IJCLS 5 (1) (2020) 63-74

IJC LS

INDONESIAN JOURNAL OF CRIMINAL LAW STUDIES
http://journal.unnes.ac.id/sju/index/php/ijcls

Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?

Massulthan Rafi Wijaya[1]
Independent Researcher on Law, Crime and Technology
Ridwan Arifin
Faculty of Law, Universitas Negeri Semarang

Received Maret 2 2020, Accepted April 2 2020, Published May 31 2020

Abstract

Cybercrime is a new type of crime arising from globalization in this world. This crime is more dangerous than other crimes because the impact can cause world war. It is undeniable that this crime in the present has grown as time goes by until now, there are many cases of this crime. All countries compete to advance their technology for positive things, but many people abuse it for negative actions. We must be vigilant if we want to use technology because there are many bad people out there, if we are negligent then we can be affected by those bad people. Then the lack of public attention now that there is a new type of crime that is more dangerous than other crimes. We must protect each other so that we are not affected by cybercrime. This crime does not only have one sector but can be in all sectors, because this crime can be said to be an extraordinary crime.

Keyword: Criminal Law; Cybercrime; Globalization; International Legal Instruments; Technology Development

INTRODUCTION

The development of globalization and information technology has brought major changes in human life. Information Technology makes the relationship of communication between people and between nations easier and faster without being influenced by space and time. Globalization is a process of changing the dynamics of the global environment as a continuation of a situation that was previously characterized by the characteristics of technological and information progress, creating interdependence, blurring boundaries (borderless). The impact of technological developments and information changes the direction of the war that is happening at this time (Ineu, 2017). World civilization in the present is characterized by the phenomenon of the progress of information and globalization that takes place in almost all areas of life. What is called globalization basically started from the beginning of the 20th century, namely when the transportation revolution began from the beginning of the 20th, namely in the event

**Email: massultanrafi@gmail.com & ridwan.arifin@mail.unnes.ac.id*
Address: Gedung K, Kampus Sekaran, Gunungpati, Semarang Jawa Tengah 50229, Indonesia
Phone/Fax: (024) 8507891

of a widespread transportation and electronic revolution and accelerating trade between nations, in addition to the increase and speed. cross goods and services.

Revolution occurs in various fields of human life such as industry, culture, education, technology, information systems and others. As has happened before, this revolution also brought rapid changes and tended to change the old standard values and paradigms (Yusda PP, 2015). The need for computer network technology is increasing (Eliasta, 2016). All parties seemed not to be left behind in taking advantage of the opportunities offered by information technology, especially with the presence of the internet that created a participatory culture . But like a currency that has two sides, the internet not only has a positive, but also a negative impact. This fact raises a new phenomenon known as cybercrime. The rise of new crimes, namely cybercrime in the era of development of communication technology is very disturbing to the public. Various kinds of crimes can be caused by using communication technology between defamation through the internet, gambling, terrorism, credit card fraud, pornography and other crimes (Christiany, 2015).

Technological developments, especially in the field of telecommunications and transportation are considered as locomotives and help accelerate the process of globalization in various aspects of life. Cyber crime is a crime committed by a person or group using computer equipment and other telecommunications equipment. Someone who masters and is able to operate a computer such as operators, programmers, analysts, consumers, managers, cashiers can do cyber crime (Ismail, 2009). As a media information provider the internet is also the largest commercial community and the fastest growing means of activity. The network system allows everyone to know and send information quickly and eliminate territorial boundaries of a country. Each country must face the fact that world information is currently built on a network offered by the advancement of technology. The development of the internet is increasingly increasing both technology and its use. Information technology today can be a double-edged sword. Information technology can contribute to the improvement of human well-being, progress and civilization, but can also be an effective means of lawlessness (*onrecht matigedaad*). In this case, the law should provide protection to internet users who have good intentions and take firm action against the perpetrators of internet crimes that cause many other people's losses (Fiorida, 2012).

From the information above there are still many people who use gadget devices ranging from mobile phones, smartphones, tablets, laptops and PCs who have been connected to the internet network, there are still many people who experience Cybercrime crime because of the ignorance of the knowledge of the Indonesian people themselves to report responsible parties who handle cases of cyber crime and their reluctance to report because police procedures are so complicated and for reporting models that are still conventional. Based on the description of the above background, that the community needs to be facilitated by a Framework by using an information system for reporting acts of crime about cybercrime which is easily accessible anywhere and anytime. and if there is a form of cooperation with competent parties to deal with cases of cybercrime, it can be integrated with the existing information system on the side of the police (Daryono & Sugiantoro, 2017).

In addition, with the development of the flow of information and technology today has become a double-edged sword, because in addition to providing a good / positive contribution to society, on the other hand it also has negative impacts. Negative impacts can arise when an error is caused by a computer device which will result in large losses for users or interested parties. Deliberate errors lead to the misuse of computers,

so the potential to use computer and internet media to carry out various crimes. Various acts of crime that use computer technology and the internet as the media, in recent times shows significant numbers, both from in terms of quantity and in terms of quality. The use of computer media and the internet as a medium for committing crimes is generally known as cybercrime. Cybercrime can also be defined as an act that violates the law by utilizing computer technology that has a basis in the sophistication of internet technology. As stated by Andi Hamzah (1989) which mean cyber-crime as a crime in the computer field in general can be interpreted as illegal computer use (Antoni, 2017). The paradigm of human communication in carrying out economic activities , business, social interaction and politics are different (Fuady, 2005).

Technological advances have brought changes and rapid shifts in a life without limits. The use of these technologies has encouraged rapid business growth, because various information can be presented through long-distance relationships and those who wish to enter into transactions do not have to meet face to face, but rather through computer equipment and telecommunications. The development of information technology also forms a new world society that is no longer hindered by territorial boundaries and has turned everything far away so that the imaginary one becomes real. But behind that progress, has also given rise to new resentment with the emergence of sophisticated crimes in the form of Cybercrime. Computer-related crimes are all forms of crime aimed at computers, computer networks and users, and traditional forms of crime that use or with the help of computer equipment. These crimes are divided into two categories, namely Cybercrime in a narrow sense and in broad terms.

Cybercrime in a narrow sense is a crime against computer systems, while Cybercrime in the broad sense includes crimes against computer systems or networks and crimes using computer facilities. The history of internal development begins with the development of information technology related to connected networks which began in 1962, when the United States Department of Defense conducted research on the use of computer technology for US air defense interests. Through its research institute, the Advanced Research Project Agency (ARPA) assigns the New Information Processing Technique Office (IPTO), namely an institution that is tasked with continuing research on the use of computer technology in the field of air defense. telecommunication technology with computers known as ARPANet (Advanced Research Projects Agency Network), which is a network system through connections between computers in vital areas in order to overcome problems in the event of a nuclear attack (Sri, 2014).

Currently internationally used for legal terms related to the use of information technology. Other terms used are virtual word law, information technology law. The term was born given the activities carried out through a network of computer systems and communication systems both locally and globally (the internet) by utilizing computer-based information technology which is an electronic system that can be viewed virtually or virtually. Then after that, a new term emerged from computer crime namely Cyber crime. Cyber Crime is a development of computer crime. Cyber crime and cyber law where this crime has violated criminal law. With the cases that occur in the virtual world, many victims have fallen, not only among teenagers but at all ages. This requires the police to act immediately in dealing with cyber crime cases whose scope of crime is very broad and even unlimited. Conventional views on cyber crime will lead to difficulties and inequalities in the process of investigation, investigation and verification where the process is not the same as the process of investigation, investigation and verification in conventional criminal cases, but we must still take a positive attitude towards the Law. Law No. 11 of 2008 concerning Internet and Electronic Transactions as a legal umbrella in the world of Cyber Crime, with the hope that it can become a

reference and one of the law literature in terms of enforcement of cyberlaw in Indonesia. In handling cybercrime cases, it is also expected that the prosecution of the police to avoid the case of cyber crime that has occurred can simply be separated from the supervision of the law, Cyber crime has an efficient and fast nature and is very difficult for investigators in making arrests of perpetrators. This is due, among other things, to the lack of understanding and knowledge of the community on the types of cyber crime, understanding and knowledge, causing obstacles in dealing with cyber crime, in this case the constraints relating to legal arrangement and the process of public oversight of any activities allegedly related to crime the cyber crime (Aco Agus & Riskawati, 2016).

Cyber crime is a crime that uses information technology and is one form transnational crime does not recognize borderless, without violence (non violence), there is no physical contact (no physically contact) and without name Characteristics of Cyber crime that makes Cyber Crime actors very difficult tracked and the criminal elements are difficult to prove, moreover the limitations of regulation. Protection of victims of cyber crime requires seriousness and high expertise from law enforcement officials, legal officers are needed who master high technology in the field of technology informatics both police, prosecutors and justice due to the existence of cyberspace border state less, in addition, a good and good cooperation is needed measured between countries both regionally and globally in order to prevent and overcoming transnational crime like ciber crime. Because of the many crime cases in the world the borderles need a rule law and its implementation in the field, cooperation between related institutions both on a national scale, regional and international in order overcome, prevent and eradicate all perpetrators of crimes that occur in cyberspace (Tanthawi, Ali Dahlan, 2014).

The internet has had a far greater impact on computer-based communication than other developments, and has also encouraged business transactions via the Internet. World-scale companies are increasingly using internet facilities. Meanwhile, transactions through electronic or on-line grew from various sectors, which then gave rise to the term; e-banking, ecommerce, e-trade, e-business, e-government, e-education and e-retailing. The development of the Internet, which is increasingly increasing in both technology and usage, brings many positive and negative impacts. cyber crime is a crime that crosses national borders, is not limited to jurisdiction, without violence, no physical contact, which can produce victims for anyone internet users seeking legal protection efforts from the government about people who are victims of cyber crime either through preventive actions or repressive through technological approaches, socio-cultural approaches, and legal approaches. An extra-territorial jurisdiction principle approach is needed in law enforcement in cyberspace, and requires cooperation between all related elements, both nationally, regionally and internationally. Furthermore, there is a need for extradition agreements between countries against perpetrators. Attacking cyber and also need to align the meaning of cyber crime in the context of invitations between all countries to facilitate law enforcement in cyber crime prevention (Arifah, 2011).

FINDING AND DISCUSSION

Cybercrime On The International Legal Instruments

The public international legal instruments that regulate cyber crime problems that are currently getting the most attention are the 2001 Convention on Cyber Crime which

was initiated by the European Union. This convention though was originally made by European regional organizations, but in its development it is possible to ratify and be accessed by any country in the world that is committed to efforts to overcome cyber crime. Countries that are members of the European Union (Council of Europe) on November 23, 2001 in the city of Budapest, Hungary have made and agreed on the Convention on Cybercrime which is then included in the European Treaty Series Number 185. This Convention will be effective after ratification by at least 5 (five) countries, including at least ratification carried out by 3 (three) member countries of the Council of Europe. The international legal instrument that regulates the problem of mayantara (cybercrime) crime which is currently the most concerned is the 2001 Convention on Cyber Crime initiated by the European Union. This Convention was formed with considerations, among others: First, that the international community is aware of the need for cooperation between countries and industries in combating cyber crime and the need to protect legitimate interests in the use and development of information technology. Second, conventions are currently needed to reduce the misuse of systems, networks and computer data to commit criminal acts. Third, there is now a growing need to ensure that a match between implementing law enforcement and human rights is in line with the European Council Convention on the Protection of Human Rights and the 1966 United Nations Covenant on Political and Civil Rights. This convention has been agreed by the European Union as a convention that is open to access by any country in the world. This is intended to be used as International Law norms and instruments in overcoming cyber crime, without reducing the opportunity for each individual to continue to develop their creativity in developing information technology (Situmorang, 2014).

Cybercrime is different from other transnational crime problems because of its global nature. To overcome this effectively, what is needed is global harmonization and cooperation, and not only regional harmonization and cooperation. In addition, with a number of regional instruments, there is a real danger that different instruments will set different harmonization standards for each member country. This action will derail global cooperation efforts, said another author as "fragmentation of international responses" to cybercrime. This can also produce "regional groups" of harmonization and cooperation, which involve countries in certain regions. global crime issues such as cyber crime, which are needed and the main key is global cooperation. Therefore, SADC countries must try to harmonize their laws with global standards so that they can work with countries around the world (Bande, 2018).

In relation to cybercrime, the point of view is internet crime which makes banks, marchants, online shops or customers victims, which can occur because of the malicious intent of someone who has the ability in the field of information technology, or someone who utilizes bank mismanagement, marchant and customer. Some forms of potential cybercrime in banking activities include:

Typo site, the perpetrator created a fake site name that exactly matches the original site and made an address similar to the original site address. The perpetrator waits for an opportunity if someone victim mistypes the address and enters his fake site. If this happens, the perpetrator will obtain user information and password for the victim, and can be used to harm the victim.

Keylogger / keystroke logger: Other modes are keylogger. This often happens in places where public internet access is like in an internet cafe. This program will record the characters typed by the user and hope to get important data such as a user ID or password. The more frequently accessing the internet in public places, the more vulnerable it is to be exposed to the modus operandi known as keylogger or keystroke

recorder. Because the computers in the internet cafe are used alternately by many people. The mode of work of this mode is actually very simple, but many computer users in public places are careless and are not aware that all of their activities are recorded by others. The perpetrator installs the keylogger program on public computers, this keylogger program will record all the keyboard buttons that are pressed by the next computer user. In other time, the keylogger installer will take the "trap" results on the same computer, and he hopes will get important information from the victims, such as a user ID and password Sniffing: an attempt to get a user ID and password by observing data packets that pass on a computer network. Brute Force Attacking: An attempt to get a password or key by trying all possible combinationWeb Deface: System Exploitation with the aim of changing the appearance of one site's home page. Email Spamming: Send junk email in the form of product advertisements and the like to someone's email address. Daniel of Service: Flooding data in very large amounts with the intention of disabling the target system.Virus worms, trojans: Deploy worm and trojan viruses with the aim to disable the computer system, obtain data from the victim system and to defame the makers of certain software (Nazarudin, 2011).

Crime in the field of information technology, also known as cyber / cyberspace crime, has to do with crime prevention, a workshop on computer related crime held at the UN Congress X April 2000 stated that member countries must try to harmonize the provisions related to criminalization, proof , and procedures (States should seek harmonization of the relevant provisions on criminalization evidence and procedure). So the problem is not just how to make criminal law policies (criminalization / formulation / legislation policies) in the field of cyber crime prevention, but how there is harmonization of penal policies in various countries. This means that the criminalization policy on the problem of cyber crime is not merely a matter of national policy (Indonesia), but also related to regional and international policies (Supanto, 2016).

According to the Convention on Cybercrime, a criminal offense can be obtainedclassified as cybercrime regulated in Articles 2-5, while the types of criminal acts are:

Illegal AccessRegulated in Article 2 Convention on Cybercrime, which reads"Each Party shall adopt such as legislative and other measures as may be necessary as criminal offenses under its domestic law, intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intentions, or in relation to a computer system that is connected to another computer system. "Illegal access covers basic violations of threats. dangerous threats from attacks on data security and computer systems. Protection against illegal access violations is an illustration of the interests of organizations or groups and people who want to regulate, run and control their systems run without any interference and obstacles.

Illegal Interception Regulated in Article 3 of the Cybercrime Convention, which reads:"Each Party shall adopt such as legislative and other measures as may be necessary to establish as criminal offense under its domestic law, intentionally, the interception without right, made by technical means, from non-public transmissions of computer data to, from within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the commitment be carried out with the same intent, or in relation to a computer system that is connected to another computer system. "And harms many people (Putra, 2014).

Indonesia as a democratic law state (democratische rehtsstaat) is considered the most important source of law, because the law is an embodiment of formalized people's

aspirations, also based on government law obtaining the main authority (attributive authority) to do legal actions (according to legaliteitsbeginsel principle known in the state administrative law). The constitutionality aspect of the formation of legislation is one of them, must be based on a system of legislation or a hierarchy of laws and regulations. However, the quality of laws and regulations in Indonesia is doubted because of the many laws declared unconstitutional by the Constitutional Court. Indonesia has accommodated constitutional testing or the so-called constitutional review and judicial review to test a law against the 1945 Constitution of the Republic of Indonesia which was carried out at the Constitutional Court (MK). But its weakness, when losses may have occurred due to the implementation of a law that is contrary to the legislation that is higher. In contrast to Indonesia, in France the constitutional testing mechanism is carried out before the relevant law officially becomes a legislative act that is generally binding and is still in the form of a preventive constitutional review. the author is interested in studying more about the model of constitutional testing in France (Constitutional Council) by paying attention to the issues of quality and substance of legislation in Indonesia (Desy, 2018).

As a legal state based on Pancasila and the 1945 Constitution of the Republic of Indonesia the time has come to optimize administrative law enforcement. Supervision of government actions is intended so that the government in carrying out its activities in accordance with legal norms. So that the government in organizing its government is always based on justice. Included in this is implementing the decisions of the State Administrative Court that have permanent legal force by state administration officials, without being preceded by a plaintiff's request for an award to the Chair of the State Administrative Court. Obligations that must be carried out by state administration officials as a form of realization are granted by the claim

The State Administrative Court includes: revocation of the relevant State Administrative Decree, meaning the disputed State Administrative Decision; revocation of the Administrative Decision of the country concerned and issue a new State Administrative Decree; issuance of State Administrative Decrees in the case of a claim based on Article 3 or fictitious negativity. This obligation must be addressed by state administration officials as a form of law enforcement in administrative law. However, in practice, not all decisions of the State Administrative Court that have legal force remain carried out by state administration officials (Untoro, 2018).

Recent changes in conditions require the government to build a government that is clean, authoritative, transparent and able to respond effectively to changing demands in line with technological advances to realize the goals of the nation and state as mentioned earlier. The change in question is utilizing the development of information technology. The demand to become a more modern nation person has been demonstrated through the creation of an electronic identity card (e-KTP) program. This program is designed to keep all resident documents in a complete database system, so that they no longer need other document files that make it inefficient when used. this program has been tried in several countries using a single identity, such as Malaysia which has MyKad (Malaysian electronic ID) and identity cards, as well as driving licenses, basic medical data, public key infrastructure, e-cash, and card transit. Thai E-ID is applied as an identity card, medical history, authentication certificate, e-border pass, and online services. Then Portugal, the five national cards that exist (identity cards, tax cards, social security cards, health service user cards, voter cards) are changed to one e-KTP card. In principle, an electronic ID card program is supported by a conventional ID card manufacturing system in Indonesia that allows one to have more than one ID. In fact, armed with several identity cards also allows someone to commit a crime in

various places without knowing the traces of previous crimes. In a criminology perspective, identity fraud through the duplication of conventional ID cards can be a person's entrance to recurring crimes. the existence of multiple identities is of course a problem that can destroy the order of life in society because of the potential for repeated childbirth. criminals or recidivists. in Indonesia, in relation to recidivists in fact the Criminal Code has provided a system of complaints to recidivists in accordance with Article 486 of the Criminal Code, where a person can be punished with a third sentence more than a normal sentence by noting that the act of the same type is done in less time from five years serving after the sentence was dropped. This weighting system is an explanation of the theory of retaliation in which the criminal is given for the purpose of deterrent effects for crime actors in the State's efforts to protect security and public order. However, this weighting system will not run smoothly if the government is unable to elaborate on the complexity of the causes of crime and solve them, because there is no single and concrete information that can be easily accessed by law enforcement (Lukitasari, 2017).

In foreign countries and Indonesia in particular, there are many cases of violations of human rights or crimes against humanity that are inseparable from the crime of cybercrime itself, where perpetrators are free to roam and even unreachable by law or in other words let the state condemn it without punishment. impunity.Impunitas namely allowing political and military leaders who are allegedly involved in cases of gross violations of human rights such as the crime of genocide, human crime, and war crimes are not tried is a phenomenon of political law that we can witness from the past century to the present. Declaration of Rights -Human rights for the country of Indonesia have existed from antiquity but have only been drawn up on the basic guidelines of this country, which are in the opening of the 1945 Constitution in which there are human rights as good people manu in vain as a personal being and as a social being which in his life all become something inherent, and confirmed in the Pancasila from the first precepts to the fifth precepts. because Indonesia is carrying out a period of change in this millennial era which greatly affects Indonesia's growth going forward (Mukhamad Luthfan Setiaji dan Ibrahim Aminullah, 2018).

Nationally and internationally, countries are trying to secure by providing protection for the community by making arrangements and in terms of technology trying to find new systems to secure their information networks. the level of crime in cyberspace or cybercrime has shown a very high increase globally, regionally and nationally, so the crime rate has increased sharply. according to the secretary general of ITU hamadoun toure, the challenge that must be faced by countries is security in cyberspace considering that almost everyone gets internet access. Global losses from cybercrime almost per year have reached 100 billion US (Sinta, 2011). In addition to child abuse materials, the digital belongings of an abuser might have contain more minor yet important pieces as like of information such as nicknames, e-mails and names of places. A thorough digital examination and appropriate analysis of this set of informations might have reveal the exact same locations or real identities of criminal associates or of the victimized children. While highly convenient for investigators, triage is essentially a quick, on-thespot digital forensic evaluation, for time-sensitive cases in particular. And In most of these all cases, investigators do not even know whether they will be able to dp the extract incriminating evidence from the seized digital materials before the operation takes place. However, for the online child abuse investigations, investigators generally have a solid a lot of the ideas about what and where the suspect might possess the illicit materials beforehand. Even in the absence of such firm knowledge, the possibility of failing to notice incriminating evidence of significant

importance makes LEAs extra cautious. Consequently, due to these complications, triage is an extremely risky method of digital forensics examination and rarely preferred in relation to online child abuse investigations (Açar, 2018).

Within the discipline of criminology and indeed more widely within all of the social science, the question of how the Internet can be and might be the one of the potentializes adolescent behavior towards delinquency remains a largely and an unexplored, yet fundamental, question. Even before the advent of the Internet, adolescence has long been viewed by developmental psychologists as a period of tremendous (and often or most of them are tumultuous) biological, psychological and social change. During the puberty time, adolescents experience rapid growth, expand their social skills and circles, as well as mature sexually. Significant brain development also occurs during this period, resulting in expanded cognitive abilities that ultimately enable more sophisticated thinking when compared to the children - particularly as it relates to abstract reasoning about the thing called as hypothetical situations. As adolescents negotiate the boundaries of this transition, they are all "increasingly receptive or active with respect to risky, albeit not necessarily illegal or anti-social in behaviorall. For some time now,all of the scholars all around the world have widely acknowledged that experimental and risk-taking behaviors are in some ways central to the adolescent condition. Such as like the experimentation has been visible in relation to the exploration of newfound sexuality in the children cybercrime , the development of the independent and coherent identities by Erikson 1968 and Kroger 2003 in his book, says that the formation of intimate and complex social relationships with peers and romantic partners as what Furman & Shaffer, 2003 in his book called Pombeni et al., 1990 and the acquisition of values/ideologies consistent with the social groups to which they belong and matched on them just like what he says in his book called as Havighurst in year 1972 (Russell, dkk, 2018).

As the examples to the consequences of the cyber bullying that happened and experienced, for those who experience it or we called them who experience it as victims and bullies, through the review of some legal studies and social studies, the author found that cyber bullying will influence their psychosocial adjustment in areas such as mental health, self-esteem, and social relationships. In respect to social relationships, for example, the results of the study conducted by Crosslin and Crosslin says on yar 2014 indicated to the that young victims of the cyber bullying may become an reticent in social situations and withdraw from interactions with others.and the Most importantly of all that is, cyber bullying may influence victims' trust in their social interaction partners in the future of their oen and real life because they want to avoid potentially possible harm from their partners as what Rivituso says in 2014. Moreover of that, cyber bullying will also give an imppact and bad effect also affect an individual's reputation, academic performance, cognition, and attitude towards school. In the case of an individual's reputation, for example, cyber bullying may have a lasting and also maybe forever in along time ahead impact on an individual's reputation because of the permanent digital footprint,O'Keefe, Clarke-Pearson, & Council on Communication and Media says in theor book that released in 2014. This means that people's interactions in the digital world can be viewed and important by users for years to come. Therefore, if a bully spreads defamatory information about the victim, it may be preserved on the whole Internet. This will harm the reputation of the victim (Sung, 2018).

Networks as a means of networked (cyber-) security governance as what Provan & Kenis in theor book . This need for additional research also stems from the debate on how governmental agencies can increase their efficiency and effectiveness in the preventing and combating cyber crime. Threats of the cyber are becoming more and

more complex since computer systems are increasingly embedded or interdependent and the number of cyber attacks continuously increases. Consequently, a sense of urgency for developing new security directions, guidelines and practices to counter cyber-risks worldwide raises in theor book , the writers is Hojsgaard Munk. Several governments already developed to the new or adapted (criminal) legislation following the signing and ratification of international agreements such as the 2001 Budapest 'Convention on Cyber crime's just like in Kerkhofs & Van Linthout said . Others joined forces and developed regional platforms - such as 'the European Cybercrime Centre (EC3)'- in view of enhancing cross-border cooperation and information exchange. However, uncertainty reigns about organisational adaptations as there remains a lack of insight about which organisation is best in the field of cyber security Smith & Ingram said that in ther book (Rafael, 2018).

CONCLUSION

Globalization is a process of changing the dynamics of the global environment as a continuation of a situation that was previously characterized by the characteristics of technological and information progress, creating interdependence, blurring boundaries (borderless). The impact of technological developments and information changes the direction of the war that is happening at this time. World civilization in the present is characterized by the phenomenon of the progress of information and globalization that takes place in almost all areas of life. What is called globalization basically started from the beginning of the 20th century, namely when the transportation revolution began from the beginning of the 20th, namely in the event of a widespread transportation and electronic revolution and accelerating trade between nations, This crime is more dangerous than other crimes because the impact can cause world war. It is undeniable that this crime in the present has grown as time goes by until now, there are many cases of this crime. All countries compete to advance their technology for positive things, but many people abuse it for negative actions. We must be vigilant if we want to use technology because there are many bad people out there, if we are negligent then we can be affected by those bad people. in addition to the increase and speed. cross goods and services, and because all of this things that is happened in the world nowaday, it is really important to us to be unware about the bullying and also the cybercrime of the young bullying, which is we should be more pay attention and give then a huge protection about that, it is really important so that they will never ever feel traumatic and afraid to live their life in the future.

BIBLIOGRAPHY

A. Aco Agus & Riskawati. (2016). Penanganan Kasus Cyber Crime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Supremasi*, *XI*(1).

Açar, K. V. (2018). OSINT by Crowd-Sourcing: A Theoretical Model for Online Child Abuse Investigations. *International Journal of Cyber Criminology*, *12*(1).

Antoni. (2017). Kejahatan Dunia Maya (Cyber Crime) dalam Simak Online. *Jurnal NURANI*, *17*(2).

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case'. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.

Bande, L. C. (2018). Legislating against Cyber Crime in Southern African Development

Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology*, *12*(1).

Brewer Russell, Cale Jesse, Goldsmith Andrew, H. T. (2018). Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents. *International Journal of Cyber Criminology*, *12*(1).

Christiany, J. (2015). Communication Patterns in Cybercrime (Love Scams Case). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *6*(2).

Daryono dan Bambang Sugiantoro. (2017). Pengembangan Framework Pelaporan Cyber Crime. *Jurnal JISKa*, *1*(3).

Desy, W. (2018). Exantereview dalam Mewujudkan Konstitusionalitas Peraturan Perundang-Undangan di Indonesia. *Indonesian State Law Review*, *1*(1).

Eliasta, K. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal TIMES*, *V*(2), 35–42.

Fiorida, M. (2012). Cyber Crime in Indonesia Law System. *Jurnal Sigma-Mu*, *4*(2).

Fuady, M. E. (2005). Cybercrime "Fenomena Kejahatan Melalui Internet di Indonesia". *Jurnal Mediator*, *6*(2).

Ineu, R. (2017). The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2).

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal INOVASI*, *6*(3).

Lukitasari, D. (2017). Problems of Creation Crime Through the Use of Democratic Database Systems in E-ID. *Indonesian Journal of Criminal Law Studies*, *2*(1).

Mukhamad Luthfan Setiaji dan Ibrahim Aminullah. (2018). Kajian Hak Asasi Manusia dalam Negara the Rule of Law: Antara Hukum Progresif dan Hukum Positif. *Lex Scientia Law Review*, *2*(2), 123–138.

Mulyadi, L. (2012). *Bunga Rampai Hukum Pidana Perspektif, Teoritis, dan Praktis*. Bandung: PT Alumni.

Nawawi Arief, B. (2013). *Perbandingan Hukum Pidana Edisi Revisi*. Jakarta: Rajawali Pers.

Nazarudin, T. (2011). Urgensi Cyberlaw di Indonesia dalam Rangka Penangan Cybercrime Disektor Perbankan. *Jurnal Sasi*, *17*(4).

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional'. *Jurnal Ilmu Hukum*.

Rafael, R. (2018). Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. *International Journal of Cyber Criminology*, *12*(1).

Sinta, D. (2011). Cybercrime dalam Abad 21:Suatu Perspektif Menurut Hukum Internasional'. *MMH*, *40*(4).

Situmorang, evi lestari. (2014). *Kajian Yuridis Pembuktian Kejahatan Mayantara (Cybercrime) dalam Lingkup Transnasional*. Universitas Sumatera Utara.

Sri, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, *1*(3).

Sung, Y.-H. (2018). Book Review of Cyber Bullying Approaches, Consequences and Interventions. *International Journal of Cyber Criminology*, *12*(1).

Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan antisipasinya dengan Penal Policy. *Yustisia*, *94*(1), 53.

Tanthawi, Ali Dahlan, S. (2014). Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia. *Jurnal Ilmu Hukum*, *2*(1).

Untoro. (2018). Self-Rescpect dan Kesadaran Hukum Pejabat Tata Usaha Negara Menuju Keadilan. *Pandecta*, *13*(1).

Yusda PP, I. (2015). Analisis Terhadap Cyber Crime dalam Kaitannya dengan Asas Territorialitas. *Jurnal TEKNOIF*, *3*(1).

Criminal Justice Quote

"Today, criminal justice functions and justifies itself only by this perpetual reference to something other than itself, by this unceasing reinscription in non-juridical systems."

Michel Foucault, Discipline and Punish: The Birth of the Prison