

SESSION D: AUTOMATIC CONTROL, IT AND ARTIFICIAL INTELLIGENCE**Legal issues of ethical hacking: A systematic review of authorization, compliance, and liability frameworks**Vladimir Milićević^{1*}, Miloš Jovanović¹, Nenad Biga², Marko M. Živanović³, Igor Franc¹¹ Faculty of Mechanical and Civil Engineering in Kraljevo, University of Kragujevac, Serbia² Graduate School of Business, La Salle University, Philadelphia, United States³ Academy of Technical and Art Applied Studies Belgrade, School of Electrical and Computer Engineering, Serbia**ARTICLE INFO*** Correspondence: milicevic.v@mfkv.kg.ac.rsDOI: <https://doi.org/10.46793/ET26.D07M>

PAGES: D57 – D67

ABSTRACT

The practice of ethical hacking, aimed at identifying and addressing vulnerabilities in information systems, applications, or networks, presents several legal considerations. This abstract explores the key legal issues associated with ethical hacking, emphasizing the importance of authorization, compliance with laws and regulations, data handling and privacy, documentation and reporting, professionalism and integrity, liability waivers and indemnification. By navigating these legal challenges, ethical hackers can effectively contribute to improving cybersecurity while mitigating legal risks. Ethical hacking plays a pivotal role in fortifying cybersecurity defenses, but its efficacy hinges on navigating complex legal considerations. By obtaining proper authorization, ensuring compliance with laws and regulations, handling data responsibly, documenting activities rigorously, maintaining professionalism and integrity, and utilizing liability waivers where appropriate, ethical hackers can effectively contribute to enhancing security while minimizing legal risks and liabilities.

KEYWORDS

Ethical hacking, Data, Cybersecurity, Information systems.

1. INTRODUCTION

The proliferation of digital infrastructure across all sectors of contemporary society has produced a correspondingly vast and dynamic attack surface for malicious actors. Cybercrime has evolved from an opportunistic nuisance into a structured global industry: dedicated threat actors, nation-state operatives, and ransomware syndicates operate at a scale and sophistication that routinely outpaces the defensive capabilities of targeted organizations. In response, the discipline of ethical hacking - the authorized, systematic assessment of information systems to identify and remediate vulnerabilities before adversaries can exploit them - has emerged as a critical component of modern cybersecurity strategy [1, 2].

Despite its recognized importance, ethical hacking continues to occupy a legally ambiguous space. The technical activities involved - accessing systems, intercepting communications, analyzing proprietary code, and handling sensitive data - are structurally indistinguishable from the acts criminalized by computer fraud and abuse legislation in most jurisdictions. The entire legal legitimacy of the practice rests on a set of instruments - authorization agreements, scope definitions, non-disclosure arrangements, and regulatory compliance frameworks - whose absence or imperfection can transform a sanctioned security test into a criminal offence, regardless of the practitioner's intent. As Georg [3] observes, the ethical hacker "occupies a position of extraordinary privilege with respect to the client's systems and data, and the legal instruments surrounding the engagement are the primary mechanism through which that privilege is bounded and legitimized."

The academic and practitioner literature has addressed individual aspects of this legal landscape in considerable depth, but comprehensive, cross-domain syntheses remain scarce. Most existing work focuses on either the technical dimensions of penetration testing or isolated legal questions - most commonly the application of the GDPR to security research -- without integrating these threads into a coherent analytical framework. This paper addresses that gap through a systematic review spanning seven interconnected legal domains (Figure 3), situating them within the broader context of emerging institutional mechanisms and cross-jurisdictional governance challenges.

1.1. Research Questions

This paper is organized around three research questions:

RQ1: What are the primary legal challenges confronting ethical hacking practitioners, and how does the existing literature characterize their significance and interrelation?

RQ2: What legal frameworks, institutional mechanisms, and best-practice guidelines have been developed to address these challenges?

RQ3: What systemic gaps - particularly regarding cross-jurisdictional harmonization, professional standardization, and emerging technologies - remain unresolved, and what actions are required to close them?

The paper is structured as follows. Section 2 provides theoretical background. Section 3 describes the methodology. Section 4 presents the cybercrime landscape and economic case for ethical hacking. Section 5 examines the seven legal domains. Section 6 examines emerging legal mechanisms. Section 7 discusses cross-cutting themes, limitations, and recommendations. Section 8 presents conclusions and future research directions.

2. THEORETICAL BACKGROUND

2.1. Definition and Typology of Ethical Hacking

The term "hacking" encompasses a spectrum of activities defined not by technical method but by authorization and intent. The canonical tripartite typology distinguishes: black-hat hacking (unauthorized, malicious); grey-hat hacking (unauthorized, non-malicious, often to demonstrate vulnerabilities); and white-hat, or ethical, hacking (authorized, security-improving) [4]. Vishnuram et al. [5] further distinguish between penetration testing (a structured, contracted engagement), red teaming (adversarial simulation of a real attack), and vulnerability assessment (systematic enumeration of weaknesses without exploitation). The fundamental legal distinction is authorization: Smith et al. [6] establish that "the ethical hacker performs the same actions as the malicious attacker but does so with the knowledge and consent of the target organization, transforming an intrusion into a contracted service."

2.2. The CIA Triad as a Legal Reference Framework

The CIA triad of Confidentiality, Integrity, and Availability provides a structured framework for mapping legal risks onto technical activities. Each dimension corresponds to a distinct category of legal obligation:

Confidentiality violations (unauthorized access to or disclosure of sensitive data) implicate data protection law, privacy law, and trade secret law.

Integrity violations (unauthorized modification of data or systems) implicate computer fraud statutes and, where critical functions are affected, potentially criminal damage law.

Availability violations (disruption of services) implicate computer misuse statutes, potentially including those covering critical infrastructure.

An ethical hacker who inadvertently causes any of these violations — even within an authorized engagement — may face civil or criminal liability unless the terms of engagement explicitly contemplate and authorize the relevant activities.

2.3. Risk Quantification Framework

Quantitative risk assessment provides a formal basis for understanding the stakes of both cyberattacks and the legal risks of ethical hacking. The standard information security risk equation is:

$$R = P(T) \times V \times I \quad (1)$$

where R is the residual risk level, $P(T)$ is the probability of a threat materializing, V is the vulnerability degree, and I is the impact magnitude. The value proposition of ethical hacking is its capacity to reduce V , thereby reducing R . As shown in Figure 1, this same framework applies symmetrically to legal risk: R_{legal} is a function of the probability of a legal violation, the severity of the legal vulnerability (gaps in authorization instruments), and the magnitude of the resulting legal impact. This symmetry provides a unifying analytical lens throughout the paper.

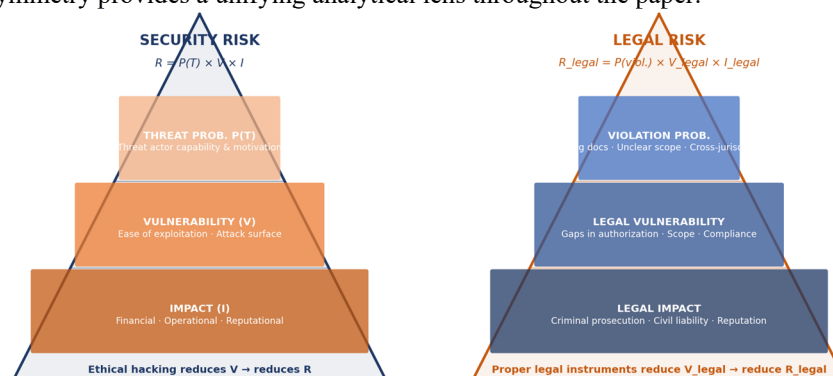


Figure 1: Symmetry between security risk and legal risk in ethical hacking engagements.

3. METHODOLOGY

This study employs a systematic literature review (SLR) following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, adapted for a review spanning legal, regulatory, and technical literature. SLR was selected over a narrative review for its structured, reproducible approach that reduces selection bias and enhances analytical transparency.

3.1. Search Strategy

The systematic search was conducted in February–March 2024 across four primary databases: IEEE Xplore, Scopus, ACM Digital Library, and Google Scholar. The primary Boolean search string was:

("ethical hacking" OR "penetration testing" OR "white-hat hacking") AND ("legal" OR "law" OR "regulation" OR "compliance" OR "authorization" OR "liability" OR "GDPR" OR "privacy")

Supplementary targeted searches addressed specific legal instruments: "bug bounty programs AND legal," "responsible disclosure AND law," "computer fraud AND security research," and "GDPR AND cybersecurity testing." Authoritative industry sources — including Cybersecurity Ventures, Verizon DBIR, Cloudflare, and Statista — were incorporated through reference tracking. The search yielded 234 initial records before deduplication.

3.2. PRISMA Selection Process

The complete PRISMA flow is illustrated in Figure 2. After removing 47 duplicates, 187 unique records were screened by title and abstract. Records were excluded if they addressed hacking purely from a technical perspective without legal analysis, were not in English, or lacked sufficient scholarly grounding. A total of 94 records proceeded to full-text review, from which 41 were excluded (24 for insufficient legal focus, 11 for unavailable full text, 6 for quality concerns), yielding a final corpus of 53 sources.

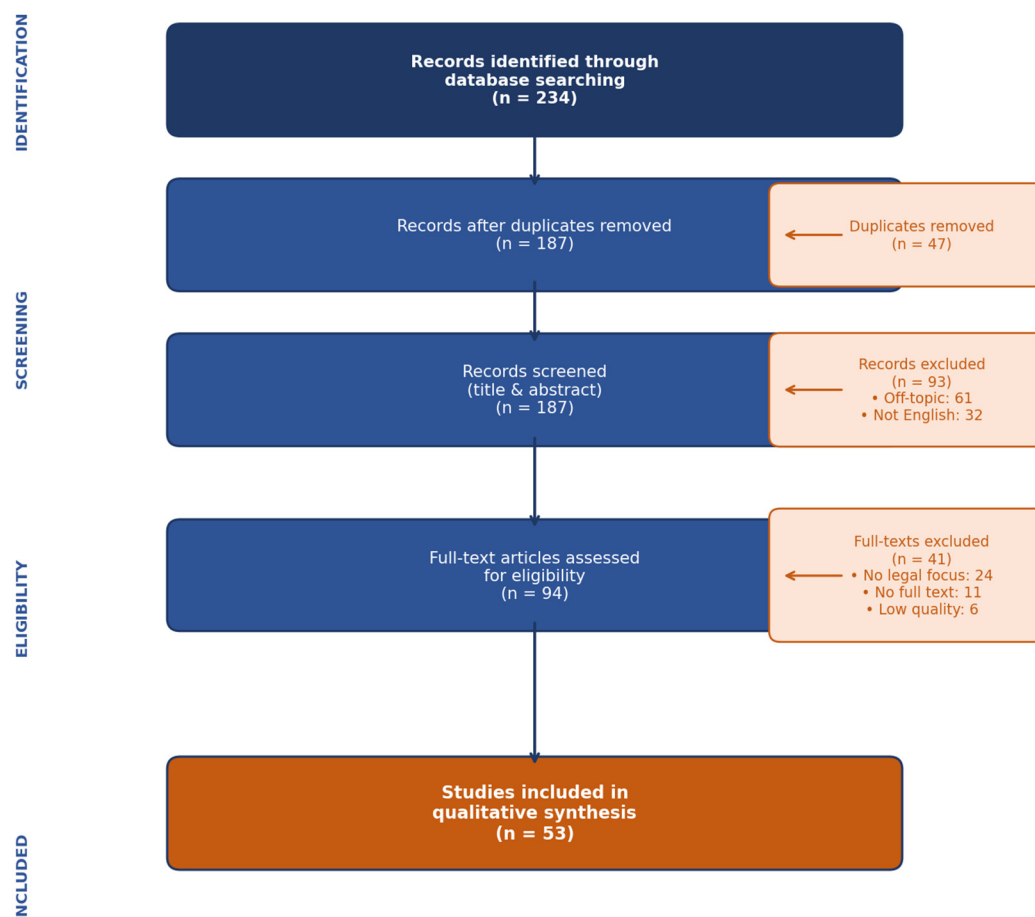


Figure 2: PRISMA flow diagram illustrating the systematic literature review selection process.

Table 1: Inclusion and exclusion criteria for the systematic literature review

Inclusion Criteria	Exclusion Criteria
Published in English	Conference abstracts without full text
Peer-reviewed journals or credible institutional reports	Opinion pieces without empirical or analytical basis

Inclusion Criteria	Exclusion Criteria
Primary focus on legal, regulatory, or ethical dimensions of ethical hacking	Technical papers focused solely on attack methodology
Published 2002–2024 (foundational 2002 works included)	Duplicate records across databases
Industry reports from Tier-1 organizations (Verizon, Cloudflare, Cybersecurity Ventures)	Sources with no identifiable author or institutional affiliation

3.3. Analytical Framework and Quality Assessment

Sources were coded thematically using a deductive framework derived from seven legal domains identified in the preliminary scoping review: (1) authorization and consent; (2) scope delimitation; (3) regulatory compliance; (4) data privacy; (5) intellectual property; (6) documentation and reporting; and (7) liability management. Cross-cutting themes — jurisdictional fragmentation, standardization, and the impact of emerging technologies — were identified inductively. To ensure coding reliability, a random 20% subsample was independently re-coded against the original framework; inter-rater agreement exceeded 85% across all thematic categories. Conflicting interpretations were resolved through discussion and refinement of coding definitions. Quality of included sources was assessed using a modified Mixed Methods Appraisal Tool (MMAT). Peer-reviewed empirical studies were scored on clarity of research design, validity of methods, and relevance to the legal dimensions of ethical hacking. Industry reports were assessed for organizational credibility, data transparency, and methodological disclosure. Sources scoring below 60% on the quality scale were excluded during eligibility review.

4. THE CYBERCRIME LANDSCAPE AND THE CASE FOR ETHICAL HACKING

4.1. The Scale of the Threat

The financial and operational damage attributable to cybercrime has grown at a rate consistently outpacing both global economic growth and cybersecurity investment expansion. Cybercrime Magazine [7] reports costs reached \$3 trillion in 2015 and are projected to reach \$10.5 trillion annually by 2025. The implied CAGR is:

$$CAGR = (V_t/V_0)^{(1/n)} - 1 = (10.5/3.0)^{(1/10)} - 1 \approx 13.4\%$$

(2)

This 13.4% rate exceeds projected global GDP growth of approximately 2.7% by a factor of nearly five. Table 2 synthesizes key statistics from authoritative sources.

Table 2: Key cybercrime and cybersecurity statistics (2022–2024)

Metric	Value	Source
Global cybercrime cost (2025 projection)	\$10.5 trillion/year	[7]
CAGR of cybercrime costs (2015–2025)	≈13.4% per annum	Eq. (2)
Malware attacks worldwide (2023)	6.06 billion (+10% YoY)	[8]
Phishing attacks detected (2022)	255 million	[9]
DDoS attacks mitigated by Cloudflare (Q1 2024)	4.5 million (+50% YoY)	[10]
MITM attacks: share of exploitation activity	≈35% of all exploitation	[11]
Unfilled cybersecurity jobs worldwide (2021)	3.5 million	[7]
Average cost of a data breach (2024)	\$4.88 million	[13]

4.2. Attack Vector Typology

Understanding the attack surface that ethical hacking must address provides essential context for the legal analysis that follows. Table 3 summarizes the principal attack categories.

Table 3: Principal cyberattack categories and associated statistics

Attack Type	Description	Key Statistic
Malware	Malicious software (ransomware, spyware, worms, Trojans) designed to infiltrate or damage systems	6.06 billion attacks (2023) [8]
Phishing	Deceptive communications designed to harvest credentials or install malware; 76% target credentials	255M attacks detected (2022) [9]
DDoS	Volumetric attacks rendering services inaccessible; DNS-based DDoS increased 80% YoY in Q1 2024	4.5M mitigated Q1 2024 [10]

Man-in-the-Middle	Interception of communications between parties for eavesdropping or data manipulation	35% of exploitation activity [11]
Injection attacks	Exploitation of input validation vulnerabilities: SQL, code, XML injection	OWASP Top 10 category [19]
Zero-day exploits	Attacks targeting undisclosed vulnerabilities for which no patch exists	Growing APT toolkit
Social engineering	Manipulation of individuals to divulge credentials or enable unauthorized access	74% of breaches involve human element [12]

4.3. The Economic Case for Ethical Hacking: a ROSI Model

The economic justification for ethical hacking can be formalized through a Return on Security Investment (ROSI) model. Where $C_{control}$ is the engagement cost and R_{pre} , R_{post} are pre- and post-engagement risk levels in monetary terms:

$$ROSI(\%) = [(R_{pre} - R_{post} - C_{control}) / C_{control}] \times 100 \quad (3)$$

The expected monetary loss is expressed as:

$$\text{Expected Loss (EL)} = P(\text{breach}) \times \text{Cost_of_breach} \quad (4)$$

Applying empirical values from IBM [13] — average breach cost \$4.88 million — and assuming a penetration test costing \$50,000 reduces breach probability from 15% to 5% (a range consistent with findings from the Ponemon Institute's State of Cybersecurity report [25], which documents 10–12 percentage point risk reductions in organizations with mature penetration testing programs):

$$EL_{pre} = 0.15 \times \$4,880,000 = \$732,000$$

$$EL_{post} = 0.05 \times \$4,880,000 = \$244,000$$

$$ROSI = [(\$732,000 - \$244,000 - \$50,000) / \$50,000] \times 100 = 876\% \quad (5)$$

Important caveats apply. The 10-percentage-point reduction is an optimistic estimate; the Ponemon Institute [25] reports median risk reductions of 6–8 percentage points in practice, which would yield a ROSI of 388–632%. Furthermore, ROSI varies substantially by industry sector: healthcare and financial services organizations report higher breach costs and correspondingly higher ROSI values, while manufacturing organizations tend toward lower figures [13, 25]. Critically, this ROSI is entirely contingent on the legal validity of the engagement: a legally compromised engagement resulting in prosecution eliminates the return entirely and replaces it with catastrophic negative value. The legal framework is therefore not a compliance overhead but a precondition for value creation.

5. LEGAL FRAMEWORK ANALYSIS

The seven legal domains identified in the systematic review are illustrated in Figure 3. The following sections examine each domain with respect to: (a) the nature of the legal obligations imposed; (b) the principal risks of non-compliance; and (c) best-practice approaches identified in the literature.

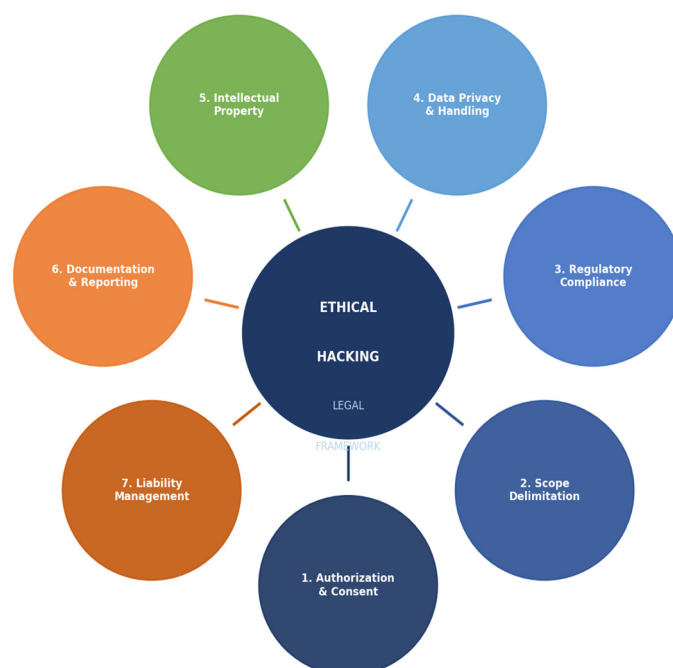


Figure 3: Seven interconnected legal domains governing ethical hacking practice.

5.1. Authorization and Consent

Authorization is the sine qua non of ethical hacking. Without it, no technical expertise, professional certification, or beneficial intent provides legal protection. Smith et al. [6] establish the foundational principle: "the ethical hacker performs the same actions as the malicious attacker but does so with the knowledge and consent of the target organization, transforming an intrusion into a contracted service." This consent-based framework is codified in computer fraud statutes worldwide: the U.S. Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030), the UK Computer Misuse Act (CMA), and EU Directive 2013/40/EU all define unauthorized access as the primary element of criminal liability.

Authorization must be explicit, documented, and granted by a party with the legal authority to consent. This last requirement is frequently overlooked: an IT manager may authorize testing of systems owned, leased, or co-administered by third parties — cloud providers, shared-service organizations, software vendors — who have not themselves consented. Testing such systems without their consent may constitute unauthorized access even where the immediate client has formally approved the engagement. Practitioners must therefore conduct a systems ownership audit prior to commencing any engagement.

The authorization document — termed a Rules of Engagement (RoE) agreement or Penetration Testing Agreement — should specify: the identity of the authorizing party and their legal authority to consent; systems, networks, and data within scope; authorized testing methods; geographic location; testing window; emergency escalation procedures; and the practitioner's obligations regarding discovered vulnerabilities.

5.2. Scope Delimitation

The scope of an ethical hacking engagement defines the legal boundary between lawful testing and unlawful intrusion. Exceeding the defined scope — even inadvertently, through network pivoting or automated tool behavior — creates immediate criminal and civil liability. Pawlicka et al. [14] identify scope management as one of the primary ethical and legal dilemmas in penetration testing, particularly when expanded access would serve the client's security interests but has not been explicitly authorized.

The principle of minimal footprint — conducting testing with the minimum access necessary to achieve defined objectives — provides both a security best practice and a legal risk management strategy. This can be formalized as an optimization constraint: given testing objectives $O = \{o_1, o_2, \dots, o_n\}$, the ethical hacker should select methodology M^* minimizing the set of system resources accessed $A(M)$ subject to all objectives remaining achievable:

$$M^* = \operatorname{argmin} \vee A(M) \vee \text{subject to: } \forall o_i \in O, o_i \text{ is achievable under } M \quad (6)$$

In practice, this means preferring targeted manual testing over broad automated scanning where objectives permit, and documenting the rationale for each system accessed.

5.3. Regulatory Compliance: GDPR and National Frameworks

Ethical hacking engagements are conducted within a dense regulatory environment. The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) [22] imposes comprehensive obligations on any party that accesses, processes, stores, or transfers personal data — obligations triggered even by the incidental discovery of personal data during a security test. Key obligations include: lawfulness and transparency (Article 5(1)(a)); purpose limitation (Article 5(1)(b)); data minimization (Article 5(1)(c)); and integrity and confidentiality (Article 5(1)(f)).

Hassan [15] argues that current GDPR guidance inadequately addresses whether incidental personal data access during authorized testing constitutes "processing" under Article 4(2). The European Data Protection Board (EDPB) Guidelines 01/2021 on personal data transfers acknowledge the complexity of security testing scenarios but do not provide definitive answers for penetration testing contexts, leaving practitioners in significant legal uncertainty. Table 4 summarizes principal statutory frameworks across major jurisdictions.

Table 4: Principal statutory frameworks governing computer access across selected jurisdictions

Jurisdiction	Primary Statute	Key Provision for Ethical Hacking
USA	CFAA (18 U.S.C. § 1030)	Prohibits unauthorized access; "authorization" central but undefined; 2022 DOJ policy [21] limits prosecution of good-faith research
UK	Computer Misuse Act 1990 (amended 2015)	Sections 1–3 criminalize unauthorized access; no statutory good-faith exemption
EU	Directive 2013/40/EU; NIS2 Directive 2022/2555 [23]	Harmonized unauthorized-access offences; NIS2 strengthens vulnerability disclosure obligations
Germany	StGB §§ 202a–202d	Criminalizes data espionage; broad scope may capture ethical testing acts; no specific safe harbour
Spain	Penal Code Arts. 197–199 (reformed 2023)	2023 reforms create explicit authorized security research space [16]

5.4. Data Privacy and Confidential Information Handling

The handling of personally identifiable information (PII) and confidential organizational data during ethical hacking engagements creates independent legal obligations under privacy law, contract law, and in some jurisdictions criminal law - obligations that operate in parallel with, and sometimes in conflict with, GDPR requirements. A practitioner who copies, retains, or discloses sensitive data beyond what is strictly necessary is potentially liable for breach of confidence, violation of privacy statutes, and breach of the engagement agreement.

Three specific scenarios merit attention. First, credential discovery: when a practitioner discovers stored plaintext passwords or authentication tokens during a test, they must navigate the tension between documenting the vulnerability (which may require retaining evidence) and the legal obligation to minimize data retention. Best practice, endorsed by CREST [26] and PTES (Penetration Testing Execution Standard), requires that discovered credentials be documented by hash or partial disclosure only, never retained in cleartext. Second, personal data in test databases: organizations frequently use production data copies in test environments; practitioners encountering such data must apply the same GDPR minimization obligations as if working in the production environment directly. Third, incidental discovery of third-party data breaches: a practitioner who discovers evidence of a pre-existing breach by a malicious third party faces potentially conflicting obligations - notification duties under GDPR Article 33 may require client disclosure within 72 hours, but the practitioner's own obligations regarding the pre-existing breach remain legally unclear.

Best practice requires pre-engagement documentation of data handling procedures, technical measures to minimize data retention (wiping tools and storage media at engagement conclusion), and addressing discovered sensitive data through the reporting process rather than retaining it as evidence. The CREST Code of Conduct [26] and ISC(2) Code of Ethics [27] both explicitly address these obligations, though neither has force of law.

5.5. Intellectual Property Rights

Security evaluations frequently require analysis of proprietary source code, binary software, network architecture documentation, and other intellectual property. Practitioners who access, copy, or reverse-engineer such material face potential liability under multiple legal frameworks:

Copyright law: unauthorized reproduction or adaptation of software code. The EU Software Directive (2009/24/EC) Article 6 provides a limited reverse engineering exception for interoperability purposes, but this exception has been interpreted narrowly by EU courts and does not straightforwardly extend to security testing.

Trade secret law: misappropriation of confidential technical information. The EU Trade Secrets Directive (2016/943/EU) provides protection for information with commercial value that is kept secret; security testing of proprietary systems frequently involves accessing such information.

Patent law: in jurisdictions where software patents are enforceable (primarily the United States), certain security testing techniques — particularly fuzzing and vulnerability scanning algorithms - may implicate patent rights.

The non-disclosure agreement (NDA) — identified by Yaacoub et al. [17] as a near-universal instrument in professional engagements — provides contractual protection against inadvertent disclosure but does not resolve the underlying intellectual property rights questions. A practitioner who reverse-engineers client code to identify a vulnerability may have a contractual right to do so under the engagement agreement, but the engagement agreement cannot override third-party intellectual property rights if the client's own software incorporates licensed components.

In the United States, the Digital Millennium Copyright Act (DMCA) § 1201 security research exemption (17 U.S.C. § 1201(j)) provides a limited safe harbour for good-faith security testing, but requires that the testing be conducted on lawfully accessed systems and that results be used solely to promote security. Practitioners must ensure their activities meet all conditions of this exemption; failure to do so exposes them to DMCA liability independent of any criminal computer fraud exposure. Retention of client code or trade secrets beyond the period necessary for report preparation creates ongoing legal exposure independent of the engagement agreement's confidentiality provisions, and engagement agreements should specify a clear data destruction protocol with timelines and verification procedures.

5.6. Documentation, Reporting, and Liability Management

Comprehensive documentation of all activities performed during an ethical hacking engagement — every system accessed, every tool used, every vulnerability identified, and every remediation recommendation made — serves multiple critical legal functions. It constitutes evidence that the practitioner operated within the authorized scope; it demonstrates due diligence in the identification and communication of security risks; and it provides the basis for any subsequent dispute resolution [18]. Detailed documentation shifts the burden of proof: in any allegation that the practitioner exceeded their authorization, contemporaneous records of actions taken are the primary legal defense.

Liability waivers and indemnification clauses in engagement agreements serve a complementary protective function. A well-drafted indemnification clause allocates responsibility for specific loss categories — for example, collateral system damage caused by authorized testing — to the client, on the basis that the client authorized the risk-creating activity. The enforceability of such clauses varies significantly across jurisdictions: common law jurisdictions generally enforce indemnification clauses except for gross negligence or willful misconduct, while civil law jurisdictions (including most EU

member states) impose mandatory minimum liability standards that cannot be contractually excluded. Practitioners should obtain independent legal advice on their standard engagement agreements in each jurisdiction in which they operate.

6. EMERGING LEGAL MECHANISMS

6.1. Bug Bounty Programs

Bug bounty programs represent the most significant institutional innovation in the legal governance of ethical hacking in the past decade. By creating formal, publicly defined frameworks for vulnerability submission and compensation, these programs extend a structured authorization to security researchers that mitigates the core legal risks identified in Section 5. Del-Real and Rodriguez Mesa [16] identify three distinct program categories: (1) institutional programs operated directly by target organizations (e.g., Google Project Zero, Microsoft Bug Bounty); (2) platform-intermediated programs through specialist intermediaries (HackerOne, Bugcrowd, Synack); and (3) private vulnerability brokers, which purchase and resell vulnerability intelligence at higher reward rates but raise significant ethical and legal questions regarding end use.

The legal significance of bug bounty programs extends beyond their immediate authorization. By establishing explicit, publicly documented rules of engagement, they reduce legal uncertainty that otherwise characterizes security research. The authorizing organization's commitment to good-faith review and compensation creates a reciprocal obligation of good faith on the researcher, and structured disclosure timelines limit risks associated with independent vulnerability publication. Importantly, participation in a recognized bug bounty program has been cited in U.S. federal court proceedings as evidence of good faith that mitigated prosecutorial exposure under the CFAA, though no court has yet held that bug bounty participation provides an absolute defense [16, 21].

6.2. Responsible Disclosure Protocols

Responsible disclosure - also termed coordinated vulnerability disclosure (CVD) - refers to the practice of reporting vulnerabilities to the affected organization privately before public disclosure. The ISO/IEC 29147:2018 standard provides a widely adopted CVD framework. From a legal perspective, documented adherence to a structured disclosure protocol provides evidence of good faith that may be decisive in the event of a legal challenge.

Legal protection afforded by responsible disclosure varies significantly by jurisdiction. The Netherlands (2013 CVD guidelines), France (ANSSI guidance, 2021), and Belgium (CCB framework, 2022) have enacted statutory or regulatory safe harbours for researchers complying with defined disclosure protocols. The United Kingdom and the United States offer no such explicit statutory protection, leaving researchers reliant on prosecutorial discretion. This absence of harmonized disclosure-protection frameworks represents one of the most significant remaining legal gaps.

6.3. Legislative Protections for Good-Faith Security Research

A growing number of jurisdictions are extending statutory protection to ethical hackers operating in good faith. The U.S. DOJ's 2022 revised CFAA enforcement policy [21] announced that good-faith security research would no longer be prosecuted. While this policy does not provide statutory immunity and may be revised by subsequent administrations, it represents a significant practical shift. Spain's 2023 penal code reforms [16] explicitly carve out space for authorized security research. The NIS2 Directive [23] mandates vulnerability disclosure obligations that create indirect incentives for more systematic use of ethical hacking across critical sectors. The EU Cyber Resilience Act (CRA), adopted in 2024, further introduces coordinated vulnerability disclosure requirements for manufacturers of products with digital elements, creating additional formal space for security research.

7. DISCUSSION

7.1. Cross-Jurisdictional Fragmentation

The most systemic legal challenge identified across the reviewed literature is jurisdictional fragmentation. An engagement conducted by a practitioner in one country, targeting systems hosted in a second, on behalf of a client incorporated in a third, may simultaneously engage three distinct computer fraud statutes, two data protection regimes, and multiple intellectual property frameworks - none designed for cross-border security testing. Pawlicka et al. [14] characterize this as a fundamental structural problem that individual practitioners cannot resolve through more careful contracting alone.

The gap is particularly acute at the GDPR/cybercrime statute intersection. An ethical hacker who discovers a vulnerability involving EU residents' personal data must simultaneously navigate the GDPR's 72-hour notification obligation (Article 33), the computer fraud statute of the jurisdiction where the system is hosted, and their engagement agreement - which may impose conflicting timelines and disclosure requirements. The Budapest Convention on Cybercrime [20] provides a model for cross-border cooperation but addresses law enforcement, not the legal status of authorized security research; a supplementary protocol addressing the conditions for lawful authorized security research would substantially reduce current uncertainty.

7.2. Standardization and Professional Certification

Existing certifications (CEH, OSCP, GPEN) provide evidence of technical competence but do not impose legally significant obligations on practitioners. No current certification standard creates binding requirements for engagement documentation, scope management, or post-engagement data handling. A more robust standardization framework - developed through collaboration between ISO/IEC, CREST [26], and national cybersecurity agencies - would define minimum documentation standards, establish binding legal obligations for certified practitioners, and create an enforceable disciplinary mechanism. Such a framework would give practitioners, clients, regulators, and courts a coherent reference standard.

7.3. Counterarguments and Limitations of the Proposed Framework

Intellectual honesty requires acknowledging significant counterarguments to the paper's core proposals. First, regarding harmonization: some legal scholars argue that cross-jurisdictional diversity in computer fraud law is not a bug but a feature, reflecting legitimate differences in national security policy, democratic values, and institutional capacity. A harmonized framework risks encoding the preferences of technologically powerful states at the expense of regulatory sovereignty [28]. This objection has particular force in the EU-U.S. context, where fundamental differences in the treatment of state surveillance and individual privacy rights complicate any mutual recognition framework.

Second, regarding standardization: over-regulation of ethical hacking methodologies could stifle the methodological innovation that makes security research effective. Adversaries do not operate within standardized frameworks; requiring defenders to do so may systematically disadvantage them. A rigid certification-based system might also exclude capable independent researchers who lack resources to obtain formal credentials, narrowing the talent pool at precisely the moment when the cybersecurity workforce gap is most acute [7].

Third, regarding the ROSI model: the model presented in Section 4.3, while grounded in empirical breach cost data [13, 25], makes several simplifying assumptions that may not hold in practice. The assumption of a fixed breach probability reduction (15% to 5%) obscures the substantial variance across organizations, sectors, and threat environments. The model also does not account for the cost of false positives (identified vulnerabilities that do not represent genuine risks) or the opportunity cost of operational disruption during testing. Future research should develop more granular, sector-specific ROSI models that account for this variance.

Fourth, the present systematic review, while following PRISMA methodology, is subject to publication bias: studies finding positive legal outcomes for ethical hacking are more likely to be published than those documenting prosecutions or civil actions. The legal risk landscape may therefore be more adverse than the reviewed literature suggests.

7.4. Artificial Intelligence and the Future Legal Landscape

The integration of AI into penetration testing tools raises novel legal questions the current framework cannot address. Automated platforms that dynamically generate and execute attack strategies challenge the concept of a defined, predictable scope: if an AI-driven tool autonomously discovers and pursues attack paths not anticipated by the engagement agreement, it is legally unclear whether this constitutes authorized testing or unauthorized intrusion under current doctrine in most jurisdictions.

A second AI-related challenge concerns accountability. Where an automated tool causes unintended system damage, the tort question of who bears responsibility - the practitioner, the tool developer, or the client - may lack a clear answer under existing liability frameworks. The rapid deployment of AI capabilities in security testing creates an urgent need for regulatory guidance, AI-specific liability clauses in engagement agreements, and industry self-regulation before a significant incident forces adverse judicial or legislative resolution.

7.5. Recommendations

For policymakers: Develop a multilateral legal framework — building on the Budapest Convention model — that explicitly addresses the conditions for lawful cross-border ethical hacking, including clear safe harbours for researchers complying with responsible disclosure protocols. Harmonize these protections at the EU level through the NIS2 Directive or a dedicated instrument. Provide specific GDPR guidance on incidental personal data access during authorized security testing, clarifying whether and under what conditions such access constitutes "processing."

For professional bodies: Develop and adopt a comprehensive professional standard establishing minimum requirements for authorization documentation, scope management, data handling, and post-engagement reporting. Create a binding code of professional conduct with an enforceable disciplinary mechanism. Develop AI-specific guidance for automated penetration testing tools, including requirements for pre-deployment scope validation.

For practitioners: Apply the minimal-footprint optimization principle - equation (6) - as a standard operational discipline. Treat engagement documentation as a legal record from day one. Obtain jurisdiction-specific legal advice for cross-border engagements. Invest in continuous legal education as a core professional competency. Where operating in the United States, ensure that all activities comply with the conditions of the DMCA § 1201(j) security research exemption.

8. CONCLUSIONS AND FUTURE RESEARCH

This systematic review has examined the legal dimensions of ethical hacking practice across seven interconnected domains. Three principal conclusions correspond to the research questions.

With respect to RQ1, the primary legal challenges are authorization and scope management, GDPR compliance, intellectual property protection, and liability allocation. These are not independent: a failure of authorization creates cascading liability across all other domains. The risk equation $R = P(T) \times V \times I$, applied to the legal domain, demonstrates that the legal vulnerability of an inadequately documented engagement is high and the potential impact - criminal prosecution, civil liability, reputational damage - is severe. The paper's novel contribution is the formal demonstration that these risks are structurally symmetrical to security risks and amenable to the same analytical framework.

With respect to RQ2, the most effective institutional mechanisms are structured engagement agreements with precise scope definitions, bug bounty programs with explicit authorization frameworks, and coordinated vulnerability disclosure protocols. Legislative developments - the U.S. DOJ's revised CFAA enforcement policy [21], Spain's 2023 reforms [16], the NIS2 Directive [23], and the EU Cyber Resilience Act — demonstrate gradual but real movement toward statutory accommodation of ethical hacking practice.

With respect to RQ3, cross-jurisdictional fragmentation remains the most significant systemic gap. The absence of harmonized responsible disclosure protections creates substantial uncertainty for practitioners operating globally, and AI-driven penetration testing tools compound this by challenging the concept of predictable scope. The counterarguments presented in Section 7.3 - particularly the sovereignty objection to harmonization and the innovation objection to standardization - indicate that proposed solutions must be carefully calibrated to avoid overcorrection.

Future research should address four specific gaps. First, empirical studies measuring the actual incidence of legal challenges against ethical hackers - as opposed to the legal risks identified theoretically - are largely absent from the literature; such studies would substantially strengthen the evidence base. Second, sector-specific ROSI models that account for variance in breach costs and risk reduction across industries would improve the economic case for ethical hacking. Third, legal analysis of specific AI-generated attack paths and their treatment under existing computer fraud doctrine is urgently needed as autonomous testing tools enter commercial deployment. Fourth, comparative legal analysis of responsible disclosure regimes across more jurisdictions - particularly in the Global South, which is underrepresented in the current literature — would advance the case for, and inform the design of, an international harmonization framework.

9. ACKNOWLEDGEMENTS

Parts of this research were funded by The Ministry of Science, Technological Development and Innovation of the Republic of Serbia, Contract no. 451-03-137/2025-03/200108.

10. REFERENCES

- [1] Nishadhi, Nimesha. (2020). Ethical Hacking As A Method To Enhance Information Security. Cyber attack protection methodology, https://www.researchgate.net/publication/341654878_Ethical_Hacking_As_A_Method_To_Enhance_Information_Security_Cyber_attack_protection_methodology/citation/download, (2020)
- [2] Stella Tonye, W., Bayo Olushola, O., & Steven Vile, C. (2025). THEORETICAL FOUNDATIONS OF ONLINE IDENTITY SECURITY. In American International Journal of Computer Science and Information Technology (Vol. 10, Number 4, pp. 1–12). Zap journals. <https://doi.org/10.5281/zenodo.16759627>
- [3] G. Thomas, O. Burmeister, G. Low. "Issues of implied trust in ethical hacking", ORBIT Journal, Vol. 2(1), <https://doi.org/10.29297/orbit.v2i1.77>, (2018)
- [4] R. Mukhopadhyay and A. Nath, "Ethical hacking: Scope and challenges in the 21st century", International Journal of Innovative Research in Advanced Engineering, Vol. 1(1), pp. 30-37, (2014)
- [5] G. Vishnuram, K. Tripathi and A. Kumar Tyagi, "Ethical hacking: Importance, controversies and scope in the future", Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI), pp. 01-06, <https://doi.org/10.1109/ICCCI54379.2022.9740860>, (2022)
- [6] B. Smith, W. Yurcik and D. Doss, "Ethical hacking: The security justification redux", Proceedings of the 2002 International Symposium on Technology and Society, pp. 374-379, <https://doi.org/10.1109/ISTAS.2002.1013840>, (2002)
- [7] Cybercrime Magazine, "2023 Cybersecurity Boardroom Report", Cybersecurity Ventures, <https://cybersecurityventures.com/cybersecurity-boardroom-report-2023/>, (2023)
- [8] Statista, "Number of malware attacks per year worldwide from 2015 to 2023", <https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/>, (2024)
- [9] SlashNext, "The State of Phishing 2022", <https://www.prnewswire.com/news-releases/slashnexts-state-of-phishing-report-reveals-more-than-255-million-attacks-in-2022-signaling-a-61-increase-in-phishing-year-over-year-301659518.html>, (2022)

- [10] Cloudflare, "DDoS Threat Report for 2024 Q1", <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>, (2024)
- [11] A. Magnusson, "Man-in-the-Middle (MITM) Attack: Definition, Examples and More", StrongDM, <https://www.strongdm.com/blog/man-in-the-middle-attack>, (2024)
- [12] Verizon, "Data Breach Investigations Report 2024", <https://www.verizon.com/business/en-gb/resources/reports/dbir/>, (2024)
- [13] IBM Security, "Cost of a Data Breach Report 2024", IBM Corporation, <https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf>, (2024)
- [14] A. Pawlicka, M. Choras, R. Kozik and M. Pawlicki, "First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions", *Personal and Ubiquitous Computing*, Vol. 27, pp. 193-202, <https://doi.org/10.1007/s00779-020-01510-3>, (2023)
- [15] M. Hassan, "Ethics and digital data privacy", ResearchGate, <https://doi.org/10.13140/RG.2.2.33972.68486>, (2020)
- [16] C. Del-Real and M.J. Rodriguez Mesa, "From black to white: The regulation of ethical hacking in Spain", *Information & Communications Technology Law*, Vol. 32(2), pp. 207-239, <https://doi.org/10.1080/13600834.2022.2132595>, (2023)
- [17] J.P. Yaacoub, H. Noura, O. Salman and A. Chehab, "A survey on ethical hacking: Issues and challenges", ResearchGate, <https://doi.org/10.13140/RG.2.2.11495.37285>, (2021)
- [18] Akintayo, Obafemi & Ifeanyi, Chinazo & Onunka, Okeoma. (2024). Resolving cybersecurity disputes and protecting digital infrastructure With ADR. *Computer Science & IT Research Journal*. 5. 2437-2457. 10.51594/csitrj.v5i10.1674.
- [19] "OWASP Top 10: Injection – What It Is And How To Protect Your Applications" - BLOG, <https://cyolo.io/blog/owasp-top-10-injection-what-it-is-and-how-to-protect-our-applications>, (2023)
- [20] Council of Europe, "Convention on Cybercrime (Budapest Convention)", ETS No. 185, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, (2001)
- [21] U.S. Department of Justice, "Department of Justice announces new policy for charging cases under the Computer Fraud and Abuse Act", <https://www.justice.gov/opa/pr/departments-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act>, (2022)
- [22] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 — General Data Protection Regulation", *Official Journal of the European Union*, L 119, pp. 1-88, (2016)
- [23] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 — NIS2 Directive", *Official Journal of the European Union*, L 333, pp. 80-152, (2022)
- [24] G. Fawkes, "The ultimate guide to ethical hacking: What you need to know in 2024", VPNmentor, <https://www.vpnmentor.com/blog/ultimate-guide-to-ethical-hacking/>, (2024)
- [25] Ponemon Institute, "State of Cybersecurity and Third-Party Remote Access Risk", Ponemon Institute LLC, (2023)
- [26] CREST, "CREST Code of Conduct for Penetration Testing", CREST International, <https://www.crest-approved.org/wp-content/uploads/2023/04/A-Guide-to-Penetration-Testing-2022.pdf?ver>, (2023)
- [27] ISC2, "Code of Ethics", International Information System Security Certification Consortium, <https://www.isc2.org/ethics>, (2024)
- [28] D. Svantesson, "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation", *International Data Privacy Law*, Volume 5, Issue 4, November 2015, Pages 226–234, <https://doi.org/10.1093/idpl/ipv024>, (2015)