JILPR Vol. 7, No. 3 June 2026
Journal of Indonesia Law & Policy Review 2715-498X

CRIMINAL RESPONSIBILITY OF INDONESIAN NATIONAL ARMED FORCES MEMBERS IN CYBER CRIME

Fera Kusumawati[1*], Supri Abu[2], Diding Rahmat[3]
[1,2,3]Marshal Suryadarma Aerospace University, East Jakarta, Indonesia
fera@gmail.com[1*], supri@unsurya.ac.id[2], didingrahmat@unsurya.ac.id[3]

Abstract

This study aims to examine the legal provisions for cybercrimes in the laws and regulations applicable to TNI members and to analyze the forms of criminal liability for soldiers committing digital crimes. The method used is normative juridical research with a statute approach and a case approach through a review of relevant laws and regulations, legal doctrines, and court decisions. The results of the study indicate that the regulation of cybercrime for TNI members is basically based on the ITE Law (Law 11/2008 jo. Law 19/2016 jo. Law 1/2024), the New Criminal Code (Law 1/2023), the Criminal Code, the Military Court Law 31/1997, and the Military Discipline Law 25/2014. However, until now there has been no norm that specifically regulates cyber-military offenses so that the potential for overlapping jurisdictions is still found, especially in the application of lex specialis KUHPM and lex generalis ITE Law. Forms of criminal liability for TNI members include individual liability, command liability, and disciplinary liability if the act does not fulfill the elements of a crime. The phenomenon of spreading hoaxes by soldiers and involvement in online gambling shows that the handling of cyber violations is still dominated by disciplinary sanctions, not criminalization. This study concludes that the lack of cyber norms within the military legal framework requires more comprehensive regulatory reform, including revising the Criminal Code (KUHPPM), aligning the ITE Law with the military justice system, and developing technical guidelines for digital evidence for soldiers involved in cybercrimes. Strengthening digital literacy, establishing data security SOPs, and clarifying jurisdictional boundaries are necessary to ensure law enforcement is fair, consistent, and in line with the principles of TNI professionalism.

Keywords: TNI, Cybercrime, Criminal Accountability, ITE Law, Military Law

INTRODUCTION

In this rapidly evolving digital era, national security is no longer solely about conventional defense. Cyberattacks represent a new form of asymmetric, unconventional conflict, where digital power instruments can be used to disrupt government stability, weaken economic systems, and disable defense infrastructure without the direct involvement of physical military forces. This paradigm shift in threats requires all defense institutions, including the Indonesian National Armed Forces (TNI), to strategically adapt to the digital realm. As a key component of national defense, the TNI now faces new challenges in the form of increasing cybersecurity risks that include the potential for military data leaks, breaches of classified information systems, and manipulation of intelligence networks.

The term cyber originates from the concept of cybernetics, which was originally used to describe control and communication systems in humans and machines. With the development of science and technology, the term has expanded its meaning to encompass all activities related to information technology, computers, and internet networks. Cyberspace is a non-physical space formed through global network connectivity, where data exchange, communication, and other digital activities take place without geographical boundaries. Thus, cyberspace has become a new environment for social, economic, political, and defense interactions that operate virtually but have a real impact on human life. In the context of law and security, cyberspace has complex characteristics due to its cross-border nature, the speed of information dissemination, and the anonymity of actors.

Criminal liability for soldiers who commit cybercrimes? Legal regulations governing this issue are currently inadequate. The Criminal Code (KUHPPM), the Military Justice Law (Law No. 31/1997), the Criminal Code, and the Electronic Information and Transactions (ITE) Law do not contain specific provisions regarding cybercrimes by TNI personnel, creating a legal gap that could potentially lead to inconsistencies between military law and national law.

On the other hand, the Indonesian National Armed Forces (TNI) has developed cyber defense capabilities through the establishment of the TNI Cyber Unit (Satsiber TNI), as stipulated in TNI Commander Regulation Number 19 of 2019 concerning the Organization and Duties of the TNI Cyber Unit. The formation of this unit demonstrates an institutional effort to strengthen the security of defense information and communication systems in the face of potential cyber disruptions or attacks. Furthermore, discourse regarding the formation of a Cyber Force as a new branch of the TNI has also emerged in several policy forums in 2024, although it is still under review and has not yet become an official decision within the TNI organizational structure.

However, as of 2025, this plan has not been legally realized due to the lack of a clear normative framework that clearly regulates the position, function, and authority of the cyber sector within the national defense system. This situation creates a gap between the advancement of defense technology and the legal readiness that governs it. Without a clear regulatory framework, increasing technical capabilities without strengthening accountability and legal oversight has the potential to backfire on the professionalism of the Indonesian National Armed Forces (TNI), open up space for the abuse of digital authority, and ultimately undermine the legitimacy of the defense institution itself.

Similarly, Delviana pushed for a revision of the TNI Law to include the digital domain and legally establish a cyber unit, highlighting the importance of aligning the law with developments in modern warfare technology.[2]Theoretically, the concept of command responsibility from international law is relevant in the cyber context, namely when a subordinate commits a violation, then the military superior can be held responsible if he is negligent in preventing or taking action (Geneva Convention, 1977).

However, when confronted with the realities of the national legal system, its implementation in Indonesia still faces various normative and institutional obstacles. To date, there are no specific regulations explicitly defining the form of criminal liability for TNI members who commit cybercrimes, thus the principle of command responsibility has not been explicitly implemented in military justice practice. Heriyanto highlighted the inconsistency between the authority of military justice and general legal norms, which creates a gap in accountability in the event of digital violations by soldiers.

The current phenomenon shows that military personnel are still tried in military courts even though they serve in civilian institutions, as stated by the Indonesian Minister of Law in March 2025. This situation then became the concern of various civil society groups who highlighted the need for clarity in the criminal accountability mechanism for TNI soldiers who serve outside the military operational environment, so that it remains in line with the principle of equality before the law (Imparsial, 2025).

In recent years, several cases of violations involving the use of technology by Indonesian National Armed Forces (TNI) soldiers have emerged in the public sphere, including the dissemination of internal information via social media, the spread of unverified news, and the involvement of members in online activities that violate military disciplinary regulations. While these cases do not always fall into the category of pure cybercrime, these findings demonstrate that the use of digital technology in the military environment requires clear regulation and oversight. The handling of these violations through disciplinary mechanisms and military justice indicates that the military legal system has internal instruments, although it still needs regulatory strengthening to address increasingly complex forms of digital violations.

Examples of cybercrimes include hacking, data breaches, online scams, malware distribution, hate speech on social media, and phishing, or online identity theft. Furthermore, attacks on critical national systems such as public networks, banking systems, and government agencies make cybercrime not just a legal issue but a serious threat to national security.

Internationally, countries such as the United States and Singapore have already established institutional frameworks for cyber defense. The United States, through the United States Cyber Command (USCYBERCOM), organizes military cyber operations and capabilities as part of its national defense structure. The absence of clear legal regulations regarding digital breaches within the military ultimately has serious implications for the effectiveness of internal oversight systems. Weak regulations and legal accountability mechanisms open up opportunities for misuse of digital access by military personnel. Data from the National Cyber and Crypto Agency (BSSN) shows that since 2019 there have been more than 79 cases of strategic data leaks, including several related to defense agency systems. This fact indicates suboptimal information security governance and weak controls over technology use and access to classified data by defense personnel.

If this situation persists without a strong and accountable legal system, the potential for digital violations by Indonesian National Armed Forces (TNI) members will not only pose a threat to national security but also erode public trust in the professionalism and integrity of the military institution. Therefore, research into the criminal liability of TNI members for cybercrimes is crucial and relevant. On the one hand, the TNI is required to strengthen its cyber capabilities to safeguard national sovereignty in the digital space; on the other hand, there must be fair, transparent, and balanced legal guarantees so that any abuse of digital power by soldiers can be accounted for proportionately.

Therefore, this research is crucial in assessing the appropriate form of criminal accountability for Indonesian National Armed Forces (TNI) members in cybercrimes. On the one hand, the TNI needs to continue strengthening its cyber capabilities to safeguard national

sovereignty in the digital space. On the other hand, fair and transparent legal guarantees are needed to ensure that any abuse of digital power by soldiers can be accounted for proportionately. This research is expected to foster a clearer understanding of the mechanisms of criminal accountability and encourage reforms to military law relevant to the challenges of the digital era.

Based on this background, the problem formulation in this research is: How are the legal regulations regarding cyber crimes in the laws and regulations that apply to TNI members and what is the form of criminal responsibility for TNI members who commit cyber crimes?

RESEARCH METHODS

The type of research used in this study is normative legal research, also known as doctrinal research (Soekanto & Mamudji, 2007). This research focuses on analyzing applicable legal norms, legal principles, legal doctrine, and the views of legal experts regarding the criminal liability of military personnel for cybercrimes. The main objective of this approach is to understand and assess the legal provisions governing the behavior of TNI members in the cyber realm, while simultaneously analyzing the relevance and application of these laws in law enforcement practices within the military environment (Marzuki, 2011).

In this study, the type of data used is secondary data, namely data obtained through literature review or library materials review. Secondary data includes various written sources relevant to the research topic, such as books, scientific journals, legal documents, legislation, doctrines, and other publications related to the problem being studied.

The data collection technique used in this study was library research. This research was conducted by collecting various legal materials relevant to the research topic, including primary, secondary, and tertiary legal sources. Primary legal sources include laws and regulations governing military criminal law, the Electronic Information and Transactions (ITE) Law, the Military Justice Law, the Military Discipline Law, and court decisions related to cybercrimes committed by members of the Indonesian National Armed Forces (TNI).

In this research, data collection was conducted through the review of secondary legal materials sourced from various written references. These documents served as the primary basis for examining the legal issues under study, then were selected, grouped, and analyzed in a structured manner to form a systematic framework.

RESULT AND DISCUSSION

Legal regulations regarding cyber crimes in the laws and regulations applicable to members of the TNI

The development of information technology has expanded the forms and patterns of crime, including in the military, necessitating clear legal norms governing the accountability of soldiers for committing cybercrimes. Although Indonesia already has general regulations on cybercrime through the Electronic Information and Transactions Law (UU ITE), specific regulations explicitly governing cybercrimes by members of the Indonesian National Armed Forces (TNI). This situation raises normative issues, particularly regarding legal certainty regarding which legal regime should be applied—general criminal law, military criminal law, or a combination of the two. Therefore, academic studies on the regulation of cybercrimes for members of the TNI are important to determine the extent to which the national legal framework is able to respond to the forms of digital violations committed by soldiers, and whether there are any gaps in norms that need to be addressed in the applicable legal system.

Therefore, the need for clearer regulations regarding cybercrime for Indonesian National Armed Forces (TNI) members is becoming increasingly relevant. Soldiers' official activities in the digital era rely not only on military discipline but also involve the use of

electronic devices, information systems, and digital communications, which have legal consequences. This situation demands certainty regarding the applicable norms when a TNI member commits a cyber offense, given that there are currently no specific regulations explicitly governing cybercrime in a military context. This absence of specific norms often results in the application of the law relying on interpretations of the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), or the Criminal Code (KUHPPM), thus creating a gap between the characteristics of cybercrime and the accountability mechanisms available under military law. Therefore, rationalizing cyber regulations for the TNI relates not only to the needs of law enforcement but also to ensuring alignment between general criminal norms and military criminal norms in addressing digital crimes.

Having identified the rational need for cybercrime regulation for military institutions, it is important to first affirm the position of the Indonesian National Armed Forces (TNI) as a legal subject within the national criminal law system. Legally, TNI members are subject to the military criminal law regime, as stipulated in the Military Criminal Code (KUHPM) and Law Number 31 of 1997 concerning Military Justice. However, the status of soldiers as citizens also places them under the scope of general criminal law, including the Criminal Code and the Electronic Information and Transactions Law (UU ITE), as long as the actions are committed outside the scope of official duties or do not fall under the category of military crimes.

These two legal regimes operate on the principle of lex specialis derogat legi generali, where special law (military criminal law) overrides general law (national criminal law) if the object being regulated falls within the military's internal domain (Hamzah, 2017). However, when an act, including a cybercrime, is unrelated to the performance of military duties or does not have the characteristics of a "military offense," general legal provisions still apply to TNI personnel as they do to other citizens (Arief, 2010). This dualistic framework demonstrates that TNI members can be held accountable under both military and general criminal laws, depending on the context and nature of their actions. Thus, determining jurisdiction is not merely a technical legal issue but also has substantive implications for cyber law enforcement patterns involving military personnel.

As a first step in understanding the cybercrime provisions applicable to Indonesian National Armed Forces (TNI) members, it is important to emphasize that Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is the primary regulation governing all forms of cybercrime in Indonesia. The ITE Law applies generally to all citizens, without exception based on professional status, position, or official status, so TNI members are, in principle, also subject to the criminal provisions contained therein. This affirmation aligns with the principle of equality before the law, which places all legal subjects on equal footing before national criminal law (Marzuki, 2011). In the context of cybercrime, the ITE Law regulates a number of offenses such as illegal access (Article 30), unauthorized interception, manipulation of electronic information, disruption of electronic systems, and the dissemination of unlawful content. The existence of these norms demonstrates that Indonesian positive law has provided a sufficiently comprehensive legal framework to address forms of digital violations, whether committed by civilians or by TNI personnel in certain situations. Therefore, the ITE Law must be understood as the main foundation in assessing criminal liability for military personnel who commit unlawful acts in cyberspace.

Article 36 of Law Number 1 of 2023 concerning the Criminal Code stipulates that a person can only be held criminally responsible if the crime is committed intentionally or through negligence. This provision reinforces the fundamental principle of criminal law, namely that there is no punishment without fault (geen straf zonder schuld). Essentially, every criminal act is considered to have been committed intentionally, unless the law expressly stipulates that negligence is also punishable. Thus, the element of fault is a primary

requirement for imposing a penalty on the perpetrator. Meanwhile, Article 37 provides an exception to this general principle by opening up the possibility of liability without fault if expressly stipulated by law. This provision accommodates the concepts of strict liability (absolute responsibility) and vicarious liability (responsibility for the actions of others). This means that under certain circumstances, a person can be punished solely because the elements of a crime are met, or can be held responsible for the actions of another party, as long as the legal basis clearly regulates this.

The increasingly rapid development of digital technology has prompted the government to update the ITE Law through two major amendments, in 2016 and 2024. Each amendment consolidated the definition of electronic crime, strengthened data protection aspects, and refined norms related to access and misuse of electronic systems (Marzuki, 2014). The 2016 revision clarified the elements of the offense and emphasized the distinction between administrative violations and criminal offenses, while the 2024 revision integrated a number of new provisions regarding electronic system security, digital evidence, electronic system administrators, and strengthened the legality of electronic documents. For members of the Indonesian National Armed Forces (TNI), these updates are of direct relevance, given that the digital activities of soldiers and military institutions are increasingly connected to the country's strategic electronic systems. Thus, the development of the ITE Law is not only responsive to the dynamics of national cyber threats but also strengthens the legal basis for assessing the criminal liability of soldiers when they commit acts that damage, disrupt, or misuse electronic systems. These gradual revisions ultimately demonstrate that national law continues to adapt to increasingly complex digital crime patterns that potentially involve military personnel in various capacities.

The regulation of cybercrime in the national context is not only based on the ITE Law, but is also strengthened through the enactment of the new Criminal Code under Law Number 1 of 2023. This modern Criminal Code for the first time includes a number of digital offenses as part of general crimes, including illegal access to electronic systems, disruption of data integrity, destruction of information systems, manipulation of digital information, and forms of conduct previously regulated only sectorally in the ITE Law. The presence of digital norms in the Criminal Code demonstrates the state's recognition of the development of forms of crime that are increasingly shifting from the physical to the electronic sphere. For members of the Indonesian National Armed Forces (TNI), the existence of this provision has particular significance because the Criminal Code acts as a lex generalis that can still be applied when soldiers commit general crimes outside the performance of official duties. This means that soldiers who commit acts such as illegal access, unlawful dissemination of electronic information, or destruction of digital data can be subject to the provisions of the new Criminal Code in addition to the ITE Law, as long as there are no specific provisions in the Criminal Code or the Military Justice Law that stipulate certain exceptions. Thus, the digital norms in the Criminal Code expand the scope of criminal liability for soldiers in the cyber context and strengthen the consistency of national law in responding to developments in information technology.

Regulations regarding criminal acts committed by TNI soldiers cannot be separated from the military legal framework, which is based on Law Number 34 of 2004 concerning the TNI and Law Number 31 of 1997 concerning Military Justice. Both regulations position soldiers as legal subjects with obligations of discipline, loyalty, and maintaining state confidentiality as fundamental elements of the military profession. The TNI Law emphasizes that every soldier must comply with national and military law, including a strict prohibition on leaking or misusing information related to official duties, which in the digital context can include the dissemination of internal data, operational documents, and access to unit electronic systems. Meanwhile, the Military Justice Law regulates the jurisdictional

mechanisms for soldiers suspected of committing crimes, including the possibility of processing cyber cases as long as the actions meet the elements of general criminal offenses or military disciplinary offenses. However, although these two laws provide a strong basis for authority, there is no single provision that explicitly regulates cybercrime in the military context. Therefore, all handling still refers to the norms of the ITE Law and the Criminal Code as general law, while military law serves as a complementary instrument to determine aspects of official duties and discipline. This regulatory gap is important to note because it shows that the Indonesian legal system does not yet provide a classification for "cyber-military offense," even though digital threat patterns involving military personnel have become increasingly relevant in recent years.

Articles 1 and 2 of the Military Criminal Code stipulate that military personnel are subject to special provisions of military criminal law. General criminal law remains applicable unless specifically stipulated in the Criminal Code. This provision acknowledges the general applicability of the national criminal law system, with exceptions if specific military norms provide specific provisions for an act.

This construction reflects the principle of lex specialis derogat legi generali, namely the principle that specific rules override general rules. In this context, the Criminal Code, as a special criminal law for soldiers, has priority when a norm meets a provision in the Criminal Code or other general criminal regulations. This means that if a crime is specifically regulated in the Criminal Code, then that provision applies, not the provision in general criminal law.

The application of this principle aims to safeguard the unique characteristics and needs of military institutions, which have a hierarchical structure, strict discipline, and strategic national interests. Therefore, in cases involving military personnel, determining the applicable norm must first determine whether the act is specifically regulated by military criminal law. If no specific regulation exists, general criminal law is applied as a supplement. This mechanism creates a balance between the principle of the unity of the national legal system and recognition of the specificity of the military profession.

The absence of specific cyber norms in the Criminal Code (KUHPM) results in the application of the ITE Law to soldiers being carried out through an interaction mechanism between lex generalis and lex specialis. On the one hand, the ITE Law applies to all citizens without exception, so TNI soldiers can essentially be subject to criminal provisions under the ITE Law when engaging in illegal access, data manipulation, or the unlawful dissemination of electronic information. However, on the other hand, the Criminal Code, as a special criminal law for the military, still holds the position of lex specialis in assessing aspects of official duty, compliance with orders, and disciplinary violations that may arise concurrently with such cybercrimes. This interaction has given rise to legal debate, particularly in determining whether soldiers should be processed directly under the ITE Law through general courts, or remain under the jurisdiction of military courts due to their membership status and the relationship of the actions to official duties. In practice, law enforcement officials tend to combine these two legal regimes, namely by using the ITE Law to determine the elements of the cybercrime, but the examination is still conducted within the framework of military courts if the perpetrator's actions are deemed related to their military status. This shows that even though relevant norms are available, the structure of their implementation does not yet have standard guidelines, thus giving rise to considerable room for interpretation in determining the locus and forum of justice.

Although the development of national regulations in the field of cybercrime has become more comprehensive following the enactment of the ITE Law and its amendments, the Criminal Code (KUHPPM), as a specific criminal code for the military, does not yet contain an offense that explicitly regulates cybercrime. This normative gap creates legal problems, because the regulations that form the basis for sentencing soldiers still rely on

conventional provisions that are not designed to address the characteristics of digital crime. In fact, cybercrime is technical in nature, cross-system, and often occurs without physical contact, so the requirements for proof are very different from traditional offenses in the military context. The absence of this specific norm impacts the dilemma of determining which lex should be applied: whether to directly use the ITE Law, or continue to prioritize the provisions of the Criminal Code based on the principle of lex specialis derogat legi generali (Arief, 2010). In certain contexts, military law enforcement tends to direct cyber acts as violations of discipline or order, rather than as criminal acts, resulting in inconsistencies in the application of the law. This normative gap is one of the central issues why the regulation of cybercrime against soldiers has not been optimal.

The lack of cyber norms in the Criminal Code (KUHP) has resulted in some digital violations being handled as disciplinary offenses under Law No. 25 of 2014 concerning Military Disciplinary Law. In practice, a number of soldiers' digital behaviors that should be classified as criminal offenses, such as the dissemination of information that violates procedures, violations of internet ethics, or the unauthorized use of digital devices, are more often processed as administrative errors. This approach is understandable, given the emphasis on hierarchy, compliance, and internal control in military training; however, it also has the potential to blur the line between disciplinary violations and cybercrimes. For example, in several public cases, soldiers who spread hoaxes during elections were processed through disciplinary mechanisms without resorting to the criminal provisions of the ITE Law, raising academic questions about whether such responses reflected the values of proportionality and legal certainty. Similarly, behavior such as soldiers' involvement in illegal access to internal networks may result only in coaching, rather than criminal prosecution. This situation demonstrates that without clear cybercrime norms in military law, law enforcement has the potential to be inconsistent and highly dependent on the interpretation of superiors and internal law enforcement.

In law enforcement practice, the application of the ITE Law to Indonesian National Armed Forces (TNI) soldiers depends heavily on the nature of the violation and the assessment of military law enforcement officials as to whether the act constitutes a disciplinary violation or meets the elements of a cybercrime. Several phenomena emerging in the public sphere indicate that digital violations by soldiers are often handled through a combination of legal instruments, such as the ITE Law, the Criminal Code, and military disciplinary regulations. For example, in the case of the dissemination of hoaxes by individual soldiers during the election period, such actions are not only viewed as a violation of military ethical norms but also potentially meet the elements of the dissemination of misleading electronic information as defined in the ITE Law. Law enforcement in such incidents typically involves investigations by the Military Police, analysis of digital footprints, and consideration of whether the act impacts the stability of the unit and the image of the institution. Another example is the phenomenon of individual soldiers' involvement in online gambling activities, which, while not always classified as a pure cybercrime, nevertheless demonstrates how soldiers' use of electronic devices and internet access can form the basis for the application of certain articles in the ITE Law and disciplinary provisions. These phenomena illustrate that in practice, military law enforcement officers apply a hybrid approach, namely combining military law norms and general criminal law to ensure that every digital violation can be prosecuted proportionally and according to context.

In the military legal system, investigations into alleged cybercrimes are conducted through a special mechanism involving the Military Police as the primary investigative institution. Cyber investigations in the military environment are complex because they rely on the ability to collect and analyze electronic evidence, which requires technical skills in digital forensics. In the initial stage, the Military Police confiscate electronic devices, examine

activity logs, and verify data authenticity. In some cases, military investigators coordinate with civilian institutions such as the National Cyber and Crypto Agency (BSSN) or the Ministry of Communication and Informatics to obtain technical support, particularly regarding data recovery, attack identification, or metadata analysis. This cross-agency coordination is crucial given that not all military units have adequate digital forensic infrastructure. Furthermore, cyber investigations involving soldiers must also consider the perpetrator's status as active military personnel, ensuring that aspects of discipline, military ethics, and command hierarchy remain integral to the law enforcement process. Given this complexity, the cyber investigation process in the military environment is not only oriented toward proving the elements of the crime, but also toward restoring the integrity of the unit's electronic systems and ensuring the security of information that could potentially impact national defense interests.

In the enforcement of cybercrime by members of the Indonesian National Armed Forces (TNI), one of the most fundamental issues lies in digital evidence, which requires different technical and procedural standards than conventional evidence. Although the ITE Law recognizes electronic information and electronic documents as valid evidence, its implementation in the context of military justice faces several obstacles, primarily due to the need for reliable digital forensics, the technical competence of military investigators, and the availability of electronic examination infrastructure. Following the 2024 amendment to the ITE Law, which expanded the scope of validity of electronic evidence, the evidentiary process has become increasingly dependent on identification procedures, activity log tracking, and the integrity of digital metadata, which are often difficult to maintain in closed military information systems. This challenge demonstrates that the quality of evidence is determined not only by the existence of electronic evidence but also by the military institution's ability to manage digital investigations that meet chain of custody and digital evidence integrity standards. Thus, the technical dimension of electronic evidence is a critical point in determining whether a cybercrime can be legally accounted for.

Besides the issue of evidence, another issue that frequently arises in the handling of cybercrimes by members of the Indonesian National Armed Forces (TNI) is the level of transparency and accountability of the judicial process. As a hierarchical and discipline-based institution, military justice is fundamentally designed to maintain internal order and is not always as open as general courts. Several academic studies have shown that the level of openness of military justice processes tends to be more limited than that of general courts, thus posing challenges from the perspective of access to information and public monitoring of cases involving soldiers (Arief, 2008). In the context of cybercrime, this condition becomes even more relevant given that digital violations often relate to sensitive information, potential data leaks, or the confidentiality of defense institutions. Therefore, the assessment of accountability cannot be simplified solely to the applicable articles, but also to how the legal process is conducted professionally and proportionally without compromising the principle of justice. This challenge demonstrates the need to strengthen transparency as long as it does not interfere with the military's strategic interests and is in line with the principle of the rule of law, which places the legal process as an objective and integral control mechanism.

From an institutional perspective, the regulation of cybercrime in legislation has several direct implications for the Indonesian National Armed Forces (TNI). Every cyber violation committed by soldiers, whether in the form of disseminating internal information, unauthorized access, or engaging in risky digital activities such as online gambling or distributing illegal content, creates an increasingly complex training burden for the unit. This burden relates not only to disciplinary aspects but also to information security and the confidentiality of strategic data within the scope of the TNI's duties. Within the framework of the TNI Law and the Military Discipline Law, the obligation to maintain state confidentiality

and comply with command instructions is a normative basis that must be upheld. However, the development of digital technology creates the potential for violations that are more difficult to detect. Therefore, military institutions are required to develop digital security standard operating procedures (SOPs), strengthen internal cyber literacy, and ensure adaptive oversight mechanisms to address new threat patterns. Several studies also emphasize that modern military organizations are obliged to enhance their information security capabilities as part of protecting national defense assets.

The interaction between cyber law and military law has significant implications for the national justice system. The issue of jurisdiction, particularly regarding whether TNI members who commit cybercrimes should be tried in military courts or general courts, remains an unresolved legal issue. Article 65 of the TNI Law provides normative guidance that soldiers should be subject to general courts when committing general crimes outside of their duties. However, in practice, the implementation of this provision often leaves diverse interpretations at the law enforcement level. This has the potential to lead to inconsistent application of norms, particularly when cybercrimes are classified as disciplinary or criminal offenses. Therefore, the national justice system needs to ensure uniform guidelines. Furthermore, Indonesian criminal law literature emphasizes that the existence of special courts must remain within the principles of the rule of law and public accountability, without neglecting the need to maintain military hierarchy and discipline (Arief, 2008). Therefore, cyber law regulations involving TNI members not only impact the perpetrators but also affect the overall credibility of the national law enforcement mechanism.

Overall, the legal regulations regarding cybercrime applicable to members of the Indonesian National Armed Forces (TNI) demonstrate that Indonesia has a number of adequate normative instruments to regulate the digital behavior of citizens, including TNI soldiers, through the ITE Law, the new Criminal Code, the PDP Law, and provisions on military discipline and justice. However, all of these regulations were primarily formulated for a general context and have not been specifically designed to address the characteristics of digital violations within the military environment, which has a command structure, strategic data confidentiality, and disciplinary standards that differ from those in civilian society. This situation creates a normative gap, particularly when it comes to determining whether a particular digital violation by a soldier qualifies as a form of disciplinary violation, a crime within the general criminal realm, or an offense specifically qualified as a military crime, and how to determine the appropriate judicial forum. Therefore, although the positive legal framework has provided a general basis for processing cybercrime, its application to TNI members still requires harmonization between regulations, technical guidelines, and clarity of jurisdiction to avoid legal inconsistencies or uncertainty. The next section will discuss further how the construction of criminal responsibility can be applied to TNI members who commit cyber crimes, including the interaction between the ITE Law, the Criminal Code, the Criminal Code, and the principles of military criminal law in the context of modern law enforcement.

Forms of criminal responsibility for TNI members who commit cyber crimes

Criminal liability is essentially a legal mechanism for determining the extent to which an individual can be held responsible for acts prohibited by law. In the military context, this concept becomes more complex due to its relevance to the status of soldiers as part of a national defense institution subject to specific regulations. The development of cybercrime presents new challenges for law enforcement, as crimes committed through electronic systems are transnational, cross-jurisdictional, and often difficult to identify. Therefore, analyzing how members of the Indonesian National Armed Forces (TNI) can be held criminally responsible for committing cybercrimes is crucial for understanding the position of soldiers as legal subjects in the digital era.

Normatively, Indonesia does not yet have a specific law that explicitly regulates cybercrime within the military. This gap results in TNI members being subject to three legal regimes simultaneously: first, general criminal law such as the Criminal Code and the Electronic Information and Transactions Law (UU ITE); second, military criminal law as stipulated in the Criminal Code and the Military Justice Law; and third, military disciplinary law as stipulated in Law Number 25 of 2014. These three legal regimes have the potential to overlap, particularly when a cyber act can be classified as both a criminal offense and a disciplinary violation. This situation makes analyzing the forms of criminal liability for TNI members require a systematic and comprehensive legal approach.

The ITE Law is the primary legal basis for prosecuting any citizen who commits cybercrime, including members of the Indonesian National Armed Forces (TNI). Provisions such as illegal access, electronic data manipulation, wiretapping, and interference with electronic systems form the basis for criminal penalties for cybercrime perpetrators. Although the ITE Law is general and applies to all citizens without discrimination, its application to TNI personnel cannot be separated from the military's jurisdictional mechanisms, which have their own internal regulations. Therefore, although the elements of the offense refer to the ITE Law, the judicial forum is often determined based on military membership status and provisions in the Military Justice Law.

Unlike the ITE Law, the Criminal Code (KUHPPM) provides a specific basis for criminal liability for military personnel. However, this instrument does not specifically address cyber crimes, so cybercrime by soldiers is usually categorized as a general offense such as abuse of office, violation of official orders, or acts detrimental to the state. Because the provisions of the Criminal Code do not yet accommodate the nature of digital crimes, criminalization of cybercrime by soldiers often has to be carried out through analogy with the articles or combined with the ITE Law. This indicates a regulatory gap that can affect the consistency of criminal liability for TNI members in cyber cases. The provisions regarding the forum for criminal liability for members of the Indonesian National Armed Forces (TNI) are essentially guided by Law Number 31 of 1997 concerning Military Justice, which stipulates that every active soldier is under the jurisdiction of military justice if they commit a crime in their capacity as a member of the military. This law establishes a special judicial structure that includes the Military Court, the High Military Court, and the Main Military Court, all of which are established to handle criminal cases involving soldiers as legal subjects. This provision interacts directly with Article 65 of Law No. 34 of 2004 concerning the Indonesian National Armed Forces (TNI), which states that soldiers are subject to military justice for crimes related to the performance of military duties, and are subject to general justice for committing general crimes outside of duty. However, in practice, this provision requires interpretation because there has not been a revision to the Military Justice Law that could clarify the operational boundaries between military jurisdiction and general jurisdiction (Law No. 31, 1997).

Therefore, the form of criminal liability imposed on TNI members who commit cybercrimes depends on the competent judicial forum, which in turn is determined by whether the act is related to official duties or falls outside the scope of military functions. In the context of cybercrimes committed by TNI members, the relationship between the Criminal Code, the Electronic Information and Transactions Law, and the Criminal Code (KUHPPM) cannot be separated because all three serve as complementary legal bases in determining the form of liability. The Criminal Code and the Electronic Information and Transactions Law provide a general framework regarding prohibited acts in the digital space, such as illegal access, data manipulation, or the dissemination of electronic information that has legal consequences. Meanwhile, the Criminal Code (KUHPPM) regulates specific provisions that apply only to soldiers, particularly regarding military discipline, the use of official facilities,

and the obligation to maintain state secrets. In practice, determining which law to apply depends heavily on the nature of the act, the official context, and the competent judicial forum.

In determining the basis for criminal liability for TNI members who commit cybercrimes, the relationship between general law and military law is inseparable. In practice, soldiers' actions are always assessed through two layers of norms: national criminal norms and military criminal norms. This is where the relevance of the principle of lex specialis derogat legi generali becomes crucial, because military law, as a special rule, will be applied first if the act is related to official duties or touches on aspects of military discipline and hierarchy. However, when the cybercrime committed by soldiers is of a general nature, such as unauthorized access to electronic systems or disseminating content prohibited by the ITE Law, general criminal provisions can still be applied as long as they do not conflict with the specific norms governing the military profession. Thus, the interaction of these two legal regimes is not mutually exclusive, but rather complementary, and the determination of the form of accountability always takes into account the character of the act as well as the perpetrator's status as a member of the TNI.

The phenomenon of cyber violations in the military environment essentially occurs more in the form of digital misbehavior than cybercrimes that fulfill the elements of a crime under the ITE Law. Therefore, a number of incidents involving soldiers in the digital realm are generally processed through military disciplinary mechanisms. For example, there was the case of the spread of hoaxes by certain soldiers in the lead-up to the election period, which demonstrates how personal social media use can have official consequences when the shared content has the potential to disrupt military order and neutrality. Another phenomenon includes soldiers' involvement in online gambling activities, where such behavior does not necessarily fulfill the elements of a cybercrime but is still processed as a disciplinary violation because it violates the ethics and honor of the military. These examples illustrate that not all digital actions by soldiers are criminal; many fall within the realm of internal discipline because they relate to compliance with the code of ethics, official orders, and the image of the military institution. Thus, analyzing military discipline is important to understand how institutions respond to soldiers' digital behavior that does not meet the elements of a crime but still impacts military integrity and order.

From a criminal law perspective, the liability of TNI members for cybercrimes can be analyzed through several forms of responsibility recognized in both criminal and military law doctrine. First, individual liability, which occurs when a soldier directly commits a prohibited act, such as unauthorized access to an electronic system or manipulation of digital data. Second, command liability, which can arise when a superior negligently allows access to an unsecured system, fails to supervise the use of official electronic devices, or fails to take precautions against potential digital violations by subordinates. Third, collective liability, which is rarely applied, can arise in unit operations or activities that involve the shared use of electronic systems and potentially lead to violations of the law. Fourth, positional liability, which occurs when a soldier uses digital authority or access to military information systems for purposes that deviate from official duties. These four forms of liability demonstrate that in the cyber context, the assessment of criminal liability depends not only on individual actions but also on organizational structure, command authority, and the use of official facilities. Therefore, analyzing the forms of liability is a key element in understanding how criminal law applies to soldiers who commit cyber violations.

The criminalization of Indonesian National Armed Forces (TNI) members in cyber cases faces a number of structural and normative obstacles. Structurally, the hierarchical and closed nature of the military justice system means that law enforcement for cybercrimes does not always operate with the same standards of transparency as regular justice. Regulatory

limitations are also a fundamental problem, as the Criminal Code (KUHPPM) does not explicitly address cyber crimes. Consequently, various digital acts such as illegal access, data misuse, or manipulation of electronic systems are often "forced" into general articles concerning disobedience, abuse of authority, or acts detrimental to official interests. This normative vacuum creates variation in law enforcement, as investigators must independently interpret the appropriateness of cyber crimes and conventional military provisions. Furthermore, digital evidence in the military presents unique challenges, given that electronic forensics requires technical competencies that are not always readily available and requires cross-agency collaboration, including the Military Police, the Audit Office, and national cyber agencies. These obstacles indicate that the criminalization of cybercrimes by TNI soldiers depends not only on written norms, but also on the institution's readiness to read and process electronic evidence professionally and accountably.

The relationship between the Criminal Code, the Electronic Information and Transactions Law (UU ITE), and the Criminal Code (UU PMK) is key in determining the form of criminal liability for TNI members who commit cybercrimes. In this context, the principle of lex specialis derogat legi generali remains the primary reference: the KUHPM, as a special military law, is essentially prioritized when the act is directly related to the performance of official duties or disrupts the internal discipline of soldiers. However, not all cybercrimes are military in nature; many are general offenses that are regulated in detail in the ITE Law, such as illegal access, unauthorized interception, data manipulation, or destruction of electronic systems. Therefore, if a soldier's actions are unrelated to official duties, do not concern military security, and are more like general crimes, the ITE Law can be applied directly as long as they do not conflict with military regulations. Within this framework, the KUHPM is not interpreted as a norm that "overrides" general criminal law, but as a complementary norm that regulates specific aspects of the military profession. This approach aligns with the doctrinal view of criminal law that accountability must take into account the nature of the offense, the perpetrator's status, and the protected legal interests. Thus, the interaction between the Criminal Code and the ITE Law confirms that TNI members remain within the reach of national criminal law, but with certain adjustments that take into account the special character of military institutions.

In cybercrimes, the elements of criminal liability remain based on the general principles of criminal law, namely intent (dolus) or negligence (culpa), the capacity to take responsibility, and the absence of justification or excuse. Characteristics of cybercrimes, such as the anonymity of the perpetrator, the use of digital devices, and the nature of the act, which can be carried out without physical contact, require a more technical interpretation of the elements of culpability. For members of the Indonesian National Armed Forces (TNI), the application of the elements of intent and negligence has an additional dimension because every soldier is bound by disciplinary obligations, obedience to orders, and a prohibition on misusing official facilities. This means that, in the military context, actions such as unauthorized access to systems, disseminating confidential digital information, or using unit communications networks for personal purposes can be considered more severe because they are carried out in an environment that demands a high level of caution. Therefore, the assessment of a soldier's culpability not only examines whether their actions meet the elements of a cyber crime under the ITE Law, but also whether they violate the norms of the military profession, which require caution, loyalty, and adherence to digital security protocols. This approach suggests that the criminal liability of soldiers in cybercrimes is a combination of general criminal law standards and the ethical standards of service inherent in their military status.

In addition to individual accountability, TNI members can also be held criminally liable based on the principle of command responsibility, particularly when cybercrime occurs

within a unit or involves the use of official facilities. This principle essentially asserts that a superior can be held responsible if he or she knows, or should have known, of a violation committed by a subordinate but fails to take adequate preventive, supervisory, or enforcement measures. In the context of cybercrime, a superior's negligence can be seen in allowing the unit's digital devices to be used without security, weak oversight of access to sensitive data, or the absence of clear instructions regarding information security standards. If a soldier experiences a data leak, the dissemination of confidential information, or unauthorized access, liability not only rests with the direct perpetrator but can also extend to the commander who negligently exercised their control function. Thus, the principle of command responsibility is highly relevant in the modern military environment, where information and communication systems are an integral part of defense operations and any lapse in oversight can have serious consequences for both the unit's and the nation's security.

CONCLUSIONS

Legal provisions regarding cybercrime for Indonesian National Armed Forces (TNI) members are still generally general in nature, as Indonesia does not yet have a specific legal regime explicitly governing cybercrime within the military. Current regulations refer to the Electronic Information and Transactions (ITE) Law, the Criminal Code (KUHP), the Criminal Code (KUHPPM), and the Military Justice Law, requiring that each case be handled in a manner tailored to the specifics of each case. The ITE Law provides criminal grounds for digital acts, such as illegal access, data dissemination, and manipulation of electronic systems, while the Criminal Code (KUHPPM) regulates internal military matters, discipline, and violations related to the command hierarchy.

Based on the overall regulatory structure, it can be concluded that the regulation of cybercrime for TNI members is not contained in a single codified instrument, but rather is layered through the ITE Law, the Criminal Code, the Criminal Code, the Military Justice Law, and the Military Discipline Law. The TNI, as a legal subject, remains subject to national regulations, but with the exception of jurisdiction when acts are related to military duties. Implementation of norms requires a harmonious interpretation of general criminal law and military criminal law to avoid legal inconsistencies and uncertainty. This situation demonstrates that Indonesia still needs technical guidelines or cyber-military regulations to ensure law enforcement against soldiers is more structured, objective, and responsive to developments in modern digital crime. Thus, existing legal regulations already provide a basis for criminalization, but still leave room for correction and renewal.

Criminal liability for TNI members who commit cybercrimes essentially follows a dual system: the general criminal law regime and the military criminal law regime. As citizens, TNI soldiers are subject to the provisions of the ITE Law and the Criminal Code if their cyber actions meet the elements of a crime, such as illegal access, data manipulation, or the distribution of prohibited electronic content. However, as active military personnel, any violations committed in the context of official duties, using military means, or impacting national defense security are processed through military criminal law instruments, including the Criminal Code and the Military Justice Law. These two regimes are not mutually exclusive, but rather work in conjunction with each other, so that law enforcement can be directed along the path most appropriate to the nature of the violation and the scope of the perpetrator's responsibility.

REFERENCES

Arief, B. N. (2008). Problems of law enforcement and criminal policy. Kencana.
Arief, B. N. (2010). Anthology of criminal law policy. Citra Aditya Bakti.
Arief, B. N. (2016). Problems of criminal responsibility in criminal law. Pustaka Magister.

Hamzah, A. (2017). Principles of criminal law (5th ed.). Rineka Cipta.
Kitab Undang-Undang Hukum Pidana (KUHP).
Kurnia, D. (2022). Cyber law & digital defense. Remaja Rosdakarya.
Marzuki, P. M. (2011). Legal research (revised ed.). Prenada Media.
Marzuki, P. M. (2014). Normative legal research methods. Rajawali Pers.
Soekanto, S., & Mamudji, S. (2007). Normative legal research. Rajawali Pers.
Suhariyanto, B. (2013). Information technology crimes (cybercrime). Rajawali Pers.
Undang-Undang Nomor 31 Tahun 1997 tentang Peradilan Militer.
Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Undang-Undang Nomor 25 Tahun 2014 tentang Hukum Disiplin Militer.
Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.