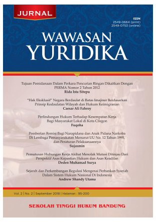
JURNAL
WAWASAN
YURIDIKA
Vol. 6 | No. 2 | September 2022 | Pages : 186-196
ACCREDITED by Ministry of Research, Technology, and Higher Education of the Republic of Indonesia,
No. 36/E/KPT/2019
http://ejournal.sthb.ac.id/index.php/jwy



# Cyber Terrorism Countermeasures in Indonesia

**Saptaning Ruju Paminto**
Fakultas Hukum, Universitas Suryakancana, Cianjur, Indonesia
✉ Corresponding author: saptaning@unsur.ac.id

*Article history:*
**DOI: 10.25072/jwy.v6i2.464**

Received: 5 April 2022 | Accepted: 25 September 2022 | Published: 30 September 2022

***Keywords:***
*Crime; Cyber; Information Technology; Terrorism.*

## Abstract

*The crime of terrorism is classified as an extraordinary crime, along with various other forms of radicalism. Recent acts of terrorism are suspected to be the result of massive activism from cyberspace. The purpose of this study is to examine efforts to counter cyber terrorism. This research is descriptive with normative juridical research type, using literature studies through a theoretical approach, and then the data is analyzed qualitatively. The results of this study were coordinating actions by making agreements with other countries related to cyber terrorism crimes (including information exchange and creating data centres on Indonesia's servers to prevent cyber-terrorist operations), with efforts to prevent and eradicate cyber terrorism activities need a lot of cooperation, both with domestic and international stakeholders.*

## A. INTRODUCTION

Cyber warfare in recent years has increased at an exponential rate, generally carried out by hacktivists, government and non-government institutions, non-state actors, and terrorists. In the world of technology, the level of dependence on technology and computers is very high. The rapid development of technology and information in the 4.0 era not only provides convenient access for the community but is also followed by the emergence of some new threats. Along with its benefits, cyber technology also provides negative impacts and opportunities for irresponsible people to commit cybercrime.[1]

Cybercrime has a transnational characteristic because it is not limited by time and space, so it does not only harm individuals but also has a major impact on organizations and countries, as well as interests that are protected by law in more than one national jurisdiction.[2]

[1] Nur Qalbi. S, Fitrah Marinda, and Rina Yulianti, "Asean Against Cyber Terorrism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir," *Legislatif* 4, No. 1 (2020): 106-123, p. 107.

[2] *Ibid.*

Nowadays, globalization brings many changes, both positive and negative. Globalization brings advances in information and transportation technology and changes in political, social, and economic systems around the world. However, there are not only positive impacts caused by globalization but also negative impacts, such as encouraging the development of transnational crimes, one of which is terrorism.[3]

Terrorism, in all its manifestations, is a serious crime that threatens human values, disrupts public safety for people and goods, and is often aimed at state or military/security institutions, as well as at the personification of those who run state institutions, such as the head of state, the government in general, vital and strategic objects, and other public crowd centres.[4]

Today, terrorist organizations have mastered cyberspace and turned it into a battlefield. They no longer rely on military power such as guns, armour, and bombs alone. Instead, they have become increasingly intelligent, and their strategies and tactics are technology-oriented. Moreover, their activities are no longer limited to propaganda, fundraising, training, planning and executing physical attacks. They are expanding their field of action to attack their victims by sabotaging online infrastructure from anywhere in the world by concealing their true identity using technology. Many experts refer to these actions as "cyber-terrorism".

Based on the investigation received, it is about the occurrence of cybercrime, a virtual world where there used to be no crime, but now there is. There is a transformation of traditional crime into cybercrime. The existing provisions of Indonesia's Information and Electronic Transactions Law do not explicitly explain how these acts of cyber terrorism are carried out, for example before cyberspace existed to do things like propaganda, recruitment, and training took a very long time, but after the existence of tools that are integrated with internet connections which are now very easy to use in seconds, this can be done regardless of time and place. Examples of other crimes that did not exist before include cyber hoaxes, cyberbullying, cyber jihad, and so on. With the existence of sophisticated and recent crimes, there is a need for change and modernization to overcome cyber terrorism and the need to secure data in Indonesia, which until now still uses external servers for

[3] Linda Ayu Wardani, "Analisis Implementasi Kerja Sama Filipina Dan Amerika Serikat Dalam Penanggulangan Aksi Terorisme Di Filipina," *Journal of International Relations* 4, No. 4 (2018): 675-683, p. 675.

[4] Muhammad Ali Zaidan, "Pemberantasan Tindak Pidana Terorisme: Pendekatan Kebijakan Kriminal," *Seminar Nasional Hukum Universitas Negeri Semarang* 3, No. 1 (2017): 149-180, p. 150.

data centres. The ease of data centre construction by the government to move all data to servers located in Indonesia has begun gradually in 2021. The existence of data centres in Indonesia is to minimize the opportunity for cyber terrorism to develop, both in recruitment, training, and propaganda carried out online.

As previous research conducted by Sri Ayu Astuti in her article "Law Enforcement of Cyber Terrorism in Indonesia", explains that the recent acts of terrorism are suspected to be the result of massive activism from cyberspace. Crimes related to ideology and brainwashing about the understanding of the state and its recruitment by conducting active communication using technological tools are the main activities driven by the interests of radical groups to carry out their actions. A clear example that can be seen today is the radical organization better known as ISIS (Islamic State of Iraq and Sham/ Syria) using social media networks to recruit new members and continue to strongly publicize the existence of the group as a new state power that will lead the caliphate on earth and in various ways carry out acts of terror through cyberspace.[5]

In addition, there is also research conducted by Gracesy Prisela Christy in her journal about "Countering Cyber-Terrorism Through Radical Website in the Perspective of Pancasila Democracy'', as cyber terrorism is declared as an extraordinary crime and has an impact on the stability of state security caused by terrorist crimes that have begun to spread into cyberspace.[6] Based on the results of the analysis of previous research, the author supports the ideas and adds suggestions that the government seeks to strengthen regulations to overcome the handling of cyber-terrorism crimes by improving the management of information and electronic transactions along with the infrastructure and regulation.

Since the beginning of the terror movement in Indonesia, the existence of terrorism in Indonesia has been associated with the Jemaah Islamiyah (JI) group, a radical Islamic group that is considered a serious threat to security in Southeast Asia.[7] National Police Chief General Listyo Sigit Prabowo said his agency had arrested 217 suspected terrorists in five months. Namely, from January to May 2021, "209 are in the process of investigation and 8 suspects

[5] Sri Ayu Astuti, "Law Enforcement of Cyber Terrorism in Indonesia," *Rechtsidee* 2, No. 2 (2015): 157-178, p. 160.

[6] Gracesy Prisela Christy, "Penanggulangan Cyber-Terrorism Melalui Website Radikal Dalam Perspektif Demokrasi Pancasila," *Paulus Law Journal* 1, No. 2 (2020): 59-71, p. 70.

[7] Debora Sanur L, "Dalam Melindungi Keamanan Nasional (War on Terror in Indonesia to Protect National Security)," *Politica* 7, No. 1 (2016): 25-47, p. 26.

have been dealt with firmly," Sigit said at a Working Meeting with the House of Representatives Law Commission, Wednesday, June 16, 2021. Sigit continued, the most National Police Chief General Listyo Sigit Prabowo said his agency had arrested 217 suspected terrorists in five months. Namely, from January to May 2021, "209 are in the process of investigation and 8 suspects have been dealt with firmly," Sigit said at a Working Meeting with the House of Representatives Law Commission, Wednesday, June 16, 2021. Sigit continued, the most arrests of suspected terrorists came from the bomb case that exploded in front of the Most Sacred Heart of Jesus Church, also known as the Cathedral Church in Makassar, South Sulawesi, on March 29. The suicide bombers were a husband and wife team, Muhammad Lukman Alfarizi (25 years old) and Yogi Safitri Fortuna aka Dewi Juwariya (22 years old). Both are affiliated with the Jamaah Ansharut Daulah (JAD) network, which pledges allegiance to the Islamic State of Iraq and Syria (ISIS) group.[8]

The Information and Electronic Transactions Law is expected to overcome various cyber crimes and is strengthened by the provisions of Law Number 15 Year 2003 on the Eradication of Criminal Acts of Terrorism. The purpose of this study is to examine efforts to overcome cyber terrorism in Indonesia.

## B. RESEARCH METHODS

This research is descriptive with normative juridical research type, using literature studies through a theoretical approach, and then the data is analyzed qualitatively. This research is descriptive with normative juridical research type. The data used is secondary data which includes primary legal materials, secondary legal materials, and tertiary legal materials. Data is collected through the literature study collection technique by collecting data from several previous cases (events), reviewing the results of the previous studies, and explaining issues related to countering cyber terrorism. The approach used in this research is the theoretical approach, and then the data collected is analyzed qualitatively.

## C. RESULTS AND DISCUSSIONS

One of the backgrounds taken is the existence of cyberspace, which used to be crimes committed conventionally or manually, with the existence of cyberspace, it is completely changed into crimes that use information

[8] Hussein Abri dan Syailendra Persada, "Kapolri Listyo Sigit: 217 Teroris Ditangkap Dalam Lima Bulan," Nasional Tempo, last modified 2021, https://nasional.tempo.co/read/1473369/kapolri-listyo-sigit-217-teroris-ditangkap-dalam-lima-bulan, accessed 5 October 2021.

technology facilities combined with internet connections, crimes that know no boundaries, places, and can be done in seconds to carry out their actions. Cyber terrorism crimes committed at this time have been very difficult to track stepping on the IV Industrial Revolution in this developing country, while in the future, it is necessary to improve the law to be able to ensnare cyber terrorists who use technological tools and facilities in carrying out their actions. According to "The Cyber Index" released by United Nations Institute for Disarmament Research (UNIDIR), cyberattacks can be defined as unauthorized attempts to infiltrate, gain access to, or disable computers, systems, or networks (Cyberattacks are often broadly as unauthorized penetration of computers or digital networks).[9] Therefore, cybersecurity can be defined as "the collection of tools, policies, security concepts, security protections, guidelines, risk management approaches, measures, training, best practices, assurances, and technologies that can be used to protect cyber environments and organizations and user assets.[10] Cyber warfare is warfare conducted in cyberspace through cyber facilities and methods.[11] The United Nations (UN) does not yet have an official definition of cyber terrorism or terrorism itself, but broadly speaking, cyber terrorism can be understood as unauthorized attacks or threats of attacks against computers and cyber networks to terrorize people, groups, or governments.[12]

International law does not certainly mention the meaning or definition of the word cyber terrorism, but it explicitly mentions and prohibits "terrorist measures" and "terrorism acts" regulated in the provisions of Article 33 of the Geneva Convention and Article 43 clause (2) and (3) of Additional Protocol I 1997.[13] Article 33 of the fourth 1949 Geneva Convention related to the Protection of Civilian Population in Time of War states that "Collective punishment and all measures of intimidation or terrorism are prohibited", while Article 4 of Additional Protocol II to the 1949 Geneva Convention concerning the Protection of Victims of Non-International Armed

[9] James Andrew Lewis and Götz Neuneck, *The Cyber Index International Security Trends and Realities* (Switzerland: United Nations Institute for Disarmament Research, 2013), p. 10.

[10] Sri Cahaya Khoironi, "Analysis Cyber Security Culture Training Needs as an Effort to Develop Country Civil Aparatures Competency in Digital Era," *Jurnal Studi Komunikasi Dan Media* 24, No. 1 (2020): 37-56, p. 42.

[11] Cameron H. Bell, "Cyber Warfare and International Law: The Need for Clarity," *Towson University Journal of International Affairs* L1, No. 2 (2018): 21-22, p. 22.

[12] M Dogrul, A Aslan, and E Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *3rd International Conference on Cyber Conflict*, 2011, 29-43, p. 36.

[13] International Humanitarian Law and Terrorism: Questions and Answers, ICRC, 2011, https://www.icrc.org/en/doc/resources/documents/faq/terrorism-faq-050504.htm, accessed 29 September 2021.

Conflicts, prohibits "terrorism acts" against people who are not or no longer part of the fighting.

The two Additional Protocols to the Geneva Conventions also prohibit actions aimed at spreading terror among civilian populations,[14] as stipulated in Article 51 of Additional Protocol I to the 1949 Geneva Conventions on the Protection of Victims of International Armed Conflicts 1977 and Article 13 clause (2) of Additional Protocol II to the 1949 Geneva Conventions on the Protection of Victims of Non-International Armed Conflicts 1977, states that "Civilian populations, as well as individual civilians, shall not be the object of attacks. Acts or threats of violence whose primary purpose is to spread terror among the civilian population are prohibited".

The categories that distinguish cyber terrorism from terrorism in general are:

1. Conducted through cyberspace by individuals, groups, or organizations that are directly influenced by some terrorist movement and/or its leaders;
2. Motivated by a desire for political or ideological change;
3. This leads to violence that achieves physical and psychological impacts beyond direct victims or targets.

Although the different patterns caused by terrorism, in general, are more physical in terms of the consequences of the attack, cyber terrorism is more non-physical, but still, civilians are the victims of terrorism activities.[15]

The approach to effectively combat cyber terrorism is divided into 2 (two) following main forms:

1. Hybrid Cyber Terrorism
   Hybrid cyber terrorism is the use of the internet for terrorist activities such as propaganda, recruitment, radicalization, fundraising, data mining, communication, training, and planning of actual terrorist attacks.[16]
2. Pure Cyber Terrorism
   Pure cyber terrorism refers to direct attacks against a victim's cyberinfrastructure (such as computers, networks, and the information stored on them) to achieve political, religious, and ideological goals. Destructive and disruptive cyber terrorism can be further distinguished:
   a. Destructive cyber terrorism is the manipulation and corruption of information system functions to damage or destroy virtual and physical assets. The most popular weapons are the use of computer viruses and worms; trojans and ransomware.
   b. Disruptive cyber terrorism is described as hacking designed to

[14] *Ibid.*

[15] Mayssa Zerzri, "The Threat of Cyber-terrorism and Recommend Actions for Countermeasures," C·A·Perspectives on Tunisia 4 (2017): 2-6, p. 2.

[16] *Ibid.*

take down websites and disrupt normal lifestyles, which depend on the critical infrastructure supporting medical utilities, transportation and financial systems.[17]

The United Nations has been setting the agenda on counter-terrorism for decades, but the attacks on the United States on September eleventh two thousand and one (September 11, 2001) prompted the UN Security Council to adopt Resolution 1373, establishing for the first time the United Nations Counter-Terorrism Committee, hereafter referred to as the CTC.[18]

Five years later, all member states of the UN General Assembly agreed for the first time on a strategic framework for countering terrorism, which came to be called the Counter-Terrorism Strategy. Within this strategy, there are four pillars of a global strategy to counter terrorism as follows:

1. Addressing conditions conducive to the spread of terrorism;
2. Preventing and combating terrorism;
3. Developing the capacity of member states to prevent and strengthen the role of the UN system on terrorism;
4. Ensure respect for human rights for all and the role of law as the fundamental basis for countering terrorism.[19]

These four global strategies become instruments to enhance the international community's effort against terrorism. Looking at the four pillars of the global strategy that have been put forward in The UN Global Counter-Terrorism Strategy, the task of the CTC is to provide capacity development assistance to member states and implement counter terrorism projects around the world in line with the four pillars of the global strategy.

Terrorism is a phenomenon, both practically and legally, war cannot be waged against a phenomenon, but only against identified parties to an armed conflict. For this reason, it is more appropriate to speak of a "War Against Terrorism" rather than a "War on Terrorism".[20]

Over the years, the UN and the governments of each country have passed many conventions and laws that adapt to cyber-terrorism attacks. The Budapest Convention about Cybercrime (2001) was passed by the Europe Council to standardize national laws and regulatory measures regarding cybercrime and related issues, including criminal prosecution and

[17] *Ibid*.

[18] Reni Windiani, "Peran Indonesia Dalam Memerangi Terorisme," *Jurnal Ilmu Sosial* 16, No. 2 (2018): 135-152, p. 146.

[19] *Ibid*.

[20] International Humanitarian Law and Terrorism, *loc. cit.*

jurisdiction.[21] There is also an African regional convention, the African Union Convention on Cybersecurity and Personal Data Protection (2014) adopted in 2014. This convention promotes regional cooperation and provides a legal framework to strengthen cybersecurity and combat cybercrime.[22]

More than a year after the adoption of the draft convergence law (an approach to delivering interventions that are carried out in a coordinated, integrated and joint manner to prevent stunting to priority targets), although the draft law has not been ratified by signatories, many countries have used it as a guide to enact domestic cybercrime laws.[23] International institution such as the International Telecommunication Union (ITU) launched the Global Cybersecurity Agenda (GCA) guided by the High-Level Experts Group (HLEG), a group of cybersecurity experts, who provide information and recommendations on strengthening cybersecurity to member states and relevant stakeholders working on this issue.[24] The Cyber Index released by the United Nations Institute for Disarmament Research (UNIDIR).[25] There are many other organizations, and conventions passed by UN and regional institutions that list legal solutions and measures that states can comply with. The CIA, INTERPOL, and many organizations, both governmental and non-governmental have been targeted and are at war with cybercriminals. Non-state actors have always been the primary target of these government organizations for information regarding government documents, plans, nuclear codes, and so on.

The effort against cyber terrorism requires a multidimensional and comprehensive strategic approach to be implemented, including strengthening cooperation between all public and private sector stakeholders. In this case, the governments include security forces, cyber security experts, telecommunications network operators, internet service providers, and civil society. Strengthening the capacity of stakeholders (cyber security specialists, law enforcement agencies, and judiciary), as well as civil society by raising awareness on cyber security to prevent threats.

[21] David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?," *International Cybersecurity Law Review* 1, No. 1-2 (2020): 63-72, p. 65.

[22] Uchenna Jerome Orji, "The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability?," *Masaryk University Journal of Law and Technology* 12, No. 2 (2018): 91-130, p. 92.

[23] *Ibid*.

[24] International Telecommunication Union (ITU), "Overview Cybersecurity," *Series X: Data Networks, Open System Communication and Security* X, No. 1205 (2008): 2-3, p. 1.

[25] Cameron H. Bell, *loc. cit.*

Accurate analysis of cyber terrorism is very important, namely studying the objectives, motivations, and resources used, monitoring strategies and activities, as well as analyzing and evaluating its risk of damage. In line with this, it is necessary to formulate several national strategies, such as the National Cyber Security Strategy that aims to develop and enhance cyber security in Tunisia to make it safe and resilient against cyber threats. The strategy should outline objectives and implementation plans to help create conditions for all stakeholders to work effectively on cyber security, and raise awareness and knowledge across society.

Coordinate actions and make agreements with other countries regarding crimes related to cyberterrorism (including information exchange to prevent cyberterrorism operations). Organize the prevention and treatment of these crimes and the exchange of information and evidence. This will include the activation of extradition agreements for cybercrime offences. Promote the exchange of information, best practices, and lessons learned between countries in preventing and countering cyber terrorism.

## D. CONCLUSIONS

Measures are taken to raise awareness among citizens, judicial, and law enforcement agencies on the importance of computer crime prevention, educate judges, officials, and law enforcement agencies on financial crimes and cyber crimes, and expand codes of conduct for computer use and teaching, information technology curriculum, and victim protection policies. Calls on member states to strengthen international action to combat cybercrime recommends to the UN Committee on Crime Prevention and Control, the dissemination of guidelines and standards to help member states combat cybercrime at national, regional and international levels to support and develop further research and analysis, find new ways to deal with the problem of cybercrime in the future and finally consider cybercrime in the implementation of extradition agreements and cooperative assistance in the field of crime prevention. It can also be known that to prevent and eradicate cyber terrorism, a lot of cooperation with national and international stakeholders is needed to combat cyber terrorism in Indonesia, the government maintains infrastructure such as cyber security in Indonesia, supported by strict regulations to fulfil the rules.

## REFERENCES

Abri, Hussein, dan Syailendra Persada. “Kapolri Listyo Sigit: 217 Teroris Ditangkap Dalam Lima Bulan.” *Nasional Tempo*. last modified 2021. https://nasional.tempo.co/read/1473369/kapolri-listyo-sigit-217-teroris-ditangkap-dalam-lima-bulan. accessed 5 October 2021.

Astuti, Sri Ayu. “Law Enforcement of Cyber Terrorism in Indonesia.” *Rechtsidee* 2, no. 2 (2015): 157–178.

Bell, Cameron H. “Cyber Warfare and International Law: The Need for Clarity.” *Towson University Journal of International Affairs* L1, No. 2 (2018): 21–22.

Dogrul, M, A Aslan, and E Celik. “Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.” In *3rd International Conference on Cyber Conflict*, 29–43, 2011.

Gracesy Prisela Christy. “Penanggulangan Cyber-Terrorism Melalui Website Radikal Dalam Perspektif Demokrasi Pancasila.” *Paulus Law Journal* 1, No. 2 (2020): 59–71.

Heylaw Edu. “Mengenal Ancaman Tindak Pidana Terorisme Sebagai Extraordinary Crime Menurut Hukum Pidana Internasional.” *Artikel Hukum Hukum Pidana*. https://heylawedu.id/blog/mengenal-ancaman-tindak-pidana-terorisme-sebagai-extraordinary-crime-menurut-hukum-pidana-internasional.

International Telecommunication Union (ITU). *Overview of Cybersecurity. Series X: Data Networks, Open System Communication and Security*. Vol. X, 2008.

International Humanitarian Law and Terrorism: Questions and Answers, ICRC, 2011, https://www.icrc.org/en/doc/resources/documents/faq/terrorism-faq-050504.htm. accessed 29 September 2021.

Khoironi, Sri Cahaya. “Analysis Cyber Security Culture Training Needs as an Effort to Develop Country Civil Aparatures Competency in Digital Era.” *Jurnal Studi Komunikasi dan Media* 24, No. 1 (2020): 37–56.

L, Debora Sanur. “Dalam Melindungi Keamanan Nasional (War on Terror in Indonesia to Protect National Security).” *Politica* 7, No. 1 (2016): 25–47.

Lewis, James Andrew, and Götz Neuneck. *The Cyber Index International Security Trends and Realities*. Switzerland: United Nations Institute for Disarmament Research, 2013.

Mayssa Zerzri. “The Threat of Cyber-terrorism and Recommend Actions for Countermeasures.” *C·A·Perspectives on Tunisia* 4 (2017): 2–6.

Orji, Uchenna Jerome. “The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability?” *Masaryk University Journal of Law and Technology* 12, No. 2 (2018).

S, Nur Qalbi., Fitrah Marinda, and Rina Yulianti. "Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir." *Legislatif* 4, No. 1 (2020): 106–123.

Wardani, Linda Ayu. "Analisis Implementasi Kerja Sama Filipina Dan Amerika Serikat Dalam Penanggulangan Aksi Terorisme Di Filipina." *Journal of International Relations* 4, No. 4 (2018): 675–683.

Wicki-Birchler, David. "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?" *International Cybersecurity Law Review* 1, No. 1–2 (2020): 63–72.

Windiani, Reni. "Peran Indonesia Dalam Memerangi Terorisme." *Jurnal Ilmu Sosial* 16, No. 2 (2018): 135–152.

Zaidan, Muhammad Ali. "Pemberantasan Tindak Pidana Terorisme: Pendekatan Kebijakan Kriminal." *Seminar Nasional Hukum Universitas Negeri Semarang* 3, no. 1 (2017): 149–180.