Factors Causing Cybercrimes Committed by Foreigners in Bali Viewed from a Criminological Perspective

Putu Sekarwangi Saraswati
Faculty of Law, Universitas Mahasaraswati Denpasar, Denpasar, Indonesia
Kamboja Street, No.11A Dangin Puri Kangin, Denpasar, Bali, Indonesia 80233
sekarwangisaraswati@unmas.ac.id

Abdul Kadir Jaelani
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Ir. Sutami street, No. 36 Kentingan, Jebres, Surakarta, Jawa Tengah, Indonesia 57126
jaelaniabdulkadir@staff.uns.ac.id

***Abstract*— One of the negative impacts of tourism development in Bali triggers the development of criminal acts committed by foreigners. The purpose of this study is to find out (1) the factors causing the occurrence of cybercrimes committed by foreigners in Bali and (2) efforts to overcome cybercrimes committed by foreigners in Bali. The research method used is a type of normative legal research. The results of the research show (1) The factors causing the occurrence of cybercrimes committed by foreigners in Bali have three elements: an act that is against the law, carried out by the foreigner, and carried out for personal and group gain while on the other hand harming the other party either directly or indirectly. Pressure is generally caused by individual behavior that causes them to commit crimes. Another cause of crime is the opportunity (opportunity). The opportunity is wide open for foreigners in Bali to commit crimes, including cybercrime; (2) Efforts to overcome cybercrimes committed by foreigners in Bali can be carried out by implementing cyber law or legal policies in the cyber field. However, the legal system in Indonesia has not explicitly regulated cybercrime.**

***Keywords*— *Bali; Cybercrime; Foreign*; Person.**

I. INTRODUCTION

Tourism is one of the world's most important sectors of the economy. Tourism is one of the main drivers of the world economy because several advantages can provide substantial foreign exchange, expand employment opportunities, and introduce the country's culture. Tourism has become one of the largest economic sectors, has the fastest growth rate, and is one of many countries' primary sources of income. Tourism is one of the critical drivers of a country's socio-economic progress through foreign exchange earnings, job creation, business opportunities, and infrastructure development.

The United Nations World Tourism Organization (UNWTO) estimates that international tourist arrivals will reach 1.8 billion by 2030, with an annual growth rate of 3.3 percent. The UNWTO estimate indeed lures tourism business actors from various countries.[1] Now, many new tourist destinations are outside the traditionally favorite destinations, such as Europe and North America. The Asia and Pacific region is estimated to have higher growth than other regions; even in certain countries, the growth is much higher. For Indonesia, this is an opportunity as well as a challenge in the development of national tourism.

Bali Province is one of the provinces in Indonesia that develops its tourism through cultural tourism.[2] Cultural tourism is tourism that uses the cultural potential of an area to be used as a tourism object.[3] Each district/city in Bali Province has a unique culture and tradition with the characteristics of each area that attracts tourists to vacation on the island of Bali. In addition, the island of Bali has complete natural panorama elements to be used as tourist attractions, such as lakes, rivers, mountains, beaches, and forests that extend from the west to the east coast of Bali.

The world has recognized Bali as one of the main tourist destinations in Indonesia. The number of tourists, both foreign tourists and domestic tourists, visiting Bali always increases from year to year. The increase in tourist visits to Bali occurs because of the natural and cultural attractions for tourists. In addition, the increase also occurred due to the development of infrastructure and other facilities. Bali's Ngurah Rai Airport, since 3013, has expanded and improved its facilities with a fund of IDR 2.8 trillion, which includes the expansion of domestic and international departure and arrival terminals.[4] With the renovation of Ngurah Rai Airport in 2013, its

A. K. Jaelani et al. (eds.), *Proceedings of the International Conference on Cultural Policy and Sustainable Development (ICPSD 2024)*,
Advances in Social Science, Education and Humanities Research 869,
https://doi.org/10.2991/978-2-38476-315-3_91

capacity increased from 14 million passengers to 25 million, or an increase of 78.57%. This figure is the largest airport capacity in Indonesia today (Immigration Office Class I Special Ngurah Rai Bali, 2013).

Data from the Bali Provincial Tourism Office in 2018 shows that foreign tourist visits in the last ten years have increased from 1,664,854 people in 2007 to 6,598,903 people in 2017, which means an increase of 4,934,049 people or an increase of 296.37%. It shows that the tourism sector in the Province of Bali is showing good development, as seen from the economic impact that contributed to the Province of Bali's Regional Original Income (PAD). The increase in tourist visits to Indonesia also allows the Bali tourism sector to play a role as a source of state revenue obtained from tourist consumption during visits to tourist destinations in Bali Province.

Although the increase in the number of foreign tourists in Bali has a positive impact on the PAD of the Province of Bali, it cannot be denied that the increase in foreign tourist visits also has a negative impact, one of which is the increase in crime or criminal acts committed by foreigners who come to Bali.

Statistical data from the Immigration Office Special Class I Ngurah Rai Bali shows the number of foreigners involved in general and specific crimes or crimes in Bali, ranging from the lightest cases, such as abuse of residence permits, causes of traffic accidents, murder, drugs, pedophilia. Until last, cybercrime has been increasing. Furthermore, the criminological statistical data available at the Bali Police shows that in mid-2018, hundreds of Chinese citizens were arrested by the Bali Police in two areas in three locations. The perpetrators were arrested in connection with cases of cyber fraud or internet crimes. From the three locations, the Bali Police arrested 103 Chinese citizens.

Both locations are in Denpasar, and one is in Badung. The three locations where hundreds of Chinese citizens were arrested, including Jalan Mutiara Abianbase No. 1, Mengwi, and Badung, have arrested 49 people. With evidence, there are 51 telephones, 1 laptop, 43 passports, 5 cellphones, two routers, two printers, 26 units of Hub. The second location is Jalan Beduga XI Number 39 Denpasar. At that location, the police arrested 32 people with evidence of 20 cell phones, 13 routers, two laptops, and one passport. At the same time, the third crime scene is at Jalan Gatsu I Number 9 Denpasar. The Bali Police arrested 33 people with evidence of 3 routers, 2 laptops, 38 passports, and 1 hub.

The perpetrators have committed fraud. The victim is another Chinese national. They have deceived the Chinese themselves. By calling from here, they persuade the victims to transfer money to the perpetrators. In acting as committing fraud, the perpetrator has a mode of claiming to be the victim's family. In addition, the perpetrators also claimed to be law enforcement officers from China, so these victims felt threatened. Not only that, they also claimed to be from the hospital and said the victim's family had an accident. Based on the background stated above, the research objectives are to find out (1) the factors causing the occurrence of cybercrimes committed by foreigners in Bali; and (2) efforts to combat cybercrimes committed by foreigners in Bali.

II. LITERATURE REVIEW

A. Cybercrime

Cybercrime is a criminal act that utilizes technology, from devices to internet networks.[5] Cybercrime cases aim to harm others by committing theft, hacking, fraud, spreading viruses, and other digital crimes. During the period of technological development, cybercrime cases have become increasingly prevalent throughout the world, and the types of crimes vary. One example of cybercrime in Indonesia is the data leakage of 91 million Tokopedia users sold on the black market in 2021. Therefore, users are harmed because data such as names, mobile phone numbers, and application passwords are widely spread. Meanwhile, companies are also harmed because this eliminates public trust in them. As mentioned above, the number of cybercrime cases that occur varies greatly. Some types of cybercrime are as follows. (1) Phishing. The first type of cybercrime is phishing. Phishing is an online fraud involving luring others to divulge their data. Usually, the data that is trying to be requested is a credit card number, OTP code, or others, depending on the purpose of the fraudster. The trick is that the perpetrator sends a link to a fake company site that will automatically steal a person's identity if clicked. (2) Identity Theft. One type of cybercrime is identity theft or identity theft committed to commit a crime. Generally, the perpetrator hacks or accesses the network to obtain users' personal information on a website or application. (3) Cyber Terrorism. Another type of crime is cyberterrorism. Cyberterrorism is an attack on a country's networks, devices, or information systems in order to intimidate the government because of an interest. Usually, cyber terrorism harms and threatens the safety of the country. (4) Content Crime. One of the most common cybercrimes is content crime. This crime generally involves plagiarism, hoaxes, and the spread of indecent or racial content. (5) OTP Fraud. Then one type of cybercrime is OTP or one-time password fraud. The OTP is a one-time code usually sent by the application system to a mobile phone number or email to register a new account. Although it aims to provide additional security, many cybercriminals have unfortunately used OTP. Typically, scammers will contact someone to ask for an OTP code in order to provide a favor. After that, the perpetrator can steal personal data and even some funds in the bank. (6.) Carding. Carding is the following type of cybercrime. Please note that carding involves transacting money with other people's credit card data. This data is obtained using various methods, such as hacking sites or planting hardware on ATMs in shopping places. (7) Cyberbullying. Another type is cyberbullying or online bullying. It involves netizens constantly mocking or blaming someone until they may be mentally shaken. Nowadays, cyberbullying is common in cyberspace. (8) Cyber Extortion. One type of cybercrime is cyber extortion, which is online extortion carried out by threatening someone using essential data on their device. Usually, this is done with ransomware, which is malware that makes the device inaccessible until the owner pays the amount of money requested by the perpetrator. It is detrimental because essential data on the device can be lost or traded. (9) Downloading Potentially Unwanted Programs (PUPs). One type of cybercrime case is the download of PUPs, programs inserted in applications or software. So, when downloading an application or software, this program will be downloaded automatically. In general, PUPs are malware of the adware or spyware type. By downloading this malware, one's data can be jeopardized. (10) Cracking. Cracking is a type of cybercrime committed by entering the device's system. To do this, the perpetrator first removes the device's security system. That way, the perpetrator can implant malware, steal the victim's data, or create pirated software. (11) Hacking. Hacking is a type of cybercrime similar to cracking. It is the act of forcibly accessing a device's system to gain an advantage. Indeed, some hacking is done with good intentions. However, many criminals use this method to harm others. Generally, they do this to damage a system, steal someone's data, and expose some private information to the public. (12) Distributed Denial of Service Attacks (DDoS). DDoS attacks are another type of cybercrime case. Please note that this attack targets a server network to harm the company. The trick is that the perpetrator will overload the website traffic very high. That way, the website will be down, so its users cannot access it. (13) Spamming. Another common type of cybercrime is spamming. Spamming is done by spreading messages intensely and en masse. Usually, this action is spam emails offering obscure products to links containing viruses. (14) Cyberstalking. The last type is cyberstalking, which is the act of harassing or intimidating a victim online by spying on their activities on the internet. Usually, this crime is followed by false accusations, threats, insults, and other harassing actions on social media. In general, perpetrators commit this crime with spyware to track all activities on the victim's device. The activities accessed are search history, sent messages, applications on the device, and financial transactions.

B. Criminological Perspective

Criminology is a science that studies crime from various aspects. The word criminology was first put forward by a French anthropologist P. Topinard (1830-1911). Criminology consists of two syllables, namely the word "crime," which means crime, and "logos," which means science so that criminology can mean the science of crime. P. Topinard defines "Criminology as a science that aims to investigate the symptoms of crime as widely as possible (theoretical criminology or pure criminology).[6] Theoretical criminology is a science based on experience, which, like other similar sciences, pays attention to symptoms and investigates the causes of these symptoms in the ways available to them. " Edwin H. Sutherland defines criminology as follows: "Criminology is the body of knowledge regarding delinquency and crime as social phenomena. Crime, according to the views of criminology experts in general, means human behavior that violates norms (criminal law/crime/criminal law) is detrimental, annoying, and causes victims, so it cannot be allowed. Meanwhile, criminology pays attention to crime, namely: (1) Perpetrators who have been found guilty by the court; (2) In white collar crime, including those resolved non-penal; (3) Behavior that is decriminalized; (4) Population of perpetrators who are detained; (5) Actions that violate norms; (6) Actions that receive social reactions. The criminal law enforcement process is interrelated with criminology because criminology can provide input to criminal law, especially why people commit crimes, the causal factors, and what efforts must be made so that law enforcers do not violate the law. For that reason, criminology studies the causes, improvements, and prevention of crime as a human phenomenon and can collect contributions from various sciences.

III. METHOD

The research method used in this research is normative legal research. Normative legal research (normative legal research) is research conducted by reviewing the laws and regulations that apply or are applied to a particular legal problem.[7] Normative legal research examines law from an internal perspective, with the object of research being legal norms.[8] Normative research is often referred to as doctrinal research, whose objects of study are statutory regulations and library materials. Normative legal research, also called focused research, examines the application of rules or norms in positive law. According to I Made Pasek Diantha, normative legal research provides juridical arguments when there are vacancies, ambiguities, and conflicts of norms. Furthermore, this means that normative legal research plays a role in maintaining critical aspects of legal scholarship as a normative science.

IV. RESULT AND DISCUSSION

A. Factors Causing Cyber Crimes Committed by Foreigners in Bali

Modern human life today cannot be separated from even sometimes very dependent on advances in advanced technology (high tech or advanced technology) in information and electronics through international networks (Internet).[9] The existence of the Internet is used by the world community from various circles for various activities, such as seeking information, sending information, and conducting business or non-business activities. These activities are known as telematics activities (cyber activities). In cyber activities, the role of technology is enormous because the higher the technology, the more excellent the opportunity for people to use the Internet in their daily lives. Internet users are divided into passive and active users. Passive users only open web pages on the Internet (browsing) or read information without interacting with vendors/administrators or other Internet users. Active internet users interact with vendors or other internet users, for example, by shopping online, sending electronic mail (e-mail), and so on. This active user can also use internet media to carry out actions categorized as telematics crimes (cybercrimes).[10] Cybercrime or telematics crime is a crime committed using the Internet. For example, carding is a cybercrime involving stealing credit card data from a bank customer so that the carder (carder) can use the data for personal gain.

Other crimes are credit card theft, hacking websites, intercepting other people's data transmissions, such as e-mail, and manipulating data by setting up unwanted commands for computer programmers. So, it is possible to have formal and material offenses in computer crimes.[11] A formal offense is the act of someone entering someone else's computer without permission, while a material offense is an act that causes harm to other people. Cybercrime has become a threat to stability, so it is difficult for the government to balance the techniques of crime committed with computer technology, especially Internet and intranet networks.

Cybercrime or telematics crimes use computers to achieve the crime's goals (computer as a tool) and computers as a target for crime (computer as a target).[12] The originality of cybercrime is where the computer is the target. For example, the spread of viruses or malicious ware, while crimes where computers are used as tools are traditional crimes that use computers as a means (for example, fraud or fraud that uses electronic mail to disseminate information for the fraudster). The losses arising from this cybercrime are increasing from year to year. Losses for this crime will continue to double yearly, if not immediately anticipated.

Regarding the nature and scope of cybercrime, some experts argue that cybercrime is not a new crime but a traditional crime committed in cyberspace. Using new tools to assist perpetrators in committing crimes is only a crime.[13] Cybercrime is almost the same as 'old fashioned' non-virtual crime. Peter Grabosky calls it 'old wine in new bottles.' Some other experts argue that cybercrime is a new form of crime that is different from crimes in the real world. The focus of the novelty of cybercrime lies in the socio-structural characteristics of the environment (cyberspace) where the crime occurs. According to Susan W. Brenner, there are types of cybercrime that are indeed new crimes, as well as traditional types of crimes that use computers as a tool. To commit a crime. The types of cybercrimes that can be considered as 'new crimes,' for example, hacking, cracking, DDoS attacks, and viruses, are included in the 'crimes in which the computer is the target of the criminal activity.' Types of cybercrime that are 'not new crimes,' for example, online fraud, theft of funds or information, embezzlement, forgery, stalking, and making and distributing child pornography, are included in the category of "crimes in which the computer is a tool. used to commit a crime; and the type of cybercrime which is included in the category of crimes in which the use of the computer is an incidental aspect of the commission of the crime", such as someone using a computer to write a letter containing threats. In this case, computers are only used as evidence. Yvonne Jewkes has almost the same view as Susan Brenner, who holds that cybercrimes can be classified into the following two categories:

1. New crimes using new tools.

   Crimes that cannot be committed any other way or against other types of victims, such as hacking and viruses.

2. Old crimes using new tools.

   Conventional crimes committed using computer technology and new information technology include fraud, identity theft, and stalking.

According to David Wall, the Internet, especially cyberspace, has created not only cases of 'old wine in new bottles' or 'new wine in new bottles' but also cases that include 'new wine in no bottles.' In the latter sense, cybercrime is not only crimes committed using or through information and communication technology; new crimes occur without physical space and time. Only actions and consequences that occur can be identified in physical space and time.

Based on the description above and observations of various forms/types of cybercrime, cybercrime includes traditional crimes that use information and communication technology as tools or media and new crimes that can only occur in cyberspace or the Internet.

Judging from criminological theory, especially micro theories (micro theories), a person/group of people in society commits a crime or becomes a criminal (criminal etiology).[14] Concretely, these theories are more inclined to a psychological or biological approach. Included in these theories are Social Control Theory and Social Learning theory. Third, Bridging Theories do not fall into the macro/micro theory category and describe the social structure and how a person becomes evil. However, the classification of these theories often discusses epidemiology, which explains crime rates and the etiology of criminals. Included in this group are Subculture Theory and Differential Opportunity Theory.

Muhammad Mustafa further explained the causes of crime, including cybercrime, with the Fire Triangle Theory as described as follows[15]:

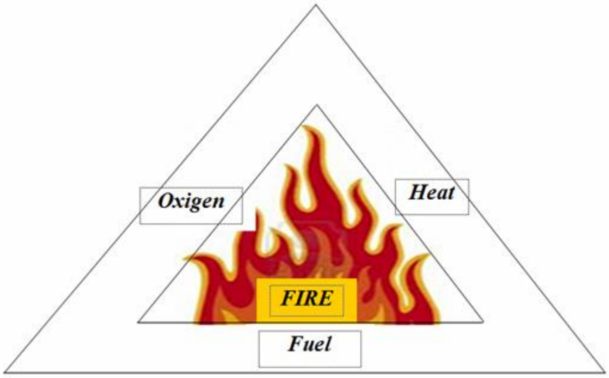

Figure 1. Fire Triangle Theory

In the Fire Triangle theory, crime is likened to a standard that occurs when the three elements of fire, namely oxygen (oxygen), heat (heat), and fuel (fuel), meet, and then a fire will occur. The cause of the fire, when drawn into the cause of crime, crime can occur because of pressure. Pressure can occur from the perpetrator's financial condition (financial pressure). If this pressure is met with opportunity (opportunity) and there is justification from the perpetrator (rationalization), then a crime can be committed by anyone, including foreigners in Bali.

Crime generally occurs because of three main things: the pressure to commit a crime, the opportunity that can be exploited, and the justification for the act. In principle, the causes of cybercrimes committed by foreigners in Bali have three elements: illegal acts carried out by the foreigner for personal and group gain while harming the other party either directly or indirectly.

Pressure is generally caused by individual behavior that causes them to commit crimes.[16] It could be that the pressure is due to financial problems (financial pressure) triggered by an excessive lifestyle, a greedy attitude, and a lot of debts or dependents, which causes a person to be "forced" to commit a crime. Bad habits that are ingrained and cannot be eliminated just like also make a person motivated to commit crimes, especially if these habits require quite a lot of funds such as gambling, liquor, and prostitution. All of these habits require substantial funds to fulfill. That is why someone who is addicted to these bad habits can commit crimes.

Another cause of crime is the existence of opportunity. Foreigners in Bali have wide-open opportunities to commit crimes, including cybercrimes. Visa-free visits and the weak supervision of foreigners in Bali have opened up opportunities for foreigners visiting Bali to commit these crimes.

B. Efforts to Combat Cyber Crime Committed by Foreigners in Bali

Cybercrime prevention policies with criminal law include penal policy, which is part of the criminal policy (crime prevention policy). From the point of view of criminal policy, crime prevention efforts (including overcoming cybercrime) cannot be carried out only partially with criminal law (penal means); they must also be taken with an integral/systemic approach. As a form of high-tech crime that can transcend national borders (transnational/transborder), it is natural that cybercrime prevention efforts must also be taken with a technological approach (techno prevention). In addition, a cultural/cultural approach, a moral/educational approach, and even a global approach through international cooperation are needed.

The operationalization of penal policy includes criminalization, decriminalization, penalization, and depenalization. The enforcement of criminal law is highly dependent on the development of legal politics, criminal politics, and social politics. Therefore, law enforcement does not only pay attention to autonomous law but also to social problems and the science of social behavior.

About the policy of criminalizing acts in cyberspace, in a workshop on computer-related crime held at the X United Nations Congress in April 2000, it was stated that member countries must try to harmonize provisions relating to criminalization, proof, and procedures (states should seek harmonization of the relevant provisions on criminalization evidence and procedure).[17] So the problem is not just how to make a criminal law policy (criminalization policy/formulation/legislation) in the field of cybercrime prevention but how there is harmonization of penal policies in various countries. It means that the criminalization policy on cybercrime is not solely a matter of Indonesian national policy but is also related to regional and international policies.

Five things need to be considered by legislators to criminalize cybercrime, namely:

1. Criminalization must be an effort that supports the ultimate goal of criminal policy, namely protecting and prospering society.
2. The act that will be criminalized is reproached by the community.
3. It is necessary to take into account the advantages and disadvantages of criminalization.
4. Efforts should be made to prevent over-criminalization, which can indirectly affect the community's interests.
5. There needs to be an adjustment between law enforcement and law enforcement capabilities.

Criminalization policies or formulations of criminal law in Indonesia related to cybercrime problems so far can be identified as follows:

1. In the Criminal Code (KUHP)

The formulation of criminal acts in the Criminal Code is mostly still conventional and has not been directly linked to the development of cybercrime; besides that, there are also various weaknesses and limitations in dealing with technological developments and high-tech crime, which vary widely.[18] For example, the Criminal Code has difficulties in dealing with credit card counterfeiting and electronic fund transfers because there are no special rules.[19] The existing provisions only concern (a) oath/false statement (Article 242); (b) shying away from currency and banknotes (Articles 244-252); (c) counterfeiting stamps and marks (Articles 253-262); and (d) falsification of letters (Articles 263-276).

2. Laws outside the Criminal Code (KUHP)
    a. Law Number 36 in 1999 concerning Telecommunications threatens criminal acts against (1) manipulating access to telecommunications networks (Article 50 jo 22); (2) causing physical and electromagnetic disturbances to telecommunications operations (Article 55 jo 38); (3) intercepting information through telecommunications networks (Article 56 jo 40).
    b. Article 26A of Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning Eradication of Criminal Acts of Corruption; Article 38 of Law Number 15 of 2002 concerning the Crime of Money Laundering; and Article 44 paragraph (2) of Law Number 30 of 2002 concerning the Corruption Eradication Commission; recognize electronic records as valid evidence.
    c. Law Number 32 of 2002 concerning Broadcasting, among others, regulates criminal acts:
        1) Article 57 jo 36 paragraph (5) threatens to be punished for broadcasts that (a) are slanderous, inciting, misleading, and/or lying; (b) highlight elements of violence, obscenity, gambling, narcotics, and drug abuse; or (c) opposing ethnicity, religion, race, and between groups.
        2) Article 57 jo 36 paragraph (6) threatens to punish broadcasts that ridicule, demean, harass, and/or ignore religious values, Indonesian human dignity, or damage international relations.
        3) Article 58 jo 46 paragraph (3) threatens criminal action against commercial advertising broadcasts which include: a) promotions related to the teachings of religion; ideologies, individuals and/or groups, which offend and/or demean other people, other ideologies, other individuals, or other groups; b) promotion of liquor or the like and addictive substances or substances; c) promotion of cigarettes that demonstrate the form of cigarettes; d) things that are contrary to public decency and religious values; and/or e) exploitation of children under the age of 18.
    d. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law)[20], Chapter VII Prohibited Acts, contains criminal provisions for any person who intentionally and without rights or against the law distributes and/or transmits and/or make accessible electronic information and/or electronic documents. The criminalization of cybercrime, especially in the ITE Law, can be divided into two categories: acts that use computers as a means of crime and acts that make computers a crime target. A crime that uses computers as a means is any action that utilizes computer data, computer systems, and computer networks as tools to commit crimes in cyberspace instead of real space. A crime that targets a computer is any act using a computer that is directed at computer data, computer systems, computer networks, or all three together. The act is carried out in cyberspace, not real space, so all activities prohibited by laws and regulations occur in cyberspace.

Many Internet crimes, such as cybercrimes, are committed by foreigners in Bali, but only a few cases have reached the court level. This is because the judge himself has not received electronic evidence, such as digital signatures, as valid evidence. Thus, cyber law is not only necessary but also necessary to face the current reality, with the increasing number of cybercrime activities and demands for cross-border transactions in the future.

Therefore, as a country affected by these developments and changes, Indonesia must formulate legal instruments to support business activities more broadly, including those carried out in the virtual world, without ignoring what happened. The existing legal instruments plus cyber law will further complement the existing legal instruments. This initiative is vital and urgent to be carried out, along with developing these new business patterns. Cyber law is needed to regulate new crimes that can be categorized as cybercrimes.

V.CONCLUSION

Based on the results and discussion described above, it can be concluded that the factors causing cybercrime committed by foreigners in Bali have three elements, namely, illegal acts carried out by the foreigner and carried out for personal and group gain while on the other hand harming the other party either directly or indirectly. Pressure is generally caused by individual behavior that causes them to commit crimes. It could be that the pressure is due to financial problems (financial pressure) triggered by an excessive lifestyle, a greedy attitude, a lot of debts or dependents, and soon, which causes a person to be "forced" to commit a crime. Bad habits that are ingrained and cannot be eliminated just like also make a person motivated to commit crimes, especially if these habits require quite a lot of funds, such as gambling liquor, and prostitution. All of these habits require substantial funds to fulfill. That is why someone who is addicted to these bad habits can commit crimes. Another cause of crime is the existence of opportunity or opportunity. The opportunity is vast for foreigners in Bali to commit cybercrimes. The crime of visa-free visits and the weak supervision of foreigners in Bali have opened up opportunities for foreigners to commit these crimes. Efforts to combat cybercrimes committed by foreigners in Bali can be carried out by implementing cyber law or legal policies in the cyber field. The legal system in Indonesia has yet to regulate cybercrime specifically. Some existing regulations, both in and outside the Criminal Code, can temporarily be applied to several crimes. However, some crimes cannot be anticipated by the ITE Law that is currently in effect. To combat cybercrime, which has a higher crime rate in Indonesia, the government needs to revise the ITE Law that has been drafted. The government should correct everything contained in the ITE Law; points may need to be revised so that cyber law in Indonesia can be appropriately implemented. Thus, cyber law is not only a necessity but a necessity to face the current reality, with the increasing number of cybercrime activities and the demands of foreign trade communications (cross-border transactions) in the future. Therefore, as a country affected by these developments and changes, Indonesia must formulate legal instruments to support business activities more broadly, including those carried out in the virtual world, without ignoring what happened. This is because the existing legal instruments plus cyber law will further complement the existing legal instruments. This initiative is vital and urgent to be carried out, along with developing these new business patterns. The recommendations that can be described are as follows: (1) Cyberlaw needs to be explicitly made by a specialist to facilitate law enforcement against these crimes. (2) There is a need for special procedural laws that can regulate, such as relating to types of legal evidence in cybercrime cases, granting special powers to investigators in carrying out several necessary actions in the context of investigating cybercrime cases, and others. (3) Specialization of investigators and public prosecutors can be considered a way to enforce Cyber Law. It is recommended that cyber police be established in Indonesia. Cyber police can be formed from a combination of Polri units and various competent groups in the IT and cyber world. The formation of the cyber police can be said to be similar to the formation of the KPK in Indonesia. The difference is that the KPK is tasked with tackling corruption, while the cyber police are tasked with tackling cybercrime. Establishing cyber police is expected to reduce cybercrime in Indonesia.

REFERENCES

[1] A. Spenceley and A. Rylance, “The contribution of tourism to achieving the United Nations Sustainable Development Goals,” *A Res. agenda Sustain. Tour.*, pp. 107–125, 2019.

[2] I. W. Rideng, I. N. P. Budiartha, and I. N. Sukandia, “The development of bali tourism through cultural and local wisdom of customary village,” *Int. J. Entrep.*, vol. 24, no. 5, pp. 1–6, 2020.

[3] A. K. Jaelani, R. D. Luthviati, R. O. Kusumaningtyas, S. Al Fatih, and A. Siboy, “Legal Protection of Balinese Traditional Law During Global Tourism Destination Development,” *KnE Soc. Sci.*, 2024.

[4] F. H. Murcahyo and S. Subekti, “SUPERVISION AND ENFORCEMENT OF IMMIGRATION FOR FOREIGNERS WHO COMMIT VIOLATIONS IN INDONESIAN TERRITORY,” *Equal. Int. Law J.*, pp. 46–59, 2023.

[5] R. D. Hapsari and K. G. Pambayun, “Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis,” *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023.

[6] A. Suhaemin and M. Muslih, “Karakteristik Cybercrime di Indonesia,” *Edulaw J. Islam. Law Jurisprudance*, vol. 5, no. 2, pp. 15–26, 2023.

[7] S. H. M. S. Prof. Dr. I Made Pasek Diantha, *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Prenada Media, 2016. [Online]. Available: https://books.google.co.id/books?id=-MpADwAAQBAJ

[8] P. Mahmud Marzuki, “Penelitian Hukum,” *J. Penelit. Huk.*, p. 181, 2019.

[9] M. W. AS, I. W. G. Wiryawan, and K. S. L. PP, "FAKTOR PENYEBAB TERJADINYA KEJAHATAN CYBER CRIME YANG DILAKUKAN OLEH ORANG ASING DI BALI DITINJAU DARI PERSPEKTIF KRIMINOLOGI," *J. Yusthima*, vol. 1, no. 01, pp. 58–70, 2021.

[10] M. E. Fuady, "Internet: Teknologi Pencipta Dunia 'Cyber,'" *MediaTor*, vol. Vol.6, no. No.2, pp. 255–264, 2005, [Online]. Available: http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107

[11] M. Yar and K. F. Steinmetz, *Cybercrime and Society*. in Core textbook. SAGE Publications, 2019. [Online]. Available: https://books.google.co.id/books?id=gpuHDwAAQBAJ

[12] M. Bachmann, "Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime," *International Criminal Justice Review*, vol. 18, no. 2. p. 246, 2008. [Online]. Available: http://search.proquest.com/docview/210497998?accountid=130689%5Cnhttp://godot.lib.sfu.ca/godot/hold_tab.cgi?sid=proquest:proquest&genre=unknown&aulast=Bachmann%2C+Michael&atitle=Cybercrime%3A+The+Investigation%2C+Prosecution%2C+and+Defense+of+a+Computer-R

[13] S. Furnell, "Cybercrime: The Transformation of Crime in the Information Age – By D.S. Wall," *The British Journal of Sociology*, vol. 59, no. 1. pp. 177–179, 2008. doi: 10.1111/j.1468-4446.2007.00187_8.x.

[14] Marwin, "Penanggulangan Cyber Crime Melalui Penal Policy," *J. Huk. Ekon. Syariah*, vol. 5, no. 1, pp. 31–40, 2013.

[15] M. Mustofa, *Metodologi penelitian kriminologi*. Prenada Media, 2015.

[16] B. N. Arief, "Kapita Selekta Hukum Pidana." 2013.

[17] G. M. Swardhana and I. K. R. Setiabudhi, "Buku Ajar Krimonologi dan Viktimologi," p. hal 60-63, 2016.

[18] B. N. Arief, *Pembaharuan hukum pidana dalam perspektif kajian perbandingan*. Citra Aditya Bakti, 2005. [Online]. Available: https://books.google.co.id/books?id=XeMQAAAACAAJ

[19] J. R. Batmetan, "Analisa Penyebab Terjadinya Cybercrime (Study Kasus: Yhummy Online Shop)," 2018.

[20] A. E. Boyle and C. Redgwell, *Birnie, Boyle, and Redgwell's international Law and the environment*. Oxford University Press, 2021.