IDR
Romanian Diplomatic Institute

Ministerul Afacerilor Externe

# Romania in the European and international governance of coordinated vulnerability disclosure and security research

Teodora Curelariu


POLICY FORUM no. 8/2026

# Romania in the European and international governance of coordinated vulnerability disclosure and security research[1]

**Teodora Curelariu**[2]

*PhD candidate, Université Grenoble Alpes & Inria*

Policy Forum no. 8 / 2026

Published by: Romanian Diplomatic Institute

ISSN: 3119-8562

**Abstract**

As cyber threats intensify and societies become increasingly dependent on digital infrastructures, software vulnerabilities can no longer be understood solely as technical defects. They have become legal, institutional, strategic and diplomatic concerns. This article examines coordinated vulnerability disclosure (CVD) and security research at the intersection of Romanian law, European Union law and international cybersecurity cooperation. It situates Romania within an evolving framework shaped by the NIS2 Directive, emerging European vulnerability-management mechanisms and the Budapest Convention. Under Romanian law, the issue arises from the tension between the criminalisation of unauthorised access and related computer offences under Articles 360–366 of the Criminal Code, and the new national cybersecurity framework established by Emergency Ordinance No. 155/2024, approved and amended by Law No. 124/2025. Although the ordinance initially left the legality of the technical research preceding a report uncertain, a law adopted by Parliament in June 2026 would introduce conditional criminal-law protection for specified conduct where the research and reporting requirements are met. The article argues that CVD and legitimate security research are not merely technical practices, but mechanisms for building trust between authorities, researchers, the private sector and international partners. The effective implementation and clarification of this protection for necessary, proportionate and non-destructive research would strengthen Romania's domestic resilience and support a coherent Romanian position in European and international debates on vulnerability governance, researcher protection and cyber diplomacy.

**Keywords**: Romania, coordinated vulnerability disclosure, security research, European Union, Budapest Convention, legal safe harbour, cyber diplomacy.

[1] This publication draws exclusively on open-source materials. The opinions expressed herein are solely those of the author and do not necessarily reflect those of the institution.

[2] tcurelariu@gmail.com

## INTRODUCTION

Imagine that a researcher identifies a potential vulnerability in software used by a hospital, a public authority, an essential service or critical infrastructure. To produce a credible report, the researcher may need to interact with the system and verify that the vulnerability is real. That limited verification can help prevent a cyberattack, but it may also resemble **unauthorised access** under criminal law. The central policy question is whether Romanian law allows responsible researchers to perform the minimum testing needed to protect the public before an attacker exploits the same vulnerability. The issue is not limited to how organisations patch known flaws. It also concerns whether the state provides lawful and trusted channels through which vulnerabilities can be discovered and reported before they are exploited.

**Vulnerability research and coordinated vulnerability disclosure (CVD) are therefore closely connected.** A vulnerability cannot normally be assessed and remediated through CVD unless it has first been discovered and sufficiently validated to support a credible report. Yet validation may involve scanning, enumeration, authentication testing or a limited proof of concept, precisely the acts that may be characterised as **unauthorised** or **attempted access** under criminal law. Independent researchers can identify weaknesses that escape internal testing, certification and routine assessments, particularly after deployment and in systems combining software, cloud services and third-party components.

**When the legal consequences of proportionate testing are unpredictable, researchers may refrain from participating in CVD**, leaving vulnerabilities unreported (Pupillo et al. 2018, 53–54). A state that protects only the final report but leaves the preceding research legally uncertain regulates only half of CVD.

This relationship between research and remediation explains **why CVD has become part of the European cybersecurity framework**. The NIS2 Directive requires national strategies to promote and facilitate CVD and Member States to designate a CSIRT as the national coordinator, acting as a trusted intermediary (European Parliament and Council 2022, arts. 7(2)(c) and 12(1)). The Cyber Resilience Act requires manufacturers to establish vulnerability-handling processes and report actively exploited vulnerabilities, while the Cybersecurity Act integrates vulnerability assessment and management into European certification (European Parliament and Council 2024, arts. 13 and 14(1), Annex I, Part II;

European Parliament and Council 2019, art. 51(d)). Together, these instruments treat vulnerability information as a resource for collective resilience and strengthen its receipt, coordination and remediation. They govern what organisations must do once vulnerability information exists but do not harmonise the conditions under which external researchers may lawfully produce it.

The consequences of unremediated or poorly coordinated vulnerabilities can extend far beyond the initially affected system. Following WannaCry, Microsoft President Brad Smith compared the release of the exploit to "the U.S. military having some of its Tomahawk missiles stolen", illustrating the risks created when exploitable vulnerabilities are retained and later disclosed outside a controlled remediation process (Smith 2017). WannaCry showed how an exploit originally developed as part of a state cyber capability can cause widespread harm once it enters the public domain, while Log4Shell showed how a vulnerability in a widely reused software component can expose products, organisations and critical services across multiple sectors and jurisdictions. In Romania, the preamble to Emergency Ordinance No. 155/2024 refers to an incident in the first quarter of 2024 that affected 26 hospitals through a managed service provider and had a direct impact on vital services provided to the population (Romanian Government 2024, preamble). **Vulnerability governance is therefore part of national resilience, supply-chain security and cyber diplomacy**, not a purely technical function.

Romania has a particular interest in addressing **the resulting legal gap**. Its public administration, economy and essential services depend on products, services and infrastructure with cross-border supply chains and technical dependencies. As an EU and NATO Member State, a Party to the Budapest Convention and host to both the Council of Europe Cybercrime Programme Office (C-PROC) and the European Cybersecurity Competence Centre (ECCC), Romania is both responsible for improving domestic vulnerability management and well placed to contribute to European and international debates on cybercrime law, researcher protection and responsible state behaviour.

Romania's framework has evolved substantially. ENISA's 2022 comparative study classified Romania among the Member States without a national CVD policy. Emergency Ordinance No. 155/2024 subsequently established a statutory coordination mechanism and designated the National Cyber Security Directorate (DNSC) as the national CVD coordinator and trusted intermediary. The ordinance regulates reporting, anonymous submissions, communication with affected providers and cross-border coordination. It nevertheless preserves the application of the Criminal Code, leaving the legal effect of compliance initially

uncertain. In June 2026, Parliament adopted a law that would introduce Article 365[1] into the Criminal Code and exclude criminality for specified acts where the cumulative conditions of Article 36(5) and (6) are met. Pending promulgation and entry into force, the reform represents a significant but incomplete move towards conditional statutory protection (Romanian Parliament 2026).

This paper argues that Romania has created an institutional mechanism for receiving and coordinating vulnerability reports and has begun to secure the legal path through which they are produced, although the proposed protection remains conditional and incomplete. The objective is not to exempt security researchers from criminal law or to authorise unrestricted testing, but to distinguish necessary, proportionate and non-destructive research from harmful intrusion, data extraction, persistence and disruption. The question is consequently narrower than whether ethical hacking should be permitted in general. It concerns the legal treatment of limited acts undertaken to establish that a weakness exists, assess its security relevance and communicate enough evidence for remediation. The legality of the conduct should therefore depend on its scope, purpose, effects and the researcher's subsequent behaviour.

The analysis combines three levels. **At national level**, it examines the relationship between Articles 360–366 of the Criminal Code, the mechanism created by Emergency Ordinance No. 155/2024 and the conditional protection proposed by Article 365[1]. **At European level**, it considers Directive 2013/40/EU, NIS2, the Cyber Resilience Act and the Cybersecurity Act. **At international level**, it assesses access to a computer system "without right" under the Budapest Convention and the recognition of legitimate security research in the United Nations Convention against Cybercrime. The paper then proposes a legal and diplomatic agenda for Romania.

## WHY COORDINATED VULNERABILITY DISCLOSURE DEPENDS ON SECURITY RESEARCH

### From vulnerability discovery to coordinated remediation

A vulnerability is a weakness that can be used to compromise a digital product or system. Vulnerability management covers the broader response, from identifying and assessing the weakness to fixing it, distributing the correction and monitoring the result. CVD addresses one essential part of that response: how the person who discovers the weakness communicates

with the organisation able to remedy it and how the parties coordinate the next steps. ENISA's definition is particularly revealing: **a national CVD policy should allow and encourage research under defined rules** (ENISA 2022, 6). A reporting email address is therefore not a complete policy if researchers still do not know what they may lawfully test.

In practice, CVD begins when a possible weakness is discovered and verified enough to support a credible report. The provider then assesses the finding, develops a fix and coordinates communication with the researcher and, where necessary, other providers or authorities. The objective is to avoid both premature publication, which may expose users before a correction exists, and indefinite secrecy, which leaves the vulnerability unresolved.

Coordination is especially important where the affected party is difficult to identify or where one vulnerability is embedded in several products. The process may involve the discoverer, the reporter, the affected provider, organisations deploying the product and a CSIRT or another trusted intermediary. A trusted intermediary can reduce information asymmetries, preserve confidentiality and coordinate communication across organisational and national boundaries. Distinguishing the respective roles clarifies who may authorise testing, remediate the weakness and coordinate disclosure. CVD therefore addresses not only publication timing but the allocation of responsibilities among actors who possess different parts of the information needed for remediation.

**Different mechanisms and forms of authorisation**

CVD, vulnerability disclosure policies, bug bounty programmes and penetration testing are often grouped together, but they answer different legal questions. The distinction matters because the source, scope and legal effect of authorisation are not the same.

- **A vulnerability disclosure policy** tells researchers how to report a vulnerability and may also specify the systems and techniques that the organisation authorises.
- **A broader CVD process** may involve several providers, CSIRTs or foreign authorities, while **a bug bounty programme** adds a reward to an organisation's disclosure policy.
- **A penetration test**, by contrast, is commissioned under a contract defining the authorised systems, methods and period of testing.

These mechanisms do not provide equivalent legal protection. A contracted penetration tester has the clearest position because the client authorises specified operations on specified

systems. That protection nevertheless ends at the limits of the agreement. Testing an excluded subdomain, causing an unauthorised denial of service or accessing more data than necessary may fall outside the authorised scope. A bug bounty participant similarly relies on the programme's public rules, which may exclude subdomains, user accounts, third-party services or techniques such as social engineering. An organisation cannot authorise testing of infrastructure that it does not control, even where that infrastructure is technically connected to the programme.

**The independent researcher occupies the most uncertain position** because no permission exists in advance. The boundary between ordinary public interaction and unauthorised access must therefore be assessed after the technical act. Consulting a public webpage or repository may be performed with right, whereas using an exposed credential, executing a command, entering a restricted endpoint or accessing non-public data may constitute access without right, even where the vulnerability was discovered accidentally.

**Authorisation may remain difficult to delimit in systems relying on cloud services, external interfaces and supply-chain components**, because testing an authorised application may affect infrastructure controlled by another entity. Its scope must therefore reflect the system's actual architecture.

**The assessment must avoid two extremes**. Public accessibility does not amount to unlimited permission, but an insecure configuration should not transform every unexpected response into a criminal act. The legality of the research depends not on its label, but on the precise technical act, the source and limits of authorisation, the researcher's purpose, the effects produced and whether the interaction knowingly exceeded ordinary public access.

## Security research as the necessary upstream stage of CVD

Security research is not a single technical act. Reading public documentation or a CVE entry involves little or no interaction with the target. Scanning identifies exposed services; fingerprinting identifies the software or configuration in use and enumeration seeks more detailed information about accessible resources. Authentication testing examines whether access controls can be bypassed, while fuzzing or a proof of concept may execute commands, alter a temporary state or interrupt a service. Legal risk generally increases as research moves from passive observation to interaction with restricted resources, access to data or effects on

system operation. Treating every step as equivalent obscures both the technical reality and the researcher's actual conduct.

The Budapest Convention's Explanatory Report provides two useful limits. Access requires entry into all or part of a system, so merely sending a message or file is not automatically access. The use of a technical tool is not unlawful by itself, and interacting with a system that is freely open to the public may be performed with right (Council of Europe 2001b, paras. 46-48). Romanian guidance should build on this distinction. It should separate ordinary public interaction from active testing, access to restricted resources, access to data, persistence, modification and disruption. A researcher must stop once enough evidence exists, but the law must permit enough verification to distinguish a real vulnerability from a mere suspicion.

## ROMANIA'S REPORTING MECHANISM AND ITS EMERGING LEGAL PROTECTION

### From early international engagement to national coordination

Romania's engagement with CVD predates the 2024 ordinance. Together with Hungary and the Netherlands, it participated in an initiative developed through the Global Forum on Cyber Expertise to exchange experience concerning responsible and coordinated vulnerability disclosure. This initiative contributed to a regional project involving Czechia, Hungary, the Netherlands and Romania that sought to operationalise an Organisation for Security and Co-operation in Europe confidence-building measure on responsible vulnerability reporting (ENISA 2022, 28-33).

DNSC also operated a local reporting mechanism and acted as a trusted third party in certain disclosure processes. Nevertheless, ENISA concluded that Romania had not implemented a national CVD policy when the relevant information was collected in 2021 (ENISA 2022, 32-33). Romania was not alone. ENISA found a fragmented European landscape in which only a small group of Member States had implemented national policy requirements. More importantly, **seventeen consulted Member States identified criminal law as the most pressing legal obstacle to CVD, leading ENISA to recommend that states "define the role of ethical hackers in relevant national laws"** (ENISA 2022, 7, 62-63).

**Romania's Cybersecurity Strategy for 2022-2027** provided the political basis for reform by emphasising resilience, research, public-private-academic cooperation, information exchange and cyber diplomacy (Romanian Government 2021, secs. 4.1-4.5). **The strategy supplied the political rationale for CVD but did not provide the legal clarity researchers need in practice**. It did not explain which technical acts may be performed before a vulnerability is reported or what protection follows from responsible conduct.

**The implementation of NIS2 through Emergency Ordinance No. 155/2024**

Emergency Ordinance No. 155/2024 gave CVD a statutory place within Romanian cybersecurity governance and was subsequently approved and amended by Law No. 124/2025. Article 23 requires national cybersecurity policy to address CVD, research and development, skills, supply-chain security and cooperation among public, private and academic actors, while Article 25 empowers DNSC to regulate and manage the national CVD process.

Article 36 designates DNSC as the national CSIRT responsible for CVD and as a trusted intermediary between the reporter of the vulnerability and the producer or provider of the potentially vulnerable ICT product or service. DNSC may receive and assess reports, facilitate anonymous reporting, identify affected entities, connect the parties and support verification with the responsible provider (Romanian Government 2024, art. 36(1)-(2)). It may also negotiate disclosure and remediation timelines where several entities are affected, cooperate with other members of the EU CSIRTs Network in cases with significant cross-border impact and issue procedures, technical rules and guidance concerning reporters, affected entities and private vulnerability disclosure programmes. Any natural or legal person may report a vulnerability to DNSC, subject to compliance with applicable law (Romanian Government 2024, art. 36(2)-(3)).

The law adopted in June 2026 would also require DNSC to consult a committee without legal personality composed of authorities responsible for cybersecurity, defence, public order and intelligence under Law No. 58/2023. Although this may strengthen interinstitutional coordination, its relationship with the mechanisms already established under Article 39 of Emergency Ordinance No. 155/2024 should be clarified so that DNSC retains its role as the trusted civilian CVD intermediary (Romanian Parliament 2026; Romanian Legislative Council 2026, 2–4).

Following Law No. 124/2025, manufacturers and providers qualifying as essential or important entities must inform DNSC of vulnerabilities they identify or receive from third parties and remedy them within a timeframe agreed with DNSC (Romanian Parliament 2025).

Thus, researchers no longer need to identify and persuade every affected actor alone. Anonymous reporting is possible, and the mechanism recognises that a single component may affect several providers and jurisdictions. DNSC can therefore reduce information asymmetries and coordination costs that individual researchers cannot overcome. **The mechanism does not, however, determine whether the research preceding the report was lawful**.

**Responsible conduct under Article 36**

Besides creating a reporting channel, Article 36 also prescribes minimum conditions for the research preceding a report. **Research must be conducted in good faith, solely to improve cybersecurity and in compliance with applicable law**. It must not involve unauthorised access to or copying of file contents, deletion or modification of data, brute-force, social engineering, interruption of services, malware or techniques affecting availability. The vulnerability must be reported within 48 hours of identification and may not be publicly disclosed without DNSC's agreement (Romanian Government 2024, art. 36(5)-(6)).

Essential and important entities must establish processes for receiving, assessing and remedying vulnerability reports, cooperate with DNSC and publish contact details and reporting conditions. Article 36 therefore imposes duties on both researchers and covered entities. Researchers must minimise harm, while covered entities must be able to receive, assess and act on reports. **These conditions are consistent with recognised principles of responsible research, including proportionality and data minimisation**. They also distinguish research from extortion, destructive interference and malicious exploitation (Romanian Government 2024, arts. 3(1)(b) and 36(5)-(6)).

However, Article 36 requires compliance with existing law and preserves the application of the Criminal Code, the GDPR and other regimes (Romanian Government 2024, art. 2(5), as amended by Romanian Parliament 2025, point 1). Article 36 itself does not state that compliance excludes criminal or civil liability. This gap would be addressed by the legislative reform adopted by Parliament in June 2026 and examined below.

**Pending promulgation: conditional statutory protection for vulnerability research**[3]

At the time of writing, the Romanian Parliament has adopted a law supplementing Article 36 of Emergency Ordinance No. 155/2024 and introducing a new Article 365¹ into the Criminal Code. Pending promulgation, publication and entry into force, the existing legal framework remains applicable. The proposed provision states that conduct falling under Articles 360(1) and (3), 361 and 364 would not constitute an offence where a natural or legal person satisfies the cumulative vulnerability-research and reporting conditions laid down in Article 36(5) and (6) (Romanian Parliament 2026).

**The limited scope of Article 365¹** reflects the legislative history of the reform. The initial proposal would have applied to all offences under Articles 360-365 of the Criminal Code. The Legislative Council issued a negative opinion, reasoning that several of those offences were incompatible with the cumulative conditions in Article 36(5) and (6), which prohibit data modification, service disruption and other harmful conduct. The parliamentary committees subsequently restricted the provision to Articles 360(1) and (3), 361 and 364. Their report nevertheless recognised that legitimate vulnerability research may unavoidably involve interaction with a computer system, the incidental receipt or transfer of data and the use of specialised tools. The report is not entirely consistent on Article 360(2): **its reasoning states that this offence should not be excluded absolutely from protection, yet the amended and adopted text does not include it**. The final scope therefore represents an attempt to distinguish incidental technical consequences of legitimate testing from conduct whose completion would itself contradict the responsible-research conditions (Romanian Legislative Council 2026, 4-6; Romanian Senate 2026, 2-4 and annex).

The reform represents a significant change in Romania's approach. Compliance with Article 36 would no longer operate solely as a set of responsible-conduct requirements but would produce an express substantive criminal-law consequence. The provision would protect certain forms of vulnerability research without expressly requiring prior authorisation from the affected organisation. Romania would therefore move beyond a reporting mechanism supported only by case-by-case interpretation and prosecutorial discretion towards conditional statutory protection.

[3] This article reflects the legislative status as of 30 June 2026, the date on which the manuscript was finalised.

**The narrowing of the offences covered does not, however, resolve every legality concern**. During the legislative process, the Ministry of Internal Affairs observed that the proposed protection was not autonomous because it depended on compliance with conditions contained in Emergency Ordinance No. 155/2024, potentially affecting the foreseeability and stability expected of criminal law. The Ministry of Justice considered that the initial formulation risked an **excessively broad decriminalisation of computer offences**, whereas DNSC supported the creation of the protection but requested correction of the offences to which it applied. **These positions explain both the restricted final formulation and the continuing need for detailed administrative and prosecutorial guidance** (Romanian Senate 2026, 2-4).

The protection would nevertheless remain offence-specific rather than constituting a comprehensive safe harbour. It would not expressly cover access undertaken for the purpose of obtaining computer data under Article 360(2), data interference under Article 362, system interference under Article 363 or misuse of devices under Article 365. Nor would it expressly clarify the treatment of attempts under Article 366 or provide protection from civil liability. Its practical effectiveness would also depend on how the cumulative conditions of Article 36 are interpreted, particularly the 48-hour reporting period and the restrictions on the technical acts needed to verify a vulnerability.

## The unresolved questions in Article 36

These ambiguities now have direct criminal-law significance because the protection proposed by Article 365[1] would depend on cumulative compliance with Article 36(5) and (6) (Romanian Parliament 2026).

**First, when does the 48-hour clock start?** Vulnerability identification is often gradual: a researcher may observe anomalous behaviour and only later confirm that the weakness is reproducible and security-relevant. A rigid interpretation beginning with the first anomaly could encourage premature and incomplete reports. The period should apply to an initial notification after reasonable confirmation, with the possibility of providing additional technical information later.

**Second, what counts as circumventing a technical barrier?** Brute-force, phishing and social engineering can clearly be excluded, but some vulnerabilities consist precisely in the ability to bypass an authentication or authorisation control. DNSC should distinguish an

attempt to defeat a functioning safeguard from the minimum demonstration that the safeguard does not operate as intended.

**Third, how long may disclosure be postponed?** Temporary confidentiality is necessary while a fix is prepared, but Article 36 provides no external limit on the period during which DNSC may refuse to authorise publication of the vulnerability. Without review and presumptive timelines, coordination can turn into an indefinite embargo, leaving users unable to assess their own exposure.

**Finally, Article 2 excludes institutions** in the fields of defence, public order and national security, the Ministry of Foreign Affairs, the National Registry Office for Classified Information, law-enforcement entities and systems processing classified information. These exclusions are understandable given the sensitivity of the systems concerned, but they prevent Article 36 from supplying a uniform route for the whole public sector. Equivalent special procedures are needed so that vulnerabilities affecting excluded institutions can be reported securely without exposing operational or classified information.

| Instrument | Principal contribution | Remaining gap |
|---|---|---|
| Cybersecurity Strategy 2022–2027 | Establishes resilience, research, public-private cooperation and cyber diplomacy as national priorities. | Does not determine the legal status of security researchers. |
| Emergency Ordinance No. 155/2024 | Designates DNSC as CVD coordinator and regulates reporting, coordination and entity obligations. | Its research and reporting conditions remain open to interpretation and do not address civil liability. |
| Criminal Code, Articles 360–366 and proposed Article 365¹ | Protects systems and data against computer offences; proposed Article 365¹ would conditionally exclude criminality for specified acts complying with Article 36. | Would omit several offences and would not expressly address attempt or civil liability. |
| Law No. 361/2022 | Protects certain reports made in a professional context. | Does not create a general right for independent vulnerability research. |
| NIS2, CRA and EUVD | Strengthen national coordination, product security and European vulnerability intelligence. | Do not create a uniform European criminal-law safe harbour. |

Table 1. Key contributions and remaining gaps in Romania's legal and institutional framework for CVD and security research.

## Substantive liability and prosecutorial response

Vulnerability research raises two distinct criminal-law questions. The first is **substantive** and concerns whether the technical acts performed by the researcher satisfy the elements of illegal access or another computer offence. The second is **procedural** and concerns whether prosecution should follow where the researcher acted defensively, limited testing to what was necessary and promptly reported the vulnerability. Conduct may fall within the wording of a broadly defined offence while still presenting characteristics that weigh against prosecution (Pupillo et al. 2018, 43-46).

A prosecutorial decision not to proceed does not necessarily mean that the act was lawful, while a statutory justification changes the substantive legal character of the conduct. Conversely, the existence of a broad offence does not require authorities to ignore purpose, proportionality or the absence of harm when deciding whether a case merits investigation and prosecution. Romania's adopted reform shifts the question from whether a statutory safeguard should exist to how its conditions, limits and relationship with prosecutorial discretion should be interpreted.

## "Access without right" under the Budapest Convention

The Budapest Convention provides one of the principal international foundations for Romanian computer offences. Article 2 requires each Party to criminalise intentional access to all or part of a computer system without right, while allowing states to add limiting conditions, including the infringement of security measures, the intention to obtain data, another dishonest intention or a connection between computer systems (Council of Europe 2001a, art. 2).

The expression "without right" distinguishes criminal access from conduct that is authorised, legally permitted or otherwise justified. The Explanatory Report states that access authorised for security testing or system protection is performed with right, and that the use of a technical tool does not make access unlawful where the system is freely open to the public (Council of Europe 2001b, paras. 38, 47-48). The expression therefore leaves room for legal authorisation and other recognised justifications.

**The Convention's authors nevertheless acknowledged controversy surrounding the criminalisation of simple access**. Some states considered unauthorised entry harmful in itself, while others argued that simple entry does not necessarily cause harm and may reveal security weaknesses. Article 2 therefore permits Parties to narrow the offence by requiring the violation of security measures or a particular intention (Council of Europe 2001b, paras. 49-50). Thus, **the Convention establishes a minimum standard of criminalisation but leaves substantial discretion to domestic law**. It creates neither a status for ethical researchers nor a direct defence for good-faith researchers, leaving the meaning of authorisation, intent, necessity and justification largely to national law.

**Romania's broad offence of "access without right"**

**Article 360(1) of the Romanian Criminal Code criminalises access without right even where no data are obtained and no damage occurs**. Penalties increase where the purpose is to obtain data or where the system is protected by specialised access restrictions (Romanian Parliament 2009, art. 360). The offence therefore focuses on the unauthorised entry itself rather than on a harmful consequence.

The Romanian offence does not require circumvention of a security measure. **Its scope is therefore broader than the minimum offence required** by Article 3 of Directive 2013/40/EU, which requires infringement of a security measure, at least in non-minor cases. The European Commission identified Romania among the Member States whose provisions did not require circumvention to establish liability (European Commission 2017). A researcher may therefore face legal scrutiny even when no password, technical barrier or security control was defeated.

Article 35(2) of Law No. 161/2003 defines access without right as access performed without legal or contractual authorisation, beyond the limits of existing authorisation or without permission from the person entitled to control the system. Although the definition mentions **scientific research** among the operations for which permission may be relevant, it does not create a general research privilege. It confirms that research conducted within a computer system normally requires a legal, contractual or consensual basis (Romanian Parliament 2003, art. 35(2)). A defensive purpose may support a finding of good faith, but it does not necessarily replace authorisation.

Put simply, **a beneficial purpose does not necessarily exclude criminal intent**. A researcher may deliberately perform a test to improve security while knowing that authorisation may be lacking. Until the proposed Article 365[1] enters into force, good faith may influence the assessment of the case or the decision to prosecute without necessarily excluding the offence.

During the legislative process, the Superior Council of Magistracy also referred to Article 21 of the Criminal Code, under which the exercise of a right or the performance of an obligation may justify otherwise criminal conduct. That general justification does not itself establish a right for an independent researcher to test a third party's system without prior authorisation; it presupposes that the relevant right or obligation already exists (Superior Council of Magistracy 2026, 1-2).

**Offences beyond illegal access**

Research may also interact with Articles 361-365 of the Criminal Code. Capturing non-public traffic may fall under Article 361; changing or deleting data under Article 362; crashing a service through fuzzing or automated requests under Article 363; and copying even a small database sample to prove the flaw under Article 364. Article 365 addresses tools, passwords and programmes held or distributed for the purpose of committing these offences. A test can move from one offence to another as soon as it affects communications, data, availability or credentials. Scanners, debuggers, exploit frameworks and password-auditing software are dual-use tools whose possession and use must be assessed in light of purpose, authorisation and actual conduct.

Article 6(2) of the Budapest Convention makes this distinction explicit. The criminalisation of misuse of devices should not extend to production, distribution or possession that is not intended for committing an offence, including authorised testing or system protection (Council of Europe 2001a, art. 6(2); Council of Europe 2001b, paras. 76-77). **Treating the mere possession of a security tool as suspicious would criminalise ordinary professional practice**.

**Attempt and the criminalisation of unsuccessful research**

Romanian law also punishes attempts to commit the computer offences in Chapter VI. A researcher may therefore face legal risk even when a test fails and no access, extraction or

disruption occurs (Romanian Parliament 2009, art. 366). This matters because vulnerability research often seeks to determine whether access is possible. The concept of attempt concerns the transition within the *iter criminis*[4] from preparatory conduct to the commencement of the execution of an offence. Under Article 32 of the Criminal Code, an attempt exists where execution of the intended offence has begun but is interrupted or fails to produce its effect. Preparatory activity is not automatically punishable, but conduct directly oriented towards completion may be.

This distinction is particularly important for vulnerability research. A general port scan or ordinary request should not automatically amount to attempted illegal access because it may reveal that a service exists without entering the system. By contrast, a targeted attempt to bypass authentication, exploit a specific vulnerability, reach a restricted endpoint or execute a proof of concept may constitute the commencement of execution even if no access is obtained, depending on the technical facts and the researcher's intention. The Budapest Convention's Explanatory Report similarly distinguishes actual penetration from the mere transmission of a message or file (Council of Europe 2001b, para. 46).

**Romania's approach is stricter than the minimum required by the Budapest Convention,** whose Article 11 does not oblige states to criminalise attempted illegal access under Article 2 (Council of Europe 2001a, art. 11(2); Council of Europe 2001b, para. 120).

The same unsuccessful proof of concept may therefore be a non-punishable preparatory act in one jurisdiction and a punishable attempt in another, even though the technical conduct is identical. The absence of an express reference to Article 366 in the proposed Article 365[1] may therefore leave the treatment of unsuccessful but otherwise compliant vulnerability research uncertain (Romanian Parliament 2026).

## Why whistleblower protection is not enough for security researchers

**Security researchers are sometimes compared with whistleblowers because both may disclose information in the public interest**. Romanian Law No. 361/2022 covers infringements concerning the security of networks and information systems and protects persons who obtain relevant information in a professional context (Romanian Parliament 2022, arts. 2-3).

[4] *Iter criminis* refers to the successive stages through which an offence may develop, from preparation to the beginning of execution, completion and, where relevant, the production of the intended result.

Article 21 may protect the reporting or disclosure of information, as well as access to information available through professional duties where such access is necessary for the report, but it does not protect unrelated or unnecessary acts (Romanian Parliament 2022, art. 21). An employee who encounters a vulnerability during authorised work may therefore be protected, whereas an external researcher without a professional relationship generally is not. The law also does not automatically justify the technical steps performed before the person becomes a protected reporter.

Whistleblower law mainly protects a person who reports information encountered through work. CVD must also address a person who independently discovers and verifies a weakness. The regimes may overlap, but one cannot replace the other.

### Fundamental rights as safeguards rather than immunities

Scientific freedom protects the pursuit of knowledge, while freedom of expression protects the communication of research results. These interests are particularly strong where the research reveals risks to public safety (United Nations 1966, art. 15; European Union 2012, arts. 11 and 13; Council of Europe 1950, art. 10). These rights reinforce legal certainty and proportionality but do not create an unrestricted entitlement to access systems belonging to others. Restrictions on research and publication must nevertheless pursue legitimate aims, be foreseeable and remain proportionate.

## EUROPEAN AND INTERNATIONAL GOVERNANCE WITHOUT A COMMON RESEARCHER SAFE HARBOUR

### Researcher exposure under NIS2

European policy identified the upstream problem before NIS2. ENISA's 2016 guidance described the unintended effects of criminal and civil liability as a major obstacle to vulnerability disclosure. The Commission's 2017 cybersecurity communication called for recognition of the role of third-party security researchers and for conditions supporting CVD across the Member States. The CEPS Task Force subsequently recommended a European framework, complemented by national legislation and informed by ISO/IEC 29147 and ISO/IEC 30111, to provide legal clarity for both discovery and disclosure (ENISA 2016;

European Commission and High Representative 2017, 6; NIS Cooperation Group 2023; Pupillo et al. 2018).

EU law establishes a criminal-law baseline but leaves researcher protection largely to Member States. Directive 2013/40/EU excludes access authorised by law or by a right holder from the concept of "access without right", yet national offences still differ in their treatment of security measures, intention and authorisation (European Parliament and Council 2013; European Commission 2017). NIS2 moves beyond criminalisation by requiring Member States to promote CVD through national strategies and to designate a CSIRT able to receive reports, preserve anonymity, facilitate communication, and cooperate in cross-border cases (European Parliament and Council 2022, arts. 7 and 12). Recital 60 expressly recognises that researchers may face criminal and civil liability, and encourages "**Member States to adopt guidelines as regards the non-prosecution of information security researchers**". A recital, however, is not an enforceable defence, so NIS2 identifies the problem without closing the legal gap (European Parliament and Council 2022, recital 60).

NIS2 also provides the legal basis for the **European Vulnerability Database** (EUVD). Operational since May 2025, EUVD aggregates information on affected products, severity, exploitation status and available mitigation measures and is accessible to authorities, providers, researchers and the public. EUVD improves vulnerability intelligence but does not determine whether the underlying research was lawful. Europe is therefore developing a stronger map of vulnerabilities without an equally consistent map of the legal protection available to the people who find them.

European law thus increasingly regulates what authorities, databases and manufacturers must do once vulnerability information exists, while the conditions under which researchers may lawfully produce that information remain fragmented. Providers in jurisdictions with uncertain legal frameworks may consequently receive fewer reports, less technical cooperation and delayed warnings about cross-border weaknesses (ENISA 2016; ENISA 2022; NIS Cooperation Group 2023).

**Product responsibility under the Cyber Resilience Act**

The Cyber Resilience Act places new responsibilities on manufacturers of products with digital elements, requiring them to design products with cybersecurity in mind, maintain vulnerability-handling processes, provide contact points and issue security updates during the

support period. From 11 September 2026, manufacturers must report actively exploited vulnerabilities and severe incidents through ENISA's Single Reporting Platform, generally with an initial warning within 24 hours and a fuller notification within 72 hours (European Parliament and Council 2024, arts. 14-16).

These obligations are particularly important for long-lived and interconnected products within the CRA's scope, including industrial systems and consumer Internet-of-Things devices. Their software may remain in use for many years while suppliers, dependencies and threat conditions change. Effective vulnerability handling therefore requires both internal testing before market entry and the continuing ability to receive and act on reports from external researchers throughout the support period (European Parliament and Council 2024; Pupillo et al. 2018). The CRA strengthens manufacturers' vulnerability-handling obligations but does not determine the criminal-law status of external researchers or authorise third-party testing.

The framework remains complementary but incomplete: the CRA requires manufacturers to act, national CVD mechanisms identify where researchers should report, and national law must still determine when the preceding research is legally protected.

**The Cybersecurity Act and certification**

The Cybersecurity Act contributes indirectly through European cybersecurity certification schemes. Certification can require vulnerability assessment, security testing and procedures for managing newly discovered weaknesses. The EU Common Criteria scheme, for example, requires certificate holders to maintain vulnerability-management processes and respond to relevant information concerning certified products.

Certification may support vulnerability-management procedures, but it neither guarantees the continuing security of a product nor protects independent researchers. Certification can normalise disclosure procedures by requiring certificate holders to maintain contact points and processes for previously unknown weaknesses. It cannot replace independent discovery because it evaluates a product in a defined configuration at a particular point in time. External research remains a corrective mechanism for assumptions that later prove incomplete.

## The Budapest Convention and the limits of harmonisation

The Budapest Convention remains the principal binding international framework for computer offences and cooperation concerning electronic evidence. Its terminology shapes national laws on access, interception, interference and misuse of tools. However, it was conceived primarily as a criminalisation and cooperation treaty. It protects legitimate conduct through the expression "without right" and national interpretations of authorisation, intent and justification, without requiring CVD mechanisms or researcher safe harbours.

**The transnational character of research exposes this limitation**. The researcher, affected system, technology provider, users and hosting infrastructure may be located in different states, each of which may assert jurisdiction on the basis of territorial conduct, effects, system location or nationality. Authorisation valid under one national policy may therefore fail to prevent proceedings elsewhere, and a domestic safe harbour does not automatically travel with the researcher across borders (Pupillo et al. 2018, 46).

The Convention's flexibility has facilitated broad participation but also permits different thresholds of criminality. The treatment of security measures, attempt, good faith and authorisation may therefore change from one jurisdiction to another.

## Legitimate security research under the United Nations Convention against Cybercrime

The 2024 United Nations Convention against Cybercrime (not yet in force) follows the familiar model of criminalising intentional access without right while allowing states to add further conditions (United Nations 2024, art. 7). Its principal innovation for this paper is Article 53(3)(e), which recognises legitimate security-research activities intended solely to strengthen security and conducted under conditions prescribed by domestic law (United Nations 2024, art. 53(3)(e)). **This is politically important because a global cybercrime instrument now acknowledges that security research can contribute to prevention rather than facilitate crime.**

The provision remains limited because it appears among preventive measures rather than as an exception to the substantive offences and refers the conditions of protection back to domestic law. It encourages protection without determining which technical acts are lawful. It nevertheless gives Romania an additional diplomatic basis for advocating clearer national and international standards.

### Responsible vulnerability disclosure as an emerging international cyber norm?

The international policy framework also extends beyond cybercrime treaties. The 2015 United Nations Group of Governmental Experts (GGE) stated that **states should encourage responsible reporting of ICT vulnerabilities and share information on available remedies**. The 2021 GGE report invited states to consider impartial legal, policy and programmatic frameworks for deciding how vulnerabilities should be handled. Although non-binding, these formulations recognise vulnerability reporting and remediation as matters of responsible state behaviour (United Nations 2015; United Nations 2021).

States are therefore expected not merely to endorse responsible disclosure in diplomatic forums, but to establish trusted points of contact, workable procedures, legal certainty and channels for sharing mitigation information. The norm does not create immunity but supports the argument that domestic criminal law should not frustrate the reporting and remediation practices that states promote internationally (Global Forum on Cyber Expertise 2016; United Nations 2015; United Nations 2021).

Because European and international law do not provide a common safe harbour, national systems remain the principal laboratories for researcher protection. For instance, Belgium, the Netherlands and Lithuania illustrate three different models that could help assess and refine Romania's emerging model.

## COMPARATIVE MODELS OF RESEARCHER PROTECTION

### Belgium and conditional statutory protection

**Belgium has conditionally legalised, or more precisely decriminalised, ethical hacking.** Since 2023, a natural or legal person may investigate a potential vulnerability without the affected organisation's prior consent and may benefit from protection where statutory conditions are met. Articles 22 and 23 of the Belgian NIS2 Law of 26 April 2024 specify this framework, which applies even when the organisation has no vulnerability disclosure policy. Belgium has thus created a statutory cause of justification for certain acts that would otherwise constitute computer offences. The researcher must act without fraudulent or harmful intent and

limit the investigation to what is necessary and proportionate for identifying and reporting the vulnerability.

A simplified notification must generally be sent to the affected organisation and the CCB within 24 hours of discovery, followed by a complete report within 72 hours. Public disclosure requires the CCB's agreement, and additional prior authorisation is required for research concerning certain sensitive entities (CCB 2025). When the cumulative conditions are met, the mechanism can protect the researcher under Belgian criminal and civil law.

Romania's Article 36 contains comparable conditions, including good faith, non-disruption and rapid reporting. The proposed Article 365[1] would bring Romania closer to the Belgian statutory model by attaching criminal-law protection to compliance. Romanian protection would nevertheless remain narrower because it would apply only to specified offences and would not expressly address civil liability (Romanian Parliament 2026).

**The Dutch prosecutorial model**

The Netherlands has had a national CVD policy since 2013 and was one of the earliest European States to institutionalise responsible disclosure. Its framework relies on national guidance, organisational CVD policies and the position of the Public Prosecution Service rather than a statutory safe harbour. Ethical hacking is not an autonomous category of Dutch criminal law; the prosecutor retains discretion over whether to prosecute and considers compliance with CVD guidance (Openbaar Ministerie 2013; ENISA 2022, 29-30, 64-65).

The prosecutorial assessment considers the social interest served by the research, the researcher's purpose, subsidiarity, proportionality and conduct after discovery. Researchers who limit testing to what is necessary, avoid unnecessary access or copying of data, report promptly and cooperate with the affected organisation are distinguished from persons who establish persistence, extract databases, demand payment or publish irresponsibly. **The guidelines do not automatically prevent prosecution, but they provide the public prosecutor with an established framework for distinguishing socially beneficial security research from criminal intrusion**.

The model offers flexibility because prosecutors can consider the researcher's overall conduct, but protection remains discretionary and does not constitute an enforceable immunity. It therefore provides less certainty than the Belgian statutory cause of justification, particularly

in transnational cases, but it demonstrates how stable prosecutorial practice and published national guidance can reduce the risk of treating responsible security research in the same manner as malicious intrusion.

**Lithuania and a restrictive statutory research corridor**

Lithuania has adopted a legislative framework for vulnerability research and disclosure rather than relying primarily on prosecutorial discretion. Amendments concerning CVD entered into force in June 2021, following consultations involving the Ministry of Justice, the Prosecutor General's Office and the Police Department. The reform addressed both the right to search for vulnerabilities and the conditions governing that activity (ENISA 2022, 25-26).

Article 25 of the Lithuanian Law on Cyber Security provides that vulnerability research and disclosure may be lawful and may not give rise to liability where statutory conditions are met. **The protection covers the research activity itself**. Researchers must avoid disrupting system operation, affecting service availability or altering data, cease unnecessary testing once the vulnerability is confirmed, report through the prescribed procedure and limit access to what is necessary to identify and demonstrate the vulnerability (Lithuanian Parliament 2014, art. 25, as amended in 2024).

Because the legislation regulates vulnerability research as an activity, it may protect limited or unsuccessful tests conducted before access is successfully obtained. Protection does not, however, extend automatically to every attempted access. Conduct exceeding what is necessary, affecting data or system availability, or falling outside the reporting procedure remains subject to the ordinary offences contained in Articles 196-198 of the Lithuanian Criminal Code. Lithuania therefore offers a conditional statutory safe harbour providing stronger legal protection than a policy based solely on prosecutorial tolerance. Its weakness lies in the narrowness of the protected corridor. Strict requirements concerning necessity, cessation and rapid reporting may leave uncertainty where confirming the impact of a vulnerability requires further technical examination.

For Romania, the principal lesson is that protection should cover the research preceding the report, but its conditions must remain sufficiently flexible to accommodate the technical realities of vulnerability verification.

**Comparative lessons for Romania**

Comparative experience warns against making protection so procedurally rigid that it becomes unusable. Belgium and Lithuania demonstrate that statutory protection can extend to the research preceding a report, while the Netherlands shows the continuing value of published operational and prosecutorial guidance. Romania no longer faces an abstract choice among these models: Parliament has selected a conditional statutory approach by linking protection directly to compliance with Article 36 (NIS Cooperation Group 2023; Pupillo et al. 2018; Romanian Parliament 2026).

**The proposed Article 365[1] nevertheless creates a narrower corridor than a comprehensive safe harbour**. It would cover only Articles 360(1) and (3), 361 and 364, without expressly addressing civil liability, attempt under Article 366 or conduct falling under Articles 360(2), 362, 363 and 365. Its practical value would also depend on the interpretation of the 48-hour deadline and the technical restrictions contained in Article 36.

**Romania should therefore retain a hybrid approach. Statutory protection should be supported by DNSC and prosecutorial guidance**, while subsequent review should determine whether the excluded offences, attempted research and civil liability require further clarification or protection.

## A STRATEGIC AND DIPLOMATIC ROADMAP FOR ROMANIA

The proposed roadmap combines immediate guidance, the implementation and clarification of conditional statutory protection and longer-term institutional and diplomatic measures.

### Clarifying and operationalising the existing framework

#### *Clarifying Article 36*

The immediate priority should be the adoption of detailed DNSC guidance under Article 36(2)(i), distinguishing passive research, ordinary public interaction, scanning, active enumeration, limited validation, access to restricted resources, data extraction, persistence and system interference. It should clarify when the 48-hour reporting period begins, confirm that

an initial report may be supplemented, and define the minimum evidence needed to demonstrate a vulnerability without unnecessary access to data.

The guidance should also set expectations for organisations, including accessible reporting channels, prompt acknowledgement, continued communication with the researcher, prioritisation, remediation and coordinated publication. Legal protection alone will not encourage reporting where organisations remain silent or lack the capacity to act on a report (National Cyber Security Centre of the Netherlands 2013; Householder et al. 2017; Schaffer et al. 2023; NIS Cooperation Group 2023).

The treatment of technical barriers requires particular attention. The guidance should state when a vulnerability affecting authentication or authorisation may be demonstrated through a minimal test and which methods remain prohibited. The objective should be to enable proof of the weakness without authorising escalation beyond what is necessary. Clear disclosure timelines should also be developed. A presumptive remediation period, adjustable according to severity and complexity, would create predictability. A researcher should be able to request a review where the affected entity does not cooperate or DNSC does not authorise disclosure within a reasonable time.

***Clarifying the criminal law response***

If Article 365¹ enters into force, DNSC, the Public Ministry, DIICOT, and the Romanian Police should develop joint guidance concerning its application to vulnerability-research cases. The guidance should address the scope of the protection, purpose, proportionality, data minimisation, effects, rapid reporting, cooperation after discovery and the distinction between preparatory research and attempted access.

Such guidance would neither displace judicial authority nor extend the statutory protection beyond its legal scope. It could nevertheless reduce inconsistent treatment, clarify conduct falling outside Article 365¹ and give practical effect to Recital 60 of NIS2 concerning the non-prosecution of cybersecurity researchers.

***Adopting a national model vulnerability disclosure policy***

DNSC should publish a model policy for public institutions and private organisations. The policy should define:

- the systems and services included
- authorised and prohibited techniques
- the treatment of data encountered accidentally
- secure reporting channels and response timelines
- remediation and coordinated disclosure procedures
- a commitment concerning legal action provided that the researcher complies with the policy.

The policy should be easy to locate before testing and should explain, in plain language, the legal consequences of compliance. It should be accompanied by an RFC 9116-compliant security.txt file, allowing researchers to identify the correct contact and reporting rules directly from an organisation's domain (Schaffer et al. 2023; Foudil and Shafranovich 2022).

Official practice shows that such policies can be implemented by public authorities without creating a general permission to test every system. CISA, JPCERT/CC, the Israel National Cyber Directorate, and the Bundeswehr publish dedicated disclosure routes that identify the systems covered, the expected conduct, and the channel through which findings should be submitted (CISA n.d.; JPCERT/CC 2019; Israel National Cyber Directorate 2021; Bundeswehr 2023).

The model should establish acknowledgement targets, status updates, escalation routes and criteria for closing reports, consistent with the CERT/CC coordination model, NIST guidance and the NIS Cooperation Group's recommendations (Householder et al. 2017; Schaffer et al. 2023; NIS Cooperation Group 2023). Public-sector implementation should begin with civilian authorities and services covered by Emergency Ordinance No. 155/2024, followed by specialised arrangements for institutions excluded under Article 2. Sensitive organisations do not necessarily need to authorise broad public testing, but should provide secure channels for accidental discoveries and clearly define the forms of research they are prepared to receive.

DNSC should publish anonymised annual data on reports received, affected sectors, acknowledgement and remediation times, cross-border cases and reasons for closing reports. These indicators would permit evaluation without disclosing exploitable technical information.

**Implementing and completing conditional statutory protection**

**If promulgated and brought into force, the law would provide an express criminal-law consequence through the introduction of Article 365¹.** The immediate priority is

therefore to ensure that its requirements are interpreted objectively and consistently. Protection should remain linked to a security-improvement purpose, reasonable necessity and proportionality, data minimisation, the absence of persistence or intentional disruption, cessation once sufficient confirmation is obtained, prompt reporting and the absence of coercive demands or misuse of the information.

A subsequent review should assess whether the protection should extend to Article 360(2), Articles 362, 363 and 365 and attempts under Article 366. The relationship between compliant vulnerability research and civil liability should also be clarified. Any extension should preserve safeguards against harmful, unnecessary or disproportionate conduct while ensuring that protection covers both the report and the minimum preceding research required to produce it (Romanian Parliament 2026).

## Strengthening implementation capacity and international leadership

### *Building a national research ecosystem*

A national CVD framework requires more than legal rules. Providers, particularly small and medium-sized enterprises, may lack the expertise to assess reports, communicate with researchers and deploy patches. ENISA has warned that introducing CVD without sufficient organisational and technical capacity may create an inflow of reports that organisations cannot process effectively (ENISA 2022, 68-73). Bug bounty programmes may complement, but should not replace, a general disclosure route.

DNSC could provide technical triage, model documentation and mediation for organisations without specialised teams. Universities, research institutes, and cybersecurity companies should contribute to training, ethical review procedures and common research standards. Public bug bounty pilots could be introduced for carefully selected, non-sensitive public services. Their purpose would not only be to identify vulnerabilities, but also to test contractual language, response processes and cooperation between institutions and researchers.

### *Using Romania's institutional position for cyber diplomacy*

Domestic reform could support a broader international position. The National Cybersecurity Strategy defines cyber diplomacy as action promoting an open, stable and secure

cyberspace in which human rights, fundamental freedoms and the rule of law apply (Romanian Government 2021, secs. 4.1-4.5 and 5).

C-PROC connects Romania to the global implementation of the Budapest Convention and to capacity building in cybercrime and electronic evidence; the ECCC connects Bucharest to European cybersecurity research and industrial policy; and DNSC participates in the EU CSIRTs Network and may coordinate the disclosure of vulnerabilities with cross-border impact. Together, these institutions could support a regional directory of trusted contacts, common training for CSIRTs and criminal-justice authorities, and assistance in drafting national CVD policies (United Nations 2015; United Nations 2021; Dominioni 2023).

**At EU level**, Romania could advocate greater convergence concerning conditional researcher protection, including common criteria for necessity, proportionality, data minimisation and responsible reporting. It could support a future reassessment of Directive 2013/40/EU, whose minimum harmonisation has produced divergent national thresholds.

**Within the Council of Europe**, Romania could promote structured dialogue among criminal-justice authorities, CSIRTs, researchers and technology providers. The purpose would not be to weaken the Budapest Convention's offences, but to clarify how the concepts of access without right, intent and attempt apply to legitimate security research.

**Regionally**, Romania could provide expertise to the Republic of Moldova, Ukraine and Western Balkan states on national CVD mechanisms, prosecutorial guidance, institutional coordination and public-sector policies. This would connect cybersecurity capacity building with Romania's broader foreign-policy priorities.

The diplomatic objective should be practical rather than declaratory. Researchers should not face radically different exposure merely because a cloud service, supplier or user is located across a border. Shared minimum criteria would reduce fragmentation and support the EU digital single market. The CEPS Task Force already identified divergent rules on illegal access as a source of substantial uncertainty for cross-border research and recommended closer coordination and consideration of EU harmonisation (Pupillo et al. 2018, 40-53).

## CONCLUSION

Romania is well placed to connect domestic reform with European and international cooperation. Cybercrime prevention and researcher protection are not competing objectives,

but complementary elements of resilience. Romania has created the institutional door through which vulnerabilities may be reported, and Parliament has now taken a significant step towards providing responsible researchers with a lawful path to reach it.

The remaining task is to ensure that, if Article 365[1] enters into force, its conditions are workable and its limited scope does not leave important forms of legitimate research unprotected. Without effective implementation, warnings may still arrive late, through informal or insecure channels, or not at all, while residual legal uncertainty deters responsible researchers without discouraging malicious actors.

## BIBLIOGRAPHY

Bundeswehr. 2023. Vulnerability Disclosure Policy. 5 June 2023. https://www.bundeswehr.de/de/security-policy

Centre for Cybersecurity Belgium (CCB). 2020a. *Guide to Coordinated Vulnerability Disclosure Policies. Part I: Good Practices*.

Centre for Cybersecurity Belgium (CCB). 2020b. *Guide to Coordinated Vulnerability Disclosure Policies. Part II: Legal Aspects*.

Centre for Cybersecurity Belgium (CCB). 2025. *Coordinated Vulnerability Disclosure*. https://ccb.belgium.be/regulation/cvdp

Council of Europe. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms*. European Treaty Series No. 5.

Council of Europe. 2001a. *Convention on Cybercrime*. European Treaty Series No. 185. Budapest, 23 November 2001.

Council of Europe. 2001b. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series No. 185.

Council of the European Union. 2017. *Council Conclusions on the Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. 20 November 2017.

Cybersecurity and Infrastructure Security Agency (CISA). n.d. Coordinated Vulnerability Disclosure Program.

Dominioni, S. 2023. *Operationalizing a directory of points of contact for cyber confidence-building measures.* United Nations Institute for Disarmament Research. https://unidir.org/files/2023-05/UNIDIR_Operationalizing_Directory_Points_of_Contact_Cyber_Confidence_Building_V4.pdf

European Commission. 2017. *Report Assessing the Extent to Which the Member States Have Taken the Necessary Measures in Order to Comply with Directive 2013/40/EU on Attacks against Information Systems*. COM(2017) 474 final.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2017. *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. JOIN(2017) 450 final.

European Parliament and Council. 2013. Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union, L 218*, 8–14.

European Parliament and Council. 2019. Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification. *Official Journal of the European Union, L 151*, 15–69.

European Parliament and Council. 2021. Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. *Official Journal of the European Union, L 202*, 1–31.

European Parliament and Council. 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union, L 333*, 80–152.

European Parliament and Council. 2024. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. *Official Journal of the European Union.*

European Union. 2012. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union, C 326*, 391–407.

European Union Agency for Cybersecurity (ENISA). 2016. *Good practice guide on vulnerability disclosure: From challenges to recommendations.* https://www.enisa.europa.eu/publications/vulnerability-disclosure

European Union Agency for Cybersecurity (ENISA). 2022. *Coordinated vulnerability disclosure policies in the EU.* https://doi.org/10.2824/983447

European Union Agency for Cybersecurity (ENISA). 2025. Consult the European Vulnerability Database to enhance your digital security. 13 May 2025. https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security

Foudil, E., & Shafranovich, Y. 2022. *RFC 9116: A file format to aid in security vulnerability disclosure.* Internet Engineering Task Force. https://doi.org/10.17487/RFC9116

Global Forum on Cyber Expertise. 2016. *Coordinated vulnerability disclosure.* https://thegfce.org/wp-content/uploads/CoordinatedVulnerabilityDisclosure-1-1.pdf

Householder, A. D., Wassermann, G., Manion, A., & King, C. 2017. *The CERT guide to coordinated vulnerability disclosure.* Special Report CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. https://www.sei.cmu.edu/documents/1945/2017_003_001_503340.pdf

International Organization for Standardization. 2018. *ISO/IEC 29147:2018 Information Technology, Security Techniques, Vulnerability Disclosure*. Geneva: ISO.

International Organization for Standardization. 2019. *ISO/IEC 30111:2019 Information Technology, Security Techniques, Vulnerability Handling Processes*. Geneva: ISO.

Israel National Cyber Directorate. 2021. Vulnerabilities Disclosure Program – CVE. Gov.il, 8 April 2021. https://www.gov.il/en/pages/cve_cyber_israel

JPCERT/CC. 2019. *Vulnerability coordination and disclosure policy.* 8 July 2019. https://www.jpcert.or.jp/english/vh/vul-coordination-disclosure-policy_2019.pdf

Lithuanian Parliament. 2014. *Law of the Republic of Lithuania on Cyber Security No. XII-1428 of 11 December 2014, as amended in 2024*.

National Cyber Security Centre of the Netherlands. 2013. *Guideline for Responsible Disclosure of IT Vulnerabilities*. Ministry of Security and Justice.

National Cyber Security Directorate. Coordinated Vulnerability Disclosure – CVD. https://www.dnsc.ro/pages/CVD

NIS Cooperation Group. 2023. *Guidelines on implementing national coordinated vulnerability disclosure policies.*

Openbaar Ministerie. 2013. *Beleidsbrief Responsible Disclosure*. College van procureurs-generaal, 18 March 2013.

Pupillo, L., Ferreira, A., & Varisco, G. 2018. *Software vulnerability disclosure in Europe: Technology, policies and legal challenges.* CEPS Task Force Report. Centre for European Policy Studies.

Romanian Government. 2021. *Romania's Cybersecurity Strategy for the Period 2022–2027*. Approved by Government Decision No. 1321 of 30 December 2021. Official Gazette of Romania No. 2 bis of 3 January 2022.

Romanian Government. 2024. *Emergency Ordinance No. 155/2024 on Establishing a Framework for the Cybersecurity of Networks and Information Systems in the National Civil Cyberspace*. Official Gazette of Romania No. 1332 of 31 December 2024.

Romanian Legislative Council. 2026. *Opinion No. 152 of 23 February 2026 on the Legislative Proposal Amending and Supplementing Emergency Ordinance No. 155/2024 and Supplementing Law No. 286/2009 on the Criminal Code* (b53/11.02.2026; L133/2026).

Romanian Parliament. 2003. *Law No. 161/2003 on Certain Measures for Ensuring Transparency in the Exercise of Public Dignities, Public Functions and the Business Environment and for Preventing and Sanctioning Corruption*. Official Gazette of Romania No. 279 of 21 April 2003.

Romanian Parliament. 2004. *Law No. 64/2004 for the Ratification of the Council of Europe Convention on Cybercrime*. Official Gazette of Romania No. 343 of 20 April 2004.

Romanian Parliament. 2009. *Law No. 286/2009 on the Criminal Code*. Official Gazette of Romania No. 510 of 24 July 2009.

Romanian Parliament. 2022. *Law No. 361/2022 on the Protection of Whistleblowers in the Public Interest*. Official Gazette of Romania No. 1218 of 19 December 2022.

Romanian Parliament. 2025. *Law No. 124/2025 Approving Emergency Ordinance No. 155/2024*. Official Gazette of Romania No. 638 of 7 July 2025.

Romanian Parliament. 2026. *Law Supplementing Article 36 of Emergency Ordinance No. 155/2024 and Law No. 286/2009 on the Criminal Code*. Legislative file L133/2026, registered at the Chamber of Deputies as PL-x 350/2026. Form sent to the President of Romania for promulgation on 22 June 2026.

Romanian Senate. 2026. *Joint Report No. XIX/75 and No. LXIX/109 of 20 April 2026 on Legislative Proposal L133/2026, including the admitted amendments*.

Schaffer, K., Mell, P., Trinh, H., & Van Wyk, I. 2023. *Recommendations for federal vulnerability disclosure guidelines.* NIST Special Publication 800-216. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-216

Smith, B. 2017. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Microsoft On the Issues, 14 May 2017. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Superior Council of Magistracy. 2026. *Letter No. 3/2807 of 24 March 2026 concerning Legislative Proposal b53/11.02.2026 on the amendment of Emergency Ordinance No. 155/2024 and the Criminal Code*.

United Nations. 1966. International Covenant on Economic, Social and Cultural Rights. General Assembly Resolution 2200A (XXI), 16 December 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

United Nations. 2015. *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.* A/70/174, 22 July 2015.

United Nations. 2021. *Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security.* A/76/135, 14 July 2021.

United Nations. 2024. *United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes.* United Nations General Assembly Resolution 79/243 of 24 December 2024.

IDR
Institutul Diplomatic Român

**Our mission**. The Romanian Diplomatic Institute (RDI) has the mission to make a substantial contribution to increasing the quality of Romanian diplomacy through training, further education, research, the development of critical and strategic thinking and international networking. A good foreign policy serves as a beneficial domestic policy.

**Guiding principles**: human resource development, professionalism, respect and dialogue, and responsibility for the community.

Based on the founding legal attributions of the RDI, the further development of the Institute is carried out, according to the needs identified in the MFA, along the following four directions:

- Training and further education of diplomats and other trainees;
- Deepening the research and expertise dimension on regional and functional issues;
- Operating the RDI as a think-tank of the MFA;
- Integration of the RDI into an international network of similar relevant institutes.

**Author**: Teodora Curelariu is a PhD candidate in international law and cybersecurity at Université Grenoble Alpes in France, in collaboration with Inria, the French national research institute for digital science and technology.

**Policy Forum** features contributions authored by experts outside RDI.

IDR Policy Forum
ISSN 3119-8562
ISSN-L 3119-8562

Editor, layout, and graphics: Claudiu Codreanu

Cover photo: https://unsplash.com/photos/a-laptop-computer-sitting-on-top-of-a-desk-nBXwqxjDa5c

The Romanian Diplomatic Institute
https://www.idr.ro/en/ | secretariat@idr.ro
Primăverii 17, sector 1, Bucharest, 011972