

CRIMINOLOGY APPROACH IN SOLVING CYBER CRIME

Azhar AR¹, Yasmirah Mandasari Saragih², Fauzan³

^{1,2,3} Universitas Pembangunan Panca Budi, Indonesia

Keywords

Cybercrime, Forms of cybercrime, Criminological Theory, Resolution strategies

Cybercrime, as a modern form of criminal activity, presents unique challenges due to its reliance on information and communication technology, the anonymity of perpetrators, and its cross-jurisdictional nature. This phenomenon encompasses a wide range of illegal activities, including hacking, identity theft, the spread of malware, on line fraud, and child exploitation in cyberspace. While legal frameworks and technological measures are essential in combating cybercrime, they are often insufficient to address the complex and evolving nature of cybercrime. The criminological approach provides a multidimensional perspective for understanding society's motives, behavior and responses to cybercrime. By integrating criminological theories, such as labeling theory and routine activity theory, this approach explores the root causes of cybercriminal behavior. Additionally, criminology offers insights into preventative measures and the development of more effective policies to mitigate cybercrime. This paper highlights the importance of applying a criminological framework to analyze cybercrime and proposes strategies for solving it through a combination of legal, technological interventions.

Email :
adek170873@gmail.com
yasmirahmandasari@gmail.com
fauzan123.dosen@gmail.com

Copyright 2024 Fox Justice : Journal Legal studies


INTRODUCTION

Development technology information And communication has bring impact big in various aspect life human , good in a way individual , social , and global. Digital technology is now become the part that is not inseparable from activity everyday , such as communication , transaction economy , education , until entertainment . However , in come back various benefits offered , progress technology also creates challenge new in the form of threat cybercrime , which is known as act criminal cyber (Yar, 2019).

Action criminal cyber or cybercrime refers to a variety of action violate law that is carried out through , using , or target technology information and communication . Its forms are very diverse , starting from from hacking , theft identity (*identity theft*), spread of malware, compromise of personal data , to more form complex like online fraud , the spread of information false (*hoax*), as well as exploitation sexual child in world virtual (Finklea, 2022). Crime This No only impact on individuals as a direct victim , but also has potential big For threaten stability economy , security national , and harmony public .

Indonesia, as one of the countries with the world's largest internet user , no escape from threat act criminal cyber . Paradox in enforcement law criminal in Good state institutions police , prosecutors , courts and also agency government others that cause Indonesia to often cornered in the eyes of international (Yasmirah, 2021)institutions . As example protracted settlement case crime is one of them is Cybercrime (Yasmirah, 2022), Report from *National Cyber and Encryption Agency (BSSN)* shows that amount incident cyber in Indonesia Keep going increase every the year , Good from aspect frequency and also its complexity (Yasmirah F. , 2022).

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

 License (CC BY-NC 4.0)

Situation This become challenge Serious for government , society and business world For protect digital infrastructure , data personal , as well as interest public from various threats in cyberspace.

One of characteristics unique act criminal cyber is its borderless nature , in where perpetrator can operate from country other without must present in a way physique on location crime . In addition , the anonymity offered by digital technology makes it difficult identification the perpetrator , while speed development technology make pattern crime cyber Keep going changed . As a result , enforcement law traditional often not capable face complexity crime cyber This in a way adequate .

In context this , approach multidisciplinary become very important For complete effort enforcement existing law . Criminology is knowledge knowledge that studies symptoms crime as wide as possible (criminology) theoretical and criminology pure). Criminology in the narrow sense learn crime . Criminology in a broad sense learn penology And methods Which related with Action Which nature non -penal.

Wrong One discipline knowledge Which relevant is criminology . As knowledge Which learn phenomenon crime , behavior perpetrator , And response public to crime , criminology offer various theories and perspectives that can help understand act criminal cyber in a way more deep . For example , theory strain can used For analyze motivation economy or pressure social that encourages individual do crime cyber , while theory opportunity highlight importance strengthening system security For reduce chance perpetrator . Criminology is knowledge from various knowledge knowledge that studies crime as phenomenon social which includes studies about characteristics law criminal , existence crime , influence crime towards the victim , the method repetition crime , attributes criminals and their characteristics and workings system law criminal ⁷ .

Approach criminology learn development and growth behavior those who have lead to crime ⁸ . Approach criminology also allows identification factors that influence increasing risk act criminal cyber , good from aspect individual , social , and structural . In addition , criminology can give guide for government And public in to design strategy prevention And Handling Which more effective , like strengthening literacy digital, collaboration cross country, And development technology detection crime .

This article focus on how approach criminology can used For understand And finish act criminal cyber . The problem main Which discussed covering How theories criminology like theory strain, theory opportunity , theory control social , and theory routine activity can explain motivation perpetrator And pattern act crime cyber ; how approach This can help formulate effective prevention strategies ; and How method based on criminology can applied in effort handling and settlement case act criminal cyber . In other words, the article This try answer question about how far is the approach criminology can contribute in face challenge complex and detrimental cybercrime public .

METHODS

Study This use method study normative with approach conceptual approach and approach statute approach This chosen Because objective main study is For analyze and understand act criminal cyber from perspective criminology , as well as explore How theories criminology can applied in finish act criminal cyber .Technique collection data done with method studies library (*library research*) For to obtain material law and relevant literature . Literature used covers books criminology , journal international about crime cyber , report official from institution security cyber , and document regulation legislation .

RESULTS AND DISCUSSION

Based on data published by the National Cyber and Crypto Agency (BSSN), the number of attack cyber in Indonesia on year 2023 increase sharp compared to year previously , with part big case involving data hacking , malware distribution , and online fraud . In the context this , law criminal functioning as tool For give sanctions to perpetrator crime cyber that violates norms and provisions applicable law . Criminal law is the law that

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

studies actions that can punished and punishment Which can dropped . Law criminal functioning For protect public from act criminal cyber with set regulations Which criminalize various form crimes that occur in cyberspace.

Action criminal cyber , or known Also as cybercrime, is form crime which is conducted with use technology information And communication as tool , media, or target . Crime This covers various activity illegal Which utilise network internet or device technology digital. Action criminal cyber is crime Which done through media digital, Which covers various type violation Which done use system computer , internet network , or device technology others . He mention that act criminal cyber including in category crimes that can harm individuals , organizations , even countries in scale big .

Meanwhile , according to a expert a lot of criminology write about cyber crime , consider that act criminal cyber is form crimes that " use technology For violate law ". McGuire emphasized that crime cyber can leading on activity organized Which very harm , like theft personal data in scale big , attack to infrastructure critical , and distribution information fake that can influence opinion public in a way wide .

In a more detailed definition wide , action criminal cyber is crimes committed in the world virtual, Good For steal , damage , access data without permission , or do other acts that violate law through technology . Some form act criminal cyber frequently happen includes :

1. Hacking (Hacking)

hacking is one of the form crime the most frequent cyber occurs , where the perpetrator try For get unauthorized access legitimate to in system computer or network For steal data or damage existing system . Hacking can done with various method , start from attack directly on the network computer until use device soft a destroyer called malware ¹³ .

2. Theft Identity (Identity Theft)

In the case of this , the perpetrator steal information the victim's personal details , such as number identity , card credit , or personal data others , for unattainable goals valid , such as open Bank account or do transaction with Name victim ¹⁴ (McGuire, 2018). Action criminal This often happen through technique *phishing* or attack *social engineering* .

3. Distribution Malware

Spread device soft dangerous (viruses, worms, ransomware) for to infect system victim's computer . Malware is used by the perpetrator For damage device computer , steal personal data , or request ransom For restore infected data or locked by ransomware. Malware attacks can cause damage Which significant on infrastructure technology information , especially in sector business and government ¹⁵ .

4. Fraud On line (Online Fraud)

Online fraud is use digital technology for manipulate individual or organization , with objective steal data personal , Money, or goods . Fraud This can done with trick the victim into giving information sensitive , make fund transfers, or buy products that are not There is .

5. Exploitation Sexual Child

Using digital media to do exploitation to children , such as spread pornography child or online grooming highlights exploitation sexual child as one of the form crime cyber that has impact very serious social ¹⁷ .

6. Attack Denial of Service (DoS/DDoS)

Targeted attacks For make system or online service no can accessed by user . Attack This often done For stop operational business or damage reputation organization that becomes target . In a DDoS attack , the perpetrator use a number of big device Which infected For send traffic to target in simultaneously , making it more difficult For detected and stopped ¹⁸ .

In Indonesia, action criminal cyber set up in a number of regulation , among them :

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

1. Constitution Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) which has updated with Constitution Number 19 of 2016. This law arrange action violate law in cyberspace, including pollution Name well , hacking , and spreading news fake (hoax)¹⁹ .
2. Criminal Code (KUHP) : Articles certain in the Criminal Code can applied For a number of case cybercrime²⁰ .
3. Constitution Number 27 of 2022 concerning Personal Data Protection : Rules new This give protection law against personal data digital users , including sanctions against violation²¹ .

A. Theory Criminology Which Relevant in Action Criminal Cyber

Approach criminology can help in understand motivation perpetrator and found solution For handle act criminal cyber . Some theory relevant criminology among others:

- a. Theory Strains (Robert K. Merton, 1938)
According to theory strains, crime happen Because existence tension or pressure Which experienced individual in a way continuous In context act criminal cyber , tension This can in the form of need economy , pressure social , or ambition For get confession . For example , the perpetrator hacking often motivated by the desire For prove ability technically to online community²² .
- b. Theory Opportunity (Clarke & Felson, 1993)
This theory explain that crime happen when There is adequate opportunities , such as weakness system security , lack of supervision , or ignorance user . In the case of crime cyber , perpetrator utilise gap security , like password Which weak or lack of data encryption , for perform the action²³ .
- c. Theory Control Social (Travis Hirschi, 1969)
Hirschi state that crime can prevented through control social Which strong , like moral values , bonds social , and strict laws . In the context of crime cyber , regulation Which strict , education ethics digital, And improvement awareness public can functioning as form social control²⁴ .
- d. Theory Activity Routine (Cohen & Felson, 1979)
This theory state that crime happen when perpetrators , targets, and lack thereof supervision meet in the same time and space . In cyberspace, the conditions This created when individual accessing unauthorized sites safe , use device without protection , or download application from unreliable source²⁵ .
- e. Theory Labeling (Howard Becker, 1963)
In crime cyber , theory This can used For analyze How labeling to perpetrators , such as "hackers" or "cybercriminals," influence identity and behavior they . Labeling This sometimes strengthen identity perpetrator as criminals , so that push they For Keep going do criminal act .²⁶

B. Strategy Completion Action Criminal Cyber Based on Criminology

1. Enforcement Law Based on Technology
Enforcement law must equipped with adequate digital infrastructure . Apparatus enforcer law need get training about technology information and cybercrime in order to be able to face challenge unique from act cyber crime²⁷ .
2. Improvement Digital Literacy
One of method effective For prevent crime cyber is with increase community digital literacy . Educational programs about security cyber , such as personal data protection and strong password management , must introduced in schools and communities . With increase understanding public about potential threat And ways protect data personal they in world virtual, opportunity the occurrence crime cyber can be minimized²⁸ .
3. Development Technology Prevention
Use technology such as artificial intelligence (AI) and machine learning can help detect and prevent act

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

criminal cyber in real-time. Technology this can also used For analyze patterns crime and identify threat new .

Approach criminology give framework strong theoretical For understand motivation perpetrator , pattern crime , and its impact towards the community. With integrate theory criminology in prevention and enforcement strategies law , government can create a more approach comprehensive in handle act cyber crime ²⁹ .

CONCLUSION

Action criminal cyber is modern crime Which can analyzed through various theory criminology . Strain Theory explains that pressure social can push somebody do crime cyber For fulfil needs . Learning Theory Social show that behavior crime cyber can studied through interactions in online communities . While that , Choice Theory Rational highlight that perpetrator act based on calculation profit and loss . Routine Activity Theory reveals the importance of vulnerable and weak targets supervision in support the occurrence crime . In addition , Control Theory Social explain that weakness bond social can increase risk involvement in crime , and Labeling Theory suggests impact labeling social on identity perpetrator . Understanding to theories This important For designing prevention and response strategies crime cyber in a way effective . Completion act criminal cyber requires a comprehensive, well -founded strategy perspective criminology . Enforcement law based on technology become step important For detect , track and take action perpetrator crime cyber in a way effective through use device advanced software and systems . Improvements digital literacy aims For build awareness public about risk crime cyber as well as method protect yourself , so that reduce number of potential victims . In addition , the development technology prevention , such as system more data security strong and tools detection automatic , can prevent opportunity the occurrence act criminal cyber . Approach this , if applied in a way integrated , can create a more digital ecosystem safe and secure .

REFERENCE

- Abrosimova, Galina Alexandrovna. "Digital Literacy and Digital Skills In University Study." *International Journal of Higher Education* 9, No. 8 (2020): 52–58
- Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427.
- Buku**
- Becker, H. S. (1963). *Outsiders: Studies in the Sociology of Deviance*. Free Press
- Clarke, R. V., & Felson, M. (1993). *Routine Activity and Rational Choice*. Transaction Publishers.
- Cohen, L. E., & Felson, M. (1979). Routine Activity Theory and Crime Prevention. *American Sociological Review*.
- Finklea, K. M., & Lynch, M. (2012). *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Congressional Research Service
- Hirschi, T. (1969). *Causes of Delinquency*. University of California Press.
- McGuire, M. (2018). *Cybercrime: A Global Perspective*. Oxford: Oxford University Press.
- Merton, R. K. (1938). Social Structure and Anomie. *American Sociological Review*.
- Siahaan, S. (2012). *Keamanan Informasi dan Kejahatan Siber: Suatu Perspektif Hukum*. Jakarta: RajaGrafindo Persada.
- Prof. Dr. Yasmirah Mandasari Saragih S.H., M.H., Fatmawati, I., & Hasibuan, S. A. (2022). Tindak Pidana Cyber Crime Teknologi Informasi Di Kepolisian Indonesia . *Penerbit Tahta Media*
- United Nations Office on Drugs and Crime (UNODC). (2021). *Cybercrime Prevention and Response Toolkit*.

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

- Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd Edition). SAGE Publications. Prof. Dr. Yasmirah Mandasari Saragih S.H., M.H. (2021). *Pengantar Teori Kriminologi dan Teori Dalam Hukum Pidana*. Medan: Cattleya Darmaya Fortuna.