

Indonesia in Efforts to Overcome Black Propaganda Cyber Terrorism as An Organized Cyber Crime

M. Reza Fahmil Hakim, S.H. (Corresponding author)
Faculty of Law, Brawijaya University, Jl. Veteran, Malang 65145
E-mail: hunterfox573@gmail.com

Milda Istiqomah, S.H., MTCP, Ph.D.
Faculty of Law, Brawijaya University, Jl. Veteran, Malang 65145
E-mail: milda.istiqomah@ub.ac.id

Dr. Faizin Sulistio, S.H., LL. M.
Faculty of Law, Brawijaya University, Jl. Veteran, Malang 65145
E-mail: faizin@ub.ac.id

Abstract

In this era 4.0, the influence of globalization is very strong, notably in the field of science, technology, information, and communication. Those are growing so rapidly. The world is moving in a new direction and demanding to follow its development is no exception with Indonesia. As a developing country, Indonesia must be able to afford to enrich its people and can bring its people to the new direction. This phenomenon of the development of science, technology, information and communication is also followed by the emergence of new threats to commit cybercrime. One of the big challenges today is Terrorisme which is done with technology or called Cyber Terrorism. Terrorist groups that use social media are spreading their terror propaganda. In analyzing author used a method normative juridical research, in which this method analyzes problems and cases by comparing the laws that are in society to the rules of norms that apply nationally and internationally. On this issue, the author concluded an Indonesian concept in an effort to solve the problem. This paper provides to against the mechanism of resolving the issue of black propaganda disseminated through social media by cyber terrorism actors in Indonesia. Also, the explanation and implementation of Indonesia concept to overcome cyber terrorism crimes, which is applied in preventing black propaganda by terrorist groups through social media.

Keywords: Cyber terrorism, Social media, Black propaganda

DOI: 10.7176/JLPG/119-07

Publication date: March 31st 2022

1. Introduction

The rapid development of technology and information in era 4.0 not only provides easy access for the community, but is also followed by the emergence of a number of new threats. Along with its benefits, cyber technology also has a negative impact and opportunity for irresponsible people to commit cyber crime.¹ The impact of information openness and widespread communication in a space of time or known as cyber space (cyber space) can have a negative impact and result in legal problems. The types of threats posed by the sophistication of cyber technology are cyber war, terrorism, pornography, illegal trade, and other threats.² The phenomenon of cyber crime over time is increasing, even the mode of crime is increasingly diverse.³ Crimes that were originally conventional and direct such as acidification, theft, defamation, pornography, gambling, fraud, even terrorism crimes can now be committed through social media. Cyber crime has a transnational nature because it is not limited in space and time so that it not only negatively affects individuals, but also has a major impact on organizations and countries and interests protected by law in more than one national jurisdiction. Until now, regional and international efforts to create comprehensive cybersecurity have been made, but unfortunately it seems slow. Similarly, Indonesia's efforts to adopt a comprehensive ASEAN cooperation framework to achieve cybersecurity cooperation. Until now, a comprehensive ASEAN cybersecurity framework has not been developed despite various official meetings by ASEAN. Indonesia itself, has ratified Law No. 5 of 2009 on the Ratification of the United Nations Convention Against Transnational Organized Crime. According to TNI Commander Marshal Hadi Tjahjanto there are five global constellations that have the potential to become a

¹ Ersya, M. P. 2018. Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Moral and Civic Education*, Vol. 1 No. 1, Page 50–62.

² Nursita, R. D. 2019. Cyberspace: Perdebatan, Problematika, Serta Pendekatan Baru Dalam Tata Kelola Global. *Dauliyah*, Vol. 4, No. 1, Page 80–99.

³ Gani, H. A., & Gani, A. W. 2019. Penyelesaian Kasus Kejahatan Internet (Cyber Crime) dalam Perspektif UU ITE No. 11 TAHUN 2008 dan UU No. 19 Tahun 2016. *Peran Penelitian dalam Menunjang Percepatan Pembangunan Berkelanjutan di Indonesia*, (11), 121–129. Makassar.

national defense and security threat so that the Indonesian state must be aware of it. These threats are the new world order, terrorism, cyber warfare, the United States and Indonesia are most often vulnerable to the Indonesian sea area.

According to Article 6 of Law No. 5 of 2018 on combating terrorism, the characteristics of acts of terrorism are acts that intentionally use violence or threats of violence that cause an atmosphere of terror or fear of people widely, cause mass casualties by depriving independence or loss of life and property of others, or causing damage or destruction to strategic vital objects, environmental or public facilities or international facilities. When compared to other crimes, terrorism is a unique crime and has elements that distinguish terrorism from other crimes, in terrorism there are extreme elements, which has a specific purpose, the use of technology both in the field of weaponry and other technologies such as communication technology and information and done with closed movements.¹

James A. Lewis defines cyber terrorism as the use of computer network devices to shut down national infrastructure, disrupt or intimidate a government or citizen. At the ratification of Indonesia ratifying the Convention for the Suppression of Terrorist Bombings, stated that all countries should be prepared in all respects for the prevention of acts of terrorism and cooperate in raising public awareness in combating terrorism including cyber terrorism.²

Cyber terrorism is seen as one of the most extraordinary crimes. Cyber terrorism is related to ideology and brainwashing about understanding the state by actively communicating using technology and becomes the main activity carried out by radical groups to carry out their actions. Terrorist groups make social media as one of the media to spread their terror propaganda. Based on the data obtained, about 97.4% of the total internet users in Indonesia are social media users so that it becomes a shot to spread radicalism propaganda.

According to Irawan Sukarno there are three forms of propaganda, namely: a) white propaganda, is propaganda that disseminates ideological information by mentioning the source; b) gray propaganda, is propaganda carried out by obscure groups aimed at confounding the minds of others, sheep fighting and gossip; c) Black propaganda, is propaganda that spreads false information to bring down the morals of opponents who are not ethical and tend to think unilaterally. Black propaganda is widely found in cyberspace with misleading content and justifies the negative messages and activities contained in it. The spread of black propaganda content is radical and certainly has a bad impact not only for citizens as individuals but also for the international community.

One example of black propaganda that has occurred in Indonesia claims by Australian media, the ABC which states that one of the mosques in Jakarta became the meeting place of ISIS sympathizers and there is footage of the meeting uploaded to YouTube which is considered as ISIS propaganda. Not only Indonesia, southeast Asian countries such as Malaysia and the Philippines are being targeted by the spread of propaganda by the Islamic State terrorist group through social media, by uploading videos on YouTube and claiming that ISIS is gathering Muslim soldiers from all over the world.³

The rise of cyber terrorism by spreading black propaganda not only harms a handful of parties but also the international community in various parts of the world. The government is expected to manage opinions on social media from the propaganda of terrorist groups that spread provocative issues. The magnitude of losses suffered by many countries including Indonesia due to black propaganda as one of the acts of cyber terror to update the law to issue new criminal acts. It is also to examine more deeply about the problems posed by black propaganda carried out by cyber-terrorism actors and express the efforts of the State of Indonesia in tackling cyber terrorism crimes, because it is a danger to target terrorist groups in carrying out their crimes and also as an effort to overcome organized cyber crime. So this article raises the question of the formulation of the problem, namely: 1) How is Indonesia's Efforts in Overcoming Black Propaganda of Cyber Terrorism? 2) How is the Implementation of Indonesian Law in Overcoming Cyber Terrorism?

1.1 Indonesia's Actions to Overcome Black Propaganda as Cyber Terror Acts

Alongside with the development of information technology, terrorist groups also began to take advantage of their sophistication through the internet because they were more effective in disseminating their propaganda to influence the ideology and behavior of the people they targeted for the process of recruiting new members and carrying out acts of terror. Propaganda that often causes unrest for the international community including Indonesia itself is caused by black propaganda disseminated through social media as part of cyber-terror acts.

Indonesia is a legal country that is regional in Southeast Asia. It has ratified the ICCTSB, the international convention of terrorism suppression of bombings, which aims to combat terrorism crimes to achieve peace between nations and regional stability, however, although this convention as a shield to the perpetrators of

¹ Wahid, A., Sunardi, M. I. S. (2011). *Kejahatan Terorisme Perspektif Agama, HAM, dan Hukum*. Bandung: Refika Aditama. Page. 40

² Putri, J. S. E. (2019). *Kejahatan Cyber Terorism dalam Hukum Pidana di Indonesia 1*. Surabaya. Page. 4-5.

³ Hidayat, A. (2015). *ASEAN dan Penanggulangan Terorisme: Beberapa Catatan*. Taken From ASEAN Studies Center UGM. Website: <https://asc.fisipol.ugm.ac.id/2015/08/27/648/> Diakses pada tanggal 23 Desember 2020.

terrorism organizations but still cannot include non-vital acts of terrorism such as cyber terrorism. Although Indonesia joins ASEAN which serves to combine the collective strength of countries that are members of ASEAN has not been able to build defense in the field of security, especially against cyber terrorism. In ASEAN there are several cooperations that include terrorism as one of the scopes of its work. For example ASEAN Convention on Counter Terrorism (ACCT), ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Regional Forum (ARF) dan ASEAN Defence Ministers Meeting (ADMM), and ASEAN-Russia Seniors Officials Meeting (ARSOM).

Indonesia through the AMMTC is actively making efforts to tackle terrorism but there has been no specific effort to tackle cyber terrorism itself. AMMTC only focuses on solving conventional terrorism cases so it seems to have a slow movement in overcoming this even more with the use of technology by terrorist groups. This is evidenced by the index score of terrorism in ASEAN countries that are unstable and do not show a significant decrease in terror acts.¹

Table 1. Terrorism Index Scores in Southeast Asian Countries 2

STATES	YEAR		
	2018	2019	2020
Filipina	7.29	7.27	7.098
Thailand	7.19	7.279	6.708
Indonesia	4.67	4.755	4.429
Myanmar	4.24	4.08	4.167
Malaysia	3.04	3.579	2.691
Laos	0.08	0.038	0.695
Kamboja	0.31	0.153	0.077
Vietnam	0	0	0
Singapura	0	0	0

Furthermore, the table above shows that AMMTC efforts are still less effective because of the very significant difference in index scores between one country and another. This proves that the AMMTC's goal has not been achieved, which is to build solutions to the handling of terrorism and regional security, especially in Indonesia. In terms of regulations the Indonesian government issued Law No. 5 of 2018 on changes to Law No. 15 of 2003 on Combating Terrorism And Law No. 2008 on Information, Technology and Electronics (ITE) of both Laws has not met the elements of cyber terrorism crimes. The terrorism law materially explains that what terrorism means is any person who scares or terrors the community and causes chaos or disobedience from the notion of terrorism in article 1 number 2 of Law number 5 of 2018 on Combating Criminal Acts:

“Terrorism is the act of using violence or threats of violence that creates an atmosphere of terror or widespread fear that can cause mass casualties and / or cause damage or destruction to vital strategic objects, environments, public facilities, or international facilities with ideological, political, or security motives.”

The essence of the article is terrorists are carrying out bombs or attacks that cause fear in the public against vital objects in the environment in the community, the criminal act of cyber terrorism is the same as terrorists who have described the article of the terrorism law but different objects of destruction are through the media carried out by perpetrators of cyber terrorism crimes through cyberspace or non-vital objects that can damage electronic devices or make trouble in the media. social. Furthermore, the ITE Law still does not regulate the criminal act of cyber terrorism, because in the article listed the ITE Law is still considered ambiguous or rubber is not in accordance with the norm in the making of the Law. From the summary, the need for law enforcement to make new laws in anticipation of cyber terrorism crimes given the principle of legality of criminal law which essentially cannot be punished if there is no rule of law, then Indonesia should be a criminal law.

Examples of cases of black propaganda that have existed in Indonesia are the dharmais hospital attack that was operating suddenly the electricity was extinguished and the perpetrator asked for a ransom, the case information was found the virus "I Love You" and "Love Bug" which spread quickly, known to originate from the Philippines. These viruses cause enormous damage to computer devices and electrical components at the hospital. Based on the data, the "I Love You" virus can penetrate 10 computers in the hospital network and cause

¹ Sekretariat Nasional ASEAN-Indonesia. (n.d.). ASEAN Ministerial Meeting on Transnational Crime (AMMTC). Diambil dari <http://setnas-asean.id/asean-ministerial-meeting-ontransnational-crime-ammtc>. Diakses pada tanggal 25 Desember 2020

² Yovantra, M. F., Afifuddin, M., & Saragih, H. J. R. 2018. Indonesia dan Kerja Sama Keamanan ASEAN Untuk Mengatasi Terorisme Melalui AMMTC. Manajemen Pertahanan, Vol. 4, No. 1, Page 46–60.

huge financial losses on the computer network and even create terror throughout the hospital and eliminate or eliminate the e-mail system at the dharmais hospital. This virus was found in other countries that can cause ATMs in Belgium to malfunction for some time. Examples of cases of black propaganda that have existed in Indonesia are the dharmais hospital attack that was operating suddenly the electricity was extinguished and the perpetrator asked for a ransom, the case information was found the virus "I Love You" and "Love Bug" which spread quickly, known to originate from the Philippines. These viruses cause enormous damage to computer devices and electrical components at the hospital. Based on the data, the "I Love You" virus can penetrate 10 computers in the hospital network and cause huge financial losses on the computer network and even create terror throughout the hospital and eliminate or eliminate the e-mail system at the dharmais hospital. This virus was found in other countries that can cause ATMs in Belgium to malfunction for some time.

In connection with the explanation of the case above, it can be known that the CT crime is a cross-border crime based on technology, which can unsettle society on a much broader (global) level. Given also that Indonesia in cyber crime is ranked first in cybercrime (using the internet) has replaced Ukraine which was previously ranked first. Seeing this fact, it is necessary to conduct a serious review of ct criminal countermeasures policy which is part of the type of cyber crime itself.

In an effort to tackle cyber terrorism crimes juridically Indonesia has not made the regulation, this article will hope that Law No. 5 of 2018 on Combating Terrorism Crimes, Cyber terrorism regulations can be formulated also in Law No. 19 of 2016 on Changes to Law No. 11 of 2008 on Information and Electronic Transactions given that this crime focuses in the realm of electroconics. If this problem is formulated into this Law, then its function as supporting Law No. 5 of 2018 on combating terrorism crimes that will later appear synchronization between these two articles with the legal methods that are sought to eradicate and overcome cyber terrorism crimes which is one type of cyber crime.

1.2 Implementation of Cyber Terrorism as an Effort to Overcome Black Propaganda as an Act of Cyber Terrorism in Indonesia

Terrorism is considered an extraordinary crime because it threatens human rights so it requires extraordinary handling efforts as well. Cyber terrorism which became a new form of terrorism crime makes social media to disseminate ideology in the form of propaganda to recruit new members and publicize their actions as a form of threat aimed at disturbing the community. The series of actions carried out by terrorist groups on social media is a form of black propaganda.

At the institutional level, the AMMTC already has various programs to tackle terrorism, but on a practical level has not been fully implemented properly evidenced by the data in table 1.1. In fact, if each of these programs is implemented as appropriate, then the goals that AMMTC wants to achieve can be realized so as to create a conducive situation in the southeast Asian region. This is because there are too many programs that are not implemented by the AMMTC so that the series of actions carried out does not run effectively.

In Indonesia itself, cyber terrorism is one of the objects in the scope of work in several agencies such as the National Agency for Counter Terrorism (BNPT) and the State Cyber and Password Agency (BSSN) which is shaded by the Coordinating Ministry for Political, Legal and Legal Affairs, the Ministry of Defense, the Ministry of Law and Human Rights, the Ministry of Communication and Informatics, the Indonesian Police and the State Intelligence Agency. Lack of coordination and human resources, especially the database field in these agencies, led to ineffective counter-terrorism in the country.

Ictsb convection is a concept of cooperation between countries that concentrates on tackling black propaganda and terrorism attacks as part of cyber terror. The implementation of such convection can be described under the following schemes:

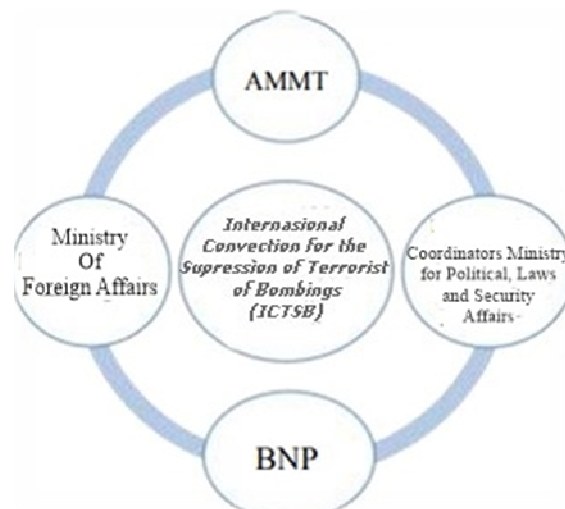


Figure 1: ICTSB Convection Against Terrorism Scheme

Based on the above scheme can be explained as follows: (1) The concept of international convection cooperation for the Supression of Terrorist of Bombings is organized through the ASEAN Ministreal Meeting on Transnational Crime (AMMTC), (2) the Ministry of Foreign Affairs and the Coordinating Ministry for Political, Legal and Security Affairs in coordination to cooperate with the AMMTC in implementing AACT in Indonesia through the National Agency for Counter Terrorism (BNPT).

The mechanisms for implementing the International Convection for the Supression of Terrorist of Bombings are as follows:

1. Cooperation between ASEAN member states indirectly strengthens relations and mutual respect for the ASEAN community which can further reduce the risk of conflict in the Southeast Asian region. Intensive communication is also expected to open new opportunities for the development of science, especially in the field of technology for ASEAN member countries. Communication conducted by ASEAN countries to establish cooperation relations focused on data, national borders, state structures, economy, technology, education, law and so on is called international communication.

The application of international communication has a great influence to unite perceptions in deciding a policy, equal purpose, vision and mission related to the protection of citizens for the development of terrorist groups' crimes in disseminating provocations through social media. In the international communication process, communicators and negotiators are needed who play an important role to carry out communication as well as possible in order to get cooperation support with other countries. Communicators and negotiators must be good at using body and verbal language and have good strategic skills so that the parties involved in cooperation are not easily emotional when listening to the other person without causing debate. In addition, the appearance of communicators and negotiators must be interesting and charismatic so as to evoke an aura of leadership and not be easily dropped by the parties concerned.

2. In addition to cooperation between ASEAN member countries, cooperation between countries and the private sector such as SafeNet Inc., Google and Facebook companies is also needed to improve the technology infrastructure of ASEAN member countries. SafeNet Inc. A company that manufactures technology security products, it offers data protection solutions such as public and information security infrastructure. Meanwhile, Google and Facebook companies focused on providing communication and information services with forms of social media platforms began to be widely used proven based on information from We are Social, as of July 2019 has calculated about 113.3 million people around the world have used social media.¹

While in Indonesia social media users reached 65 million people.² The large number of people accessing social media leads to the need for cooperation between the state and technology and media product providers to filter out negative content that can affect a nation's ideology through black propaganda on social media. The form of cooperation that can be done between the state and the company is collaborating to disseminate positive information to the public as social media users and

¹ Kemp, S. (2019). Global Social Media Users Pass 3.5 Billion. Taken From <https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion>. Diakses pada tanggal 27 Desember 2020.

² Kominfo: Pengguna Internet di Indonesia 63 Juta Orang. (n.d.). Taken From https://www.kominfo.go.id/content/detail/3415/kominfo-pengguna-internet-di-indonesia-63-jutaorang/0/berita_satker. Diakses pada tanggal 27 Desember 2020.

be responsible for the operation of social media in accordance with Article 16 paragraph (1) of the ITE Law which reads as follows:¹

- a. May display electronic information and/or electronic documents in full in accordance with the retention period stipulated by the Laws and Regulations;
 - b. Can protect the availability, integrity, authenticity, confidentiality, and torture of such electronic information;
 - c. Can operate in accordance with procedures or instructions in organizing such electronic systems;
 - d. Equipped with procedures or instructions announced in the language of information, or symbols that can be understood by the parties concerned with the implementation of the electronic system, and
 - e. Have a continuous mechanism for the newness of clarity and responsible procedures or instructions.
3. Human resource development in Indonesia is needed to support the implementation of ICTSB convection. This mechanism can be implemented by expert exchange programs or exchange experts to absorb science in the field of technology, especially cyber terrorism and exchange experience in overcoming black propaganda spread by terrorist groups on social media. The expert exchange program is carried out by the exchange of experts from both practitioners and academics in the field of technology and law between southeast Asian countries that are members of ASEAN whose implementation is regulated by the AMMTC in accordance with the approval of the countries concerned. This program is carried out to improve quality by conducting comparative studies to information and communication technology institutions or companies abroad. Through these activities, expert exchange participants have the opportunity to see, compare and assess the quality of information technology from other countries. Furthermore, expert exchange participants can learn things that are the advantages of the institution or company they visit. The expert exchange program is expected to deepen the knowledge of experts in the field of technology and law, improve technology management skills in their respective countries and enrich the experience of experts who will certainly develop the human resources of Southeast Asian countries.

The expert exchange mechanism that will be implemented is to review and evaluate a rule of law related to part of an internal state regulatory structure that is the result of observations from other legal states so as to find new legal norms both long-term and short-term in the future. The last thing, made external from research that has been carried out in the form of reports in the form of verbal minutes or statistics for development in a structured manner and understood as a reference in the formation of regulations that are progressive.

To support the implementation of legal norms, the need for a report on detailed technical references and is realistically implemented and useful for the development of technology and information in the future that supports new and creative innovations to work optimally in the era of globalization 4.0 in producing products or services to protect citizens from the negative impacts disseminated by cyber terrorism groups on social media.

1.3 Conclusion

Based on the description of the discussion of the above problem formulation, this article draws the following conclusions below:

1. Efforts made by the State of Indonesia in overcoming black propaganda and cyber terrorism crimes seem less effective due to factors: there is no law governing cyber terrorism and still use conventional means in overcoming cyber terror in this case black propaganda disseminated through social media. The need to make new legal regulatory efforts to overcome these criminal acts.
2. The concept of cooperation in the implementation of ICTSB and AMMTC convection in southeast Asian countries which is a special effort in addressing the issues of the spread of black propaganda as part of cyber terrorism on social media but the concept is less effective also because too many institutions are involved so that the process of resolving cases of cyber terrorism as transnational crime is less effective due to the unstructured subordination between relevant institutions and lack of human resources.

References

- Astuti, S. A. (2015). Law Enforcement of Cyber Terrorism in Indonesia. *Rechtsidee*, 2(2)
- Ersya, M. P. (2018). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Moral and Civic Education*, 1(1).

¹ Pasal 16 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

- Fredayani, E. (2019). Alasan Pembentukan Kerja Sama Keamanan ASEAN Australia dalam Menghadapi Isu Terorisme. *Insignia Journal of International Relations*, 6(2).
- Hidayat, A. (2015). ASEAN dan Penanggulangan Terorisme: Beberapa Catatan. ASEAN Studies Center UGM. [Online] Available: <https://asc.fisipol.ugm.ac.id/2015/01/10021>.
- Ilham, M. (2019). Kepanjangan ASEAN – Pengertian, Sejarah, Anggota, Tujuan dan Prinsip. [Online] Available: https://materibelajar.co.id/kepanjanganasean/#Kepanjangan_ASEAN.
- Jati, M. I. (2019). Manajemen Media sebagai Intervensi dalam Menanggulangi Isu Provokatif di Medsos. *Jurnal Ilmu Kepolisian*, 13(2).
- Kemp, S. (2019). Global Social Media Users Pass 3.5 Billion. [Online] Available: <https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion>.
- Kominfo: Pengguna Internet di Indonesia 63 Juta Orang. (n.d.). [Online] Available: https://www.kominfo.go.id/content/detail/3415/kominfo-penggunainternet-di-indonesia-63-juta-orang/0/berita_satker
- Peter Mahmud Marzuki. 2010. *Penelitian Hukum*. Jakarta: Prenada Media Group
- Putra, B. K. B. (2018). Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) di Indonesia Pamulang Law Review *Journal of Law*, 1(1).
- Putri, A. (2017). Sosial Media sebagai Sarana Propaganda Terorisme?. [Online] Available: <https://www.kompasiana.com/anndyadp95/sosial-mediasebagai-sarana-propaganda-terorisme?>
- Raharjo, A. (2018). Propaganda dan Pelaksanaan Pilpres 2019. [Online] Available: <https://www.kompasiana.com/aryoraharjo/propaganda-dan-pelaksanaanpilpres-2019#>
- Sari, A. P. (2016). Media Australia Sebut Masjid di Jakarta Sebar Propaganda ISIS. [Online] Available: <https://www.cnnindonesia.com/internasional/mediaaustralia-sebut-masjid-di-jakarta-sebar-propaganda-isis>
- Sekretariat Nasional ASEAN-Indonesia. (n.d.). ASEAN Ministerial Meeting on Transnational Crime (AMMTC). [Online] Available: <http://setnasasean.id/asean-ministerial-meeting-on-transnational-crime-ammtc>
- Wahid, A., *et al.* 2011. *Kejahatan Terorisme Perspektif Agama, HAM, dan Hukum*. Bandung: Refika Aditama.