International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 09-03-2026, Accepted: 09-04-2026, Published: 24-04-2026
Volume 12, Issue 2, 2026, Page No. 205-208

Cyber criminal policy in maintaining public security and order in the jurisdiction of the Aceh Regional Police

T Ricki Fadlianshah[1], Dahlan[2], Teuku Saiful[2]
[1] Department of Law, University Syiah Kuala Banda Aceh, Indonesia
[2] Lecture, Department of Law, University Syiah Kuala Banda Aceh, Indonesia

Abstract
Cybercrime is a crime against computer systems or networks and crimes that use computer facilities. The modernization process in using information technology has given rise to crime patterns that are increasingly easy to commit, so that it is necessary to implement swift, precise and transparent countermeasures. Cybercrime in the jurisdiction of the Aceh Regional Police requires quite serious attention. Based on reports from the Aceh Regional Police units and their ranks in the last five years between 2020 and 2025, there have been 378 (one hundred and fifty-eight) cybercrimes consisting of defamation, fraud, illegal access, threats, hoaxes, gambling and others that have occurred quite high which have resulted in unrest in the community. This study uses an empirical legal research method or known as empirical law research. Criminal policies that can be implemented in overcoming cybercrime start from the reformulation of penal policies consisting of repressive action against cybercrime perpetrators in the Aceh Regional Police jurisdiction, strengthening coordination in the criminal justice system to overcome cybercrime, prioritizing the resolution of cybercrime cases based on restorative justice. Non-penal policies in combating cybercrime are implemented through community empowerment in combating cybercrime and intensified cyber patrols by the Cyber Unit of the Aceh Regional Police's Criminal Investigation Directorate.

Keywords: Cybercrime, criminal policy, police, aceh

Introduction
In the current era of globalization, many cases occur through the use of information technology or the internet. Therefore, the law must not "lag behind." This term refers to the rapid development of society, and legal regulations are no longer appropriate or even non-existent (Abdul Muthalib: 2018) [1].
The law is said to lag behind when the legal norms stipulated in statutory regulations fail to fulfill their function of maintaining order in society or providing legal certainty in relations between citizens and their respective countries.
Indonesia is the fourth-largest country in the world in terms of internet usage. According to databoks, the number of internet users in Indonesia has continued to increase over the past five years, with 204.7 million internet users in Indonesia by early 2025. Compared to 2018, the number of national internet users has jumped 54.25%.
On the other hand, the increasing use of the internet has led to the development of information technology, leading to an addiction to technology, and a surge in more modern criminal ideas called cybercrime, which can disrupt security stability (Fitriani Ahlan Sjarif: 2024).

Research Method
The type of research used in this study is empirical-juridical, namely, a comprehensive study through direct observations and interviews at the research location. To complement this research, a literature review was also conducted, including reviewing several laws and regulations related to the problem under study, which served as secondary material in this study.
Empirical legal research, also known as sociological legal research, is also called field research. This empirical legal research starts from primary data, namely data obtained directly from the community as the primary source through field research, which is conducted through observation and interviews, observation, and questionnaire distribution. Therefore, empirical-juridical research is understood as a legal research method that seeks to examine law in a concrete sense, or in other words, to observe how law works in society.

Discussion
In the era of the Industrial Revolution 4.0, society is evolving towards a new, global society. This has resulted in shifts and changes in values, norms, morals, and ethics. This is due to the rapid development of science and technology, which has been utilized in society, having a significant impact on human development and civilization, both negative and positive.
The development of science and technology aims to transform human life toward a better, easier, faster, cheaper (efficient), and safer one. However, in its use, new problems arise, which are the negative impacts of this development.
The negative impacts that arise include deviations that negatively impact users and the misuse of technology for criminal acts, known as cybercrime. Rapid technological advancements have given rise to cybercrime, which has negative impacts. On the one hand, technology has enabled convenient communication through social media and the ability to pay bills through e-banking. On the other hand, this same technology has also paved the way for criminal activities such as hacking, where individuals exploit vulnerabilities in systems to steal sensitive information. These negative impacts highlight the importance of maintaining strong cybersecurity measures in the digital age (Muhammad Hatta: 2020).
Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) contains provisions governing the

crime of hacking in Article 30 paragraphs (1), (2), and (3). Based on these provisions, individuals who unlawfully attempt to infiltrate or gain access to another person's electronic system will be considered violating the law. Furthermore, Article 46 paragraphs (1), (2), and (3) of the ITE Law outlines criminal sanctions for those found guilty of violating the provisions of Article 30. These two articles work together to ensure that individuals involved in hacking activities are held accountable for their actions (Raodia: 2019).

The development of digital technology has brought about significant changes in various aspects of people's lives. The internet facilitates communication, economic transactions, and rapid and widespread access to information. However, on the other hand, these technological advances also open up opportunities for cybercrime, such as online fraud, defamation, the distribution of illegal content, system hacking, and the misuse of personal data (Barda Nawawi Arief: 2010).

Cybercrime is a serious concern for law enforcement officials, including the Indonesian National Police. Investigators, as law enforcement officers at the regional level, play a crucial role in combating and enforcing the law against cybercrime in the Aceh region. Law enforcement against cybercrime has its own characteristics because perpetrators can be transnational and even international, and requires specialized technical expertise.

Law enforcement against cybercrime within the jurisdiction of investigators is based on the provisions of applicable laws and regulations, particularly the Electronic Information and Transactions Law (UU ITE). In practice, investigators, through the Directorate of Special Criminal Investigation (Ditreskrimsus), handle public reports and complaints regarding cybercrime.

The law enforcement process begins with the inquiry stage, then the inquest, and ends with the transfer of the case to the prosecutor's office. In cybercrime cases, police officers are required to possess technical skills in collecting and analyzing digital evidence. This presents a unique challenge due to the complex and dynamic nature of cybercrime.

Law enforcement against cybercrime within the jurisdiction of investigators is guided by the provisions of laws and regulations, particularly the Law on Information and Electronic Transactions. Case handling is carried out by the Directorate of Special Criminal Investigation (Ditreskrimsus) through the stages of inquiry, inquest, and the transfer of the case to the prosecutor's office.

In practice, police officers are required to be capable of collecting and analyzing digital evidence. This shows that the success of cybercrime law enforcement is highly dependent on the technical capabilities and professionalism of law enforcement officers (Soerjono Soekanto: 2014).

Table 1: Types of ITE Crimes, Criminal Threats, and Case Examples

No.	Types of Crimes	Act	Criminal Threats	Cases
1	Content that violates morality	Article 27 p. (1)	Maximum imprisonment of 6 years and/or a maximum fine of IDR 1 billion (Article 45 paragraph (1))	The distribution of pornographic videos via instant messaging applications is being handled by the Directorate of Special Criminal Investigation..
2	Online gambling	Article 27 p. (2)	Maximum 6 years in prison and/or a maximum fine of Rp1 billion	Management of online gambling sites and promotion through social media revealed by investigators.
3	Defamation	Article 27 p. (3)	Maximum imprisonment of 4 years and/or a maximum fine of IDR 750 million (Article 45 paragraph (3))	Public reports regarding Facebook posts accusing someone of committing a crime without evidence.
4	Blackmail/Threats	Article 27 p. (4)	Maximum 6 years in prison and/or a maximum fine of Rp1 billion	The case of threats via WhatsApp with a request for money was handled by cyber investigators.
5	Fake news that harms consumers	Article 28 p. (1)	Maximum imprisonment of 6 years and/or a maximum fine of IDR 1 billion (Article 45A paragraph (1))	Online buying and selling fraud (fictitious) via marketplaces and social media.
6	Hate Speech	Article 28 p. (2)	Maximum 6 years in prison and/or a maximum fine of Rp1 billion	Social media posts that sparked hostility between community groups in Aceh.
7	Threat of Violence	Article 29	Maximum imprisonment of 4 years and/or a maximum fine of Rp. 750 million (Article 45B)	Sending messages threatening violence via electronic media against specific individuals.
8	Illegal Acsess (hacking)	Article 30 p. (1) and p. (2)	Maximum imprisonment of 6–8 years and/or a maximum fine of Rp. 600 million–Rp. 800 million (Article 46)	Hacking of victims' social media and email accounts for fraudulent purposes.
9	Electronic Manipulation/Disappearance	Article 32 p. (1)	Maximum imprisonment of 8 years and/or a maximum fine of IDR 2 billion (Article 48 paragraph (1))	Deletion of electronic data belonging to the victim resulting in economic loss.
10	Electronic System Disturbance	Article 33	Maximum imprisonment of 10 years and/or a maximum fine of IDR 10 billion (Article 49)	An attack on an institution/agency's electronic system that causes the system to be temporarily paralyzed.
11	Electronic Information Falsification	Article 35	Maximum prison sentence of 12 years and/or a maximum fine of IDR 12 billion (Article 51 paragraph (1))	Falsification of proof of transfer and electronic documents in online fraud cases.
12	Actions that cause harm to others	Article 36	Following the criminal threat of the main article (Article 51 paragraph (2))	Online fraud causing significant financial losses to victims in Aceh.

Based on investigator data for the 2020–2025 period, the number of cybercrimes shows a fluctuating trend with an upward trend. A significant increase occurred in the 2021–2023 period, which correlates with the increased use of social media, electronic transactions, and online activities following the Covid-19 pandemic.

Statistically, the average growth rate of cybercrime cases reached double-digit percent per year, particularly for online fraud and defamation. This condition indicates that cybercrime has become a dominant form of crime compared to conventional crime. When classified based on the offenses or articles formulated in the ITE Law, the composition of cybercrimes in the investigator's jurisdiction is dominated by:

1. Online Fraud and Fake News Harming Consumers (Article 28 paragraph (1) in conjunction with Article 45A of the ITE Law) → Ranked first with the highest percentage.
2. Defamation and Insults (Article 27 paragraph (3) in conjunction with Article 45 paragraph (3)) → Generally occurs through social media such as Facebook and WhatsApp.
3. Hate Speech Based on SARA (Article 28 paragraph (2)) → Although smaller in number, it has a broad impact on social stability.
4. Illegal Access and Account Hacking (Article 30 of the ITE Law) → Tends to increase in recent years.

Statistically, according to the data in the table above, more than 60% of cybercrime cases handled by investigators are directly related to economic losses and social conflicts occurring within their jurisdiction. When analyzed using the Case Clearance Ratio, the data shows that investigators' cybercrime case resolution rate is in the range of 65-80% per year. This ratio is considered quite good, but there are also several obstacles in cybercrime cases:

a. Using anonymous accounts;
b. Involving servers or perpetrators outside Aceh, and;
c. Involving cross-border transactions.

Based on these facts, it shows that quantitatively, case-handling capacity has increased, but qualitatively, it still requires strengthening in the field of digital forensics. Statistically, there is no direct correlation between the severity of criminal penalties and the frequency of cybercrimes. For example, Article 35 of the ITE Law, which carries a penalty of up to 12 years in prison, is relatively rare, but cybercrimes stipulated in Articles 28 paragraph (1) and 27 paragraph (3) are the most frequently violated, despite carrying a lighter penalty. This indicates that the effectiveness of criminal penalties has not fully functioned as a deterrent, making a preventative approach and digital literacy crucial. From a criminal statistics perspective, Cybercrime data from investigators shows that:

a. Cybercrime has become a dominant technology-based crime;
b. Crime patterns are opportunistic and based on victim negligence;
c. Law enforcement tends to be reactive, following public reports.

Based on the statistical analysis of cybercrime cases conducted by investigators from 2020 to 2025, there is a trend of increasing cases, particularly those related to online fraud and defamation. This condition indicates that cybercrime has developed into a dominant form of crime and requires adaptive, technology-based law enforcement strategies supported by increased public digital literacy.

Crimes committed through information and telecommunications media by illegally accessing computer networks via the internet represent a new form of crime or a new and contemporary dimension, and are therefore often known as cybercrime. Cybercrime is a relatively new form of crime compared to other forms of conventional crime (street crime). Cybercrime emerged simultaneously with the birth of the information technology revolution.

In a narrow sense, cybercrime is an illegal act that targets computers or digital devices, either in terms of system security or data. Broadly speaking, cybercrime encompasses all forms of crime directed against computers or digital devices, computer networks, and their users, as well as conventional crimes involving computer equipment.

Conclusion

Law enforcement regarding cybercrime within the jurisdiction of the Aceh Regional Police is guided by statutory provisions, specifically the Electronic Information and Transactions Law. Case handling is carried out by the Special Criminal Investigation Directorate through the stages of inquiry, inquest, referral to the prosecutor's office, and presentation of evidence in court. This law enforcement process is divided into three aspects: investigation, prosecution, and court hearings, where weaknesses remain and have not been optimal.

Obstacles to combating cybercrime within the Aceh Regional Police jurisdiction include suboptimal cybercrime law enforcement mechanisms, a lack of a practical plan for combating cybercrime, and the need to establish a dedicated cyber unit within the Aceh Regional Police. This unit must possess the necessary knowledge, skills, and attitude to handle cybercrime cases. Finally, a significant obstacle to combating cybercrime is the low level of public awareness of cyber law.

Suggestion

Suggestion: The Aceh Regional Police Chief, Up. The Head of Operations and the Directorate of Special Criminal Investigation (Dir Reskrimsus) should establish units within each Aceh Regional Police (Polda Aceh) and establish a Memorandum of Understanding (MoU) with Komdigi, Telecommunications Providers, the Financial Services Authority (OJK), Banking Institutions, and Public Service Providers engaged in Electronic Transaction Information (ITE) activities. These organizations have duties and responsibilities in the Information Technology (IT) sector and have targets for improving public understanding and utilization of IT to reduce opportunities for cybercrime. They should also conduct monthly analyses and evaluations.

References

1. Muthalib A. Legal Changes Due to Changes in Time, Place, and Circumstances. Jurnal Hikmah, 2018, 15(1).
2. Noorhaliza AK. Friedman's Law Enforcement Theory Regarding the Issue of Narcotics Use for Medical Purposes: Relevance to Moral and Legal Considerations. Nusantara: Journal of Education, Arts, Sciences, and Social Humanities, 2024, 1(2).
3. Erdiansyah. Regulation of Cyber Crime in Indonesian Criminal Law. Thesis, Postgraduate Program in Law, Islamic University of Indonesia, Yogyakarta, 2007.
4. Atmaja IGBAK. The Role of Cyber Law in Law Enforcement Against Cyber Crime. Aktual Juctice: Scientific Journal of the Master of Law Postgraduate Program, Ngurah Rai University, 2025, 10(1).

5. Siregar JLH. The Role of Police Investigators in Proving Cyber Crimes. Thesis, Postgraduate Program, Master of Business Law, Medan Area University, Medan, 2010.
6. Aldriano MA, Priyambodo MA. Cyber Crime from a Criminal Law Perspective. Citizenship Journal, 2022, 6.
7. Wibowo MSI, *et al*. Technical and Legal Obstacles in the Investigation Process of Cyber Crimes in Indonesia. Rewang Rencang: Jurnal Hukum Lex Generalis, 2024, 5(7).