Justitia Jurnal Hukum, Vol 10, Issue (2), 2026: 318-337
ISSN: P-2579-9983, E-ISSN: 2579-6380
DOI: https://doi.org/10.30651/justitia.v10i2.30250

Decriminalizing Ethical Hacking through Penal Policy Exemptions to Counter Transnational Cyber Crime

Moh. Abd. Rauf[1*], Naem Allahrakha[2]

[1] KH Achmad Siddiq Jember State Islamic University, Indonesia
[2] Tashkent State University of Law, Uzbekistan
*Corresponding author: m.abdrauf18@gmail.com

Article history
Received : January 11, 2026
Accepted : September 22, 2026
Published : October 01, 2026

Abstract

This study examines the critical failure of domestic cybersecurity legislation, highlighting how outdated penal provisions actively criminalize ethical security researchers and inadvertently assist transnational cybercriminal syndicates. The national digital defense model confronts a profound jurisprudential dilemma where broad statutory formulations of unauthorized access under Articles 30 through 36 of the Electronic Information and Transactions Law expose white-hat hackers to severe criminal liability. This normative legal research evaluates the dangerous regulatory ambiguity surrounding ethical hacking in Indonesia against advanced penal exemption frameworks used in global jurisdictions. Findings reveal that the Indonesian criminal justice system enforces strict liability for digital intrusions, completely failing to distinguish malicious cyberattacks from good-faith forensic vulnerability testing. This absence of mens rea evaluation creates a systemic chilling effect, paralyzing proactive digital defenses and actively deterring critical threat reporting. Achieving proportional penal protection requires comprehensive legislative reform that embeds a mandatory penal exemption doctrine for authorized digital forensics. The state must explicitly decriminalize ethical hacking, establish standardized vulnerability disclosure protocols, and implement a pretrial forensic audit mechanism to guarantee absolute legal immunity for researchers securing the national digital ecosystem.

Keywords: Cybercrime; Decriminalization; Mens Rea; Penal Policy; White Hat Hackers.

INTRODUCTION

Digital technology primarily drives socio-economic transformation while simultaneously introducing severe systemic threats that test national cybersecurity structures. International law enforcement reports indicate a dramatic 39% increase in cyberattacks across the Asia Pacific region, highlighting a growing vulnerability to transnational cybercrime. Indonesia occupies a precarious position within this landscape because rapid digital adoption severely outpaces the development of adequate cyber resilience. Official statistics record more than 212 million active internet users nationwide engaging in extensive e-commerce and electronic governance. This massive expansion proceeds without a corresponding enhancement in domestic, penal, and cybersecurity capacity, leaving numerous institutional entities permanently exposed to aggressive data breaches (Rampášek et al., 2026).

National Cyber and Crypto Agency data substantiates this insecure condition, recording approximately 1.2 billion attempted cyberattacks targeting governmental and financial sectors in a single year. These attacks predominantly exploit unpatched security vulnerabilities in critical digital systems operating under weak configurations. Organizations could identify and remediate many of these severe vulnerabilities at an earlier stage through the active engagement of ethical security researchers commonly known as white-hat hackers (Vostoupal et al., 2024). These skilled professionals have advanced technical expertise and voluntarily help identify security flaws before malicious actors exploit them. Their proactive forensic intervention serves as an essential first line of defense in protecting proprietary digital infrastructure and essential public services from transnational criminal syndicates.

The strategic contributions of white-hat hackers remain trapped in a profound jurisprudential failure within Indonesia's national penal model. Ethical hackers face the constant threat of arbitrary criminalization despite directing their actions exclusively toward enhancing public cybersecurity. Articles 30 through 36 of the Electronic Information and Transactions Law, along with Article 521 of the Indonesian Criminal Code, are the primary penal instruments invoked to prosecute unauthorized access. The overly broad statutory formulation of these provisions enforces a strict liability paradigm that completely fails to distinguish between actors operating with malicious intent or mens rea and security researchers conducting forensic audits in good faith. This legislative ambiguity causes legitimate defensive testing to be erroneously classified as criminal offenses, creating a severe chilling effect that leads researchers to refrain from reporting critical national vulnerabilities.

Empirical evidence demonstrates that early vulnerability disclosure mechanisms prevent approximately 78% of data breach incidents. Jurisdictions globally recognize this reality by implementing penal exemption policies and standardized reporting protocols to decriminalize ethical security research. The United States utilizes Digital Millennium Copyright Act provisions, while Singapore

enforces its Cybersecurity Act to protect ethical vulnerability discovery through explicit statutory safe harbors. Indonesia continues to lag significantly behind in establishing comparable protective legislative frameworks (Bellaby, 2023). The state must cultivate a supportive penal environment that empowers security actors operating in favor of the public interest rather than intimidating them through obsolete and vaguely drafted criminal statutes.

Existing academic literature reveals a significant research gap regarding this specific intersection of penal policy and digital security. Previous studies have not specifically analyzed the destructive conflict between Articles 30 through 36 of the Electronic Information and Transactions Law and Article 521 of the Criminal Code, which imposes unwarranted criminal liability on white-hat hackers. Prior studies have also failed to formulate a comprehensive penal exemption model based on comparative international decriminalization mechanisms. Addressing this fundamental jurisprudential deficiency requires a rigorous examination of the national penal model. This study analyzes the legal protection of white-hat hackers within the Indonesian regulatory system and proposes a mandatory penal exemption doctrine that uses a pretrial forensic audit mechanism to balance national cybersecurity imperatives with strict legal certainty.

Vostoupal analyzed the legal dimensions of cybersecurity vulnerability disclosure by examining legislative frameworks, including European directives (Vostoupal et al., 2024). Their study specifically investigated legal risks, including criminal, administrative, and civil liabilities, that security researchers routinely face during vulnerability identification. The authors emphasized the persistent absence of safe harbor protections across multiple jurisdictions and argued for explicit legislative interventions to shield ethical researchers from prosecution. This scholarly contribution aligns directly with discussions surrounding responsible disclosure protocols, bug bounty initiatives, legal immunity frameworks, and the systemic mitigation of criminalization risks.

Recent comparative research examined European legal frameworks to evaluate whether existing regulations adequately protect security researchers conducting vulnerability discovery and disclosure in good faith (Rampášek et al., 2026). The analysis focused primarily on criminal liability thresholds, safe harbor provisions, and coordinated vulnerability disclosure frameworks across diverse national jurisdictions. The findings showed that legal uncertainty remains a primary deterrent to security professionals sharing critical threat information with system owners. This European perspective reinforces the argument that the problems confronting white-hat hackers extend far beyond technical cybersecurity management into fundamental issues of legal certainty and criminal justice.

Foudil introduced the security protocol standard known as Request for Comments 9116, which establishes a standardized file format to aid in security

vulnerability disclosure (Foudil & Shafranovich, 2022). To address the recurring difficulty security researchers face in locating official reporting channels, this technical standard encourages organizations to publish standardized contact information and structured reporting procedures. Technical standardization complements legal protections by ensuring vulnerability discoveries follow safe, transparent communication pathways. This practical framework provides essential support for setting standardized vulnerability disclosure protocols as a core pillar of modern regulatory reform.

Existing academic literature reveals a distinct research gap at the intersection of domestic penal provisions and the absolute decriminalization of ethical hacking practices in developing digital economies. Prior studies have largely focused on Western regulatory models or technical mitigation strategies while neglecting the systemic penal failures created by broad unauthorized access statutes such as Articles 30 through 36 of the Electronic Information and Transactions Law and Article 521 of the Criminal Code. Moreover, academic inquiries have rarely examined how a comprehensive penal exemption doctrine integrating absolute legal immunity, standardized disclosure protocols, and pretrial forensic audit mechanisms can be operationalized within a developing national legal system to counter transnational cybercrime. Addressing this profound scholarly void requires a dedicated investigation into how to harmonize national penal models with international best practices on decriminalization.

This study analyzes the unwarranted criminalization of white-hat hackers within the Indonesian regulatory framework and proposes a mandatory penal exemption doctrine that balances national cybersecurity imperatives with strict legal certainty. The research evaluates domestic statutory ambiguities and strict-liability paradigms alongside comparative international decriminalization mechanisms to develop a comprehensive penal policy reform strategy. By bridging the gap between forensic vulnerability disclosure protocols and formal penal immunity, the study provides actionable policy recommendations to safeguard ethical security researchers and strengthen national digital resilience against escalating global cyber threats.

METHODS

This study employs a normative juridical research methodology to systematically analyze legal norms, foundational penal principles, and the harmonization of positive law relevant to the decriminalization of white-hat hackers (Marzuki, 2019). This methodological framework identifies legislative gaps in the national penal structure and explores adaptive models of penal exemption by evaluating international decriminalization best practices. The research uses three distinct analytical approaches. The statutory approach examines primary legislative products governing electronic systems and criminal liability paradigms. The

conceptual approach evaluates core penal doctrines related to ethical hacking, mens rea evaluation, and strict legal certainty. The comparative approach analyzes penal exemption frameworks and forensic vulnerability disclosure protocols adopted in foreign jurisdictions.

Data collection is conducted through comprehensive library-based research, compiling and examining primary, secondary, and tertiary legal materials. Primary legal materials consist of binding statutory regulations, including Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 27 of 2022 concerning Personal Data Protection, alongside official regulatory guidelines issued by the National Cyber and Crypto Agency. Secondary legal materials comprise scholarly journal articles, authoritative books on cyber law, academic research reports, and conference proceedings discussing international penal policy, criminal liability, and forensic ethical hacking. Tertiary legal materials include legal dictionaries and standard reference works to support precise penal interpretation (Efendi, 2022).

Legal materials were collected through a rigorous process of identification, classification, and systematic review of relevant sources. The collected materials were analyzed using qualitative legal analysis through statutory interpretation, conceptual analysis, and comparative legal reasoning. This process identifies normative ambiguities and inconsistencies in existing penal provisions, particularly the broad definition of illegal access, which exposes security researchers to unwarranted criminalization risks under a strict liability paradigm (Rizkia & Fardiansyah, 2023). Comparative insights derived from foreign jurisdictions were examined to extract adaptive penal exemption elements that can be adjusted to the domestic legal context. The final analytical findings provide the foundation for formulating a comprehensive mandatory penal exemption doctrine that balances national cybersecurity protection with strict legal certainty for all relevant stakeholders and secures the digital ecosystem against transnational cybercrime.

RESULT AND DISCUSSION

Transnational Cybercrime and the Urgency of Forensic Digital Defense

The contemporary digital era is marked by an unprecedented acceleration of technological integration across all sectors of global society. Digital transformation is a primary driver of profound socio-economic advancement while simultaneously generating highly complex criminogenic vulnerabilities (Fiorinelli & Zucca, 2024). The exponential growth of cross-border digital connectivity creates expansive attack surfaces that transnational cybercriminal syndicates aggressively exploit. Modern cyber threats have evolved from isolated individual activities into highly organized, industrial-scale operations capable of crippling critical national infrastructure.

International law enforcement agencies continuously monitor this escalating threat matrix to understand shifting global attack patterns. The 2024 INTERPOL report reveals an alarming reality for regional digital security, documenting a 39% increase in sophisticated cyberattacks across the Asia Pacific region. This statistical surge demonstrates the growing attractiveness of emerging digital economies as primary targets for malicious cyber syndicates operating beyond traditional jurisdictional boundaries. The Asia Pacific region experiences this massive escalation because rapid technological adoption often outpaces the development of robust legal and technical defenses.

Indonesia occupies a highly precarious position within this volatile regional threat landscape. The nation shows an exceptionally high rate of digital technology adoption, driven by its large population and aggressive economic digitalization strategies (Spyropoulos, 2025). The 2023 report published by the Indonesian Internet Service Providers Association confirms this reality, recording an active user base of more than 212 million individuals nationwide. This monumental demographic shift reflects rapid systemic digitalization encompassing critical sectors including government administration, digital banking, public education, and sprawling e-commerce networks. This rapid digital expansion proceeds without a corresponding, comprehensive strengthening of domestic cybersecurity capacity and penal deterrence. This structural imbalance between widespread technological reliance and weak forensic defense capabilities creates severe systemic vulnerabilities. Transnational cybercriminals readily exploit this developmental gap to launch devastating attacks against underprepared institutional targets. The national drive toward comprehensive digital governance and financial inclusion inadvertently widens the attack surface for malicious actors seeking financial extortion or unauthorized data acquisition (Bozzini, 2025).

Empirical evidence of this severe national vulnerability emerges directly from official state monitoring authorities. The National Cyber and Crypto Agency recorded approximately 1.2 billion attempted cyberattacks targeting vital government and financial sectors in 2022. This staggering volume of malicious cyber activity underscores the relentless pressure placed upon national digital infrastructure by global criminal enterprises. An analysis of these attack patterns shows that malicious actors largely succeed by exploiting known, unpatched security vulnerabilities. Many institutional electronic systems run on outdated software architecture or operate with fundamentally weak security configurations. Bureaucratic inefficiencies and severe budgetary constraints often delay the timely implementation of critical security patches across sprawling institutional networks. These delayed administrative responses provide malicious syndicates with expansive temporal windows to penetrate sensitive databases. Systemic failures to maintain rigorous forensic hygiene

turn routine technical oversights into catastrophic organizational vulnerabilities that threaten national data sovereignty.

Traditional cybersecurity paradigms that rely exclusively on static perimeter defenses prove profoundly inadequate against modern, sophisticated threat vectors. Institutional Information Technology departments often operate under severe resource constraints and struggle to maintain continuous surveillance across increasingly complex digital ecosystems (Kumar, 2024). The inherent asymmetry of cyber warfare places defensive teams at a permanent structural disadvantage. Defensive architectures must flawlessly protect every node within an expansive network, while attackers need only discover one unpatched vulnerability to achieve total system compromise. This asymmetric reality dictates that passive defensive strategies can no longer guarantee organizational security against transnational extortion. Institutions must transition toward proactive threat intelligence and continuous, aggressive forensic vulnerability discovery. Relying solely on internal security audits proves insufficient because internal teams often suffer from systemic operational blindness regarding their own network models. External independent perspectives remain absolutely vital for identifying hidden logical flaws and complex configuration errors that internal developers routinely overlook during the software deployment lifecycle (Walshe & Simpson, 2022).

Cultivating a proactive defense ecosystem requires integrating specialized human capital with advanced forensic technical capabilities. Ethical security researchers, commonly known as white-hat hackers, constitute an indispensable strategic resource for building resilient national digital infrastructure. These highly skilled professionals voluntarily or professionally use advanced penetration testing methods to identify critical system flaws before malicious actors can exploit them. Their specialized technical interventions serve as a crucial first line of penal defense in detecting and mitigating severe cyber threats. White-hat hackers simulate the same methods used by malicious syndicates to expose hidden vulnerabilities without malicious intent or operational harm. This proactive vulnerability identification allows organizations to implement robust remediations and permanently seal attack vectors. Strategically deploying ethical hackers effectively neutralizes the asymmetric advantage cybercriminals traditionally enjoy (Walshe & Simpson, 2023).

Many public and private organizations lack the internal technical capacity to autonomously execute comprehensive forensic vulnerability discovery across their sprawling digital assets. The specialized skill sets required for advanced penetration testing remain scarce and highly expensive within the conventional labor market. Engaging the broader ethical hacking community through collaborative security initiatives provides institutions with scalable access to elite global cybersecurity talent. In the absence of such proactive collaborative involvement, numerous critical vulnerabilities remain deeply concealed within institutional networks. These hidden

flaws inevitably remain dormant until transnational black-hat hackers eventually discover and exploit them. Successful malicious exploitation triggers cascading organizational failures, resulting in substantial financial losses, irreversible reputational damage, and severe disruptions to essential public services (Xiong et al., 2023). Protecting national critical information infrastructure requires active participation from the independent forensic research community.

Maximizing the strategic potential of the ethical hacking community requires a supportive, legally secure operational environment grounded in progressive penal policy. Indonesia must actively facilitate the existence and specialized role of white-hat hackers through a clear regulatory framework providing absolute legal immunity. Ethical researchers must feel entirely secure from the threat of arbitrary prosecution when conducting good-faith vulnerability discovery. A robust national cyber defense model cannot rely solely on hardware or software solutions. Human intelligence and collaborative forensic engagement represent the ultimate deciding factors in securing complex digital ecosystems against relentless malicious intrusion. Building this collaborative ecosystem requires harmonizing technical security imperatives with progressive penal policies designed to protect individuals acting in the public interest (Zhao et al., 2023).

The ongoing escalation of unmitigated cyber threats creates profound socio-economic consequences for Indonesia's developing digital economy. Frequent data breaches compromise millions of citizens' sensitive personal information and systematically erode public trust in electronic governance initiatives. The financial sector faces immense operational risks as sophisticated ransomware syndicates target critical banking infrastructure and payment gateways. Disruptions to these digital financial arteries immediately paralyze the economy and deter vital foreign direct investment. Global investors demand rigorous data protection standards and stable digital infrastructure before committing capital to emerging markets. The inability to secure domestic digital platforms directly undermines broader national economic development strategies. Recognizing cybersecurity as a fundamental pillar of macroeconomic stability requires elevating proactive vulnerability management to the top-level national penal policymaking.

In the Indonesian context, digital vulnerability extends beyond technical software flaws to include deep structural deficiencies in organizational security culture. Many institutions approach cybersecurity as a secondary administrative compliance requirement rather than a core operational necessity designed to thwart cybercrime (Li & Zhao, 2022). This reactive mindset leads to chronic underinvestment in advanced threat detection capabilities and ongoing forensic security training. Employees often lack the digital literacy needed to spot sophisticated social engineering attacks or even basic phishing campaigns. Technical vulnerabilities multiply exponentially when combined with a widespread organizational failure to

prioritize fundamental cyber hygiene. Addressing this multifaceted vulnerability matrix requires a holistic transformation of institutional security cultures alongside the active deployment of external ethical hacking resources (Zrahia et al., 2024).

The massive scale of the contemporary cyber threat landscape dictates an immediate paradigm shift in national digital governance and penal enforcement. The recorded billions of attempted intrusions underscore a permanent state of low-intensity digital conflict targeting Indonesian infrastructure. Relying on outdated reactive security models virtually guarantees eventual catastrophic system failure and compromises national sovereignty. The state must aggressively mobilize all available defensive resources to confront this relentless external pressure. The independent ethical hacking community represents a highly potent yet severely underutilized forensic asset in this ongoing digital struggle. Integrating their advanced technical capabilities into the national defense architecture provides the most viable strategy for identifying and neutralizing systemic vulnerabilities before they trigger massive socio-economic damage. This strategic integration absolutely requires dismantling the existing structural and penal barriers that currently prevent security researchers from safely contributing to the national interest.

Strict Liability and the Criminalization of Forensic Audits

The fundamental jurisprudential failure in providing penal protection for white-hat hackers in Indonesia lies in the severe ambiguity and systemic overgeneralization of existing statutory provisions. Articles 30 through 36 of the Law on Electronic Information and Transactions, alongside Article 521 of the Indonesian Criminal Code, constitute the primary penal instruments utilized by law enforcement to prosecute cyber offenses. These legislative texts use overly broad terminology to define the core parameters of illegal access or unauthorized system intrusion. The statutory language completely fails to explicitly distinguish between destructive acts carried out with malicious intent and forensic defensive actions performed in good faith by cybersecurity researchers (Sridhar & Ng, 2021). This structural legislative failure means that activities fundamentally intended to strengthen digital systems face an extremely high risk of being classified as serious criminal offenses. Routine defensive methodologies, including advanced penetration testing and comprehensive vulnerability assessments, technically fulfill the formal material elements of unauthorized access under the current rigid textual interpretation of the law (Barre, 2025).

The ambiguity surrounding the exact legal definition of illegal access represents the principal source of normative uncertainty threatening the ethical hacking community. Indonesian positive law provides no clear penal criteria for which specific forms of unauthorized digital access might be ethically or professionally justified in the context of national security. The existing regulatory

model lacks any formal recognition of industry-standard forensic security practices such as responsible vulnerability disclosure. The state provides no penal exemption framework designed to accommodate or protect voluntary penetration testing conducted entirely in the public interest. This regulatory loophole dangerously blurs the legal boundary between legitimate forensic security efforts and unlawful cybercrime. Individuals possessing advanced cybersecurity expertise who act with benevolent intentions face a profound dilemma. The rigid application of these broad statutes can turn highly skilled digital defenders into potential criminal suspects simply for interacting with vulnerable public or private networks.

The tangible real-world consequences of this absolute lack of legal clarity manifest clearly through several disturbing cases involving the direct criminalization of well-intentioned security researchers across Indonesia. One prominent and highly damaging example occurred in 2021, when a dedicated cybersecurity researcher identified a critical vulnerability in an official e-government application. The researcher followed ethical protocols by reporting the discovered system flaw directly to the relevant administrative authorities. The institutional response completely ignored the benevolent forensic nature of the intervention. The government agency immediately reported the researcher to law enforcement authorities, resulting in criminal charges for illegal access (Plantin & Hurel, 2025). The researcher faced severe legal prosecution despite acting with a clear, demonstrable intention to help the state remedy a dangerous system weakness. This case established a deeply troubling legal precedent, revealing major deficiencies in digital literacy among state administrators and law enforcement personnel. The aggressive prosecution exposed severe regulatory weaknesses in how the state addresses the increasingly complex dynamics of modern cyber threats.

The immediate psychological impact of this aggressive penal uncertainty is a critical vulnerability within the broader context of national cybersecurity. The persistent threat of arbitrary prosecution generates a massive chilling effect, paralyzing the entire ethical hacking community. This sociological phenomenon refers to a debilitating condition where white-hat hackers and independent security researchers actively refrain from participating in vulnerability reporting due to well-justified fears of criminalization. The apprehension gripping the security community remains entirely well-founded because empirical cases demonstrate that even ethically motivated actions routinely result in severe criminal sanctions. The lack of clear statutory distinctions between good-faith research and malicious hacking leaves technical experts exposed to unpredictable penalties. Skilled professionals deliberately choose silence over civic duty to avoid catastrophic personal and professional ruin. Unreported vulnerabilities remain actively deployed within critical public networks and silently await discovery by sophisticated transnational cybercriminal syndicates (Green et al., 2024).

The ethical hacking community's active contribution is indispensable for early detection and proactive prevention of massive data breaches. A comprehensive study published by the European Union Agency for Cybersecurity explicitly indicates that early vulnerability disclosure mechanisms could successfully prevent approximately 78% of all recorded data breach incidents. This powerful statistical evidence underscores that the active involvement of white-hat hackers is not merely an optional administrative benefit but an absolute necessity for building and strengthening national cyber resilience. The widespread chilling effect directly sabotages this vital defensive mechanism by effectively silencing the most capable forensic digital defenders operating within the nation (Ahmed et al., 2021). The state unintentionally protects malicious actors by intimidating the very individuals possessing the technical capability to expose hidden systemic flaws. Cultivating a supportive, enabling penal environment that empowers security actors operating in the public interest is a fundamental sovereign imperative, not a trivial regulatory adjustment.

Analyzing this dilemma from the perspective of criminal law theory reveals a serious conflict between formal legal compliance and substantive material justice. The Indonesian criminal justice system often applies the principle of legality in a highly rigid, purely formalistic manner in cyber offenses. Law enforcement agencies focus exclusively on whether a security researcher technically bypassed a digital barrier or accessed an electronic system without explicit prior administrative authorization. This formalistic approach completely ignores the fundamental criminal law doctrine of material unlawfulness. An act should not be considered a crime if it causes no societal harm and serves substantial public benefit. Ethical hacking interventions specifically intended to secure critical national infrastructure against malicious exploitation inherently lack this vital element of material unlawfulness (Savaş & Karataş, 2022). The current statutory framework fails to provide judges and prosecutors with appropriate doctrinal tools to evaluate the underlying intent and the ultimate societal benefit of responsible vulnerability disclosure.

Modern criminal jurisprudence universally recognizes that imposing severe penal sanctions requires the definitive establishment of malicious intent, or mens rea. Indonesian cyber legislation's complete failure to distinguish between benevolent forensic security auditing and malicious data theft represents a critical regression in penal theory. The mental element of a crime constitutes the fundamental dividing line between a dedicated public servant and a dangerous digital criminal. When the state rigidly prosecutes ethical hackers based solely upon the technical actus reus of system penetration, it essentially criminalizes intellectual curiosity and civic responsibility. This strict liability approach to cyber intrusions fundamentally contradicts the progressive evolution of modern criminal justice. Evaluated against established international legal standards, the Indonesian framework appears obsolete and ill-

suited to govern the complex realities of the twenty-first-century digital ecosystem (Del-Real & Díaz-Fernández, 2022).

The ongoing criminalization of ethical hacking actively degrades national strategic positioning in an increasingly hostile global digital landscape. The state must clearly distinguish between malicious hacking that causes actual harm and forensic cybersecurity practices grounded in professional ethics and positive intent. Integrating specific penal exemptions for defensive practices into the national regulatory framework is urgent; it is not a distant legislative goal. Without adaptive penal reform, this country risks losing strategic, highly valuable cybersecurity human resources. Frustrated security professionals often move to foreign jurisdictions offering robust legal protections and lucrative operational environments for ethical research. This massive brain drain strips the nation of critical technical expertise exactly when domestic institutional networks face unprecedented levels of external cyber aggression. Falling further behind in confronting the continuously evolving escalation of global cyberattacks guarantees devastating long-term consequences for the national digital economy.

Ambiguity in unauthorized access provisions also directly threatens the viability of emerging collaborative security initiatives. Several government agencies and progressive private sector entities have cautiously begun experimenting with bug bounty programs designed to incentivize ethical vulnerability reporting. The broad phrasing of both the Electronic Information and Transactions Law and Article 362 of the Indonesian Criminal Code leaves a major legal risk for any individual participating in these formal programs (Janovec, 2025). Laws regarding the taking of another person's property can be interpreted broadly to include unauthorized forensic access to proprietary electronic data. Independent researchers participating in officially sanctioned bug bounty initiatives continue operating entirely within a perilous legal grey area. A sudden shift in institutional leadership or a misunderstanding by internal legal departments can instantly transform an authorized security test into a devastating criminal complaint. This persistent structural risk severely limits the effectiveness and scalability of all domestic vulnerability discovery programs.

Securing the national digital frontier absolutely requires dismantling these obsolete penal ambiguities (Kianpour & Raza, 2024). The legislative branch must urgently modernize the statutory definition of illegal access to explicitly include authorized security research and good-faith vulnerability disclosure. Statutory language must demand concrete proof of malicious intent or demonstrable material harm before triggering criminal prosecution for cyber intrusions. Eliminating the pervasive chilling effect demands a definitive legal guarantee that ethical researchers will face no arbitrary retaliation for fulfilling their civic duty to protect public infrastructure. Transforming white-hat hackers from potential criminal suspects into

legally protected strategic partners is the only viable way to secure complex institutional networks against sophisticated external threats. The survival of the Indonesian digital ecosystem depends entirely on replacing the current environment of legal intimidation with a progressive framework of collaborative forensic cyber defense.

Penal Gaps and the Mandatory Pretrial Forensic Audit Doctrine

An in-depth analysis of Indonesian cyber law doctrines reveals three fundamental penal gaps that significantly impede comprehensive protection and the strategic empowerment of ethical hackers. These structural deficiencies severely paralyze proactive digital defense mechanisms and demand immediate comprehensive penal policy reform. The first major gap is the lack of an operational definition of forensic ethical hacking in national statutory legislation. Failing to establish precise legal boundaries creates immense systemic confusion during regulatory enforcement (Dizon & Upson, 2021). Distinguishing forensic actions performed in good faith to enhance system security from malicious hacking activities, defined as mens rea, becomes practically impossible for law enforcement authorities. This definitional gap forces numerous cybersecurity activities with inherently beneficial, defensive characteristics to operate under the constant threat of criminalization. The lack of explicit statutory recognition restricts the operational movement of ethical security researchers while actively suppressing vital technological findings across the domestic cybersecurity ecosystem.

The second critical legal deficiency centers on the total absence of formal penal exemption granting absolute legal immunity to individuals or entities that responsibly report system vulnerabilities. The lack of explicit decriminalization safeguards directly discourages security researchers from discovering and disclosing network vulnerabilities. Technical experts fear arbitrary criminal prosecution under broad penal provisions related to illegal access or electronic system interference despite operating with strictly benevolent intentions. Vulnerability disclosure transforms into an inherently high-risk activity in the absence of robust penal protection. This precarious legal environment systematically undermines collective national efforts to improve digital resilience. Security professionals deliberately withhold critical threat intelligence to avoid devastating legal retaliation from defensive corporate or governmental system operators (Snail ka Mtuze & Musoni, 2023).

The third major structural gap is the Indonesian state's failure to establish integrated national protocols governing responsible forensic vulnerability disclosure. Responsible disclosure is a crucial procedural framework that dictates how independent researchers must communicate discovered vulnerabilities to system owners securely and ethically. These standardized protocols are absolutely vital for establishing basic operational transparency and mitigating severe conflicts between

external security researchers and internal system operators. The current lack of standardized, official protocols often causes catastrophic miscommunication and dangerous misinterpretation of technical motives. Initial vulnerability reports routinely escalate into hostile legal disputes because system owners mistakenly perceive benevolent security warnings as aggressive extortion attempts or preliminary cyberattacks. Without a secure, legally recognized reporting channel, well-intentioned hackers remain vulnerable to institutional hostility and unwarranted criminal charges.

Addressing these profound structural deficiencies requires looking beyond domestic legal paradigms to examine successful penal policy frameworks implemented across progressive foreign jurisdictions. Several nations recognize the indispensable strategic role of ethical hackers in strengthening national cybersecurity models by actively adopting comprehensive statutory penal exemptions. These legal mechanisms explicitly protect individuals who conduct system testing or report vulnerabilities in good faith from arbitrary criminal prosecution. The United States provides a powerful comparative example through Section 1201 of the Digital Millennium Copyright Act by granting specific legal exemptions for security research and ethical system testing. This progressive penal approach encourages active engagement from the independent cybersecurity community by entirely removing the fear of criminal sanction. Singapore implements an equally progressive approach through the Cybersecurity Act 2018, which establishes highly standardized protocols for official vulnerability reporting. This official governmental channel ensures responsible reporting while guaranteeing timely technical follow-up by relevant state authorities (Schaffer et al., 2023).

These international examples show that adequate regulatory support allows a nation to mobilize ethical hackers as invaluable strategic partners in building a resilient digital ecosystem. Indonesia has tentatively begun experimenting with bug bounty programs as a proactive measure to identify network vulnerabilities. Initiatives led by the National Cyber and Crypto Agency, alongside private-sector organizations, aim to encourage ethical hackers to identify and report systemic flaws. These initial programmatic efforts remain highly fragmented and completely lack a solid statutory foundation. Participation in such programs exists entirely in a terrifying legal grey area because explicit statutory authorization for bug bounty practices is completely absent from Indonesian positive law. Broad textual interpretations allow law enforcement to charge program participants under Article 362 of the Indonesian Criminal Code concerning the unlawful taking of property. This pervasive legal uncertainty places participating ethical hackers at massive personal risk despite their vital contributions to public interest.

Closing these three identified legal gaps requires a comprehensive reformulation of penal policy. Establishing a highly effective regulatory framework

for modern cybersecurity cannot be undertaken unilaterally by the state apparatus. Achieving a sustainable and balanced legal ecosystem requires comprehensive harmonization among multiple strategic stakeholders encompassing government institutions, active cybersecurity communities, and major industry associations. This reality demands the rapid implementation of a collaborative penal exemption framework jointly formulated by the state and civil society. This collaborative model is vastly superior to a rigid, state-centric approach that relies entirely on bureaucratic government initiative. Multi-stakeholder penal policy offers greater flexibility to respond to rapid technological advancements while strengthening the regulatory framework's substantive legitimacy through active expert participation. Involving non-state actors in the complex rule-making process helps ensure the resulting regulations remain adaptive and can foster an inclusive cybersecurity ecosystem.

The proposed adaptive penal exemption model is intended to achieve a proportional balance between urgent national cybersecurity requirements and the fundamental constitutional principle of legal certainty. This comprehensive framework is constructed upon three core programmatic pillars designed to optimize the strategic potential of white-hat hackers (van Daalen, 2022). The first and absolutely most critical pillar involves profoundly amending the Electronic Information and Transactions Law while aggressively accelerating the enactment of the comprehensive Cybersecurity and Resilience Bill. This foundational legislative reform must explicitly define forensic ethical hacking in positive law to permanently distinguish legitimate security testing from malicious cybercriminal conduct. The revised statutory definition must set clear, rigid parameters that specify what constitutes unauthorized access in the context of ethical hacking. The legislation must explicitly declare that pre-authorized penetration testing or responsible vulnerability disclosure conducted in good faith should never be classified as criminal activity. Incorporating the fundamental principle of benevolent intent, or mens rea, as a key determinant of cyber criminality provides the ultimate penal protection for dedicated security researchers.

The second strategic pillar of the proposed model mandates the immediate national standardization of forensic vulnerability disclosure protocols. The government must empower the National Cyber and Crypto Agency alongside the Ministry of Communication and Digital Affairs to formulate comprehensive official protocols governing every phase of vulnerability reporting. These national protocols must provide accessible, highly structured guidelines for white-hat hackers on how to report technical vulnerabilities (Maurushat & Nguyen, 2022). The guidelines must meticulously specify the appropriate institutional contact points and the critical technical information required to ensure efficient remediation. Establishing secure, heavily encrypted communication platforms is essential for transmitting highly sensitive vulnerability data without risking catastrophic interception by malicious actors. The standardized protocol must also impose a strict, systematic timeline,

compelling system owners to swiftly verify and address reported vulnerabilities. Maintaining absolute confidentiality during the remediation window prevents premature exploitation by malicious syndicates. This pillar also requires integrating formal recognition mechanisms, including national hall of fame programs, to appropriately recognize white-hat hackers who contribute to public security.

The third and final pillar focuses entirely upon establishing a robust multi-stakeholder collaboration mechanism designed to guarantee absolute penal immunity. Implementing a comprehensive decriminalization framework requires structured operational schemes involving both state and private actors. Organizations must proactively issue explicit written pre-authorization to white-hat hackers, inviting them to conduct security assessments under legally binding clauses that provide full liability protection. Government institutions and private entities must rapidly expand official bug bounty programs under a unified national legal framework, ensuring absolute protection for compliant researchers. The national legislature must incorporate a dedicated good-faith clause directly into primary statutory regulations. This specific clause must explicitly state that individuals conducting hacking activities for legitimate security research purposes shall enjoy absolute immunity from all criminal sanctions (Zhao et al., 2024).

The establishment of an independent Pretrial Forensic Audit Board introduces a profound structural safeguard into the national criminal justice apparatus. Evaluating complex cyber intrusions frequently demands an extraordinary level of technical comprehension that traditional prosecutors and judges simply do not possess. Law enforcement personnel routinely struggle to distinguish between a sophisticated malicious data extraction attempt and a highly technical vulnerability demonstration conducted purely for defensive purposes. The Forensic Audit Board bridges this massive epistemological gap by functioning as a mandatory expert mediator during the preliminary investigation phase of any cybercrime allegation involving an unauthorized access charge. Before police investigators can officially elevate a security researcher to the status of a criminal suspect, the law would require the Forensic Board to conduct a comprehensive technical and ethical review of the incident (Chen & van der Ham-de Vos, 2026). The council would rigorously evaluate the researcher's underlying intent alongside the specific technical methodologies employed and the potential societal benefit of the disclosure. This mandatory expert intervention prevents ambitious prosecutors from destroying the lives and careers of brilliant young technologists based upon fundamental misunderstandings of actus reus and mens rea within complex network structures.

Implementing this comprehensive three-pronged penal exemption model guarantees profound macroeconomic benefits for the entire Indonesian digital ecosystem. Eradicating the fear of arbitrary criminalization directly incentivizes the rapid growth of a massive domestic cybersecurity talent pool. Brilliant technologists

will choose to stay in the country and contribute their invaluable skills to securing national critical infrastructure rather than fleeing to other countries that offer stronger legal protections. A legally secure domestic environment fosters the aggressive expansion of local cybersecurity startups and specialized technical consultancies. Global investors rigorously evaluate the baseline digital security of emerging markets before committing substantial capital to massive technological infrastructure projects. Demonstrating a progressive, legally sophisticated approach to vulnerability management signals to the international community that Indonesia is a safe, highly stable destination for advanced digital investment. The active normalization of ethical hacking transforms a previously marginalized subculture into a highly respected professional pillar of the modern national economy. Securing the boundless potential of the digital future absolutely requires fully empowering the dedicated individuals possessing the unique capability to defend it.

CONCLUSION

The Indonesian cybersecurity framework confronts a profound jurisprudential failure that actively undermines national digital resilience by failing to protect well-intentioned security researchers. The excessively broad formulation of unauthorized access under Articles 30 through 36 of the Electronic Information and Transactions Law and Article 521 of the Indonesian Criminal Code exposes ethical hackers to severe, unwarranted criminal liability under a strict-liability paradigm. The statutory language entirely fails to distinguish between malicious cyber intrusions driven by criminal intent and benevolent forensic vulnerability testing conducted strictly in the public interest. This severe legislative ambiguity generates a massive chilling effect, paralyzing the ethical hacking community and deterring the critical reporting of systemic digital flaws. The nation continues to lose vital forensic defense resources while sophisticated transnational cybercriminal syndicates relentlessly exploit unpatched vulnerabilities across critical governmental and financial infrastructure.

Addressing this precarious situation requires an immediate shift from rigid, formalistic criminalization to a progressive strategy of mandatory penal exemptions. The structural analysis reveals three major penal gaps: no statutory definition of forensic ethical hacking, no penal immunity mechanisms, and no integrated vulnerability disclosure protocols. Bridging these critical deficiencies requires a comprehensive penal policy framework that aligns national cybersecurity imperatives with clear legal certainty. The legislative branch must urgently amend existing cyber laws and accelerate the enactment of the Cybersecurity and Resilience Bill to explicitly recognize good-faith security research. The revised statutory framework must require concrete proof of malicious intent, or mens rea, before triggering criminal prosecution for electronic system intrusions.

The state must also standardize forensic vulnerability disclosure procedures through the National Cyber and Crypto Agency to ensure safe, transparent communication channels between independent researchers and institutional system operators. Securing the overarching digital ecosystem requires robust statutory penal exemptions and liability protections. Expanding official bug bounty programs alongside explicit statutory good-faith clauses provides the legal protection needed for proactive vulnerability discovery. Establishing an independent Pretrial Forensic Audit Board will prevent arbitrary prosecution by ensuring technical experts evaluate the underlying intent of complex cyber incidents before law enforcement initiates formal criminal proceedings. Adopting this adaptive penal exemption framework will transform white-hat hackers from potential criminal suspects into legally protected strategic partners who can permanently secure the Indonesian digital economy against escalating global threats.

ACKNOWLEDGMENTS

The authors express their profound gratitude to the KH Achmad Siddiq Jember State Islamic University and the Tashkent State University of Law for providing the essential institutional support and academic resources necessary to conduct this comprehensive legal and penal policy research. Special appreciation is directed toward the National Cyber and Crypto Agency and the Ministry of Communication and Digital Affairs for their invaluable insights regarding national digital defense strategies and forensic vulnerability disclosure frameworks. The researchers also extend their sincere thanks to the anonymous reviewers and the editorial board of Justitia Jurnal Hukum for their rigorous intellectual critiques that significantly elevated the substantive depth and analytical precision of this manuscript.

REFERENCES

Ahmed, A., Deokar, A., & Lee, H. C. B. (2021). Vulnerability disclosure mechanisms: A synthesis and framework for market-based and non-market-based disclosures. *Decision Support Systems*, *148*, 113586.

Barre, G. (2025). From breakers to builders: The role of bug bounty hunters in strengthening organizational cybersecurity. *Information*, *16*(3), 209.

Bellaby, R. W. (2023). An ethical framework for hacking operations. In *The Ethics of Hacking* (pp. 32–52). Bristol University Press.

Bozzini, D. (2025). The regimes of ethical hacking: moral projects and the emergence of a market for vulnerability. *Information, Communication & Society*, 1–18.

Chen, T.-H., & van der Ham-de Vos, J. (2026). Vulnerability disclosure or notification? best practices for reaching stakeholders at scale. *Digital Threats: Research and Practice*, *7*(1), 1–20.

Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. *International Cybersecurity Law Review*, *3*(2), 313–343.

Dizon, M. A. C., & Upson, P. J. (2021). Laws of encryption: An emerging legal framework. *Computer Law & Security Review*, *43*, 105635.

Efendi, J. (2022). *Metode Penelitian Hukum Normatif dan Empiris Edisi Kedua*. Prenada Media.

Fiorinelli, G., & Zucca, M. V. (2024). Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU. *CEUR WORKSHOP PROCEEDINGS*, *3731*, 1–16.

Foudil, E., & Shafranovich, Y. (2022). *Rfc 9116: A file format to aid in security vulnerability disclosure*. RFC Editor.

Green, A. W., Oliver, D., & Woszczynski, A. B. (2024). To report or not to report? Extending protection motivation theory to vulnerability discovery and disclosure. *Computers & Security*, *142*, 103880.

Janovec, A. (2025). Regulatory Security Governance at the National State Level: Is Cybersecurity Governed by Experts? *International Review of Public Policy*, *7*(7: 3).

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, *5*(1), 169–212.

Kumar, J. (2024). Legal Protection To Ethical Hacking In India (Current Scenario and Way Ahead). *Available at SSRN 4912640*.

Li, Y., & Zhao, L. (2022). Collaborating with bounty hunters: how to encourage white hat hackers' participation in vulnerability crowdsourcing programs through formal and relational governance. *Information & Management*, *59*(4), 103648.

Marzuki, P. M. (2019). *Penelitian Hukum* (Cetakan Ke). Kencana.

Maurushat, A., & Nguyen, K. (2022). The legal obligation to provide timely security patching and automatic updates. *International Cybersecurity Law Review*, *3*(2), 437–465.

Plantin, J.-C., & Hurel, L. M. (2025). The platformization of cybersecurity: uncovering articulation work in bug bounty platforms. *Information, Communication & Society*, 1–14.

Rampášek, M., Andraško, J., Sokol, P., & Hamulak, O. (2026). Hunting for vulnerabilities: call for European protection of security researchers. *Journal of Cybersecurity*, *12*(1), tyag002.

Rizkia, N. D., & Fardiansyah, H. (2023). *METODE PENELITIAN HUKUM (NORMATIF DAN EMPIRIS)*. Penerbit Widina. https://books.google.co.id/books?id=2X1JEQAAQBAJ

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*,

3(1), 7–34.

Schaffer, K. B., Schaffer, K. B., Mell, P., Trinh, H., & Van Wyk, I. (2023). *Recommendations for federal vulnerability disclosure guidelines*. US Department of Commerce, National Institute of Standards and Technology.

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299–323.

Spyropoulos, F. (2025). Technoethics and hackers in a 'hybrid'world: thoughts in the light of digital criminology. *Journal of Cyber Policy*, *10*(1), 34–50.

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity*, *7*(1), tyab007.

van Daalen, O. (2022). In defense of offense: information security research under the right to science. *Computer Law & Security Review*, *46*, 105706.

Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P., & Malinka, K. (2024). The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. *Computer Law & Security Review*, *53*, 105988.

Walshe, T., & Simpson, A. (2023). Towards a greater understanding of coordinated vulnerability disclosure policy documents. *Digital Threats: Research and Practice*, *4*(2), 1–36.

Walshe, T., & Simpson, A. C. (2022). Coordinated vulnerability disclosure programme effectiveness: Issues and recommendations. *Computers & Security*, *123*, 102936.

Xiong, Q., Lian, S., Zeng, Z., He, R., Zhu, B., & Yang, X. (2023). An empirical analysis of vulnerability information disclosure impact on patch R&D of software vendors. *Journal of Intelligent & Fuzzy Systems*, *44*(1), 839–853.

Zhao, L., Yu, X., & Zhou, X. (2023). The impact of regulatory mechanisms on vulnerability disclosure behavior during crowdsourcing cybersecurity testing. *Electronic Research Archive*, *31*(11), 1.

Zhao, L., Yu, X., & Zhou, X. (2024). Regulatory mechanism of vulnerability disclosure behavior considering security crowd-testing: An evolutionary game analysis. *Plos One*, *19*(6), e0304467.

Zrahia, A., Gandal, N., Markovich, S., & Riordan, M. (2024). The simple economics of an external shock to a bug bounty platform. *Journal of Cybersecurity*, *10*(1), tyae006.