact point and specify secure transmission and review arrangements. Any cooperation pathway must account for inconsistent criminalization, public-policy exceptions, data-protection requirements and the risk of prosecution for protected speech. Such safeguards are not an obstacle extraneous to security; they define whether acquired evidence can reliably and lawfully support an adjudication. [R08-R09, R20-R21]

### **Fundamental rights and proportionality**

#### **Legality and the danger of elastic labels:**

Criminal law's legality principle requires reasonably ascertainable offences and penal consequences. "Cyberterrorism" is rhetorically powerful but too indeterminate to displace the enacted conditions for a specific charge. The relevant EU provisions are structured around defined predicate offences, a seriousness condition and terrorist purposes, while Iranian adjudication must use the actual elements of the applicable Iranian statutory provisions. A systematic risk is that a broad description of online ideology or disruptive protest may overshadow the physical or economic seriousness of the event and the accused's state of mind. Courts should reason from legal elements to the facts, not from an incident label to presumed elements. [R01, R03-R04, R20]

Article 11 of the Iranian law uses a public-security-related purpose and the EU terrorism directive uses its particular list of aims; the mental formulations should not be treated as word-for-word equivalents. Interpretation also depends on authoritative judicial practice and the remainder of the domestic legal framework. Under the EU Charter, rights to private life, data protection, expression, effective judicial protection and legality of offences and penalties are relevant to the measures used in cyber investigations and online-content regulation. The existence of a serious threat does not by itself eliminate the need for a competent decision maker, a lawful basis and reviewable limits. [R01, R04, R26]

**Surveillance, content moderation and defensive monitoring:**

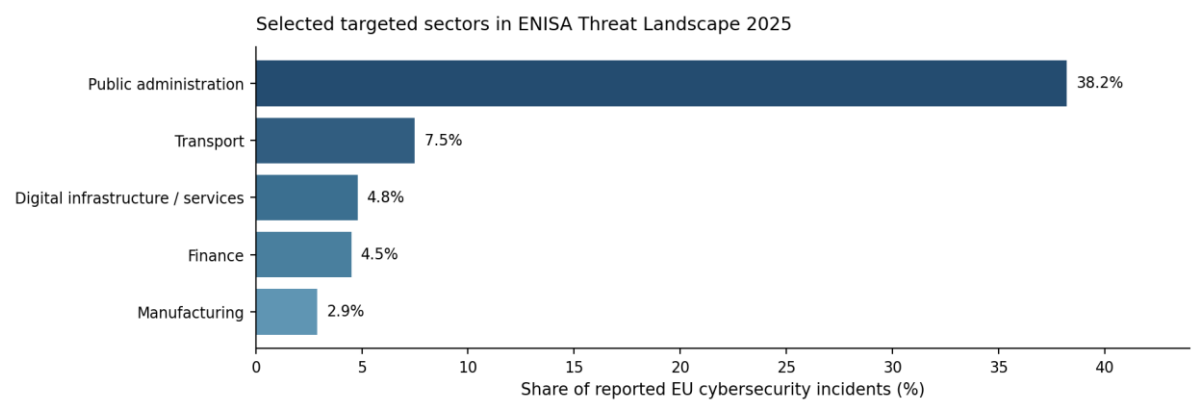
Defensive cybersecurity often requires examination of traffic patterns, identity information or device events. Such processing can be necessary to protect users while simultaneously exposing sensitive facts about workers, customers and unrelated correspondents. In the EU, GDPR principles and sectoral rules must be examined together; a statutory obligation to manage cyber risk does not automatically make all conceivable personal-data processing proportionate. Recent academic analysis of NIS2 and data-protection law highlights the need to identify an appropriate processing basis, purpose limitation, access restrictions and retention rationale in the relevant setting. The same functional questions are useful comparators for Iranian preservation and investigative powers, without incorrectly claiming that EU data-protection legislation applies to all Iranian processing. [R05, R25]

Online content remedies raise a different set of concerns. Rapid removal can prevent the circulation of operational material for attacks, but inaccurate classification can also interfere with journalism, documentation of abuses, counter-speech and lawful research. The EU’s terrorist-content regulation contains procedures and safeguards rather than

simply treating all extremist-seeming material as removable. A balanced legal design differentiates material directly covered by statute from commentary about it, documents evidence before removal when appropriate, and makes mistakes contestable. The 2024 Commission report evaluates implementation of that specific content framework; it does not establish that content removal is an effective substitute for securing energy or healthcare systems. [R10-R11, R20]

**Recent threat context: what the empirical record can and cannot show**

ENISA’s 2025 landscape reviewed 4,875 incidents occurring between 1 July 2024 and 30 June 2025. Its accompanying release reported that distributed-denial-of-service attacks constituted 77% of reported incidents and that the largest shares of targeted sectors included public administration (38.2%), transport (7.5%), digital infrastructure and services (4.8%), finance (4.5%) and manufacturing (2.9%). The chart below displays only those five selected categories; they are not intended to sum to 100%. ENISA’s dataset is a cybersecurity reporting and analytic sample rather than a representative count of legally adjudicated terrorist attacks, and the percentages must not be transported into a “cyberterrorism rate.” [R15, R23]



**Figure 2.** Selected sector shares in ENISA Threat Landscape 2025, reporting period July 2024-June 2025; general cybersecurity incidents, NOT classified terrorist attacks. Source: ENISA (2025) [R15, R23].

The ENISA Threat Landscape 2026, published on 22 September 2026, reports observations for January-December 2025 and describes continued pressure on public administration and essential or important entities, including ideology-linked DDoS, alongside ransomware and other threat classes. Because the editions cover different reporting periods and may apply different selection or classification methods, their percentages should not be read as a direct longitudinal measure without a common denominator and comparable inclusion criteria. This is particularly important when comparing a national criminal statute with EU-wide incident monitoring: neither the covered population nor the legal outcome is the same. [R15-R16]

For legal research, the incident record is nevertheless useful in two bounded ways. It demonstrates the operational relevance of continuity and supplier dependencies and identifies sectors in which fact patterns may arise. It also explains why ex ante resilience regulation and prompt preservation of logs matter even when terrorist attribution remains unproved. It cannot show that any named legal framework caused a trend or that incidents attributed by an agency to hacktivists met a criminal terrorist-intent test. A future empirical project would have to link incident-level technical records to adjudicated offence elements, procedural outcomes, sectoral denominators and clearly stated inclusion criteria. [R05-R08, R15-R16]

### **Reform and implementation options**

#### **A narrowly framed offence test:**

An administrable legal approach should test four elements in order: the intentional unauthorized cyber predicate; serious actual or legally specified threatened harm; the protected target and cross-system causal pathway; and the specific terrorist purpose required by applicable law. An additional cross-check asks whether conduct is instead ordinary cybercrime, legitimate authorized testing, protected speech or activity governed primarily by administrative resilience rules. Legislatures considering clarification should define the threshold through observable harm and precise mental elements, not through a generic reference to political opposition or “insecurity.” This is a proposed analytical checklist, not a claim that both legislatures have enacted an identical four-part test. [R01, R03-R04, R20]

For Iran, a focused legislative review could consider whether express rules are needed to distinguish exceptional cyber interference intended to intimidate a population or coerce public authorities from aggravated interference with essential services under Article 11. Any drafting exercise should preserve the existing statutory text unless deliberately amended, articulate whether threatened as well as realized harm is covered, and specify how the new rule interacts with ordinary cyber offences and general terrorism provisions. For EU Member States, the corresponding issue is consistent national treatment of the cross-referenced aggravations and terrorist aim, without automatic conversion of all malicious activity against critical infrastructure into a terrorist offence. Both tasks call for published interpretive guidance and judicially reviewable evidentiary criteria. [R01, R03-R04]

#### **Resilience without criminal-law shortcuts:**

An essential-services protection program should identify critical dependencies, credible high-impact scenarios, supplier risk, secure-by-design procurement, emergency manual workarounds, offline recovery and tested continuity plans. Such safeguards have value regardless of who launches an attack. Lawmakers should specify which operators have which responsibilities, how incident information reaches competent response bodies and which information can later be transferred to criminal investigators under a separate lawful basis. The EU’s current instruments offer examples of differentiated sectoral and product obligations, but the precise institutional design appropriate to Iran would require mapping its existing sectoral rules and operational capacities, not copying a supranational directive verbatim. [R05-R07, R12-R14]

A related safeguard is to separate “security reportability” from “criminal reportability.” A major outage can trigger an urgent resilience notification without resolving whether any human committed a

crime; a criminal referral may follow when there are articulable facts indicating unauthorized conduct. Parallel processes should maintain protected incident information, structured audit trails and unambiguous points of contact so that organizational candour during response is not penalized through unsupported inference of terrorist involvement. Regulatory compliance can be independently investigated where applicable, but the result should not be allowed to substitute for proof of a different defendant’s intent. [R05-R08]

#### **A safeguarded cross-border evidence protocol:**

A model request protocol would separate an immediate, narrowly tailored preservation request from a subsequent legally authorized production request. It would state a specific offence, data category, relevant account or service, time range, necessity explanation and expected disclosure channels; it would also record preservation duration, limits on secondary use and remedies for affected persons. A rapid operational contact point is valuable only if it operates within clear domestic authorization and adequate review. EU e-evidence legislation provides a recent regional reference point but does not itself supply universal cross-border authority over Iranian providers or third-country authorities. [R01-R02, R08-R09]

Cooperation proposals should anticipate difficult cases in which a request concerns expression that is criminal in one jurisdiction but protected in another. Independent scrutiny of dual criminality where applicable, serious-harm thresholds, human-rights risk, data minimization and defence access can reduce abuse and strengthen eventual evidentiary reliability. Recent scholarship on fragmented international cybercrime regimes and the human-rights stakes of the UN cybercrime negotiations supports treating these as design questions rather than assuming universal agreement on all categories of online crime. In a concrete prosecution, treaty reservations, national implementing rules and court practice would still control the outcome. [R20-R21]

#### **Limitations and future research**

This article is a desk-based comparison of accessible legal texts and selected recent institutional material; it is not a comprehensive reconstruction of every Iranian regulation or every EU Member State’s implementing legislation. It does not analyze a harmonized database of court judgments, military cyber operations, classified intelligence rules or operational cooperation practices. The lack of a common quantitative denominator precludes claims about comparative rates of cyberterrorism, conviction, deterrence or regulatory success. Its original contribution is a functional map that prevents four frequently conflated matters technical incident, cybercrime, terrorism offence and

resilience violation from being treated as legally interchangeable. [R01-R21]

Follow-on work should code a defined sample of national statutes and judgments against a common set of elements: predicate conduct, target, severity, purpose, attempt and participation, provider obligation, evidence authority, rights safeguard and outcome. Iranian-language case law and sectoral regulations should be translated and independently verified by qualified legal researchers. EU Member State national transposition, judicial interpretations and regulator enforcement should be sampled with dates rather than inferred from EU directives alone. Longitudinal incident analysis would additionally require reproducible case identification and an explicit decision on whether legally adjudicated terrorism, alleged intent or general cyber threat activity is being measured. [R03-R09, R15-R16]

### Conclusion

Iranian and EU law can both reach substantial unauthorized interference with data and information systems, including critical services, but the selected texts assign different roles to terrorism-specific purpose, essential-service targeting and distinct preventative duties. Iran's Computer Crimes Act provides general interference crimes, Article 11's essential-service aggravation, jurisdictional connectors and evidence measures. The EU explicitly links specified aggravated information-system interference to the terrorist-offence framework and overlays a wider set of operators, financial, critical-entity, product and response obligations. These structural observations do not resolve the content of every additional Iranian rule or national EU implementing provision, and no simple comparative enforcement conclusion follows. [R01-R14]

The central conclusion is methodological and practical: a rigorous cyberterrorism analysis must prove the underlying offence, the legally required seriousness and terrorist purpose, and individual responsibility; meanwhile, infrastructure protection and lawful evidence preservation should proceed on their own grounds. Recent EU legislation and 2025-2026 cybersecurity reporting make those distinctions more consequential, not less. Cooperation will be more defensible where requests are precise and reviewable, and where liability is not inferred from ideology, incident volume, jurisdictional location or organizational non-compliance. Definitional precision, victim-centered resilience, forensic reliability and effective safeguards belong in the same legal design, without collapsing into a single undifferentiated label. [R01-R23]

### Disclosure Statement

No potential conflict of interest reported by the authors.

### Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

### Authors' Contributions

All authors contributed to data analysis, drafting, and revising of the paper and agreed to be responsible for all the aspects of this work.

### References

- [R01] Islamic Republic of Iran. (2009). [Computer Crimes Act \(Law No. 71063\)](#), arts. 1-11, 28 and 32-34 [Persian original; English excerpts in UNODC SHERLOC].
- [R02] United Nations Office on Drugs and Crime. (n.d.). [SHERLOC legislative database](#): Iran, Computer Crimes Act, arts. 28-31.
- [R03] European Parliament and Council. (2013). [Directive 2013/40/EU on attacks against information systems](#). Official Journal of the European Union.
- [R04] European Parliament and Council. (2017). [Directive \(EU\) 2017/541 on combating terrorism](#). Official Journal of the European Union.
- [R05] European Parliament and Council. (2022). [Directive \(EU\) 2022/2555 on measures for a high common level of cybersecurity across the Union \(NIS2\)](#).
- [R06] European Parliament and Council. (2022). [Regulation \(EU\) 2022/2554 on digital operational resilience for the financial sector \(DORA\)](#).
- [R07] European Parliament and Council. (2022). [Directive \(EU\) 2022/2557 on the resilience of critical entities \(CER\)](#).
- [R08] European Parliament and Council. (2023). [Regulation \(EU\) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence](#).
- [R09] European Parliament and Council. (2023). [Directive \(EU\) 2023/1544 on designated establishments and legal representatives for gathering electronic evidence](#).
- [R10] European Commission. (2024). [Report on implementation of Regulation \(EU\) 2021/784 on addressing dissemination of terrorist content online](#), COM (2024) 64 final.
- [R11] European Parliament and Council. (2021). [Regulation \(EU\) 2021/784 on addressing the dissemination of terrorist content online](#).
- [R12] European Commission. (2024). [Implementing Regulation \(EU\) 2024/2690: cybersecurity risk-management measures and significant incidents for specified NIS2 digital providers](#).
- [R13] European Parliament and Council. (2024). [Regulation \(EU\) 2024/2847 on horizontal](#)

- cybersecurity requirements for products with digital elements (Cyber Resilience Act).
- [R14] European Parliament and Council. (2025). Regulation (EU) 2025/38 on measures to strengthen cyber solidarity and incident response capacities (Cyber Solidarity Act).
- [R15] European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025 (reporting period: 1 July 2024-30 June 2025).
- [R16] European Union Agency for Cybersecurity (ENISA). (2026). ENISA Threat Landscape 2026 (reporting period: January-December 2025), published 22 September 2026.
- [R17] Financial Action Task Force (FATF). (2026, June 19). High-Risk Jurisdictions Subject to a Call for Action.
- [R18] Council of Europe. (2026). Convention on Cybercrime (ETS No. 185): chart of signatures and ratifications, status page.
- [R19] Kian pour, M., Earls Davis, P. A., & Windekilde, I. M. (2025). Digital sovereignty in practice: analyzing the EU's NIS2 directive. *International Journal of Information Security*, 24, Article 167.
- [R20] Tropina, T. (2024). "This is not a human rights convention!": the perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*, 9(2), 200-220.
- [R21] Fidler, M. (2025). Fragmentation of international cybercrime law. *University of Louisville Law Review*, 2025, 737 et seq.
- [R22] European Commission. (2026). ProtectEU-related counter-terrorism agenda, COM (2026) 101 final (contextual policy document, not binding legislation).
- [R23] European Union Agency for Cybersecurity (ENISA). (2025). EU consistently targeted by diverse yet convergent threat groups (summary of ENISA Threat Landscape 2025).
- [R24] Iranian legal text repository. (2009). Computer Crimes Act, Persian full text (cross-check of Articles 8-11 and 32-34).
- [R25] European Union. (2016). Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
- [R26] European Union. (2012). Charter of Fundamental Rights of the European Union, especially arts. 7, 8, 11, 47-49 and 52.
- [R27] European Parliament and Council. (2019). Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment (adjacent financial-crime law, not a terrorism offence).