CRIMINAL LAW POLITICS IN HANDLING THE CASES OF CYBERCRIME IN INDONESIA

Fany Sri Yiniartie, University Islam Bandung
Dose Hudaya, University Islam Bandung
Eni Dasuki Suhardini, University Islam Bandung
Sujasmin, University Islam Bandung

ABSTRACT

The article aims to find out how the law in Indonesia enforces the law on cyber crime within the policy politics system of criminal law. The research has employed normative juridical method and used field data as the data for the research. The cybercrime case has increased significantly in number in 2020 compared to that in 2019. The data show that the highest number of cybercrime case type is the case of spreading provocative content. The politics of criminal law to handle cybercrime case in Indonesia is firmly regulated in Kitab Undang-Undang Hukum Pidana (KUHP) (Criminal Code) which regulates the various modus of criminal acts, in Law No. 36 of 1999 concerning Telecommunication, Law No 8 of 1997 concerning Company Documents, Law No. 25 of 2003 concerning Change on Law No 15 of 2002 concerning Money Laundry, Law No. 15 on Terrorism Acts Eradication, and in Law No. 11 of 2008 on Information and Electronic Transaction.

Keywords: Cyber Crime, Criminal law, Crime Sentencing.

INTRODUCTION

Telecommunication technology has brought human beings to a new civilization with its social structure and norms system. This means the society develops towards a globally structured new society in which the borders between nations disappear (Abddul, 2010). The cutting-edge feature of computers in the form of their speed and accuracy in in finishing works has decreased the number of labor force, the fund, as well as reducing the possibility of making mistakes in doing the job. This advantage has also created heavy dependence of the society on computers. Internet technology, in addition, has generated a lot of convenience in everyday life for many of its users not only for communicating but also for effective and efficient business transaction (Abdul, 2005). In this globalization and modern era, everyone becomes so dependent on the internet in particular and the social media. Soekanto suggested that the development in technology will go hand in hand with the emergence of various changes in society (Soerjono, 1980). The negative impacts of technology development will come about if the is an error generated by the computer. This will cause a great loss for the users and the concerned parties. The deliberate mistakes made lead to the misuse of the computers. The globalizing feature of being "users friendly" that technology has now more become forces Indonesians to follow the trend of using more technology. Information technology can be used for positive purposes which will benefit its users; they can exchange information easily and fast. On the contrary, technology can also be used for negative purposes; it can be used to facilitate cybercrime. Crimes often follow and adapt to the development technology and cybercrime is the form of crime that is resulted from the development of information technology (Yurizal, 2015).

Cybercrime activities include credit card theft, sites hacking, data intercepting, and data manipulating through virus spread. Cybercrime has become a threat to the international

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

stability. The government is faced with difficult challenge to deal with crimes assisted by computer technology such as the internet and intranet (Andysah, n.d). The rapid development of the internet is not without problem. The use of the internet also invites crimes. Cyberspace is a borderless media as it is wired to the computer net that is connected to the world. Cyberspace crime does not recognize a state's border or a nation's border. This crime creates myriad of problems in especially law crime and jurisdiction. Jurisdiction is the power or the competence of a state law on people, objects or events. The cybercrime requires a firm legal handling. Meanwhile discussing law regulating cybercrime is a challenge because the statutory regulations regulating such crime in Indonesia has only "been around not for a long period of time." Cybercrime is a crime act that has a distinct characteristic unlike that of general criminal act in terms of the perpetrators, the victims, modus operandi, and the crime sites. The law enforcing system for information technology related crimes are being faced with herculean challenges. Cybercrime demands a serious handling to eradicate. To obtain a clear picture of civil law politics on cybercrime in Indonesia, research needs to be conducted.

Research Method

The present research has employed normative juridical method, emphasizing on law as a norm. The present research aims to portray a detailed and thorough reality conforming to a phenomenon. The data for the research were collected by positioning the researchers as the key instrument and as the analysist of the issue investigated. The data used in the present research were the field data taken from PartoliSiber in the form of statistical data on cybercrime case happened in Indonesia in 2020. The research is qualitative in nature, describing the politics of criminal law in handling cybercrime cases in Indonesia based on valid data. The data used in the present research were secondary data; the research used supporting literature related to the issue investigated.

LITERATURE REVIEW

Cybercrime

The rapid development of information technology is the impact of the human's need that grows more and more in its complexity for information. The relation between information and communication network technology has resulted in a really wide cyberspace. This enormously wide cyberspace contains collection of information that can be accessed by anyone through computer networks called internet (Arsyad, 2011). Cybercrime or a crime done in cyberspace is a criminal act that makes use of the computer or computer network as the tool, and as the site where the crime take place. It is also called virtual world crime (Fairuz, 2019). Cybercrime is technically complex and legally delicate. The rapid progress in information and communication technology and disparity between law systems globally serve as a tough challenge for first respondent, investigation authority, prosecution agency and criminal justice administration. Cybercrime can simply be defined as an act against law that is done by making use of the sophisticated computer and telecommunication technology-based internet. The Prevention of Crime and the Treatment of Offenders in Havana, Cuba in 1999 and in Wina, Austria in 2000, identified two popular terms (Yurizal, 2015).

a. Cybercrime in its narrow sense is a computer crime, which is an illegal or violating act that directly attacks computer security system and/or data processed by computer.
b. Cybercrime in its wide sense is a computer related crime, which is an illegal or violating act related to computer system or computer network.

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

Based on the above definitions, cybercrime can be referred to an act that is against the law which is done using computer network as its facility or a computer as its object to both take advantage of and harm others. Generally, cybercrime perpetrator makes use of computers as the tool for their crime. The computers are used to plan, organize, and do their criminal act. Many of cybercrime perpetrators use computer network to execute their criminal act. This allows them not to directly meet their victims. Another characteristic of this type of crime is that it can be carried out across countries. Cybercrime is the type of across-countries crime that is the most frequently done. This is made possible by the nature of the internet that crosses countries' border.

The Politics of Criminal law

Scholars for example, Mahfud MD, Sagih , and K. Harman have conducted a quite deep analysis on the law politics. Their analysis shows that law politics has become an important part of the development of law studies in Indonesia. Their analysis can serve to facilitate our understanding of law politics in terms of its theorical conception and as point to go for further analysis. We, however, still need such sectoral law politics as civil law studies, the politics of criminal law, the politics of administrative law, and other studies of law to develop the law in the future. This development indicates that law studies in sociological jurisprudence have gained more space and attention in addition to juridical normative approach. Existence has served as the signs stipulating rules of game for each citizen without exception in order for their behavior, social construction, politicss, religion, culture and other aspects of their life run in accordance with the law. Rule of game that is called "law" should be enforced in order for each member of the society can all enjoy a peaceful, safe, orderly, mutual respect life. The state apparatuses are the ones who are responsible for using the law as a weapon to combat against any form of crime that will, is taking place, and has threatened Indonesians. The state apparatuses are required put in their best effort to keep a pace with the development of the crime world, especially the development of cybercrime that is growing more and more concerning. They have to serve as the main subject that combat against cybercrime.

Rahardjo in his Ilmu Hukum defined law politics as activities to select and the way that are going to be used to achieve a given social and law purpose in a society. Meanwhile Nusantara defined law politics as legal policy that is going to be applied or administered nationally by given state governance. He further explained that law politics covers: (1) consistent enforcement of existing rule of law; (2) law establishment whose core is the updating of the existing law based on new legal acts; (3) the affirmation of the functions of legal enforcement institutions as well the coaching of their members; and (4) increasing people's awareness of the law according to the perception of the decision makers. Based on different interpretation and understanding of the law politics as well as leaning on Mahfud's idea, we can say that law politics has two inseparable sides which are (1) law politics as "legal policy" of the state institutions in laws making, and (2) law politics as a tool to assess and criticize whether or not an already made law is in accordance with the legal policy's framework to achieve the state's goals.

When law politics is discussed in connection to the achievement of the state's goals, the law politics summarizes the following points (Mokhammad, 2014):

a. The State Objective expected by the Indonesians as an orientation and guidance for law politics, including basic values of the state's objectives in national law establishment;
b. Formulation of national law system as a way to realize the state's objective and factors influencing it;
c. Planning and framework in the formulation of legal policy;
d. The content of national law and the factors influencing it; and

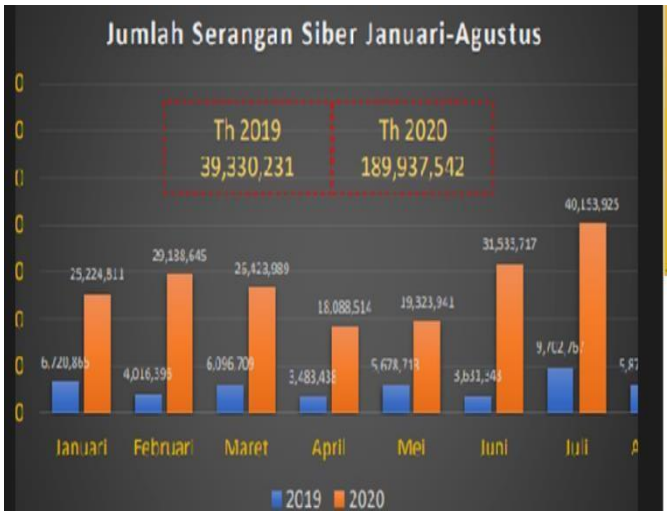
Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

e. Legal control with national legislation program (Prolegnas) and judicial review, legislative review and others.

DISCUSSION

Cybercrime Cases in Indonesia in 2020

The effort put in and the policy to make good civil law regulation can in essence not be separated from the objective to countermeasure the crime. Therefore, the policy or the civil law is also part of criminal politics. In other words, seen from the perspective of criminal politics, civil law politics is identical to, "the policy of crime countermeasure through civil law". The countermeasure efforts against crime through civil law are in essence also part of the law enforcement effort (especially law civil enforcement). Therefore, the politics or civil law policy is often considered to be part of law enforcement policy.



PICTURE 1
THE COMPARISON OF CYBER CRIME CASE IN 2019 AND 2020

According to Kurniawan, the Head of Sub Directorate of Vulnerability and Risk Assessment of National Critical Infrastructure III BSSN, there was an increase of 189 million people in cybercrime case in Indonesia in 2020 compared to 39 million people in 2019. This increase is contributed by the society's pattern of life in Indonesia which has undergone a significant change since the county was hit by Covid 19. Social distancing which has made Indonesians to work, learn, and carry out most of their activities online at home using the Internet is believed to contribute to the increase. The high use of the Internet has enabled many Indonesians to access various crimes.

Present Civil Law Politics in Handling Cybercrime Cases in Indonesia

The development of technology and technology of information has brought about many benefits in the utilization of business transaction. Nevertheless, virtual world is sometimes used to serve as the space for netizens to interact as they do in real world (Indriani, 2021). The virtual world also possesses its own problems contributed by the misuse of the technology which causes legal issue. Law instruments provide a foundation or guidance for the law enforcers to enforce the laws on the cybercrime perpetrators. There are a lot of cases of cybercrime in Indonesia. Maskun suggested that in Indonesia, criminal act using computers in Indonesia has been the type of crime that is challenging to classify as a criminal act

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

(Maskun, 2013). As a positive law, the making of law regulating cybercrime should go the mechanism of law making. It is Ius Constitutum which means it should at the same time becomes a positive law which imposes sanction on the event or the criminal act using computers.

a. The application in the articles of KUHP (Criminal Code) in the case that makes computers as the target of the criminal act and the case which uses a computer as the means of committing the crime.

1. Article 362 KUHP on theft (carding case);
2. Article 378 KUHP on fraud (fraud through website; the perpetrator pretend that they sell things);
3. Article 311 KUHP Defamation (through the Internet by sending emails to the victims or their friends)
4. Article 303 KUHP Gambling (online gambling game);
5. Article 282 KUHP Pornography (spreading pornography through the internet).;
6. Article 282 and 311 KUHP (on the case of photo or private vulgar films spread in the Internet);
7. Article 378 and 362 (on Carding case because the perpetrators commit fraud by pretending, they wish to pay their debt using stolen credit card).

b. Law No.36 Year 1999 on Telecommunication, (Internet misuse that disturbs public or private order) (Law No.36, 1999).

According to Article 1 Law Number 36 of 1999, telecommunication is any transmitting, sending, and/or receiving and any information in the form or signs, writing, graphics, sound and sound through wire systems, optics, radio, or other electromagnetic systems. Based on this definition, the Internet and all its facilities are a form of communication tool because they can send and receive any information.

c. Law No. 8 of 1997 concerning Company Documents (Law no. 8, 1997).

With the enactment of Law no. 8 of 1997 dated March 24, 1997 concerning Company Documents. One of its articles regulates the possibility of storing company documents in electronic form (paperless). This law acknowledges that company documents stored in electronic media can be used as legal evidence.

d. Law No.25 of 2003 concerning Amendment to Law No.15 of 2002 concerning Money Laundering

This law is the most powerful law for an investigator to obtain information about suspects who commit fraud via the internet because it does not require long and time-consuming bureaucratic procedures. Fraud is one type of crime contained in article 2 verses 1.

e. Law No. 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism (Law No. 15, 2003).

Law no. 15 of 2003 regulates electronic evidence in accordance with Article 27, namely other evidence in the form of information that is spoken, sent, received or stored electronically with optical devices or the likes. Digital evidence or electronic evidence plays a very important role in investigating terrorism cases because currently communication between actors in the field and their leaders or intellectual actors is carried out by utilizing facilities on the Internet. The internet has been used to receive orders or to convey conditions on the ground because the perpetrators know that tracking communication done through the Internet is more difficult than tracking communication via mobile phone. In addition to searching for

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

information using search engines and doing propaganda through bulletin boards and mailing lists, facilities that are often used are e-mail and chat rooms.

f. Law Number 11 of 2008 concerning Information and Electronic Transactions

After law no. 11 of 2008 concerning electronic transactions has been issued by the government, almost all cybercrime problems are regulated by the law. The problems contained in Law no. 11 of 2008 regarding electronic transactions are as follows:

Pornography

Article 27 paragraph (1) of Law no. 11 of 2008 states, "Every person who deliberately and without rights distributes and/or transmits and/or makes electronic information and/or electronic documents that have content that violates decency accessible." The criminal sanctions to be imposed in Article 45 verse (1) is as follows: "Everyone referred to in Article 27 verse (1), verse (2) verse (3) or verse (4) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 100,000,000.00 (one billion rupiah). In article 52 verses (1) of Law no. 11 of 2008, it is stated, "In the case of a crime as referred to in Article 27 verse (1) concerning decency or sexual exploitation of a child, it is subject to an aggravation of punishment of one third of the principal crime.

Computer-Related Betting (Gambling *via* Computer)

In this case, gambling using a computer as a means of its modus operandi is subject to Article 27 verse (2) of Law no. 11 of 2008 which reads as follows:

"Every person who knowingly and without rights distributes and/or transmits and/or makes Electronic Information and/or Electronic Documents containing gambling content accessible".

Illegal Content (Defamation)

According to article 27 verse (3) of law no. 11, of 2008. Regarding the criminal sanctions, it is stated in Article 45 of Law No. 11 of 2008. In the case of this type of crime, it can be charged with Article 28 verse (1) and verse h (2) depending on the modus operandi used.

Computer-related Extortion and Threats

Extortion and threats through computers are regulated in Article 27 verse (4) of Law no. 11 of 2008. This type of crime, in accordance with the provisions of Article 45 verse (1) of Law no. 11 of 2008, can be sentenced with a maximum imprisonment of 6 (six) years and a maximum fine of Rp. 1.000.000.000,00 (one billion rupiah).

Infringements of Privacy and Cyber Aspersions

In law no. 11 of 2008 this type of crime is regulated in Article 28 verse (1) and verse (2). Based on article 45 verse (2) law no. 11 of 2008, this type of crime may be sentenced to a maximum imprisonment of 6 (six) years and a maximum fine of Rp. 1.000.000.000,00 (one billion rupiah).

Unauthorized Access to Computer and Service

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

Crimes by using or infiltrating a computer network system illegally are regulated in Article 30 verse (1), verse (2), and verse (3) of Law no. 11 of 2008. Article 46 verse (13) states, "Anyone who meets the requirements as referred to in Article 30 verse (3) shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiah)."

Illegal Interception in the Computers, Computers System, and Computer Network Operation

This type of cybercrime is regulated in Article 31 verse (1) of Law no. 11 of 2008. Article 31 verse (1) and (2) stipulates that the perpetrators shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah).

Misuse of Computer Equipment or Computer Software Piracy

This type of crime is regulated in Article 43 verse (1) and verse (2) of the Electronic Transaction Law. The sanction for this type of cybercrime is regulated in Article 49 of the Electronic Transaction Law. Based on article 33 the perpetrators shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 10,000,000,000.00 (ten billion rupiah).

g. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions concerning Regulation of Electronic Transactions and Regarding Cybercrimes

Outside the Criminal Code, there is also crime of specific insults. Specific insults in this sense are different from specific insults in the Criminal Code. Specific insults in the Criminal Code are insults that are regulated outside Chapter XVI of the Criminal Code. Such specific insults are spread in certain types of criminal acts. Meanwhile, specific insults outside the Criminal Code that are now contained in our legislation are special insults (defamation) in Law Number 19 of 2016 concerning ITE. In the ITE Law number 19 of 2016, there are 19 forms of criminal acts in Article 27 to Article 37. One of which is a specific offense of humiliation, which is contained in Article 27 paragraph 3, which states that: "everyone intentionally and without rights distributes and/or transmits and/or makes it accessible and makes electronic information and/or documents containing insults and/or defamation contents (Alicia, 2020).

Politics of Criminal Law in Handling Cybercrime Cases in Indonesia in the Future

It is imperative that we manage government affairs in the field of cyber security through the formulation of governance that can effectively be implemented in Indonesia. The large number of cyber infrastructures owned by the private sector makes collaboration between the government and the private sector (public-private partnership) a concept that will create effective cyber security. This new concept has now been widely applied in countries that have paid more attention to cyber security earlier than Indonesia. Based on the various explanations that we have so far regarding both the losses resulting from cyber-attacks and regulations that have not been adequate in providing protection for cyber security to protect public security, it is necessary to have special arrangements that are able to cover all aspects of cyber security. The principles contained in the Cyber Security and Resilience Bill underlies the implementation of Cyber Security in the efforts of prevention, response, and recovery

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

from cyber incidents or cyber-attacks. Prevention, countermeasures, and recovery efforts are only a broad part of several Cyber Security implementation efforts. There are many other, more practical and even technical measures that need to be regulated in the Cyber Security and Resilience Bill. In the study, this principle will reflect aspects of life related to the Cyber Security and Resilience Bill. It is expected that the existing principles can later describe the clarity of objectives, institutional matter, conformity of the law, and transparency.

The reflection of the principle in the various realizations of aspects of life in the Cyber Security and Resilience Bill will eventually serve as the basic principle for the formation of good Laws and Regulations. This principle serves as a basic reference if there is a debate, conflict, or discrepancy both from the laws and regulations and the implementation of existing provisions later on in the community. When all those come about, we will return to see the existing principles. This means that a concrete statutory regulation is based on a broader concept of principles. If there is a potential for debate when the regulation is applied, the regulation will be withdrawn to see the principles of the existing regulations. Revisiting the basic concept is expected to be able to resolve the debate that will arise.

CONCLUSIONS

Countermeasures against Cybercrime in Indonesia have now been carried out with the enactment of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions concerning Electronic Transaction Arrangements and Regarding Cyber Crimes. With the enactment of this law, it is hoped that every form of cybercrime will be dealt with in accordance with the rules in the law in addition to the Criminal Code (KUHP) which regulates various modes of crime. With the enactment of Law no. 19 of 2016, we then can have a firm and clear stance that Cybercrime is a criminal act that is prohibited by law and every perpetrator will be punished according to the applicable law. The Politics of Criminal Law or criminal law countermeasures in dealing with cybercrime cases in Indonesia in the future require the principles contained in the Cyber Security and Resilience Bill which underlies the implementation of Cyber Security in the efforts to prevent, overcome, and recover from cyber incidents or cyber-attacks. Prevention, response, and recovery efforts are only a broad part of several efforts to organize Cyber Security. There are still many other more practical and even technical measures that need to be regulated in the Cyber Security and Resilience Bill.

REFERENCES

Abdul, W.M.L. (2005). *Kejahatan Mayantara*: Cyber Crime, Bandung: Refika Aditama.

Alicia, L. (2020). Juridical Review of the Crime of Defamation According to the Criminal Code and Law Number 19 of 2016 concerning ITE. *Journal of Lex Crimen, 9*(1).

Arsyad, S. (2001). *Cyber Crime*, Jakarta: Milestone Publisher.

Benny, K.H. (2001). *Political Configuration and Judicial Power in Indonesia*, Jakarta: Elsam

Bintan, R.S. (2001). *Politics of law*, Jakarta: Utomo.

Fairuz Rhamdhatul Muthia dan Ridwan Arifin. (2019). Criminal law study in the Mayantara crime (Cybercrime) case in defamation cases in Indonesia. *Resam Legal Journal, 5*(1).

Indriani, B.M., & Robert, N.W. (2021). Juridical study of cybercrime management and law enforcement. *Jurnal Lex Crime, 10*(5).

Law No. 36 of 1999 concerning Telecommunications, (misuse of the Internet that disturbs public or private order).

Law No. 8 of 1997 concerning Company Documents.

Law No. 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism.

Law Number 11 of 2008 concerning Information and Electronic Transactions.

Maskun (2013). *Kejahatan Siber Cyber Crime*, Jakarta: Kencana Prenada Media Group.

Mahfud, M.D. (1998). *Legal politics in Indonesia*, Jakarta: LP3ES.

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.

Mokhammad, N. (2014). *Politics of criminal law: Conception of reforming criminal law in the ideals of the state of law*, Malang: Setara Press.
Satjipto, R. (2000). *Legal studies*, Bandung: Citra Aditya Bakti.
Soerjono, S. (1980). *Principles of sociology of law*, Jakarta: Rajawali Press.
Yurizal.(2015). *Cyber Crime Law Enforcement*, Malang: Media Nusa Kreatif.
Yurizal.(2015). *Cyber Crime Law Enforcement*, Malang: Media Nusa Kreatif.

Received: 03-Jan-2022, Manuscript No. ASMJ-21-9712; **Editor assigned:** 05- Jan -2022, PreQC No. ASMJ-21-9712 (PQ); **Reviewed:** 19-Jan-2022, QC No. ASMJ-21-9712; **Revised:** 26-Jan-2022, Manuscript No. ASMJ-21-9712 (R); **Published:** 09-Feb-2022

Citation Information: Yiniartie, F.S., Hudaya, D., Suhardini, E.D., & Sujasmin. (2022). Criminal law politics in handling the cases of cybercrime in Indonesia. *Academy of Strategic Management Journal, 21*(S4), 1-9.