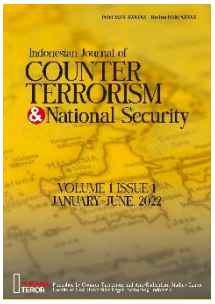
Indonesian Journal of Counter Terrorism and National Security
Volume 1 Issue 1 (January-June 2022), pp. 67-90
ISSN XXXX-XXXX (Print) XXXX-XXXX (Online)
https://doi.org/10.15294/ijctns.v1i1.56729
Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Counter Terrorism and Anti Radicalism Studies Center, Universitas Negeri Semarang, INDONESIA
Available online since January 31, 2022

Hoax and Provocative Contents by Muslim Cyber Army (MCA) and Its Enforcement in Indonesia

Nungki Wahyuni*
Indonesian Anti-Hoax Movement, Jakarta, Indonesia

Dinh Mai Nguyet
Ho Chin Minh city Open University, Vietnam



ABSTRACT: The existence of globalization with marked advances in technology and communication does not only have a positive impact on society. It is undeniable that the negative impact always lurks the people who take advantage of these advances. One of the negative impacts that arise is the existence of crimes that occur in cyberspace or cyber crime or commonly known as cybercrime. Recently, Indonesia was faced with one of these forms of cybercrime, namely an organization calling itself the Muslim Cyber Army. The motives of the actions and the impacts left by the existence of the Muslim Cyber Army can be identified and studied further by looking at the laws and regulations in Indonesia and their relationship with one of the fields of legal study, namely Law and Technology.

KEYWORDS: Muslim Cyber Army, Cyber Crime, Hoax, National Security, Law Enforcement

* *Corresponding author's email: nungkiwahyu@gmail.com*
Submitted: 09/11/2021 Reviewed: 22/11/2021 Revised: 27/12/2021 Accepted: 25/01/2022

How to cite:
Wahyuni, Nungkin, and Dinh Mai Nguyet. "Hoax and Provative Contents by Muslim Cyber Army (MCA) and Its Enforcement in Indonesia". *Indonesian Journal of Counter Terrorism and National Security* 1, No. 1 (January-June, 2022): 67-90.

I. INTRODUCTION

The development of globalization which has begun to enter the joints of people's lives has basically become a dilematic for community, in one side it provides a positive impact but in the other side the negative impact is also become a real challenge, especially today. On the one hand, the development of globalization has a positive impact on people who can take advantage of the development of globalization properly and maximally. However, on the other hand, the development of globalization also has a negative impact on society with the many facilities that have been provided by the development of these technologies.[1]

One area that is quite clearly influenced by the development of globalization, especially technology, is the field of information and communication technology or some call it the field of telematics. The term information technology or telematics refers to the development of convergence between telecommunications, media, and informatics technology which originally each developed separately.[2]

---

[1] Carl Dahlman, "Technology, globalization, and international competitiveness: Challenges for developing countries." *Industrial development for the 21st century: Sustainable development perspectives* (2007): 29-83; U. Salam, et al. "Indonesia case study: Rapid technological change–challenges and opportunities." *Pathways for Prosperity Commission Background Paper Series* (2018).

[2] Besse Sugiswati, "Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi di Era Informasi." *Perspektif* 16, No. 1 (2011): 59-72; Hendro Setyo

Advances in information technology that seem to make the world borderless from globalization while making it easier for everyone to communicate with anyone and from any corner of the world are also inseparable from negative impacts. One of the negative characteristics of the emergence of globalization which also has an effect on advances in technology and information is that it can lead to interdependence and blurring of national boundaries (borderless).[3] Another impact that also lurks users who take advantage of these technological advances is the emergence of crime in the cyber world or other names, namely the virtual world commonly known as cybercrime. Basically, cybercrime is one type of legal field whose settings are included in the criminal law group. Where the criminal law can be defined as a legal rule that binds to an act that fulfills certain conditions an effect in the form of a crime.[4] So, basically criminal law is based on two things, namely actions that meet certain conditions and the second is criminal.

Understanding Cybercrime according to Gregory is a form of virtual crime by utilizing computer media connected to the internet, and then exploiting other computers that are also connected to the internet. The existence of holes or security gaps in the operating system causes weaknesses and openings that can be used by perpetrators or commonly known in the cyber world, namely hackers, crackers and script kiddies to infiltrate the computer.[5]

Wahyudi, and Mita Puspita Sukmasari. "Teknologi dan Kehidupan Masyarakat." *Jurnal Analisa Sosiologi* 3, No. 1 (2018).

[3] J. A Scholte, *Globalization: A Critical Introduction*, (London: Palgrave, 2000), pp. 154-155.

[4] Sudarto Sudarto, *Hukum Pidana I*, (Semarang: Penerbit Yayasan Sudarto, 2019), pp. 13-14.

[5] Dista Amalia Arifah, "Kasus Cybercrime di Indonesia." *Jurnal Bisnis dan Ekonomi* 18, No. 2 (2011).

Indonesia as one of the countries in the world is inseparable from the number of cyber crimes or hereinafter referred to as cybercrime with the large number of internet users, especially social media in Indonesia. One of the hottest cases that recently occurred is the existence of a group in cyberspace, especially those engaged in the sphere of social media, calling themselves the Muslim Cyber Army which is said to have emerged from various sources when a discourse related to blasphemy was reported in various media in Indonesia. Indonesia, where one of them is when reporting on cases of blasphemy that occurred in the capital city by spreading news and news that the members themselves claim is the truth even though if you look at it from the point of view of the community in general it is just fake news or just hate speech that doesn't mean anything. and violates the general truth.

By looking at law enforcement in Indonesia regarding the high number of cases of cybercrime in the country, especially the case of the Muslim Cyber Army, a study of what and how is the correlation between law, especially the field of Law and Technology studies as well as laws and regulations that serve as guidelines for the authorities in resolving related cases. cybercrime will be discussed further in the results and discussion section of this paper.

II. METHODS

The method of writing this paper is a literature study. Literature studies are all efforts made by researchers and writers to collect information relevant to the topic or problem that will be or is being researched where the topic or problem raised in this paper is related to the cybercrime case by the Muslim Cyber Army group in legal and legal studies. laws and regulations. Literature study is a data

collection technique by conducting a review study of books, literatures, notes, and reports that have to do with the problem to be solved and discussed.

1. Source and Type of Data

   The data used in the preparation of this paper comes from various literatures related to the spread of hoaxes by the Muslim Cyber Army from a legal and technological perspective. Some of the main types of references used are law and technology books as well as books related to cybercrime or related, laws and regulations, national journals, and other sources that are still related to the theme. The types of data obtained are varied, namely qualitative and quantitative.
2. Data Collection

   The writing method is a literature study where information is obtained from various literatures and is compiled based on the results of the study of the information obtained. Paper writing is attempted to be interrelated with one another and in accordance with topics related to cybercrime cases committed by the Muslim Cyber Army in the perspective of law and technology as well as legislation.
3. Drawing Conclusion

   Conclusions are obtained after looking back at the problem formulation of the topics raised in the paper and discussion. The conclusions drawn reflect the subject matter of the paper.

III. THE RELATIONSHIP BETWEEN THE MUSLIM CYBER ARMY GROUP *&* THE CYBERCRIME: AN INDONESIAN EXPERIENCE

Cyberspace is a space where communities are connected to each other using a network, for example the internet to carry out various daily activities.[6] In its current development, the Internet has a negative impact if we look at the facts on the ground. One theory state, crime is a product of society it's self, which can be interpreted that society itself produces crime.[7] Crimes that occur as a negative impact of the development of internet applications are often referred to as cybercrime.[8]

In accordance with the global nature of the internet, the scope of this crime is also global or global. Cybercrime is often carried out transnationally, crossing national borders, causing difficulties in ascertaining the jurisdiction of state law that applies to perpetrators of cybercrime crimes. The characteristics of the internet where people can pass around without an identity (anonymous) which can allow for various malicious activities that are not touched by the law.[9]

Threats in cyberspace are dominated by non-state actors or actors or it can be said that these actors are not people who sit on government benches (non-state actors) such as individuals known as hackers, hacker groups, terrorism, the activities of hackers, organized criminal

---

[6] Kementerian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, (Jakarta: Kemhan RI, 2014), pp. 5-6.

[7] Eva Argarini Pratama, "Optimalisasi Cyberlaw untuk Penanganan Cybercrime Pada E-Commerce." *Bianglala Informatika* 1, No. 1 (2013).

[8] Abdul Wahid and Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, (Bandung: PT Refika Aditama, 2010), p. 45.

[9] Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional." *Jurnal Ilmu Hukum Jambi* 5, No. 2 (2014): 95-109.

groups, non-government organizations (NGOs), and the private sector (such as security companies, internet companies and carries) can also be feared to threaten national defense and sovereignty.[10] In essence, cybercrime includes all criminal acts related to information, and the information system itself, as well as communication systems which are a means for delivering or exchanging information with other parties.[11]

Crimes committed in cyberspace or hereinafter referred to as cybercrime are having various forms of criminal acts, which can be further described as follows.[12]

1. *Unathorized Access to Computer System and Service*, is a crime committed by entering or infiltrating a network system or someone's computer without permission.
2. *Illegal Contents* is a crime committed by entering data or information into the Internet system, such as social media or personal websites about something that is not true, lies, unethical, and is considered unlawful. For example, the act of containing false news or slander with the aim of destroying the dignity or self-esteem of the other party targeted by the perpetrator.
3. *Forgery of data,* data forgery is a crime committed by falsifying data on important documents stored in a scripless document that is carried out via the Internet. This crime is usually committed against e-commerce documents.

---

[10] Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense." *Jurnal Pertahanan & Bela Negara* 7, No. 2 (2017): 35-50.

[11] D. M. Arief and Elisatris Gutom, *Cyberlaw Aspek Hukum Teknologi Informasi*, (Bandung: PT. Refika Aditama, 2009), p. 67.

[12] Petrus Reinhard Golose, "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri." *Buletin Hukum Perbankan* 4, No. 2 (2006).

4. *Cyber Espionage*. This type is a crime committed by utilizing the Internet network to carry out spying on other parties which is usually carried out against business rivals and important data by entering the computer network system of the intended target party.
5. *Cyber Sabotage and Extortion*. Cyber sabotage and extortion are a crime committed by disrupting, or destroying data, computer programs or computer network systems connected to the Internet. For example, by spreading a computer virus when the victim is browsing or browsing the Internet.
6. *Offense against Intellectual Property*. This crime is a crime committed by way of being directed against intellectual property rights owned by other parties on the Internet. For example, impersonating the appearance of a web page on a site belonging to someone else illegally.
7. *Infringements of Privacy*. This crime is a crime that is usually committed by addressing a person's personal information stored in a computerized personal data form, which if known by others, can harm the victim materially or immaterially. For example, credit card numbers, hidden disease defects, ATM Pin numbers, and so on.

These various crimes have developed into many forms, not only in the form of fraud through cyberspace, but also various crimes such as incitement, provocation, fake news, and various hate speech content which not only triggers public reaction and increases crime rates, but also creates an attitude of fanaticism towards certain groups that result in various social, cultural, and even economic frictions (for example, boycotting products). Various provocations through cyber media are carried out to attack certain groups or cause unrest in the

community, one of which is the case of the Muslim Cyber Army (MCA) in Indonesia.

In a further context related to the Muslim Cyber Army (MC), from several news sources and articles with themes related to the Muslim Cyber Army, especially an article written and published in internet media, which carries the title "Scanning MCA Activities in Socio-Political Contest in Indonesia" by Damar Juniarto as Regional Coordinator of SAFEnet in the Southeast Asia Freedom of Expression Network explained that MCA which stands for Muslim Cyber Army, which sometimes also uses other names such as Cyber Muslim Army or Muslim Mega Cyber Army is a the identity used by a number of people on the internet network or the public is more familiar with the term netizen on Indonesian social media who performs a certain action in the name of protection of a religion that is predominantly embraced by the Indonesian people.

Many claims have been made by MCA members that at first the MCA did not intend to interfere in Indonesia's domestic political affairs and that was not the MCA's area of study. However, when a blasphemy case came to the public, MCA members who had the perception and a veneration that a leader should be a Muslim then started spreading questionable news regarding the case.[13]

Another source of writing on the internet revealed that the Muslim Cyber Army was originally a group that hated the government. It was

---

[13] Ahmad Zaki Mubarak, "Keterkaitan Radikalisme Agama dengan Fenomena Hoaks." *TRENMA: Jurnal Pesantren dan Madrasah* 1, No. 1 (2018); Wahyudi Akmaliah, "Bukan Sekedar Penggaung (Buzzers): Media Sosial dan Transformasi Arena Politik." *MAARIF* 13, No. 1 (2018): 9-25. *See also* Muzayyin Ahyar, "Aksi Bela Islam: islamic clicktivism and the new authority of religious propaganda in the millennial age in Indonesia." *Indonesian Journal of Islam and Muslim Societies* 9, No. 1 (2019): 1-29.

also explained that they had various reasons for being in opposition to the government. They are administrators and loyal members of various "Islamic" groups whose task is to produce information waste, hate speech to spread hate, terror, blasphemy, and criticism where they themselves make claims for their actions in the name of Allah, habib and ulama.[14]

According to those who claim to be MCA, Damar Juniarto's writings reveal that MCA is often written as an organization without a form, without a chairman, without a building and without a salary, and without capital. It was also revealed that some even imagine MCA as a shadowy group that acts like the Anonymous group which is an Activist group or "Hacktivists" which was formed in 2003 where in 2011 Time magazine listed Anonymous's name as one of the most influential people in the world.[15]

According to the same source written by Damar Juniarto, broadly speaking, there are a number of characteristics of MCA that can be directly recognized by the public, namely as follows:

1. Calls itself MCA, Muslim Cyber Army, Cyber Muslim Army, MMCA. As an identity, MCA is found in various forms used by someone who recognizes himself as an MCA, namely used as

---

[14] Dieqy Hasbi Widhana, "Mengklaim "Bela Ulama, Muslim Cyber Army Produksi Sampah Informasi", *TIRTO* <https://tirto.id/mengklaim-bela-ulama-muslim-cyber-army-produksi-sampah-informasi-cFxp>, 2018. *See also* Tafri Bahrur Risqi Sirojuddin, "Studi kritis Narasi kebencian Muslim Cyber Army di Media Massa", *Dissertation* (Surabaya: UIN Sunan Ampel Surabaya, 2018); Puput Lestari, "Analisa Wacana Kritis Fenomena MCA (Muslim Cyber Army) Pasca Aksi Bela Islam di Instagram." *FIKRAH* 6, No. 1 (2018): 25-48; Tessa Shasrini, and Yudi Daherman. "Aktivisme Cyber Army di Media Sosial." *Medium: Jurnal Ilmiah Fakultas Ilmu Komunikasi* 6, No. 2 (2018): 61-67.

[15] Damar Juniarto, "The Muslim Cyber Army: what is it and what does it want?." *Indonesia at Melbourne* 20 (2018).

an account name, as an avatar/profile picture, as a group or Facebook page name, embedded in biographical information, or stated publicly.

2. Choose to work in groups or collectives where this MCA group or collective moves in groups that can be identified from the identity it shows. The self-referral of a bee as is often conveyed by those who claim or know MCA actually refers to the mention of a passage which reads: "The parable of a believer is like a bee, he eats clean, releases something clean, perches on a clean place and does not damage or destroy anything break (which he seized)" (adapted from the words of Ahmad, Al-Hakim, and Al-Bazzar). Where basically bees always live in large colonies, never alone. They also work collectively, and each has its own task.
3. Continuously convey the same message on social media. This same message can be scanned from voicing hashtags (hashtags/hashmarks) or keywords simultaneously and consecutively many times within a certain time so that they can send and deliver messages quickly in the online realm. Examples of messages and hastag ini socia media that were distributed in March 2018 were #GaduhkarenaAhok, #RakyatBersamaFPI, #BubarkanGMBI, #CopotKapoldaJabar, #PenjarakanAhok.

The name of the Muslim Cyber Army group became the name of a group that is familiar to the ear and surfaced during the 2017 DKI Jakarta Regional Head Election where basically MCA is an active supporter on social media who so upholds Islamic leadership that MCA claims to be a group that fights for interests. Muslims and tried to thwart the victory of Basuki Tjahaja Purnama and Djarot Saiful Hidayat.

Some of the stages carried out by the accounts of MCA members against those who are indicated to have committed a criminal act that is considered close to blasphemy, especially those that become the grip of MCA members in acts of persecution, which include the following stages.

1. STAGE 1: Targeting
    a) Invitation to collect targets
    b) Target data collection
    c) Viral more widely
2. STAGE 2: Invitation to Hunt
    a) Invitation to do a hunt
    b) Hunt coordination
3. STAGE 3: Mobilization
    a) Forcing an apology
    b) Documentation
    c) Go viral on social media
4. STAGE 4: Criminalization
    a) Taken to the police station
    b) Requesting detention

Based on data analysis from an article entitled "*Memindai Aktivitas MCA Dalam Kontestasi Sosial-Politik di Indonesia*" by Damar Juniarto as Regional Coordinator of SAFEnet (Southeast Asia Freedom of Expression Network) it is revealed that it is actually MCA that is developing and disturbing social media in Indonesia and interfering in the affairs of Indonesia. Indonesia's domestic politics in the last two years from 2017 to 2018 now that the MCA is not the MCA that has existed and developed long ago. So, it can be concluded that the Muslim Cyber Army organization is not a single organization. Another fact states that the MCA, which first developed in the past,

was an organization that was reluctant to deal with domestic political policy matters. In contrast to the MCA organization which has re-emerged recently. In addition, from the confession of one MCA member based on Damar Juniarto's writings that the MCA organization that first existed in the past has now disappeared, it can be concluded that the current MCA organization is not the same organization as the old MCA organization.

If you look at the actions of MCA members who spread a concept, teaching, or argument where the truth of the whole cannot be accounted for and the truth still has to be questioned, it is something that is included in the category of cybercrime crime type of illegal contents. Where the meaning of illegal contents, as already in the previous discussion, is that the type of cybercrime crime category of illegal contents is a crime committed by entering data or information into the Internet system, such as social media or personal websites about something that is not true, lying, unethical, and considered unlawful. So that some of the activities carried out by MCA members by spreading false and untrue concepts or teachings, spreading slander can be categorized as cybercrime, including illegal contents.

IV. MUSLIM CYBER ARMY CASE IN THE LEGAL PERSPECTIVE

Indonesia as a legal state where all actions taken by the government and citizens must be guided by the applicable laws and regulations. Where according to Plato's view that good state administration is based on good (law) arrangements.[16]

[16] Tahir Azhary, *Negara Hukum*, (Jakarta: Bulan Bintang, 1992), p. 66.

With the developments in the aspect of globalization, it also has an impact on many areas of life that are affected, including in the field of information and communication technology where the Indonesian people are increasingly facilitated in accessing various information contained on various online platforms on the Internet as well as making it easier for all citizens to communicate with everyone. in any corner of the world. With the various positive impacts that have been obtained by globalization, Indonesia will also inevitably experience negative impacts from these advances, especially with the existence of various cybercrimes which are increasingly emerging, especially threats that come from organizations on behalf of themselves as the Muslim Cyber Army.

Along with the development of the use of the Internet, those who have the ability in the computer field and have certain intentions or intentions can take advantage of the presence of computers and the existence of the Internet to commit crimes or delinquency that can harm other parties.[17]

With the various threats of cybercrime that come, it cannot be denied that a legal state like Indonesia needs regulations that regulate cybercrime crimes that threaten the security of citizens in general as well as protect the unity and integrity of the Unitary State of the Republic of Indonesia which is trying to be destroyed by other parties, one of which is by utilizing the development of globalization by committing cybercrime crimes, such as the one carried out by the Muslim Cyber Army group which began to interfere in Indonesian domestic politics on the negative side.

---

[17] Nazarudin Tianotak, "Urgensi Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan." *Jurnal Sasi* 17, No. 4 (2011).

Indonesia as a state of law as previously explained, apparently also has legal instruments and laws and regulations that specifically discuss information and electronic transactions, including regulating crimes related to cybercrime as stipulated in Law Number 11 of 2008 concerning Information and Transactions Electronic.[18] On the basis of the regulation and formation of the law, it is stated in Article 5 paragraph (1) and Article 20 of the 1945 Constitution of the Republic of Indonesia.

If it is connected and associated with the act of spreading fake news by members of the Muslim Cyber Army with Law No. 11 of 2008 concerning Information and Electronic Transactions, the regulation regarding the spread of fake news or hoaxes is regulated in Article 28 paragraph (1) of the law which stated that "Everyone intentionally and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions" [*Setiap orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik*].

If it is seen in the elements of the article which states that the spread of false and misleading news is related to lies that result in 'consumer losses in Electronic Transactions', while in the case of the Muslim Cyber Army it is not at all related to Electronic Transactions or there are consumers who feel aggrieved. To overcome this, in Law no. 11 of 2008 concerning Information and Electronic Transactions is regulated more deeply and has a wider reach in relation to the spread of fake news in accordance with the category of actions carried out by members of the Muslim Cyber Army group, namely Article 28

---

[18] Yahfizham Yahfizham. "Moral, Etika dan Hukum (Implikasi Etis dari Teknologi Informasi dan Komunikasi)." *Iqra': Jurnal Perpustakaan dan Informasi* 6, No. 01 (2012): 09-18.

paragraph (2) which stated that "Every person intentionally and without rights distributes information that is intended to create feelings of hatred or hostility towards certain individuals and/or groups of people based on ethnicity, religion, race, and inter-groups" [*Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan*].

In addition, in relation to 'spreading false, fake news or what is commonly called a hoax, apart from being regulated in Article 28 paragraphs (1) and (2) of Law no. 11 of 2008 which can ensnare the perpetrators of members of the Muslim Cyber Army is also known in Article 311 paragraph (1) of the Criminal Code can also ensnare members of the Muslim Cyber Army who in addition to spreading false news also commit acts of slander and defamation, namely where on The article states that "Anyone who deliberately attacks the honor or reputation of a person, by accusing something with the intention of making it public, is threatened with libel, with a maximum imprisonment of nine months or a maximum fine of three hundred rupiahs" [*Barangsiapa sengaja menyerang kehormatan atau nama baik seorang, dengan menuduh sesuatu hal yang maksudnya tentang supaya hal itu diketahui umum, diancam karena pencemaran, dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah*].

In addition to being mentioned in the articles mentioned above, the act of spreading misleading news such as those carried out by members of the Muslim Cyber Army group can also be given a criminal threat by referring to Law Number 1 of 1946 concerning the Criminal Law Regulations Articles 14 and 15 which reads as follows.

Article 14

(1) "Whoever, by broadcasting false news or notification, intentionally causes trouble among the people, shall be punished by a maximum imprisonment of ten years" [*Barangsiapa, dengan menyiarkan berita atau pemberitahuan bohong, dengan sengaja menerbitkan keonaran di kalangan rakyat, dihukum dengan hukuman penjaran setinggi-tingginya sepuluh tahun*]

(2) "Whoever, by broadcasting a news or issuing a notification that can cause trouble among the people, while he should be able to think that the news or notification is a lie, is sentenced to a maximum imprisonment of three years" [*Barangsiapa, dengan menyiarkan suatu berita atau mengeluarkan pemberitahuan yang dapat menerbitkan keonaran di kalangan rakyat, sedangkan Ia patut dapat menyangka bahwa berita atau pemberitahuan itu adalah bohong, dihukum dengan penjara setinggi-tingginya tiga tahun*].

Article 15

"Anyone who broadcasts uncertain news or news that is excessive or incomplete, while he understands, at least should be able to suspect that such news will or has been able to cause trouble among the people, is punished with a maximum imprisonment of two years" [*Barangsiapa, menyiarkan kabar yang tidak pasti atau kabar yang berkelebihan atau yang tidak lengkap, sedangkan Ia mengerti setidak-tidaknya patut dapat menduga bahwa kabar demikian akan atau sudah dapat menerbitkan keonaran di kalangan rakyat, dihukum dengan hukuman penjara setinggi-tingginya dua tahun*].

With so many laws and regulations governing the act of spreading fake news or lying and misleading, it can be said that Indonesia has implemented the principle of being a state of law by having guidelines in the form of these laws and regulations. The next step

that needs to be done is to improve law enforcement in Indonesia related to cybercrime crimes committed by various parties including those committed by the Muslim Cyber Army group.

The birth of Law No. 11 of 2008 concerning Information and Electronic Transactions, we should be able to face it with a positive attitude, because the law can be used as a legal umbrella in the world of cybercrime or cybercrime, with the hope that the existence of this law can be a reference and a form of literature. in the form of laws in terms of cyberlaw enforcement in Indonesia. [19] In handling cybercrime cases, it is also expected that there will be maximum from various parties, especially the police to avoid cybercrime cases, one of which is the act of spreading false and misleading news by the Muslim Cyber Army organizational group that has occurred can just be apart from legal supervision. In addition, the public should also be introduced to more about Law No. 11 of 2008 concerning Information and Electronic Transactions so that later the public can know more about cyberlaw and help reduce cybercrime activities in Indonesia.[20]

With several articles that regulate the act of spreading false, false and misleading news, it is necessary for legal practitioners to consider in choosing and determining which articles of the law are suitable to be imposed on members of the Muslim Cyber Army who carry out their actions through Internet-based social media. In addition, the recognition of the principle in criminal law which reads lex specialis

---

[19] Andi Aco Agus, and Riskawati Riskawati. "Penanganan Kasus Cyber Crime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)." *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya* 11, No. 1 (2016).

[20] Yasmirah Mandasari Saragih, and Andysah Putera Utama Siahaan. "Cyber Crime Prevention Strategy in Indonesia." *SSRG International Journal of Humanities and Social Sciences* 3, No. 6 (2016): 22-26.

derogat legi generali provides a deeper understanding that laws which are more specific in nature and material content override provisions in laws that are general in nature. Where if you look at some of the laws that have been described previously, the law that is more suitable for perpetrators of spreading false and misleading news by members of the Muslim Cyber Army is Law Number 11 of 2008 concerning Information and Electronic Transactions, especially Article 28 paragraph (1) and (2).

The participation of various parties is very necessary to do. The existence of laws and regulations that regulate but are not accompanied by the implementation of law enforcement and legislation is tantamount to the non-functioning of the law in a country that recognizes itself as a state of law. The implementation of law enforcement also needs to be carried out so that there are no more criminal acts that occur in cyberspace (cybercrime) so that there are no more hidden threats that intend to destroy the security and unity of the Unitary State of the Republic of Indonesia which has been formed for many years with efforts that are not easy.

V. CONCLUSION

This study confirmed and concluded that the developments in the aspect of globalization also have an impact on many areas of life that are affected, including in the field of information and communication technology where the Indonesian people are increasingly facilitated in accessing various information contained on various online platforms on the Internet as well as making it easier for all citizens. society in communicating with all people in all corners of the world. With the various positive impacts that have been obtained by globalization, of course, Indonesia will also inevitably experience

negative impacts from these advances, especially with the existence of various cybercrime crimes, especially with the presence of a group that calls themselves the Muslim Cyber Army. With so many laws and regulations governing the act of spreading fake news or lying and misleading, it can be said that Indonesia has implemented the principle of being a state of law by having guidelines in the form of these laws and regulations. The next step that needs to be done is to improve law enforcement in Indonesia related to cybercrime crimes committed by various parties including those committed by the Muslim Cyber Army group. Therefore, it also highlighted that in handling cybercrime cases, it is also hoped that the maximum from various parties, especially the police, to avoid cybercrime cases, one of which is the act of spreading false and misleading news by Muslim Cyber Army organizations that have occurred can just be out of reach of law.

ACKNOWLEDGMENTS

None.

COMPETING INTERESTS

The Authors declared that they have no competing interests.

REFERENCES

Agus, Andi Aco, and Riskawati Riskawati. "Penanganan Kasus Cyber Crime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)." *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya* 11, No. 1 (2016).

Ahyar, Muzayyin. "Aksi Bela Islam: islamic clicktivism and the new authority of religious propaganda in the millennial age in Indonesia." *Indonesian Journal of Islam and Muslim Societies* 9, No. 1 (2019): 1-29.

Akmaliah, Wahyudi. "Bukan Sekedar Penggaung (Buzzers): Media Sosial dan Transformasi Arena Politik." *MAARIF* 13, No. 1 (2018): 9-25.

Arief, D. M., and Elisatris Gutom. *Cyberlaw Aspek Hukum Teknologi Informasi*. (Bandung: PT. Refika Aditama, 2009).

Arifah, Dista Amalia. "Kasus Cybercrime di Indonesia." *Jurnal Bisnis dan Ekonomi* 18, No. 2 (2011).

Azhary, Tahir. *Negara Hukum*. (Jakarta: Bulan Bintang, 1992).

Dahlman, Carl. "Technology, globalization, and international competitiveness: Challenges for developing countries." *Industrial development for the 21st century: Sustainable development perspectives* (2007): 29-83.

Golose, Petrus Reinhard. "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri." *Buletin Hukum Perbankan* 4, No. 2 (2006).

Juniarto, Damar. "The Muslim Cyber Army: what is it and what does it want?." *Indonesia at Melbourne* 20 (2018).

Kementerian Pertahanan Indonesia. *Pedoman Pertahanan Siber*, (Jakarta: Kemhan RI, 2014).

Lestari, Puput. "Analisa Wacana Kritis Fenomena MCA (Muslim Cyber Army) Pasca Aksi Bela Islam di Instagram." *FIKRAH* 6, No. 1 (2018): 25-48.

Mubarak, Ahmad Zaki. "Keterkaitan Radikalisme Agama dengan Fenomena Hoaks." *TRENMA: Jurnal Pesantren dan Madrasah* 1, No. 1 (2018).

Pratama, Eva Argarini. "Optimalisasi Cyberlaw untuk Penanganan Cybercrime Pada E-Commerce." *Bianglala Informatika* 1, No. 1 (2013).

Putra, Akbar Kurnia. "Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional." *Jurnal Ilmu Hukum Jambi* 5, No. 2 (2014): 95-109.

Rahmawati, Ineu. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense." *Jurnal Pertahanan & Bela Negara* 7, No. 2 (2017): 35-50.

Salam, U., et al. "Indonesia case study: Rapid technological change–challenges and opportunities." *Pathways for Prosperity Commission Background Paper Series* (2018).

Saragih, Yasmirah Mandasari, and Andysah Putera Utama Siahaan. "Cyber Crime Prevention Strategy in Indonesia." *SSRG International Journal of Humanities and Social Sciences* 3, No. 6 (2016): 22-26.

Scholte, J. A. *Globalization: A Critical Introduction*. (London: Palgrave, 2000).

Shasrini, Tessa, and Yudi Daherman. "Aktivisme Cyber Army di Media Sosial." *Medium: Jurnal Ilmiah Fakultas Ilmu Komunikasi* 6, No. 2 (2018): 61-67.

Sirojuddin, Tafri Bahrur Risqi, "Studi kritis Narasi kebencian Muslim Cyber Army di Media Massa", *Dissertation* (Surabaya: UIN Sunan Ampel Surabaya, 2018).

Sudarto, Sudarto. *Hukum Pidana I*. (Semarang: Penerbit Yayasan Sudarto, 2019).

Sugiswati, Besse. "Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi di Era Informasi." *Perspektif* 16, No. 1 (2011): 59-72.

Tianotak, Nazarudin. "Urgensi Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan." *Jurnal Sasi* 17, No. 4 (2011).

Wahid, Abdul, and Mohammad Labib. *Kejahatan Mayantara (Cybercrime)*. (Bandung: PT Refika Aditama, 2010).

Wahyudi, Hendro Setyo, and Mita Puspita Sukmasari. "Teknologi dan Kehidupan Masyarakat." *Jurnal Analisa Sosiologi* 3, No. 1 (2018).

Widhana, Dieqy Hasbi. "Mengklaim "Bela Ulama, Muslim Cyber Army Produksi Sampah Informasi", *TIRTO* <https://tirto.id/mengklaim-bela-ulama-muslim-cyber-army-produksi-sampah-informasi-cFxp>, 2018

Yahfizham, Yahfizham. "Moral, Etika dan Hukum (Implikasi Etis dari Teknologi Informasi dan Komunikasi)." *Iqra': Jurnal Perpustakaan dan Informasi* 6, No. 01 (2012): 09-18.

An idea is nothing but Information, it won't do us any harm until we accept it as perception of truth in our mind, which in time will potentially evolve and construct major events in history.

Djayawarman Alamprabu
Feared Intellectualism