Reconstruction of the Regional Cyber Police Decentralization Model Based on Regional Digital Risks in Strengthening Cyber Law Enforcement in Indonesia

Ninda Krisnawati Septarini Hulu, Henry Aspan, Fitri Rafianti

Abstract

The development of cybercrime in Indonesia shows increasing complexity that is no longer uniform, but rather influenced by the characteristics of digital risks that differ in each region, such as the level of internet penetration, information technology infrastructure, digital economic activity, human resource capacity, and community vulnerability to various forms of cyberattacks. However, the current model of cyber law enforcement in Indonesia still tends to be centralized through a centralized coordination pattern, which has implications for limited institutional responses to the dynamics of cybercrime that are developing rapidly and contextually at the regional level. This condition raises issues about the effectiveness of law enforcement because the characteristics of cyber threats in urban areas, industrial areas, border areas, and areas with low levels of digital literacy have different risk patterns, requiring a more adaptive institutional approach based on local needs. This study aims to analyze the weaknesses of the current centralized model of cyber law enforcement in addressing the characteristics of regional-based cybercrime in Indonesia and to formulate an ideal decentralized model of regional-level cyber police based on regional digital risks to strengthen the effectiveness of cyber law enforcement in Indonesia. The research method used is normative legal research with a statutory, conceptual, and comparative approach through an analysis of cyber law regulations, police institutional policies, the theory of decentralized law enforcement, the concept of risk-based governance, and the development of national cybersecurity policies. The results of the study indicate that the current centralized model of cyber law enforcement has weaknesses in the form of slow responses to regional-based digital incidents, limited regional cyber risk mapping, low early detection capacity at the regional level, and less than optimal integration between digital intelligence, cyber investigations, and local community-based prevention. Therefore, it is necessary to reconstruct the decentralized model of cyber police at the regional level based on regional digital risks through the formation of adaptive regional cyber police units, regional digital risk classification systems, strengthening vertical-horizontal coordination, and the integration of surveillance and rapid response technologies to realize cyber law enforcement that is more responsive, effective, and oriented towards protecting the digital security of the community.

Keywords: *Cyber Police; Decentralization; Regional Digital Risks; Cyber Law Enforcement; Cyber Security.*

Ninda Krisnawati Septarini Hulu[1]
[1]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: qrizzzna24@gmail.com[1]

Henry Aspan[2], Fitri Rafianti[3]
[2,3]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: henryaspan@yahoo.com[2], fitrirafianti@dosen.pancabudi.ac.id[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The development of information and communication technology has transformed patterns of social, economic, governmental, and community interaction into an increasingly complex digital space. This rapid digital transformation has had a positive impact on the efficiency of public services, technology-based economic growth, and expanded access to information. However, it has also given rise to new forms of crime that utilize cyberspace as the primary medium for committing crimes. The cybercrime phenomenon in Indonesia has shown a significant escalation, including online fraud, electronic system hacking, personal data theft, malware distribution, attacks on digital infrastructure, electronic-based financial exploitation, and cybercrimes that threaten the stability of public and private information security. In this context, the state is required to implement a cyber law enforcement system that is not only responsive to technological developments but also able to adapt to the characteristics of digital threats that are dynamically evolving across Indonesia.[1]

As the primary legal basis, regulations regarding electronic activities and cybercrime in Indonesia began with Law Number 11 of 2008 concerning Electronic Information and Transactions, which was subsequently amended by Law Number 19 of 2016 and most recently refined by Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law. These regulatory changes demonstrate the state's recognition of the dynamic development of cybercrime, which demands updates to legal instruments to remain relevant to the complexity of digital threats. However, these regulatory updates have not been fully accompanied by the reconstruction of cyber law enforcement institutions that are adaptive to the characteristics of regionally based digital risks. The cyber law enforcement system still tends to place case handling capacity, digital intelligence, and investigative coordination within a centralized institutional framework, resulting in suboptimal responses to regional variations in digital threats.[2]

This issue is relevant because Indonesia is an archipelagic nation with highly heterogeneous levels of digital development across regions. Metropolitan areas with high internet penetration and intensive digital economic activity have different cyber threat characteristics than rural areas, border regions, or areas with low digital literacy. In large cities, threats tend to be related to attacks on digital payment systems, electronic identity theft, phishing, and technology-based financial crimes, while in certain regions the threats are more dominant in the form of online fraud, social media abuse, exploitation of public data, and the distribution of illegal content based on digital networks. These varying characteristics indicate that digital risks have regional digital risk patterns that require different law enforcement approaches and cannot be addressed uniformly through overly centralized institutional models.[3]

From a criminal policy perspective, the centralized model of cyber law enforcement has several structural limitations. Overly centralized institutional patterns often delay early detection, risk mapping, and investigative responses due to coordination gaps between the central and regional governments. Furthermore, the limited number of cyber units at the regional level means that local law enforcement officials lack the capacity to fully recognize the characteristics of specific digital threats in their regions. This situation has the potential to reduce the effectiveness of cyber law enforcement because institutional responses are not adaptive to local needs, while cybercriminals move quickly and flexibly, exploiting weaknesses in uneven digital surveillance systems.[4]

From the perspective of the theory of decentralization of law enforcement, the effectiveness of legal institutions is greatly influenced by the organization's ability to adapt policies and operational mechanisms to the social, geographic, and risk characteristics of a particular region. Decentralization is not intended to weaken central control, but rather to reconstruct the distribution of authority that allows for strengthened local responses through the development of institutional capacity based on regional needs. In the context of cyber law enforcement, this approach opens up space for the establishment of a regional-level cyber

police model capable of mapping local digital risks, early threat detection, public cybersecurity education, and rapid response to digital incidents developing specifically in a given region.[5]

On the other hand, the current centralized model of cyber law enforcement also faces challenges in cross-regional coordination and data integration. Cyber threats are inherently borderless, allowing perpetrators to launch attacks from different regions with impacts that spread nationally and internationally. However, this cross-border nature does not mean that all policies must be fully centralized; rather, it requires a multi-level coordination model capable of integrating local capacity building with national control systems. Therefore, the need for a decentralized cyber police model based on regional digital risks is increasingly relevant as an effort to build a more responsive, integrated, and contextual law enforcement system. [6]

Another problem lies in the lack of a regional digital risk classification that can serve as a basis for policy on the distribution of cyber law enforcement resources. To date, strengthening the capacity of regional cyber officers has tended to be administrative in nature and has not been based on risk indicators such as the level of digital attack threat, the intensity of e-economic activity, the level of public digital literacy, the vulnerability of electronic system infrastructure, and the potential for local cybercrime. Consequently, strengthening cyber institutions at the regional level has not been carried out proportionally and based on factual needs. This situation indicates the need for a reconstruction of the institutional model that places regional digital risk as the primary basis for the formation of regional cyber police units.[7]

The need to reconstruct a decentralized cyber police model at the regional level is ultimately a logical consequence of the increasingly complex and diverse development of digital threats in Indonesia. The existence of the Electronic Information and Transactions Law and its amendments has provided a normative basis for cyber law enforcement, but the effectiveness of law implementation remains dependent on institutional design that can respond adaptively to social realities and digital risks. Therefore, this research is crucial in analyzing the weaknesses of the current centralized cyber law enforcement model and formulating an ideal decentralized cyber police model at the regional level based on regional digital risks to strengthen the effectiveness of cyber law enforcement in Indonesia.[8]

The main weakness of the centralized model of cyber law enforcement in Indonesia lies in the imbalance between the complexity of locally evolving digital threats and the institutional response capacity, which remains concentrated in central mechanisms. The author argues that this overly centralized pattern has led to cyber law enforcement being reactive and administrative, rather than preventive and adaptive to changing digital threat patterns at the regional level. This argument is based on the fact that the characteristics of cybercrime do not develop homogeneously across Indonesia, but are instead influenced by the level of internet penetration, patterns of digital economic activity, the level of technological literacy of the public, and the vulnerabilities of electronic systems that vary across regions. Therefore, a uniform institutional model potentially faces limitations in detecting, mapping, and responding to digital threats that are locally characteristic and rapidly evolving.

Empirically, the increasing intensity of digital technology use across various regions demonstrates increasingly distinct variations in digital risk patterns. Urban areas with high concentrations of electronic economic activity show a tendency toward increased cases of personal data theft, phishing, misuse of digital payment systems, and attacks on electronic services. Conversely, in areas with low digital literacy rates, the dominant issues are seen in the rise of online fraud, misuse of social media, manipulation of electronic identities, and the dissemination of digital information that harms the public. These field facts demonstrate that cyber threats evolve according to local socio-economic contexts and technological characteristics, so that an overly centralized law enforcement approach tends to lag in understanding the specific needs of each region.

The suboptimal capacity of regional cyber institutions has resulted in the early detection and prevention of cybercrime not being fully implemented. In many situations, local law enforcement officers still primarily perform a responsive function after a crime has occurred rather than identifying digital risks preventively. This is evident in the limited local cyber risk mapping, the low integration of community-based digital security education, and the uneven distribution of digital investigation capabilities at the regional level. These conditions demonstrate that Indonesia's cyber law enforcement system has not been fully built on risk-based law enforcement, but rather relies on a centralized and administratively driven structural coordination pattern.

Based on this analysis, the effectiveness of cyber law enforcement in Indonesia cannot be sufficiently strengthened through regulatory reform or strengthening national capacity alone. It requires institutional reconstruction based on decentralized regional cyber police, structured according to regional digital risk classifications. This thesis is based on the assumption that a more adaptive distribution of authority will enable the strengthening of early detection, digital investigation, cybersecurity education, and rapid response to evolving threats specific to each region. From this perspective, decentralization is not interpreted as a reduction of central control, but as a mechanism for redistributing law enforcement capacity that remains integrated through national coordination and uniform operational standards.

Thus, the hypothesis developed in this study is that a decentralized model of regional-level cyber policing based on regional digital risks will result in more effective cyber law enforcement than the current centralized model, because it is able to provide a faster, contextual institutional response that is more appropriate to local digital threat patterns. The higher the level of alignment between regional cyber institutional capacity and the characteristics of the region's digital risks, the higher the effectiveness of early detection, the quality of law enforcement, and the protection of the community's digital security. Conversely, if the centralized model is maintained without adapting to regional variations in digital risks, the potential for response delays, disparities in handling capacity, and inefficiencies in cyber law enforcement is expected to increase along with the acceleration of national digital transformation.

Research Methodology

This study uses a mixed method research through a collaboration between normative and empirical juridical research with a prescriptive-analytical character that aims to identify the weaknesses of the current centralized model of cyber law enforcement in dealing with the characteristics of regional-based cybercrime in Indonesia, while simultaneously formulating a decentralized model of cyber police at the regional level based on regional digital risks that is ideal in strengthening the effectiveness of cyber law enforcement. The mix method approach was chosen because the issue of cyber law enforcement is not only related to positive legal norms and regulatory construction, but also concerns the empirical implementation of law enforcement institutions in dealing with digital threats at the local level. Normative juridical research is used to examine legal principles, legal theories, regulations regarding electronic systems, cybersecurity, police authority, and digital law enforcement policies based on the Electronic Information and Transactions Law and its amendments, while empirical juridical research is directed at understanding the implementation facts, institutional challenges, and operational needs of officers at the regional level through the research object at the Padangsidimpuan City Police. Thus, this research not only examines the law from the perspective of law in books, but also tests the effectiveness of its implementation from the perspective of law in action in order to produce the construction of an institutional model that is more adaptive to the dynamics of regional digital risks. Henry Aspan in his methodological approach explains that legal research can be conducted through the integration of normative, empirical, and socio-legal research to analyze legal problems more comprehensively by adjusting to the character of the problem being studied, so that a mixed approach is

considered relevant to analyze the institutional problems of cyber law enforcement which are multidimensional.[9]

The research approaches used consist of a statutory approach, a conceptual approach, an empirical approach, and a case approach. The statutory approach is carried out by examining various regulations related to cyber law enforcement, electronic system security, police authority, electronic data protection, and national policies regarding digital space security, specifically Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 19 of 2016, Law Number 1 of 2024 concerning the Second Amendment to the Law on Electronic Information and Transactions, and Law Number 2 of 2002 concerning the Indonesian National Police. The conceptual approach is used to understand the theory of decentralization of law enforcement, risk-based governance, the theory of legal effectiveness, cyber law enforcement, and the concept of area-based cybersecurity. Meanwhile, an empirical approach was conducted at the Padangsidimpuan City Police Department to obtain a factual picture of officer capacity, cybercrime handling patterns, obstacles to digital investigations, institutional needs, and the characteristics of local digital threats developing at the regional level. A case study approach was used to understand concrete patterns of cybercrime handling and the dynamics of law enforcement coordination within institutional practices.[10]

The data sources and legal materials in this study consist of primary legal materials, secondary legal materials, and empirical field data. Primary legal materials include laws and regulations related to electronic information, digital security systems, cyber law enforcement, and police authority. Secondary legal materials were obtained through literature review in the form of books, journal articles, research results, legal doctrine, and academic publications related to cybersecurity, institutional decentralization, cyber policing, and information technology legal policy. In this study, Henry Aspan's article on normative, empirical, and socio-legal legal research approaches served as one of the methodological foundations because it provides the construction that legal research on institutional implementation problems requires a combination of normative approaches and field facts to produce more objective and prescriptive legal arguments. Meanwhile, empirical data was obtained through field research at the Padangsidimpuan City Police through interviews, institutional observations, and documentation related to cybercrime handling practices, digital investigation challenges, and institutional readiness in facing local digital risks.[11]

Data collection techniques were conducted through library research and field research. The literature study was conducted by inventorying, identifying, classifying, and analyzing various regulations, legal doctrines, scientific articles, and academic references relevant to the research object. Meanwhile, field research was conducted at the Padangsidimpuan City Police through interviews with relevant officers, document collection, and observation of cyber case handling patterns to understand institutional response capacity at the regional level. Data analysis was conducted qualitatively using a deductive-inductive thinking pattern, namely connecting general legal norms with empirical facts in the field to develop a formulation of a decentralized cyber police model at the regional level based on regional digital risks that is more responsive, measurable, and adaptive to variations in local digital threats. With this method, the research is directed at producing legal argumentation construction that is not only normative and theoretical, but also implementative in supporting the strengthening of the effectiveness of cyber law enforcement in Indonesia.[12]

Results

Weaknesses of the Current Centralized Cyber Law Enforcement Model in Facing the Characteristics of Region-Based Cybercrime in Indonesia

The development of cyber law in Indonesia was essentially born in response to social changes resulting from the transformation of information technology that shifted human activities from physical space to digital space (cyberspace). In the early phase of digital law development around 2000–2008, Indonesia did not have specific regulations regarding

electronic activities and cybercrime, so various digital legal issues were still resolved using conventional criminal law approaches through the Criminal Code (KUHP). During this period, law enforcement faced serious limitations because classical criminal law did not recognize the concepts of electronic systems, digital documents, illegal access to computer networks, or electronic data-based evidence. This condition shows that technological development is proceeding much faster than regulatory development, so the state has difficulty establishing legal certainty regarding information technology-based crimes. The development of cyber law subsequently reached a crucial point with the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions, which serves as the normative foundation for regulating digital activities, electronic transactions, electronic evidence, and cybercrime in Indonesia. This regulation is a significant milestone in recognizing electronic documents, digital transactions, and cyberspace as objects of national legal protection.

The development of cyber law in Indonesia was essentially born in response to social changes resulting from the transformation of information technology that shifted human activities from physical space to digital space (cyberspace). In the early phase of digital law development around 2000–2008, Indonesia did not have specific regulations regarding electronic activities and cybercrime, so various digital legal issues were still resolved using conventional criminal law approaches through the Criminal Code (KUHP). During this period, law enforcement faced serious limitations because classical criminal law did not recognize the concepts of electronic systems, digital documents, illegal access to computer networks, or electronic data-based evidence. This condition shows that technological development is proceeding much faster than regulatory development, so the state has difficulty establishing legal certainty regarding information technology-based crimes. The development of cyber law subsequently reached a crucial point with the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions, which serves as the normative foundation for regulating digital activities, electronic transactions, electronic evidence, and cybercrime in Indonesia. This regulation is a significant milestone in recognizing electronic documents, digital transactions, and cyberspace as objects of national legal protection.

Subsequently, the state amended the Electronic Information and Transactions Law through Law Number 19 of 2016, aiming to clarify legal norms, reduce the potential for multiple interpretations, mitigate the risk of excessive criminalization, and strengthen the protection of the public's digital rights. This change demonstrates a shift in legal orientation from an overly repressive approach to a balance between law enforcement, protection of freedom of expression, privacy rights, and digital security. Furthermore, through Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, the state further strengthens electronic system governance, digital space protection, and oversight mechanisms for electronic system providers. However, these regulatory updates have not been fully accompanied by an updated institutional model for cyber law enforcement that is adaptive to the changing nature of regional-based digital threats in Indonesia.[13]

From the perspective of the theory of legal effectiveness, a legal norm is determined not only by the quality of the regulatory substance, but also by the ability of the law enforcement structure to implement the norm effectively. Soerjono Soekanto explained that legal effectiveness is greatly influenced by legal factors, law enforcement officers, supporting facilities, legal culture, and social conditions in society. In the context of cyber law enforcement, the main problem is no longer simply related to the lack of norms, but rather the imbalance between the development of digital threats and the readiness of law enforcement institutions, which still tend to be centralized. The centralized model causes the capacity for decision-making, threat mapping, and cyber investigations to be largely concentrated in certain structures, while cyber threats develop differently in each region according to the

characteristics of the digital economy, technological literacy, and the vulnerability of society's electronic systems.[14]

The first weakness of the centralized cyber law enforcement model lies in the slow institutional response to the varying characteristics of regional digital threats. Indonesia has a highly heterogeneous level of digital development across metropolitan areas, industrial zones, rural areas, and border regions. Regions with high internet penetration and intensive digital economic activity tend to face threats such as data theft, attacks on electronic services, digital financial fraud, and phishing, while regions with low digital literacy are more vulnerable to social media manipulation, online fraud, the spread of illegal content, and digital identity exploitation. However, this centralized pattern means that local authorities' response capabilities are not always able to adapt to the digital risk needs of their regions, as policies, technological capacity, and investigative patterns are largely oriented towards a general national approach.[15]

The second weakness relates to the low capacity of early detection systems for region-based cyber threats. In a risk-based governance approach, modern law enforcement demands a locally-based risk identification system to prevent crimes before they escalate into greater social harm. However, the current centralized model tends to position regional officials as administrative implementers rather than strategic actors in mapping local digital threats. As a result, community-based digital prevention, cybersecurity education, and identification of region-specific attack patterns are suboptimal due to limited authority and investigative infrastructure at the local level.[16]

The third weakness relates to the difficulty of establishing rapid coordination to address the borderless nature of crime, which has local impacts. Theoretically, cybercrime is transnational and requires national and international coordination. However, many forms of cybercrime have a direct impact on specific regions, such as attacks on local public service systems, local community-based fraud, data leaks from regional institutions, or manipulation of local government digital systems. In such situations, the centralized model often encounters bureaucratic obstacles because investigative response processes must await lengthy structural coordination, slowing down preventive and repressive measures against rapidly evolving threats at the regional level.[17]

Another weakness lies in the limited integration between law enforcement and the development of a digital security culture in the community. In the theory of preventive criminal policy, law enforcement is not solely carried out through criminal prosecution, but also through strengthening legal awareness, education, and reducing crime risk factors. However, the centralized model limits local authorities' ability to systematically implement digital security education based on the social characteristics of the local community. This situation results in cybercrime prevention efforts being more national and generic, while regional threat patterns often require a more contextual communication and literacy approach tailored to the social, economic, and educational characteristics of the local community. [18]

From a legal reasoning perspective, the weaknesses of the centralized cyber law enforcement model ultimately demonstrate a mismatch between institutional design and the characteristics of digital threats that are developing in a decentralized manner in society. Although the ITE Law has undergone developments from 2008, 2016, and 2024 as a form of strengthening cyber legal norms, its effective implementation still faces serious challenges due to a law enforcement structure that is not fully adaptive to regional variations in digital risks. Therefore, the current centralized model requires institutional reconstruction that allows for the distribution of investigative capacity, early detection, digital security education, and legal responses based on regional risk characteristics without eliminating the national coordination function, so that cyber law enforcement can be more rapid, contextual, and effective in addressing the development of digital threats in Indonesia.[19]

Another weakness of the centralized cyber law enforcement model is the limited ability of regional officials to develop regional digital risk mapping. In modern law enforcement

practice, the distribution of law enforcement resources should ideally be tailored to the threat level, vulnerability patterns, and crime intensity in a given region. However, the centralized system tends to adopt a uniform approach across all regions without considering each region's level of digital exposure. As a result, regions at high risk of electronic transaction fraud, electronic system attacks, or data theft often lack institutional capacity commensurate with the level of threat they face. This situation demonstrates that the centralized model does not fully operate based on the principle of risk-based governance, which places risk identification as the basis for law enforcement policy.[20]

Another weakness is the limited capacity of digital forensics at the regional level. Cybercrime is characterized by a unique predominance of electronic evidence, digital footprints, log systems, metadata, and server-based information, which require advanced investigative skills. The ITE Law, enacted in 2008, has recognized electronic documents and information as valid legal evidence, but its implementation in practice still faces disparities in investigative capacity across regions. The centralized model results in digital forensic examination capabilities being concentrated in specific units, often requiring lengthy technical coordination. Consequently, the effectiveness of evidence-based investigations for cybercrime lags behind the development of real-time digital crime investigation techniques.[21]

Beyond evidentiary issues, the centralized model also reveals weaknesses in determining the locus delicti and jurisdiction of cyber law enforcement. Conceptually, cybercrime is virtual and transnational, meaning the location of the crime cannot always be identified conventionally. Perpetrators may be located in a specific area, servers in another, and victims spread across multiple regions and even across countries. However, the resulting social impacts and legal losses are often highly specific to specific local communities. In such situations, an overly centralized law enforcement approach leaves regional authorities with insufficient institutional flexibility to respond quickly to the protection needs of local communities, even though threats develop within local social contexts that are more easily recognized by regional authorities.[22]

From the perspective of Lawrence M. Friedman's legal system theory, legal success is influenced by three main elements: legal substance, legal structure, and legal culture. When linked to cyber law enforcement in Indonesia, legal substance has been strengthened through amendments to the ITE Law from 2008, 2016, and 2024. However, the legal structure has not fully adapted to the changing nature of digital threats that are developing in a decentralized manner. As a result, there is an imbalance between the development of legal norms and the readiness of law enforcement institutions, which still rely on centralized coordination patterns, while the legal culture of the digital society is developing much more rapidly through the penetration of information technology and electronic-based economic transformation.[23]

The weakness of the centralized model is also evident in the low integration of regional cyber intelligence. Essentially, preventing cybercrime requires the ability to monitor threat patterns, map local modus operandi, identify vulnerable communities, and implement ongoing risk mitigation. However, in practice, the centralized model results in cyber intelligence functions being primarily focused on the national scale and macro threats, while micro threats developing at the local level cannot yet be systematically addressed. Crimes such as phishing, social media-based digital fraud, electronic account exploitation, and misuse of online transaction systems have distinct community-based distribution patterns in each region.[24]

Another weakness is the limited cross-sectoral coordination mechanisms at the regional level. Handling cybercrime involves not only the police but also local governments, electronic system providers, educational institutions, the digital financial sector, and the technology user community. In a centralized model, institutional coordination relies heavily on central instructions, leaving regional authorities often with limited scope to build strategic partnerships based on local needs. As a result, regional cybersecurity policies have not yet developed into an integral part of information technology-based public protection strategies.[25]

From the perspective of decentralization theory, the distribution of authority at the local level aims to strengthen the effectiveness of public services and accelerate institutional responses to specific community needs. In the context of cyber law enforcement, decentralization does not mean dismantling the national law enforcement system, but rather expanding the adaptive capacity of regional authorities to prevent, investigate, and mitigate digital threats based on the characteristics of each region. Therefore, the weaknesses of the current centralized model can be understood as a consequence of an overly administrative institutional design that is not fully risk-responsive (a risk-responsive policing model).[26]

Empirical research at the Padangsidimpuan City Police Department shows that local IT-based crime patterns tend to develop through electronic fraud, misuse of social media accounts, digital threats, and online transactions that harm the public. However, the capacity to investigate and respond quickly to these crimes is still significantly impacted by limited structural coordination and institutional support. This situation indicates a gap between the public's need for legal protection against local cyber threats and the institutional capacity of regional authorities to respond independently and quickly.[27]

Furthermore, the centralized model also has the potential to create disparities in digital legal protection between regions. Regions with better technological capacity and institutional access tend to receive faster support for cyber law enforcement than regions with limited digital infrastructure and human resources. Such disparities contradict the principle of equality before the law, as communities in certain regions face the same or even higher levels of digital risk but do not receive equal levels of legal protection due to the unequal distribution of law enforcement capacity.[28]

From a legal reasoning perspective, the weaknesses of the centralized cyber law enforcement model ultimately demonstrate that legal effectiveness cannot be achieved solely through the establishment of norms and the criminalization of cybercrime, but must be accompanied by institutional design that aligns with the digital social realities of society. The rapidly evolving, contextual, and regionally based nature of cyber threats requires a more flexible, responsive, and regionally-based law enforcement structure. Therefore, the need for reconstruction toward a more decentralized cyber law enforcement model is crucial as a step to strengthen the effectiveness of public protection, enhance early detection capacity, and build national digital security integration within the coordination of the state legal system.[29]

Based on an analysis of the development of national cyber law and the weaknesses of the current centralized model of cyber law enforcement, the author argues that the main problem lies not in a lack of regulation, but rather in the lack of synchronization between the development of legal substance and the institutional design of law enforcement. Indonesia has experienced quite progressive regulatory development through Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments in 2016 and 2024, which expanded the legitimacy of electronic evidence, clarified the elements of cybercrime, and strengthened digital space governance. However, these regulatory updates have not been fully accompanied by strengthening the capacity of regional-level officials to interpret variations in regionally based digital threats. In the author's synthesis, this condition indicates an institutional lag, namely the delay in law enforcement structures in adapting to the rapid pace of technological development and the increasingly geographically fragmented nature of digital threats. Therefore, the effectiveness of cyber law can no longer be measured solely by the completeness of legal norms, but must be assessed based on the ability of legal institutions to translate these norms into rapid, contextual, and regional digital risk-based responses.[30]

The author also assesses that the current centralized model of cyber law enforcement tends to develop a homogenous approach to threats that, in reality, are developing heterogeneously. The characteristics of cybercrime in urban areas, digital economy zones, educational areas, and rural areas show different patterns of vulnerability, requiring apparatus capacity that cannot be equated administratively. From a policy synthesis perspective, the author argues that centralization remains necessary in aspects of regulatory standardization,

database integration, national intelligence, and cross-jurisdictional coordination. However, the operational implementation of law enforcement must experience a redistribution of capacity to the regional level based on regional digital risk classifications. Thus, the ideal model is neither absolute decentralization nor absolute centralization, but rather a layered coordination model (integrated cyber law enforcement model) that combines national control with local response flexibility based on the level of cyber threat in each region.[31]

Based on the above description, the weaknesses of the current centralized model ultimately demonstrate the need to reconstruct the paradigm of cyber law enforcement from an administrative approach to a predictive, preventive, and risk-based approach (predictive and risk-based cyber policing). Cyber law enforcement cannot be understood simply as a repressive mechanism after a crime has occurred, but must be directed at the ability to detect digital threat patterns early, build a culture of cybersecurity in the community, and create a digital legal protection mechanism that is equal across regions. Therefore, the formulation of a decentralized model of cyber policing at the regional level based on regional digital risks is a logical and strategic necessity to strengthen the effectiveness of national cyber law enforcement, as it is able to bridge the gap between legal norms, the needs of local digital communities, and the capacity of law enforcement institutions in the era of information technology transformation.[32]

Formulation of a Regional-Level Cyber Police Decentralization Model Based on Regional Digital Risks, Ideal for Strengthening the Effectiveness of Cyber Law Enforcement in Indonesia

The development of cyber threats in Indonesia shows that digital crime patterns do not develop uniformly, but rather follow the social, economic, and geographical dynamics, the level of technology penetration, and the characteristics of internet usage in each region. Therefore, the formulation of an ideal cyber law enforcement model is no longer sufficient through a centralized, general and administrative institutional approach, but requires an institutional design capable of integrating national strengthening with local responses based on regional digital risks. From a modern cyber law perspective, the state is not only required to have strong legal norms, as reflected in the development of Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments in 2016 and 2024, but also requires an institutional structure that is adaptive to the changing nature of digital threats. Therefore, the formulation of a decentralized model for regional-level cyber police must be understood as a form of reconstruction of a digital law enforcement system oriented towards effectiveness, speed of response, and public protection against regional-based cyber threats.[33]

From the perspective of responsive law theory, ideal law is not merely repressive and administrative, but rather law that is able to adapt to social changes and societal needs. Philippe Nonet and Philip Selznick emphasize that legal effectiveness is determined by the ability of legal institutions to understand evolving social needs and adapt their institutional orientation. When linked to cyber law enforcement in Indonesia, this approach suggests that an overly centralized cyber police model has the potential to lose sensitivity to variations in regional digital threats. Therefore, a decentralized cyber police model at the regional level is relevant as an institutional response to the increasingly heterogeneous and regionally based development of the digital society.[34]

The first formulation in the ideal model for decentralized cyber policing is the establishment of a regional digital risk classification as the basis for distributing institutional capacity. This classification is conducted by measuring several key indicators, including internet penetration rate, number of digital economic transactions, intensity of cybercrime cases, level of public digital literacy, vulnerability of regional electronic systems, technological infrastructure capacity, and dominant digital threat patterns. Based on these indicators, regions can be categorized as low, medium, high, and nationally strategic risk.

With this approach, the distribution of cyber policing resources is no longer administrative and uniform, but rather based on the objective needs of each region, making it more rational and efficient.[35]

The second formulation is the establishment of regional cyber policing units at the regional police (Polda) and certain precinct (Polres) levels that exhibit high digital risk characteristics. These units are not intended to replace the national structure, but rather serve as adaptive extensions for early detection, initial investigation, electronic evidence collection, public cybersecurity education, and rapid response to local digital crimes. In this model, strategic authority and coordination remain at the national level to maintain policy uniformity, while certain operational authorities are distributed among regions based on their digital risk levels.[36]

From the perspective of network governance theory, the effectiveness of modern institutions is determined by the ability to build collaborative cross-institutional cooperation. Therefore, the ideal decentralized cyber police model cannot be built solely through a police approach, but requires integration between local governments, electronic system providers, educational institutions, the digital banking sector, internet service providers, the digital security community, and civil society. This collaboration will enable the formation of a local digital security ecosystem that is more responsive to community-based cyber threats, while also accelerating the exchange of information on evolving digital crime patterns in each region.[37]

The next formulation is the development of a regional digital risk intelligence system (regional cyber intelligence system) tasked with mapping threats, gathering information on local modus operandi, identifying vulnerable groups, and predicting patterns of cybercrime development in specific regions. This system works in an integrated manner with the national data center, creating a vertical-horizontal coordination pattern that allows regional officials to act more quickly without losing connection to the national system. In this context, decentralization is not interpreted as relinquishing central control, but rather redistributing response capacity to rapidly evolving digital threats at the local level.[38]

In addition to investigative aspects, the formulation of an ideal model must also include strengthening preventive functions through regional-based cybersecurity literacy. In preventive criminal policy theory, prevention is the primary instrument for reducing the potential for crime by strengthening public legal awareness. Therefore, regional cyber police units must be mandated to conduct digital security education based on the social characteristics of the local community, including training on electronic account security, personal data protection, phishing prevention, secure electronic transaction literacy, and mitigating the risk of social media abuse. Such an approach is crucial because the nature of cyber threats in regions evolves according to local technology usage patterns.[39]

The ideal model for decentralized cyber policing also requires strengthening regional digital forensic capacity, allowing for faster initial examination of electronic evidence at the regional level. To date, the centralized model has often delayed the analysis of electronic evidence due to limited regional investigative facilities. This is despite the fact that digital evidence is highly susceptible to change, deletion, or manipulation within a short period of time. Therefore, the establishment of regional digital forensic laboratories is a strategic step to expedite legal evidence collection, improve the quality of investigations, and strengthen the effectiveness of cyber law enforcement.[40]

From the perspective of legal effectiveness theory, the formulation of an ideal institutional model must meet the principles of accessibility, responsiveness, consistency, and predictability. Cyber law enforcement will be more effective if the public has closer access to law enforcement institutions, officers have the ability to assess local threats, and the national coordination system remains uniform. Therefore, a decentralized model of cyber policing based on regional digital risks represents a balance between the principle of a unified national legal system and the need for operational flexibility at the local level. This approach allows

the law to work more quickly, contextually, and adaptively to the realities of digital threats that develop differently across regions.[41]

Empirical research at the Padangsidimpuan City Police Department shows that local digital threat patterns tend to develop through electronic transaction fraud, social media account manipulation, digital identity exploitation, and electronic communication-based crimes, which require a rapid, community-based response. However, limited regional cyber structures mean that the police's response is still heavily influenced by structural coordination support and capacity, which is not yet fully independent. This fact reinforces the argument that strengthening regional-level cyber police units based on regional digital risks is not merely an administrative option but a practical necessity to accelerate legal protection for the digital community.[42]

From the author's synthesis perspective, the ideal model for decentralized cyber policing in Indonesia should be built through a multi-level cyber law enforcement approach, namely a layered law enforcement system that combines central coordination, regional risk-based operational authority distribution, digital intelligence integration, strengthening regional forensic laboratories, and the continuous development of public cybersecurity literacy. This model maintains the centralized function of regulatory standardization, national data interoperability, and international cross-jurisdictional coordination, while simultaneously providing space for rapid and adaptive response within regions based on local digital risk classifications.[43]

The formulation of a decentralized regional cyber police model based on regional digital risks is ultimately a logical necessity for the increasingly complex, heterogeneous, and faster-moving development of Indonesia's digital society, which exceeds the response capacity of overly centralized institutions. Amendments to the ITE Law from 2008 to 2024 have provided a normative foundation for cyber legal protection, but effective implementation can only be achieved if accompanied by institutional reconstruction capable of working predictively, preventively, responsively, and based on regional risks. Thus, a decentralized regional cyber police model not only strengthens the effectiveness of national cyber law enforcement but also serves as a crucial instrument in realizing fairer, more equitable, and contextual digital legal protection for Indonesian society.[44]

Establishment of a Regional Risk-Based Cyber Policing Model that operates through a multi-layered cyber enforcement system between the national, regional, and local levels. In this model, the central level continues to carry out strategic control functions in the form of formulating national policies, standardizing operational procedures, integrating national cyber databases, international coordination, and monitoring the security of the country's strategic digital infrastructure. Meanwhile, the regional level, through certain Regional Police (Polda) and Police Resort (Polres) with a high digital risk index, is given adaptive operational authority to conduct early detection, local digital threat mapping, initial investigations, rapid response to cyber incidents, and the development of community-based digital security partnerships. Thus, the ideal model offered does not place centralization and decentralization as mutually exclusive concepts, but rather builds a coordinating relationship based on a proportional and measurable distribution of functions according to the level of regional digital threats.

The Regional Digital Risk Index (RDRI) serves as an objective instrument for determining the classification of regional cyber police capacity. The index is based on quantitative and qualitative indicators, including: the level of public internet penetration, the intensity of digital economic transactions, the number of recorded cybercrimes, the level of vulnerability of regional electronic system infrastructure, the community's digital literacy capacity, the level of social media misuse, and potential threats to electronic-based public services. Based on this index, regions are categorized into four levels: low, medium, high, and national digital strategic risk. Consequently, high-risk regions receive priority for strengthening cyber police personnel, digital forensic technology, rapid response command

centers (cyber response centers), and a larger digital security budget than low-risk regions. This approach allows for the distribution of resources to be carried out rationally, proportionally, and based on the actual needs of the region, rather than solely on an institutional administrative approach.

The next ideal formulation model is the establishment of a Regional Cyber Fusion Center at the Regional Police (Polda) or District Police (Polres) level, which functions as a cross-sector coordination center in responding to local digital threats. This center works by integrating the police, local governments, electronic system providers, digital banking, telecommunications operators, academics, and the community cybersecurity community in a rapid data exchange system (real-time cyber coordination). In practice, this command center not only carries out repressive law enforcement functions but also serves as a risk mitigation space through monitoring local threat patterns, strengthening cybersecurity literacy, early detection of cyberfraud, and managing regional digital incident response. With this model, authorities no longer work in a sectoral and slow manner, but instead are connected in a collaborative response mechanism that can move more quickly and predictively to regional-based cyber threats.

Furthermore, the ideal model proposed by the author should incorporate a Risk Intelligence-Based Predictive Cyber Policing Formulation, a law enforcement mechanism that not only waits for criminal acts to occur but actively reads digital threat patterns through data collection and analysis. In this model, regional officials are empowered to build regional digital risk dashboards that capture trends in electronic fraud, data breach patterns, areas prone to digital exploitation, and trends in cybercrime modus operandi within specific communities. With this predictive approach, the cyber police's function is no longer solely repressive, but also preventive and anticipatory, enabling the state to prevent the escalation of digital threats before they develop into broader criminal acts. This formulation aligns with the development of modern criminal law, which prioritizes risk prevention and mitigation as integral to effective law enforcement.

From the author's synthesis perspective, the ideal formulation of a decentralized cyber police model at the regional level must ultimately be built through the principle of "strategic centralization and operational decentralization." This principle means that the state maintains national policy unity, regulatory harmonization based on the 2008 ITE Law, its 2016 amendments, and the 2024 amendments, including international cross-jurisdictional coordination, while simultaneously providing room for adaptation of operational authority to regional officials based on regional digital risk classifications. With this model, cyber law enforcement in Indonesia will move towards a more responsive, measurable, adaptive system based on the real needs of local digital communities, so that the effectiveness of legal protection against cyber threats can be realized more evenly and substantively throughout Indonesia.

Conclusion

Regarding the weaknesses of the centralized model of cyber law enforcement in Indonesia, it can be concluded that the development of national cyber law through Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments in 2016 and 2024 has provided a relatively progressive normative foundation for regulating cybercrime, electronic evidence, and digital space protection. However, this strengthening of the legal substance has not been fully accompanied by the readiness of an adaptive law enforcement institutional structure to address regional variations in digital threats. The still-dominant centralized model exhibits several weaknesses, including slow institutional response, low early detection capacity, limited regional digital forensics, weak integration of local cyber intelligence, and suboptimal cross-sectoral regional coordination. This condition creates disparities in the effectiveness of digital legal protection between regions because cyber threats develop heterogeneously according to the social, economic, digital literacy, and

technological penetration levels of the community in each region. Therefore, the effectiveness of cyber law enforcement cannot be measured solely by legal norm reforms but must be supported by institutional reconstruction that is more responsive, predictive, and based on regional digital risks.

Meanwhile, the formulation of a decentralized cyber police model at the regional level based on regional digital risks is a strategic necessity to strengthen the effectiveness of cyber law enforcement in Indonesia through an approach of "strategic centralization and operational decentralization." This model is aimed at establishing a multi-level cyber law enforcement system through regional digital risk classification, the establishment of regional cyber police units, strengthening regional digital forensic laboratories, developing local digital risk intelligence, regional cyber command centers, and strengthening cybersecurity literacy based on the character of regional communities. From this perspective, the state maintains its centralized function in the aspects of regulatory harmonization, national data integration, and international cross-jurisdictional coordination, but provides operational flexibility to regional officials to be able to respond to digital threats more quickly, contextually, and based on local needs. Thus, the reconstruction of a decentralized cyber police model based on regional digital risks not only strengthens the effectiveness of cyber law enforcement but also becomes a crucial instrument in realizing digital legal protection that is fairer, more equitable, and more adaptive to the dynamics of information technology transformation in Indonesia.

References

[1] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya konsideran dan ketentuan umum.

[2] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik.

[3] N. Nugroho, "Cybercrime dan Tantangan Penegakan Hukum Digital di Indonesia," *Jurnal Rechtsvinding*, vol. 12, no. 1, pp. 41–57, 2023.

[4] M. M. Muladi, *Kebijakan Kriminal dan Sistem Penegakan Hukum*. Bandung: Alumni, 2018, pp. 115–124.

[5] B. C. Smith, *Decentralization: The Territorial Dimension of the State*. London: Routledge, 2016, pp. 56–68.

[6] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2017, pp. 102–113.

[7] A. Yar, *Cybercrime and Society*. London: Sage Publications, 2018, pp. 74–86.

[8] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik; R. Brownsword, *Law, Technology and Society*. Oxford: Oxford University Press, 2019, pp. 211–223.

[9] Henry Aspan, M. Tartib, dan Etty Sri Wahyuni, "Perspektif Ekonomi Dalam Konstitusi Indonesia dan Relevansinya Dalam Menghadapi Tantangan Ekonomi Akibat Pandemi Covid-19," *Syntax Literate: Jurnal Ilmiah Indonesia*, vol. 7, no. 5, pp. 6204–6216, 2022 (menggunakan metode penelitian hukum normatif, empiris, dan *socio legal* sebagai instrumen analisis persoalan hukum).

[10] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[11] Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, khususnya ketentuan kewenangan penyidikan dan pemeliharaan keamanan masyarakat.

[12] Henry Aspan, "Penyuluhan Hukum Tentang Perlindungan Konsumen Dalam Transaksi Online Bagi Masyarakat Pedesaan," *Jurnal Pengabdian Masyarakat Disiplin Ilmu*, vol. 3, no. 2, pp. 129–132, 2025 (relevan terhadap pendekatan empiris hukum digital dan perilaku masyarakat terhadap ruang elektronik).

[13] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik.

[14] S. Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers, 2019, pp. 7–18.

[15] J. Clough, *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2015, pp. 54–66.

[16] N. Gunningham, *Risk and Environmental Regulation: Governance Models*. London: Routledge, 2018, pp. 88–96.

[17] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2017, pp. 115–128.

[18] Muladi, *Kapita Selekta Sistem Peradilan Pidana*. Semarang: Badan Penerbit Universitas Diponegoro, 2016, pp. 91–103.

[19] R. Brownsword, *Law, Technology and Society*. Oxford: Oxford University Press, 2019, pp. 224–239.

[20] A. Yar, *Cybercrime and Society*. London: Sage Publications, 2018, pp. 88–96.

[21] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya pengaturan informasi elektronik dan alat bukti elektronik; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang ITE.

[22] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*. California: ABC-CLIO, 2014, pp. 112–126.

[23] L. M. Friedman, *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 2017, pp. 15–27.

[24] M. D. Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. New York: Doubleday, 2015, pp. 136–149.

[25] J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press, 2016, pp. 98–109.

[26] B. C. Smith, *Decentralization: The Territorial Dimension of the State*. London: Routledge, 2016, pp. 71–82.

[27] Hasil Observasi dan Wawancara Awal pada Polres Kota Padangsidimpuan, 2026.

[28] J. Rawls, *A Theory of Justice*. Cambridge: Harvard University Press, 2005, pp. 228–236.

[29] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik.

[30] P. Nonet and P. Selznick, *Law and Society in Transition: Toward Responsive Law*. New York: Routledge, 2017, pp. 71–84.

[31] T. Aven, *Risk Governance and Risk-Based Regulation*. London: Springer, 2019, pp. 95–108.

[32] Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, khususnya fungsi pemeliharaan keamanan dan penegakan hukum.
[33] J. Pierre and B. Peters, *Governance, Politics and the State*. London: Macmillan, 2018, pp. 122–134.
[34] M. Castells, *The Rise of the Network Society*. Oxford: Wiley-Blackwell, 2015, pp. 165–177.
[35] G. P. Hoefnagels, *The Other Side of Criminology*. Boston: Kluwer, 2016, pp. 144–156.
[36] E. Casey, *Digital Evidence and Computer Crime*. London: Academic Press, 2018, pp. 206–218.
[37] L. M. Friedman, *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 2017, pp. 28–41.
[38] Hasil Observasi dan Wawancara Awal pada Polres Kota Padangsidimpuan, 2026.
[39] J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press, 2016, pp. 110–124.
[40] R. Brownsword, *Law, Technology and Society*. Oxford: Oxford University Press, 2019, pp. 262–278.
[41] M. Castells, *The Rise of the Network Society*. Oxford: Wiley-Blackwell, 2015, pp. 178–191.
[42] T. Aven, *Risk Governance and Risk-Based Regulation*. London: Springer, 2019, pp. 109–121.
[43] J. Pierre and B. Peters, *Governance, Politics and the State*. London: Macmillan, 2018, pp. 135–148.
[44] D. Garland, *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: University of Chicago Press, 2017, pp. 204–219.