Legal Regulation of Ethical Hacking in Palestine: A Comparative Study with International Frameworks

Marah R. Hawa ,Mousa M. Farajallah,Ibrahim R Al-Sharif

***Abstract*— Palestine is experiencing a sharp rise in cyberattacks that severely affect individuals, institutions, and the national digital infrastructure. Ethical hacking represents a crucial approach to identifying and mitigating security vulnerabilities in software systems. However, a clear legal framework differentiating between ethical and malicious hacking constitutes a significant barrier to advancing this critical practice. This paper presents a comprehensive analytical study exploring the opportunities and challenges of regulating ethical hacking in Palestine. The analysis is conducted from two key perspectives: an empirical survey of Palestinian cybersecurity and legal experts to capture their insights on the urgent need for a coherent and normative regulatory framework and a critical comparison of current Palestinian legislation with advanced international and European legal standards. The study concludes that the lack of legal recognition and protection for ethical hacking in Palestine impedes efforts to strengthen national cybersecurity. Accordingly, it recommends the establishment of a practical and robust legal framework that supports and incentivizes ethical hackers, while ensuring the necessary legal safeguards to build trust within the Palestinian digital ecosystem.**

I. INTRODUCTION

Palestine is placing increasing importance on securing technological information systems within both governmental and private sector organizations due to the rising number of cyberattacks targeting the national digital infrastructure. This growing concern aligns with broader efforts to strengthen cyber law. However, this proactive model often coincides with the urgent need to accelerate the deployment of digital services, resulting in software being developed and deployed before undergoing comprehensive security testing. Consequently, such systems may be released with vulnerabilities that expose them to cyber threats [1]. Penetration testing has proven to be an effective reactive measure, enabling early detection and mitigation of security breaches. These efforts are led by "ethical hackers," also known as white hat hackers, who ethically guide cybersecurity initiatives. Their contributions are often embedded in structured programs that have received recognition in many regions. Numerous international experiences, particularly in the United States and Europe, have demonstrated the effectiveness of such programs in enhancing cybersecurity resilience [2]. In Palestine, although the need to adopt proactive cybersecurity mechanisms is widely acknowledged, their formal implementation remains limited. This is primarily due to the lack of codified legal provisions that legitimize and regulate ethical hacking practices [3]. Furthermore, ethical hackers in Palestine often operate in a legal and institutional void, lacking official recognition and structured collaboration with national agencies. Unlike in other countries where white-hat hackers are integrated into formal cybersecurity strategies, their role in Palestine remains informal and largely unsupported [4]. This study examines the potential and limitations of regulating ethical hacking in Palestine through an analytical comparison between the current Palestinian legal framework and leading international legal systems in this domain .The structure of the paper is organized as follows: Section 2 reviews the related literature on ethical hacking, its historical development, and the global legal approaches adopted to regulate it. Section 3 outlines the research methodology, including qualitative and quantitative approaches, such as expert interviews and stakeholder surveys conducted in the Palestinian context. Section 4 presents the results of the field study and highlights key patterns in the collected data. Section 5 discusses the findings through a comparative legal analysis between international frameworks and the Palestinian legal environment. Finally, Section 6 concludes the paper by summarizing the main contributions and outlining directions for future research.

II. LITERATURE REVIEW

This section examines the legal and academic literature concerning the regulation of ethical hacking. It begins with an analysis of legal frameworks and internationally recognized practices in leading jurisdictions, including the United States, Spain, and Germany. The discussion then shifts to the Palestinian context, highlighting existing legislative and regulatory gaps. Finally, the section identifies the research gap that this study aims to address by proposing a legal framework tailored to the specific needs and conditions of Palestine.

A. International Legal Approaches to Ethical Hacking

In recent years, there has been a growing interest among leading nations in regulating ethical hacking within well-defined legal frameworks, striking a balance between safeguarding cybersecurity and protecting the legal rights of security researchers. National approaches to this issue differ based on each country's legal tradition and the maturity of its digital infrastructure. This section highlights the most notable legal models adopted by several advanced jurisdictions, which may serve as valuable reference points for formulating a legal framework suited to the Palestinian context [5]. With a clear and growing recognition of the role of the "Ethical Hacker" as a vital pillar of cyber defense, the U.S. Department of Justice has comprehensively updated its policy regarding the

978-9950-8599-0-6

application of the Computer Fraud and Abuse Act (CFAA). This update explicitly exempts ethical hacking activities from federal prosecution, thereby acknowledging the importance of ethical hacking as an effective mechanism for identifying and addressing security vulnerabilities, rather than classifying such activities as hostile or criminal acts. This development represents a fundamental turning point in how cyber behavior is assessed, redefining the boundary between intentional intent aimed at causing harm and responsible intent grounded in professional ethics and social responsibility, rather than merely the form of the action. Within this framework, the ethical hacker is no longer viewed as a legal adversary but as an institutional partner contributing to the construction of a more resilient and secure cybersecurity infrastructure. Accordingly, the new policy affirms that authorized access for testing or vulnerability remediation, when conducted in good faith and under professional standards, is not considered a criminal offense. This shift reflects a progressive legal interpretation that recognizes ethical hacking not only as a technical practice but as a critical public service, effectively serving as the modern-day digital safeguard [6]. The U.S. policy supports this trend by encouraging security researchers to participate in bug bounty programs and disclosure policies, which provide a secure legal environment for responsible and regulated vulnerability reporting. The Department of Justice also emphasizes a clear distinction between malicious intent aimed at extortion or harm, which remains subject to legal prosecution, and preventive intent, which governs the actions of ethical hackers within a well-defined and ethical legal framework. Additionally, the policy clarifies those minor violations of terms of service, such as the use of fake accounts or the personal use of work devices, are not necessarily considered crimes under the CFAA unless permission is explicitly revoked through legal measures such as cease and desist orders. In doing so, the U.S. policy establishes a balanced legal framework that supports responsible security research while limiting excessive criminalization, thereby enhancing the overall effectiveness of the cybersecurity ecosystem in addressing modern challenges [7].

In the United Kingdom [8]. The practices of the modern ethical hacker continue to rely on the Computer Misuse Act 1990 (CMA), a statute enacted during a time when internet usage was minimal and the cybersecurity profession had yet to take shape. Despite advancements in digital technologies, the CMA has not been sufficiently updated to meet the challenges of today's interconnected world. According to experts, its outdated provisions inadvertently criminalize legitimate cybersecurity activities, such as vulnerability testing or forensic analysis. On December 18, 2024, during a session in the House of Lords, proposed amendments to the Data (Access and Use) Bill aimed to introduce legal defenses for cybersecurity professionals. These amendments would have allowed individuals to demonstrate that their actions were either necessary for detecting or preventing crime or justified as being in the public interest. Spearheaded by Lord Chris Holmes and Lord Tim Clement-Jones, the proposal underscored the urgent need to modernize the UK's cyber legislation [9], which has increasingly become an obstacle to lawful security operations. Despite broad support from the cybersecurity community and beyond, the UK government argued that such reforms were still "premature," opting instead to pursue consensus through a broader review led by the Home Office. This delay leaves ethical hackers operating in a legal gray zone, potentially facing criminal liability even when performing activities intended to protect public infrastructure and digital health systems. Organizations such as the NCC Group [10] have raised concerns that the lack of legal reform undermines the UK's competitive edge in the global cybersecurity arena. While countries like the United States have taken steps to support ethical hacking through clearer legal protections, the UK's stance remains comparatively ambiguous and restrictive. The continued enforcement of an unmodified CMA risks deterring skilled cybersecurity professionals and limiting the effectiveness of collaborative programs such as bug bounty initiatives and responsible disclosure frameworks. The need for legislative reform is more pressing than ever to ensure that the UK's security laws are empowered to operate effectively and are not constrained by outdated limitations or insufficient legal authority [11].

In Spain [2], the legal framework governing cybersecurity activities, including ethical hacking practices, remains rooted in outdated legislation that has not been fully adapted to address contemporary digital challenges. While there have been some positive developments, such as the Royal Spanish Academy's 2017 revision of its definition of the term "hacker" to reflect a more constructive interpretation, institutional implementation of these changes remains limited. A study in [2] highlights those existing Spanish laws, including the Penal Code, fail to offer adequate legal protection for ethical hackers. As a result, professionals conducting activities such as penetration testing or vulnerability disclosure often find themselves operating within a legal grey area. Nevertheless, certain public administrations have begun to explore progressive cybersecurity measures. For instance, in December 2020, the Generalitat de Catalunya launched a pilot Bug Bounty program in partnership with cybersecurity experts. The initiative successfully identified five security vulnerabilities, demonstrating the potential of collaborative security efforts to enhance system resilience. Building on this success, the Generalitat expanded the program in April 2023, allocating a budget of €70,000. Within the first three months, seven vulnerabilities were reported, one of which was classified as high severity. This initiative, the first of its kind within Spanish public administration, aims to foster closer collaboration with the cybersecurity community and reinforce the security posture of government infrastructure. Despite these advancements, there is a pressing need to modernize Spain's legal framework to explicitly recognize and protect the role of ethical hackers. Legislative reform in this area would not only bolster national cybersecurity efforts but also promote stronger cooperation between the public and private sectors in safeguarding digital infrastructure [2].

In Germany [12], the legal framework governing cybersecurity activities, including ethical hacking practices, is established under the German Penal Code (Strafgesetzbuch—StGB), which criminalizes unauthorized access to computer

systems. However, the law explicitly provides exceptions permitting security testing when prior consent is obtained from the system owner, thereby safeguarding security researchers operating within a clearly defined legal framework.

Germany also promotes responsible vulnerability disclosure policies, encouraging both governmental and private organizations to implement formal channels for communication and collaboration with security researchers. These policies cultivate a secure and accountable environment that enhances national cybersecurity by enabling experts to identify and remediate vulnerabilities before they can be exploited by malicious actors. Despite these advancements, there remains a pressing need to increase awareness and standardize practices across various sectors to ensure the effective enforcement of these laws and policies, as well as to build mutual trust between security researchers and system-owning entities [13].

In the Netherlands [14], the legal framework governing cybersecurity activities, including ethical hacking, is primarily established under the Dutch Penal Code, notably Section 138ab, which criminalizes unauthorized access to computer systems. However, the legislation provides certain allowances for security researchers acting with explicit consent or within the scope of Coordinated Vulnerability Disclosure (CVD) policies, thereby promoting collaboration between researchers and organizations to enhance system security. Dutch authorities actively endorse responsible disclosure practices as both a legal and ethical mechanism for identifying and reporting security vulnerabilities without fear of legal repercussions. This approach fosters mutual trust between the technical community and governmental as well as private sector entities. Nevertheless, there remains a pressing need for clearer guidelines and a more comprehensive legislative framework to offer stronger legal protections for cybersecurity professionals. Strengthening these provisions will empower ethical hackers to combat cybercrime effectively while minimizing the risk of unwarranted legal liability, ultimately contributing to the enhancement of national cybersecurity in the Netherlands.

In France [16]. The legal framework governing cybersecurity activities, including ethical hacking practices, is established under the French Criminal Code (Code pénal). Article 323-1 criminalizes unauthorized access to computer systems. However, French law provides exceptions when security testing is conducted with the explicit consent of the system owner, thereby legitimizing ethical hacking within a well-defined legal framework. Furthermore, France actively promotes responsible disclosure policies (Divulgation Responsable) [17], fostering collaboration between security researchers and organizations to effectively identify and remediate vulnerabilities without exposing researchers to legal risks. These policies aim to cultivate a culture of transparency and cooperation within the cybersecurity domain. Despite these legal provisions, the practical implementation of such laws necessitates meticulous oversight to maintain a balance between security research and regulatory compliance. Ongoing efforts focus on updating regulations and guidelines to better support ethical hackers and strengthen France's overall cybersecurity posture[18,19].

Singapore [19] adopted a comprehensive legal framework to regulate cybersecurity activities, including ethical hacking practices, through two primary laws: the Computer Misuse Act 1993 (CMA) and the Cybersecurity Act 2018. The CMA criminalizes[20]unauthorized access to computer systems, but provides a clear exception when security testing is conducted with the explicit consent of the system owner, thereby offering legal protection for security researchers. In addition, the CMA promotes responsible disclosure policies and encourages organizations to establish formal channels for collaboration with security researchers to identify and remediate vulnerabilities before they can be exploited by malicious actors. The Cyber Security Agency of Singapore (CSA) has reinforced these principles through public awareness initiatives and detailed guidelines aimed at fostering a secure and innovation-friendly digital environment. Despite these advancements [21], Implementation challenges persist, highlighting the need for further legislative clarity to strengthen legal protections for ethical hackers and to secure their role as integral contributors to Singapore's national cybersecurity architecture. While several countries have made strides toward building legal structures that support ethical hacking, recurring implementation gaps illustrate the global complexity of balancing innovation with legal responsibility. These cases provide valuable lessons for emerging contexts. In Palestine, where technological adoption is accelerating under unique political and institutional constraints, the applicability of these global models must be critically assessed. Rather than adopting foreign policies wholesale, this study aims to contextualize key international practices and extract adaptable legal elements that could form the foundation for a suitable regulatory framework in the Palestinian setting.

While Palestine[1] faces unique geopolitical constraints, it is useful to consider other fragile but non-conflict-affected states. For example, For example, countries such as Bangladesh and other fragile but non-conflict-affected states also struggle with underdeveloped cybersecurity legislation due to limited institutional capacity, lack of specialized legal expertise, and competing governance priorities[5]. These cases demonstrate that even in the absence of armed conflict, state fragility can significantly delay the adoption of legal frameworks for regulating ethical hacking. However, Palestine's situation is further complicated by the occupation, which adds external constraints to internal governance challenges.

B. Palestinian Context

In the Palestinian legal framework [1], there remains an absence of precise, official definitions for key terms such as "harmful effects" and "ethical hacker." The primary legislation governing cyber-related matters is Decree-Law No. 16 of 2017 on Cybercrime. However, this law is predominantly punitive and does not account for the intent behind cyber activities or differentiate between various forms of digital behavior [4]. As a result, all hacking activities, irrespective of the hacker's motives or objectives, are

uniformly classified as criminal offenses. This lack of legal nuance presents a significant challenge, particularly in cases involving individuals with advanced technical skills who engage in hacking for ethical purposes, such as identifying and reporting cybersecurity vulnerabilities. Palestinian law[22]currently lacks a clear framework for CVD and does not refer to bug bounty programs as legally recognized mechanisms to promote cooperation between official institutions and cybersecurity professionals. Consequently, security experts who discover technical vulnerabilities—even when acting in good faith—may still face legal consequences due to the absence of legislative safeguards. Both local and international human rights organizations, including Human Rights Watch [23], have strongly criticized the law for its vague terminology and its potential misuse in restricting freedom of expression or criminalizing the work of well-intentioned technical professionals. This underscores the urgent need to revise the legislation to bring it in line with international standards, establish explicit legal protections for ethical hackers, and enable the adoption of modern legal instruments that strengthen responses to cyber threats without undermining the rights or discouraging the contributions of cybersecurity experts [24]. The current Palestinian legal landscape exhibits significant gaps when it comes to addressing the realities of ethical hacking. Unlike jurisdictions that have introduced legal definitions and structured programs to support responsible security research, Palestine's legislation remains broad and punitive. The absence of cooperation mechanisms, such as Coordinated CVD, and the lack of explicit legal recognition for ethical intent result in a climate of legal uncertainty. While the previous sections highlighted comparative international models, this part reveals the deeper systemic and policy-level inattention within the Palestinian context. This disconnect between legal enforcement and technological practice forms the core rationale for this study, which seeks to propose a context-sensitive framework that protects ethical hackers while reinforcing cybersecurity resilience.

C. Research Gap And Motivation

A review of comparative legal literature reveals a growing global trend toward recognizing ethical hacking within well-defined legislative frameworks. Countries such as the United States[7], Netherlands [14,15], France [16], and Spain [2] have adopted clear legal models that protect security researchers and encourage the disclosure of cybersecurity vulnerabilities within a safe legal environment, supported by mechanisms such as coordinated vulnerability disclosure (CVD) and bug bounty [2,6,8] programs. Conversely, despite technological and legislative advancements in the United Kingdom[8], the Computer Misuse Act (CMA 1990) continues to pose legal barriers, as proposed reforms aimed at safeguarding bona fide ethical hackers have yet to be enacted. These international experiences illustrate that the legal challenges surrounding the regulation of ethical hacking are not confined to developing nations but are also present in some advanced jurisdictions [8] with traditional legislative structures. Despite the existence of comprehensive international frameworks and soft law instruments related to cybersecurity and ethical hacking [5], several key challenges hinder their effective implementation. First, there is a lack of harmonization between jurisdictions, which leads to inconsistent definitions of cybercrimes and uncertainty regarding the legal status of ethical hacking. Second, enforcement mechanisms at the international level remain limited, particularly in cross-border investigations. Third, divergent national interests and political sensitivities often prevent consensus on binding norms. Finally, many frameworks do not provide clear legal protections for ethical hackers acting in good faith, which contributes to legal uncertainty and discourages responsible disclosure. These challenges suggest that aligning national legislation with international norms requires not just legal adoption but also institutional readiness and cross-sectoral cooperation [13].

However, the situation in Palestine is markedly more complex due to the complete absence of a legal framework that distinguishes between ethical and malicious hackers. The existing laws lack formal definitions of essential cybersecurity concepts and provide no structured mechanisms to regulate cooperation between security researchers and public or private institutions. Furthermore, there are no coordinated disclosure policies or public programs incentivizing vulnerability reporting. The existing legislative void underscores a significant research deficiency within contemporary legal scholarship: the lack of comparative analyses aimed at contextualizing and adapting successful international models to the Palestinian legal framework. This study represents a pioneering effort in Palestine, addressing the subject of ethical hacking—a domain that has not previously received focused legal attention within the Palestinian context, particularly concerning the protection of ethical hackers and the mitigation of potential legal liabilities they may face. Accordingly, the research endeavors to bridge this gap through a comparative legal analysis and comprehensive stakeholder consultations, to propose a legislative framework that not only fortifies national cybersecurity but also provides legal safeguards for ethical hackers, recognizing them as vital contributors to the digital defense infrastructure. Table 1 illustrates a summary of legal frameworks in the Literature Review.

Table 1. Summarize the legal frameworks for protecting ethical hackers

Country	General Legal Framework	Legal Protection for Ethical Hackers
United States [7]	Computer Fraud and Abuse Act (CFAA)	Yes(Conditional)
United Kingdom [8]	Computer Misuse Act (CMA 1990)	No
Germany[12]	German Penal Code	Yes (With Explicit Consent)
Netherlands [14]	Penal Code Section 138ab	Yes(With Permission and CVD)
France [16]	Penal Code Article 323-1	Yes(With Permission Only)
Singapore[19]	Computer Misuse Act 1993 & Cybersecurity Act 2018	Yes(With Explicit Permission & Responsible Disclosure)
Palestine [1]	Cybercrime Law	No

Table 1 above provides a concise comparison of the most prominent legal frameworks in both developed and developing countries, focusing on the extent of legal protection afforded to ethical hackers. This comparison highlights the gaps and disparities in national legislation, with some countries adopting clear models to support security researchers and encourage responsible vulnerability disclosure, while others, such as Palestine, continue to lack such protections and legal regulations.

III. METHODOLOGY

This study investigates the legal gap in Palestine concerning the differentiation between ethical and malicious hacking. Employing a mixed-methods research approach that integrates both quantitative and qualitative analyses, alongside a comparative legal analysis, the study seeks to provide a comprehensive understanding of the issue. This section is divided into six subsections that provide a detailed overview of the data, the target population, and the methods used for data collection and analysis.Fig.1 represents the proposed Methodology.

Figure 1. Proposed Methodology.

Fig.1 illustrates the research methodology used in this study. It begins with data collection through a structured questionnaire and semi-structured interviews targeting professionals in cybersecurity and law. The collected data were then processed and analyzed using statistical methods and thematic analysis. Finally, the results were interpreted and compared with international legal frameworks to identify gaps and inform recommendations for Palestine.

The following sections provide a detailed description of each step in the methodology, including the study population, data collection tools, data processing, and analysis procedures.

A. Dataset Description

This study utilized two primary data sources to examine the legal regulation of ethical hacking in Palestine: First, quantitative data were collected through a structured questionnaire targeting Palestinian experts in cyber security and law, to assess awareness levels, identify legal and regulatory challenges, and evaluating the perceived need for a formal legal framework governing ethical hacking practices. Second, qualitative data were obtained from in-depth, semi-structured interviews conducted with a selected group of legal and technological professionals, aimed at gaining a deeper understanding of expert perspectives on the current legal boundaries of ethical hacking and the deficiencies within existing policies. These data sources were further complemented by a comparative legal analysis, contrasting relevant Palestinian legislation with established international legal frameworks, particularly those of the European Union and the United States. This integrative approach seeks to provide a holistic view of the legal and technical landscape in Palestine, identify critical regulatory gaps, and propose actionable criteria for developing a robust and coherent legal framework to support ethical hacking activities.

B. Study Population and Sample Size

This research targeted two main categories of the study population, carefully selected using purposive sampling to ensure the comprehensiveness and accuracy of the data in the context of studying the legal regulation of ethical piracy in Palestine. The study targeted Palestinian professionals working in cybersecurity, law, and information technology across both governmental and private sectors. A structured online questionnaire was disseminated to assess participants' awareness of ethical hacking, their views on the absence of relevant legal frameworks, and their opinions regarding the potential for a Palestinian legal model informed by global practices. To ensure statistical reliability, Cochran's formula[25] was applied to calculate the appropriate sample size using (1):

$$n_0 = \frac{z^2 \cdot p \cdot q}{e^2} \quad (1)$$

. Assuming a 95% confidence level (z = 1.96), maximum variability (p = 0.5), and a 5% margin of error (e = 0.05), the formula indicated an ideal sample size of approximately 400 respondents. Accordingly, a sample of 400 participants was utilized, which is sufficient for generalizing results within the study's scope despite logistical constraints.

In addition to the survey, semi-structured interviews were conducted with ten selected experts, including cybersecurity professionals, legal scholars, and academics. These interviews aimed to gain deeper insights into the legal and practical challenges of ethical hacking and to collect informed suggestions for potential legislative elements, such as licensing, vulnerability disclosure, and legal protections. The number of interviews was determined based on qualitative research standards to ensure data saturation, where no substantial new information is likely to emerge beyond a certain point.

C. Data Collection Tools

To achieve the research objectives and ensure methodological rigor, this study employed two complementary data collection tools: a structured questionnaire and semi-structured expert interviews. These tools were carefully developed to capture both the breadth and depth of insights regarding the legal regulation of ethical hacking in Palestine. This study utilized two complementary data collection tools. A structured questionnaire was administered to cybersecurity and legal professionals in Palestine, comprising 12 closed-ended items across four themes: awareness, legal context, challenges, and recommendations. Responses were measured on a five-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree," ensuring statistical consistency and facilitating

comparative analysis. In parallel, semi-structured interviews were conducted with selected experts to gain deeper insights into legal gaps and practical experiences related to ethical hacking. The interviews used a thematic analysis that was independently conducted by two researchers to ensure rigor and reduce potential bias, with disagreements resolved through discussion. Data collection continued until thematic saturation was reached, which was determined after conducting 12 interviews, as no new themes emerged beyond this point.

.

D. Data Analysis

Quantitative responses from the questionnaire were analyzed using descriptive statistics (frequencies, percentages, and means) via Excel to identify general trends. For the interviews, thematic analysis was used to extract key patterns and insights through manual coding, supported when necessary by MAXQDA software. This dual approach provided both statistical summaries and deeper contextual understanding of the topic. Fig.2 illustrates the analysis of the interview.

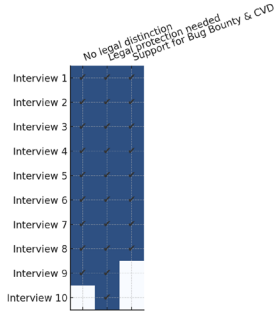

Figure 2. Code Matrix -Interview

Fig.2. The matrix shows that most interviewees discussed the lack of legal distinction, the need for legal protection, and support for bug bounty and CVD. Notably, the theme 'No legal distinction' was consistently mentioned, highlighting a common concern about the absence of clear legal frameworks.

E. Ethical Considerations

The study adhered to the highest ethical standards throughout its duration.1) Informed Consent: Written consent was obtained from all participants after they were fully informed about the research objectives, data collection methods, and any potential risks involved.2) Confidentiality and Privacy: Participants' personal information was kept confidential. Data were securely stored in password-protected files and presented in aggregated, anonymized formats in the research reports.3) Restricted Use of Data: Data were utilized solely for the specified research purposes, in compliance with both local and international data protection laws.

F. Study Limitation

Despite meticulous planning and execution, this study encountered several challenges: Access to Experts: Engaging with key experts in the field proved challenging, which may have affected the diversity and depth of the insights gathered. Sample Size: Due to constraints in time and resources, the study was limited to a smaller sample size. Availability of Official Statistical Data: The research relied on a limited or outdated set of official statistical data, potentially affecting the precision and relevance of certain analyses. Nevertheless, despite these limitations, the study provides valuable preliminary insights and lays the groundwork for future, more comprehensive research.

IV. RESULT

This section presents the findings derived from the various data collection tools employed in this study: the questionnaire and the semi-structured interviews. The data were analyzed using a mixed-methods approach that combines quantitative analysis of survey responses with qualitative analysis of the key themes emerging from the interviews. The aim is to provide a comprehensive understanding of the legal gap concerning ethical hacking in Palestine, as perceived by relevant stakeholders and experts in the legal and cybersecurity fields. The section is structured into two main parts: the first presents the results of the questionnaire, while the second highlights the main themes and insights from the interviews, setting the stage for a more in-depth discussion in the following section.

A. Survey Results

The results of the survey, which included 400 participants from cybersecurity professionals, penetration testers, legal practitioners, and government IT personnel, revealed several critical insights. Most respondents were male (59.8%), while females represented 40.2% of the sample. Professionally, 35% identified as cybersecurity experts, followed by 26.2% legal professionals, 25% penetration testers, and 13.8% government-sector technologists. Significantly, 100% of respondents indicated that the current Palestinian legal framework does not distinguish between ethical and malicious hackers, reflecting a complete lack of legal clarity in this regard. Furthermore, 62.3% of respondents strongly agreed that the law should be amended to explicitly define ethical hacking and provide protection for security researchers acting in good faith, while 25.8% agreed. The remaining responses ranged from neutral to disagreement, comprising a small minority. Regarding the adoption of modern legal tools, 74.8% considered bug bounty programs to be “critically important,” and 75.8% indicated the same for CVD policies. These results demonstrate a strong professional consensus that Palestine urgently needs a legal framework that legitimizes ethical hacking and fosters secure cooperation between researchers and institutions, aligning with global cybersecurity governance practices.

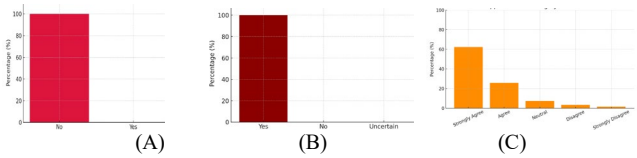

Figure 3. (A) Percentage of participants who believe Palestinian law does not distinguish between ethical hackers and malicious hackers.(B)Percentage of participants who believe there is no legal protection for ethical hackers in Palestinian law .(C) Levels of agreement on the need to amend Palestinian cyber law to recognize and protect ethical hacking.

The results revealed a unanimous perspective among participants regarding the current legal framework in Palestine. As shown in Fig. 3 (A), 100% of respondents stated that the law does not distinguish between ethical hackers and malicious hackers. Similarly, Fig.3(B) illustrates that all participants believe there is no legal protection for ethical hackers. Furthermore, as depicted in Fig. 3(C), 65% of participants strongly agreed and 25% agreed that the law should be amended to explicitly recognize and protect ethical hacking.

B. *Interview Findings*

As part of the qualitative dimension of this study, ten semi-structured interviews were conducted with cybersecurity experts and legal professionals in Palestine. The interview findings revealed a strong consensus among participants, highlighting three key themes: 90% of participants affirmed that the current Palestinian legal framework does not differentiate between ethical hackers and malicious hackers. As a result, even security researchers acting in good faith may face legal consequences due to the lack of legal clarity. 100% of respondents unanimously agreed on the urgent need for legal protection mechanisms for ethical hackers. Suggestions included the introduction of official licenses, written agreements, or limited legal immunity for researchers operating within ethical and professional boundaries. 80% expressed strong support for the implementation of a national framework for CVD and bug bounty programs, citing the success of such initiatives in advanced countries and their role in fostering effective collaboration between institutions and security researchers. These qualitative findings reinforce the results of the quantitative survey and provide further evidence of the pressing need to modernize the Palestinian cybercrime law in alignment with international best practices, Fig. 4. Illustrate these findings.

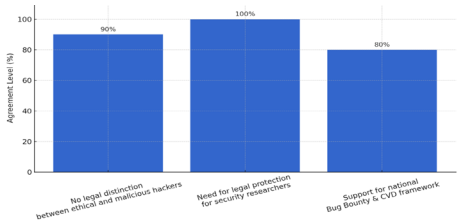

Figure 4. Interview Finding

Fig.4 Key themes derived from expert interviews regarding legal protection for ethical hackers. The figure highlights participants' support for mechanisms such as official licenses, written agreements, and conditional legal immunity. It also reflects the strong consensus (80%) on the need for a national framework supporting Coordinated Vulnerability Disclosure (CVD) and bug bounty programs, emphasizing their success internationally and relevance to the Palestinian context.

V. Discussion

The findings of this study underscore a critical and pressing gap within the Palestinian legal framework concerning ethical hacking. Despite the enactment of cybercrime legislation, notably Law by Decree No. 10 of 2018 [25], which addresses various cyber offenses such as unauthorized access and data manipulation.LawGratis, there remains a conspicuous absence of a clear legal definition and protective measures for ethical hackers. This omission leaves professionals who engage in legitimate cybersecurity activities vulnerable to legal uncertainties and potential prosecution. Participants from both the survey and interviews consistently highlighted this deficiency, expressing concerns over the lack of legal recognition and safeguards for ethical hacking practices. The current legal ambiguity not only hampers the development of a robust cybersecurity infrastructure but also discourages skilled professionals from contributing to national cyber defense initiatives. Furthermore, the study reveals a consensus on the urgent need for a comprehensive regulatory framework that distinctly differentiates between malicious cyber activities and ethical cybersecurity practices. Such a framework would not only provide legal clarity but also foster a conducive environment for professional growth in the cybersecurity sector, encouraging innovation and collaboration among stakeholders. In light of the increasing reliance on digital technologies and the escalating cyber threats facing Palestine, addressing these legal gaps is imperative. Implementing clear definitions and protections for ethical hackers is essential to fortify the nation's cybersecurity posture and to align with international best practices in digital rights and cyber governance.

1) *Comparison with International Frameworks*

The findings of this study are consistent with a growing body of international research, particularly in developing regions, which identifies the absence of legal clarity as a major barrier to institutionalizing ethical hacking. However, beyond a descriptive comparison, this section provides a more evaluative perspective on why certain international frameworks, such as those in the EU, the U.S., and select European countries, serve as effective references.

Table 2. Comparative Table: Legal and Policy Landscape of Ethical Hacking – Palestine vs. International Contexts

Country	Legal Definition of Ethical Hacking	Legal Protection for Good-faith Hackers	Coordinated Vulnerability Disclosure (CVD)	Official Licensing / Regulation of Pen Testing	Alignment with Literature
Palestine[1]	None	None	None	None	Complete gap in all dimensions
United States[7]	No explicit legal definition, but guided by policies	Yes (DoJ 2022 clarification)	Yes (CVD practices & private initiatives)	No official licensing; based on private contracts	Generally aligned with protective principles
Spain[2]	Yes, differentiates White-hat vs Black-hat hackers	Yes	Yes (legally recommended)	No central licensing, but	Strongly aligned with academic literature

				certificati ons exist	
Netherlands[14]	No explicit legal definition	Yes	Yes	No formal licensing	Supports core academic principles
United Kingdom[8]	No explicit legal definition	No (currently under debate)	Informal (industry-led initiatives)	No centralized licensing	The legal environment remains unstable
Germany[12]	No explicit legal definition	No	Informal (industry-based initiatives)	No formal licensing	Partial misalignment
France[16]	No explicit legal definition	No	Informal (industry-based practices)	No formal licensing	Partial misalignment
Singapore[19]	No explicit legal definition	No	Informal (industry standards)	Yes, formal licensing for cybersecurity providers	Strong alignment in regulatory aspects

As shown in Table .2, A critical analysis of the U.S. model, for example, reveals that its relative success does not stem from having a codified legal definition of ethical hacking, but rather from the presence of robust protective policies, a culture of public-private cooperation, and a mature cybersecurity ecosystem that encourages responsible disclosure through structured channels. These mechanisms create an enabling environment where ethical hackers are empowered rather than criminalized, which in turn improves national security responsiveness. Similarly, countries like the Netherlands and Spain, despite not having formal licensing systems, have implemented clear distinctions between malicious and ethical hacking within their legal and policy discourse. This distinction, combined with structured vulnerability disclosure platforms (CVD) and active government support for bug bounty initiatives, demonstrates that progress can be achieved without comprehensive codification, provided there is institutional recognition and operational infrastructure to support ethical practices.

In contrast, the Palestinian context suffers not merely from a lack of codified law but from a complete absence of the four foundational pillars identified in global best practices: legal definitions, protection for good-faith hackers, licensing or regulation, and a responsible disclosure mechanism. This vacuum does not just hinder innovation; it structurally disincentivizes ethical behavior in cybersecurity. As illustrated in Table 2, Palestine is the only country in the comparative analysis with a complete lack of these elements.

This disparity underscores a blind spot in much of the international literature, which often assumes the presence of baseline legal and ethical infrastructures. It also highlights a significant policy opportunity: by studying not only what other countries have done, but why those measures work in their specific contexts, Palestine can design a contextually appropriate, adaptive legal framework. Such a framework would not only promote ethical innovation but also align national practice with globally recognized cybersecurity norms. Therefore, this study calls on policymakers to consider these comparative insights not merely as observations but as actionable guidance for establishing a legal foundation that empowers ethical hacking within Palestine.

VI. Conclusion

In conclusion, the absence of clear legal frameworks and protective mechanisms for ethical hacking in Palestine creates critical challenges for cybersecurity advancement and risks penalizing individuals acting in good faith. To bridge this gap, it is essential to establish a precise legal definition of ethical hacking that differentiates it from malicious activities, alongside introducing legal protections for responsible vulnerability disclosure. Implementing a CVD framework, developing accreditation or licensing programs for ethical hackers, and enhancing awareness through education and public engagement are important steps toward fostering a responsible cybersecurity culture. Furthermore, collaboration at regional and international levels should be pursued to align Palestinian policies with global best practices. To ensure the effective enforcement of future ethical hacking legislation in Palestine, a practical roadmap is required. First, a national cybersecurity regulatory authority should be established with a clear mandate to oversee ethical hacking practices and coordinate between stakeholders. Second, CVD policies should be enacted, allowing ethical hackers to report security flaws without fear of prosecution. Third, legal amendments must include specific clauses that protect bona fide ethical hackers acting in the public interest. Fourth, the judiciary and law enforcement agencies should receive specialized training on digital evidence and cybercrime law. Finally, multi-stakeholder partnerships, including the private sector, academia, and civil society, should be fostered to create a culture of cybersecurity awareness and shared responsibility. This roadmap offers a practical foundation for transitioning from legal void to actionable and protective cybersecurity governance in Palestine .Future research should focus on empirical assessments of ethical hacking practices within Palestine, tailored policy development, evaluation of societal readiness for legal reforms, and the promotion of multi-sector cooperation to build a sustainable ethical hacking ecosystem. Addressing these priorities is imperative to enhance Palestine's cybersecurity posture and create a safe, transparent, and innovation-friendly digital environment.

References

[1] M. R. M. Elshobake and M. Laeba, "The Legal Framework of Cybercrime in Palestine," Arab Law Quarterly, vol. 37, no. 1–2, pp. 157–174, Feb. 2021, doi: 10.1163/15730255-BJA10076.

[2] 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, no. 2, pp. 207–239, May 2023, doi: 10.1080/13600834.2022.2132595.

[3] Institute for Palestine Studies, [Online]. Available: https://www.palestine-studies.org/ [Accessed: May 23, 2025].

[4] B. Amro, "Wireless and Microwave Technologies," vol. 5, pp. 19–26, 2018, doi: 10.5815/ijwmt.2018.05.03.

[5] I. Elegbe, "Cybercrime Legislation: A Comparative Analysis of Legal Frameworks, Policy Responses and Recommendations," International Journal of Education and Social Science Research

(IJESSR), vol. 7, no. 2, p. 1441, 2024, doi: 10.37500/IJESSR.2024.7211.
[6] Bleeping Computer, "U.S. DOJ will no longer prosecute ethical hackers under CFAA," [Online]. Available: https://www.bleepingcomputer.com/news/security/us-doj-will-no-longer-prosecute-ethical-hackers-under-cfaa/ [Accessed: May 23, 2025].
[7] U.S. Department of Justice, Office of Public Affairs, [Online]. Available: https://www.justice.gov/opa [Accessed: May 23, 2025].
[8] Computer Weekly, "Latest attempt to override UK's outdated hacking law stalls," [Online]. Available: https://www.computerweekly.com/news/366617109/Latest-attempt-to-override-UKs-outdated-hacking-law-stalls [Accessed: May 23, 2025].
[9] CyberUp Campaign, "Campaign responds to withdrawal of amendment to update Computer Misuse Act," [Online]. Available: https://www.cyberupcampaign.com/news/campaign-responds-to-withdrawal-of-amendment-to-update-computer-misuse-act [Accessed: May 23, 2025].
[10] NCC Group, "Now is the time to CyberUp – making the Computer Misuse Act fit for the 21st century," [Online]. Available: https://www.nccgroup.com/uk/now-is-the-time-to-cyberup-making-the-computer-misuse-act-fit-for-the-21st-century/ [Accessed: May 23, 2025].
[11] NCC Group plc, "Securing our future," [Online]. Available: https://www.nccgroup.com/ [Accessed: May 23, 2025].
[12] TechWAN, "Germany's Justice Department Drafts Law to Protect White Hat Hackers from Criminal Liability for Security-Related Intrusions," [Online]. Available: https://landian.news/article/4059.html?utm_source=chatgpt.com [Accessed: May 23, 2025].
[13] F. Cremer et al., "Cyber risk and cybersecurity: a systematic review of data availability," The Geneva Papers on Risk and Insurance - Issues and Practice, vol. 47, no. 3, pp. 698–736, Feb. 2022, doi: 10.1057/S41288-022-00266-6.
[14] Meijers Canatan Advocates, "Criminal Lawyers Amsterdam," [Online]. Available: https://www.meijerscanatan.nl/en/ [Accessed: May 23, 2025].
[15] J. Vostoupal, V. Stupka, J. Harašta, F. Kasl, P. Loutocký, and K. Malinka, "The Legal Aspects of Cybersecurity Vulnerability Disclosure: To the NIS 2 and Beyond," SSRN, 2023, doi: 10.2139/SSRN.4640775.
[16] Mondaq, "Cybersecurity Comparative Guide - France," [Online]. Available: https://www.mondaq.com/france/technology/963020/cybersecurity-comparative-guide [Accessed: May 23, 2025].
[17] Council of Europe, "France - Octopus Cybercrime Community," [Online]. Available: https://www.coe.int/en/web/octopus/-/france [Accessed: May 23, 2025].
[18] International Comparative Legal Guides, "Cybersecurity Laws and Regulations - France," [Online]. Available: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france [Accessed: May 23, 2025].
[19] International Comparative Legal Guides, "Cybersecurity Laws and Regulations Report 2025 - France," [Online]. Available: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france [Accessed: May 23, 2025].
[20] Singapore Statutes Online, "Cybersecurity Act 2018," [Online]. Available: https://sso.agc.gov.sg/Acts-Supp/9-2018/ [Accessed: May 23, 2025].
[21] Crime Research Organization, "Internet law - fighting computer crime Singapore," [Online]. Available: https://www.crime-research.org/news/01.04.2008/3286/ [Accessed: May 23, 2025].
[22] C. Ayad, "Policing the Digital Sphere: The Impact of Palestine's Cybercrime Legislation," Arab Reform Initiative, Nov. 24, 2017. [Online]. Available: https://www.arab-reform.net/publication/policing-the-digital-sphere-the-impact-of-palestines-cybercrime-legislation/?tztc=1. Accessed: May 23, 2025.
[23] Human Rights Watch, "Palestine: Reform Restrictive Cybercrime Law," [Online]. Available: https://www.hrw.org/news/2017/12/20/palestine-reform-restrictive-cybercrime-law [Accessed: May 23, 2025].
[24] Kurdi & Co., "Cybersecurity Laws in Palestine," [Online]. Available: https://kurdi.law/cybersecurity-laws-in-palestine/ [Accessed: May 23, 2025].
[25] Law Gratis, "Cyber Law at Palestine," [Online]. Available: https://www.lawgratis.com/blog-detail/cyber-law-at-palestine? [Accessed: May 24, 2025].