Volume 2, No. 9 September 2023 - (1120-1135)
p-ISSN 2980-4868 | e-ISSN 2980-4841
https://ajesh.ph/index.php/gp

CYBER TERRORIST PREVENTION STRATEGIES

Christo Febi Cahya Manafe
Terrorism Studies Study Program, School of Strategic and Global Studies, Universitas Indonesia
Email : Manafe.Christo@gmail.com

ABSTRACT:
The history of terrorism has been known since the 18th century in several countries and nations in the world, where this condition was motivated by a different mindset from the government in power at that time such as ideology, religion, culture which was then developed by a group of people who became an organization and gave birth to a revolution that had an impact on major changes in the country and the nation. However, in the 21st century, the change in acts of terrorism is very much different where what is usually better known as acts of violence, such as suicide bombings, murders, kidnappings and extortion, is currently carrying out its actions through internet-based social media by spreading the news. Hoax news so that it can easily recruit members to carry out their actions if it is categorized as Cyber terrorism is a crime using very high and advanced technology (High-Tech). The research methodology used is qualitative with literature study; study relevant scientific articles and reports from credible observer institutions, compare, conclude strategic points related to Cyber Terrorism prevention strategies. Multidisciplinary approach is used to draw a moderate and objective conclusion in relation to the issues to confered. Upon on the results of research and comparison, it may concluded that (1) law enforcement officers do not fully understand what cybercrime is. (2) The availability of funds or budget for HR training is minimal. (3) Legal awareness to report cases to the police is low.

Keywords: Cyber terrorism, Internet, Hard Approach, HR.

INTRODUCTION

Countries in the world are competing to advance their technology to increase the progress of the country and nation, especially for people who have to live side by side with technology, one of which is internet-based technology.

The development of technology and information can help develop and help facilitate various kinds of activities that can help the productivity of a community and in this case the country.A technology with the latest breakthrough which later became the turning point for technological advances during the civilization era is known as the Internet. (Wardiana, 2002) The internet or the abbreviation of*interconnection-networking*, which can be interpreted as a global communication network which can then connect billions of computer networks around the world which in use use communication media applications such as satellites and satellites telephone The Internet, which was introduced around the 1980s, has proven to be a dynamic communication tool capable of reaching people all over the world. The extraordinary development of technology has created a network that is able to penetrate all groups broadly with relatively low barriers to entry into society, where the benefits of internet development have had an extraordinary effect. Starting with the uniqueness of sharing information and ideas, unfortunately there are some bad effects of technology. this is the use of the ease of obtaining information by several Radicalism groups and organizations for their respective interests.

A media mentions that the media is very useful for perpetrators of terrorism, where a terrorist can act and play an active role in an internet page and where one of them says the internet is a special vehicle in forming a public opinion and is very global and broad both unconsciously.

Indonesia, in the face of being one of the developed countries that has been named by several other superpowers, already has sufficiently increased capabilities and technology to support and enhance economic, security, socio-cultural development in the context of realizing increased welfare for society and a just democratic system that is part of the aspirations of the virtuous Indonesian nation. faced with the outbreak of the Corona virus throughout the world which interrupted face-to-face activities and damaged the economic system so that internet-based technological capabilities were utilized to support the rotation of activities in all aspects, especially the economy and Indonesia also participated so that all people could easily access the internet, but This is used by organizations with a background in radicalism to spread terror, hoax news, search for budgetary

support and other materials and recruit new members in order to support acts of terrorism in Indonesian territory so that crime in cyberspace is increasing, including extraordinary crimes, namely those that are more terrorist in nature. known as*Cyber Terrorism.*

Phenomenon*Cyber Terror*sm that is happening in the 21st Century can be found easily in Indonesia, one way is only with an internet base one can make news or access the entire network and it doesn't require a lot of money. In its development, Indonesia has been ranked first in the world regarding problems*Cyber Terrorism* in 2004, but many cases could not be resolved completely due to problems with evidence. Due to the many challenges, including: (1) Proving the guilt of the perpetrator requires carefulness and witnesses and other supporting evidence, (2) the experience possessed by the investigative element in dealing with crimes related to high technology or cyberspace is still limited, (3) Evidence, (4) Computer Forensic Facilities.

RESEARCH METHODS

These statistical results were obtained through a search of scientific literature and expert writing. The literature in question is the results of several data sources, namely reports from official government and non-government institutions that use regulations or laws that apply to regulate these rules. This concept is one of the studies in looking for a system that is used as an indicator or benchmark for objects (individuals) who have been exposed to radicalization whether they have become nationalists or not.

This study used the literature study method by studying references to library sources as a guide material for the next method, then followed by data analysis. As for both primary and secondary data taken through references, observations, interviews and other sources that are used as supporting data. The subject in this study is a rating system that has been conceptualized through a study, by conducting a literature review (*library research*), namely reviewing some scientific literature with the acquisition of released primary data and limited to a period of no more than the last ten years. This method was chosen because there is already some scientific literature with previous primary data collection which is used as the object of analysis and the results of the accumulated method will then be used to design and establish a conclusion from the study that was compiled.

RESULT AND DISCUSSION

A. Current state of development

Before moving on to the discussion in this paper, it is best to do a Perception equation about the meaning

of *Cyber Crime* (cyber crime), what is meant by cyber crime is a crime committed and carried out with the help of an information system or computer network on a computer system or network against a computer system or network (UN congress in Vienna in 2000). While the meaning of*Cyber Terrorism* (cyber terrorism), some experts conclude that*cyber terrorism* are unlawful attacks and threats as well as attacks against computers, networks and information stored or located and working on them, which are intended to intimidate or coerce the government or its people to advance political or social goals. (Prof.Dorothy E. Denning, 2001), this definition is one of the quotes taken because*cyber Terrorism* has an understanding that is said to be a new thing and not many, especially layers of society in remote areas who have not received education or recognition about the problem of cyber terrorism crimes, and many opinions still misinterpret thata, *Cyber crime* and*Cyber Terrorism* are two crimes that are the same but are actually different even though in carrying out the action using a method based on a system or computer network and the internet, so this needs to be educated to the whole community by related institutions in charge.

In its development, there are several reasons that cause terrorist groups and organizations to carry out their actions through cyberspace. In carrying out actions to achieve a certain goal by carrying out an attack using a network or program language-based system with technology that can be said to be quite high.

There are several advantages that stand out in the activity*Cyber crime* that can be collected by the author. The advantages for perpetrators of acts of terror in cyberspace related to terrorist activities are as follows:

1. **Number of Actors**

   When viewed from the needs of the number of perpetrators, carrying out acts of terror in the digital world does not need to require a large number of perpetrators but with a small number of members and even alone (*Lone wolf*) but has special abilities such as the ability to read programs and other things that are more specific, especially the ability to hack a network and system in the government or to predetermined goals and targets, however this is very much different from open acts of terrorism, the perpetrators need certain abilities and usually coaching or special education is carried out such as physical training, bomb assembly and of course it takes quite a long time to prepare potential perpetrators of acts of terror.
2. **Actor Security**

In carrying out acts of terror, of course through cyberspace cyber terrorism crimes can be ensured that the security of the perpetrator's data is safer and more confidential because in carrying out the action it does not have to be at the target and proving the perpetrator is very difficult. This can happen if the perpetrator uses fake data in carrying out the action either by using other people's data or create fake account data in every action.

3. **Target selection**
   Then in targeting it does not take a long time to plan and can be done without anyone knowing and there is no need to think about weather problems and other aspects that need to be taken into account, therefore actors in choosing targets or targets can freely and easily take action where several targets to carry out acts of terror as well as to spread information that is causing conflict.
4. **No time limit**
   Perpetrators can easily carry out acts of terror without anyone knowing to commit data theft, system hacking, or spreading hoax news in the virtual world and perpetrators can carry out their actions from anywhere without having to approach a predetermined target or target.

Indonesia is one of the countries that has received terror attacks through cyberspace besides the United States which is the cause of Indonesia being the target of action*Cyber terrorism* is the existence of Radicalism sites which have found approximately 9,800 sites that are Propaganda about Kafir government and teach ideology that is contrary to Pancasila and 46,000 accounts that are radicalism, this is a big threat to the government if steps and decisions are not taken to deal with acts of terror in the digital world.

If you look at past history, Indonesia was involved in cyber problems when one of Indonesia's territories, namely East Timor, decided to separate from the State of Indonesia, known as Timor Leste., at that time East Timor (which later became known as Timor Leste) was under attack from various countries and organizations that supported the independence of East Timor (Timor Leste), where at that time technologically and there was no body specifically to deal with cyber crimes. This condition then occurred again around August 2010 which made all government systems unstable which had an impact on people's economic life and other fields, the attack was known as the Stuxnet Worm Virus where this virus attacked the Central Government and State public facilities where the target was directed at power generation systems in several regions of Indonesia, irrigation systems that are a necessity for the community,

especially in urban areas, even gas, which in its operation also used a digitalization system at that time which was also a government asset, was also targeted. Activity*Cyber Terrorism* not only a matter of carrying out attacks on government institutions but also being used as a supporting element to carry out conventional actions openly in the field, this happened when the Bali Bombing I incident which shocked the people of Indonesia and the world turned out to be a case of action*Cyber terrorism* the first in Indonesia which was discovered by the security forces, this is related to each other because in the planning stages and the process of preparing for the Bali Bombing attack was carried out via the internet and laptop media, then in 2017 an act of cyber terrorism was carried out at a hospital in Indonesia known as the attack Ransome Wannacry virus, this is categorized as a cyber-terrorism attack because the target is a hospital which is an important aspect that concerns the needs of many people engaged in the health sector and it is the government's duty to protect and protect it.

So many digital attacks that occurred were considered to disturb the stability of defense and security so that the Indonesian Ministry of Defense, in this case the Minister of Defense, on October 23, 2021, formed a formula in the form of*Road Map* about the national strategy to prevent threats from cyberspace that can endanger the stability of the government called*National Cyber Defence.* The current conditions and developments of the government through related institutions have been going well by always fixing deficiencies in regulations where in every improvement to existing regulations using the basis of Law number 36 of 1999, Law number 11 of 2008, Law number 14 of 2008, Law number 25 of 2009 and Perpu number 82 of 2012. Of course, do not forget the priority aspects of all regulations that are expected to be implemented by the government, including increasing awareness about cyber security and cyber threats to all elements of the general public at large. Strengthening is expected to proceed in stages, bearing in mind the previous events in Indonesia, the need for strengthening regulations and prevention, especially in aspects of business or state facilities based on broad or global services, such as health and vital country facilities such as water and electricity.

Findings like this are nothing compared to the content which can be said to be rather radical, namely containing knowledge about hiding weapons, making explosives. To avoid surveillance or supervision, where in special conditions, for example in lessons such as first aid and martial arts, all this knowledge indirectly provides training to prospective members who will be recruited without having to meet face

to face and provide training independently.

Various experts and institutions have conducted various kinds of research and studies on the Road Map which is expected to maintain the defense and security of the Indonesian State, namely the Indonesian State Road Map for developing and enhancing Indonesia's national cyber security capabilities written by a University Team from Oxford who have collaborated with kemenkominfo, Directorate General of Aptics, Telkom University with the results of issuing a book containing the results of research and studies entitled*The Future of Cybersecurity Capacity in Indonesia.* this book contains 20 Priority scales to be added to the Road Map regulation starting from the stages of planning to being determined and implemented. The concepts from research results include;

1. Development and improvement of Security*National Cyber Defence* (NCSS).
2. Strengthen the role and coordination of functions between institutions and related institutions.
3. plan important programs according to priority scale and open cooperation with all related government and non-government institutions.
4. Conduct training and technical guidance by involving all related components so as to create the expected output
5. Increase military capabilities in the field of defense and security, especially in cyberspace
6. Form a Special Team in dealing with emergencies related to National cybersecurity
7. Creating, enhancing and developing cybersecurity knowledge through cyber national security campaigns.
8. Improved National Portal and fully controlled in preventing cyber attacks in the life of society and government.
9. Building and giving trust from the public to the government in this case including online services, such as those found in e-government and e-commerce services.
10. Protecting each individual's personal data through a system*Private-online*
11. Categorizing research and education confronts cybersecurity issues and avoids gaps that already exist
12. Provide education about cyber security systems to all employees, both in government and private sectors
13. Initiate national registrations or registers for information assurance and establish a cross-sector (public and private) board of cybersecurity experts to cultivate new talent as a profession.

14. Increasing internal security by carrying out inherent supervision by government officials
15. Making Regulations that are always dynamic following developments in cyber security
16. Capacity Building for Officers in crime investigations*Cyber Terrorism* in the court
17. Creating an online Reporting Service System against cyber crimes
18. Planning The process of purchasing goods and services in order to support cyber security
19. Creating a special team under the relevant ministries in the framework of supervision and monitoring of Indonesian cyber security.
20. Provide awards and subsidies for companies that create programs to address cybersecurity issues in Indonesia to encourage sales of their products in the international market.

Positive Impact when*Road Map* can be applied, among others: (1) the direction and goals of cyber security are more directed and systematic, (2) the concepts of techniques and tactics are clear. If the concept is duplicated with other concepts, (3) the strategic concept is implemented regularly. So that if there is a deviation, various parties can provide the necessary input and suggestions so that the deviation can be redirected in the direction that has been regulated. (4) the initial situation can be easily known. That way, all the tactics and methods to be followed will not conflict with the current situation. (5) the handling methods taken can be understood by all relevant parties so that there is firmness towards the tasks assigned because there is already this confirmation, everyone knows the duties each in the implementation and handling that will be taken.

Road Map the issue of cyber national security in Indonesia is of particular concern to the government because according to survey results it states that Indonesia is a country where the people are among the top ten in the world who actively use social media. These results are based on research taken from the APJII Institute (Association of Internet Service Providers). Indonesia) where this institution carried out its latest research in 2018 it was stated that around 143 million more people or around 54.7% of Indonesia's population actively use the internet and the majority of its users are classified as workers and students in the archipelago. From this data, it is possible that the threat of cyber terrorism is also quite high, the target of which is not only to attack but to spread propaganda, spread news of lies and utterances of hatred, causing conflict based on SARA, how to assemble bombs, raising and recruiting members.

B. The expected conditions

The phenomenon of the issue of radicalism and structured terrorist activities is easy to describe by looking at the very clear features in every terror act that will be carried out, including: there are always victims who become targets or targets in acts of terror (other than the perpetrators of acts of terror) and the following characteristics is to always spread certain ideas that have a background of foreign religion and culture to the general public so that it can easily recruit new members and support funds in order to support terrorist activities that will be carried out or carried out, the next characteristic is not to hesitate to destroy and kill

or have a very serious effect on the target or victim of the terror act, then it will cause a loss (from a material and financial perspective). (Yehoshua, 2020) While the estimated effect or impact is most likely to occur if there is no specific prevention related to the public (general public) indirectly is the loss of tolerance and mutual respect in several circles and community groups based on ethnicity, race and religion, especially in Indonesia which consists of various tribes and nations. The efforts, activities or actions carried out by perpetrators of terrorism are usually carried out by several groups or individuals (lone wolves), including:

a. Explosion of bombs / bombings

Suicide bombings or car bombings are acts of terror that most often occur in public places or specific targets used by terrorist groups because they can cause harm or relatively high impact or effect, both in terms of the number of personnel losses, both fatalities and psychological impacts. experienced, then material losses such as government buildings, public facilities and historic buildings. Moulds, 2019) In addition, the use of acts of terror with suicide bombings is more popular with perpetrators of terrorism because it is easy to learn self-taught in the manufacturing process, the raw materials needed for the process production is very easy to obtain, and of course from a financial (cost) perspective it is relatively affordable for acts of terrorist actors but can have a very large impact.

Example: Bali Bombings I and II

b. **Murder**

The incident of killing with a background of radicalization is a form of terrorist act that was carried out from ancient times before other, more modern tools were found to carry out acts of terror. These acts of terror are usually carried out with targets and targets that have been determined and designed using a lot of energy and require careful planning in carrying out the action, usually those who are the targets of these acts of terror are

usually carried out against people who do not agree or who are considered to be obstructing the achievement the goals are usually more towards leaders in government, businessmen who do not provide support and are considered to bring bad influence according to the group's point of view, and finally the apparatus that deals specifically with terrorism (Military, Police and other related bodies)).

Example: Assassination of the President of the United States (John F. Kenedy)

c. Piracy

The next act of terror activity is a technique of committing piracy where acts of terror are usually carried out in groups to seize a place whether in transportation such as airplanes, ships, land transportation by force. The hijacking that is currently the most popular and has a huge impact is airplane hijacking, this is because airplane passengers consist of various passengers who have different backgrounds whether from different ethnicities, nations, religions, social strata, a public figure. which is respected so that it creates a very large effect and creates attention, especially to the public through the media with the aim of conveying the intent of the terror act.

Example: hijacking of the Garuda plane in 1981 and hijacking of an airplane in America which crashed into the WTC Building. (Wiener, 2019)

d. Interception

Deterrence is a tactic of terrorist activities carried out, this tactic requires careful planning, more manpower and considerable costs to prepare weapons and the risk of failure is higher, but if successful will get a very high effect power. therefore the scenarios implemented in Interception activities almost never fail in their implementation.

Example: Interception of the TNI who are moving places using vehicles by armed separatist groups in Papua.

e. Kidnapping

In seeking funds, there are several terrorist groups that use new techniques to support their actions, namely by carrying out kidnapping activities. if the activity is successfully carried out, a request will usually be made in the form of compensation or support for funding the organization and their activities as well as a request for the release of fellow terrorists who have been arrested by security forces.

Example: Kidnapping of American foreigners in Afghanistan to ask fellow terrorism fighters detained by the American Army to be released.

f. Robbery

Robbery and kidnapping have almost the same motives, but robbery activities are carried out to obtain the

funds needed in order to support the organization and operation of acts of terrorism.

Example: Bank Robbery, Gold Shops, and places that can support the group's operational activities.

g. Bom Api (Firebombing)

Acts of terror carried out in the form of bombing techniques using fire against a target or area that has been planned, usually this attack is aimed at areas that have a background in people who have the same thoughts but are in conflict with the terrorists so that they are considered an obstacle and the next goal is to show ability to the government, that the actions of the group are serious and capable of attacking the security system of the government.

Example: Hezbollah group rockets fired at the state of Israel as an act of revenge.

h. Armed attack

Armed attacks carried out by separatist groups, especially in Indonesian territory, especially Papua, are increasing and causing many victims, especially on the part of government officials, the TNI and POLRI.

Example: The attack on a military institution in West Papua which was carried out by the KSB Papua resulted in the death of the apparatus.

i. Cyber Terorrism

Cyber terrorism is an act of terrorism which has been carried out by many terrorist fighters with the characteristics of attacks and acts of terror against computer systems to extract important government data or destroy security systems through cyber attacks. In addition, this is done by using Internet access and social media in the context of media terror and introducing the radical organization which is filled with content containing radical ideology or understanding to the public (public) to gain sympathy, supporters and new members.

In cyber terrorism crimes there are several relevant theories such as the transfer of activities by radicalism organizations which currently often utilize technology in cyberspace (social media) known as Cyber Jihad and this is also followed by terrorist groups in Indonesia, both affiliated with Al-Qaeda such as JAS and Isis-affiliated groups such as JAK and MIT. and actions spread through social media are activities that contain violence, writings containing the Islamic State, texts about religion and propaganda writings about the lifestyle of the Islamic state which indirectly make some people believe and follow to become part of the terrorist group. modifications were even found, a school learning curriculum was found which included 6 core subjects that had been taught to approximately 13,000

children, especially history and ideology subjects, which were an effort to indoctrinate Isis which taught about death and destruction that awaited everyone who was considered lost and outside. One of their groups is an example of a letter recognition lesson where "S" is taught for snipers and 'G' for grenades, there is also a file that contains a guide for jihadists which contains tips to improve the abilities of jihadists. As for the lessons that have been infiltrated or indoctrinated include (1) English, (2) sports lessons, (3) Arabic, (4) Read Al'Quran, (5) history lessons and (6) Ideology. Findings like this are nothing compared with content that can be said to be somewhat radical, containing knowledge about concealing weapons, making explosives. To avoid surveillance or oversight, where in special conditions, for example in lessons such as first aid and martial arts, all this knowledge indirectly provides training to prospective members who will be recruited without having to meet face to face and provide training independently. Of all the activities of acts of terror can be analyzed the purpose of use for acts of terror contains about; Counter narrative, indoctrination in order to find new members, seek financial backers, train members of a military nature, provide materials and necessities needed, make plans, carry out acts of terror, prepare places to hide.

The phenomenon of cyber-terrorism in the 21st century has increased and is dynamic so that a handling strategy and techniques are always updated dynamically by following developments, one of which is:

1. **Officer Recruitment**
   Always updating existing regulations, especially the problem of professional and nationalistic human resources, it is an urgent need to regulate regulations that are specific to workers, both temporary outside cyber agencies and resource staff from other institutions that have the ability specifically in the Cyber Sector so that recruitment is flexible and not rigid but the goal is achieved, if the regulations regarding human resources have been updated and regulated so that they have confirmation about positions in work and there is no doubt in carrying out tasks because they already have a legal basis, for example being appointed as an employee remain at the institution.
2. **Cooperation**
   The need to maintain and increase Bilateral Cooperation between countries with international agencies, Cooperation involving the Military and State Crypto Agency, Intelligence Agency and other related agencies, because almost all institutions currently have their own cyber

security so there is nothing wrong with doing and the exchange of technology and data is carried out at the international and national scope to anticipate attacks that will be carried out by terrorist groups.

3. **Software**
   It is a must to always update the software owned by the Cyber Agency and develop special and periodic techniques with inherent supervision by the government by collaborating with third parties using the principle of confidentiality.
4. **Providing Education**
   Education is an important part of any new knowledge, because it is hoped that it will always provide education to all citizens starting from the security forces, both the TN-POLRI on duty in the field, the State Civil Apparatus and the general public about providing education or knowledge about terrorist cyber crimes. This, thus minimizing the occurrence of acts of terror through cyberspace.
5. **Evidence**
   In the case of cyber-terrorist crimes, there are often obstacles with evidence so that it is necessary to carry out special research and ongoing research, then the results are conceptualized and regulated in regulations so that in examination the perpetrators with existing evidence can be sufficiently punished according to law.
6. **Digital Forensic Laboratory**
   Proving, of course, requires evidence and research so that a laboratory that has international legality and high technology is needed in order to dismantle cybercrime cases in Indonesia in particular.
7. **Officer Training**
   Provision of Training to Cyber Officers starting from Field Officers to Cyber Leaders on a regular basis in accordance with the existing time period and always screening each officer so that there are no cells or potential cells of Radicalism in cyber organizations, especially officers who man the tools or strategic and authorized positions.

CONCLUSION

The regional government, in this case the National Cyber Security Agency and POLRI, as an extension of their hands in overcoming the handling of acts of terrorism on social media, play a role in facilitating the arrest, proof and prevention of acts of terrorism, which have worked very optimally and are developing rapidly, but there are several regulations that must be tightened, especially within the body. the internal body of the agency so that the Cyber Agency is getting stronger in dealing with threats and challenges that attack the

Indonesian state and government at any time, and in its implementation it is necessary to make a memorandum of understanding (MOU) between the agencies involved regarding regulations and positions to act so that officers in the field do not there are doubts and avoiding individual and group interests that take advantage of the situation and remove sectoral egos between agencies, but have the same vision and mission.

It is a necessity and has become a permanent agenda in supporting efforts to protect the country from various threats, therefore education and information are of vital importance in advancing crime prevention not only in the real world but also in cyberspace.

The virtual world provides many benefits for the wider community, but the government must always be three steps ahead in order to be able to monitor the condition of the community at large, by synergizing cooperation between all levels starting from individuals, families, educational and work institutions, to layers of government and national defense. no country is perfect, but the desire to protect the interests of the people must be an important emphasis to make all levels work together in efforts to protect the country.

BLIBLIOGRAPHY

Abingdon, A. C. M., York, N., & Routledge, N. Y. (2021). *Ronald Crelinsten. 15*(3), 3745.

Afrizal. (2019). Metode Penelitian Kualitatif: Sebuah Upaya Mendukung Penggunaan Penelitian Kualitatif dalam Berbagai Disiplin Ilmu (4th ed.). Rajawali Pers.

Akhgar,Babak et.al. (2014).Cyber Crime and Cyber Terrorism Investigator's Handbook.United States :Syngress

Aldrich, R. W. (2000). *Cyberterrorism and Computer Crimes : Issues Surrounding the Establishment of an International Legal Regime* (Issue April).

Awudumapu, A. (2013). An Overview of the Role of International Institutions and Regional Bodies in the Promotion, Enforcement and Protection of Human Rights. *Enforcement and Protection of Human Rights (August 13, 2013)*.

Chin,C.(2004).Cybercrime and cyberfraud.In H.Bidgoli.The internet Encyclopedia.Volume 1(A-f) (p.326).California:john Wiley&son.

Dreyfuss, R. (2006). *Devil's game: How the United States helped unleash fundamentalist Islam*. Macmillan.

Giantas,D&Stergiou.D (2018).From terrorism to cyber-Terrorism:the case of Isis.Hellenic institute of

strategic studies.http://dx.doi.org

Ganor,Boaz,et.all.2006.Hypermedia seduction for terrorist recruiting

Harahap, R. D. (2016). LGBT di Indonesia : Perspektif Hukum Islam, HAM, Psikologi dan Pendekatan Maṣlaḥah. Al-Ahkam, 26(2), 223. https://doi.org/10.21580/ahkam.2016.26.2.991

Hikam, M. A. S. (2016). *Deradikalisasi: peran masyarakat sipil Indonesia membendung radikalisme*. Penerbit Buku Kompas.

https:/ Peta Masa Depan Keamanan Siber Indonesia – Ditjen Aptika (kominfo.go.id)

Jaishankar,K.(2008).Space Transition Theory of cyber crimes,in scmallager,F.&Piattaro,M.(Eds).Crimes of the internet.(pp.283-301).upper saddle river,NJ:Prentice Hall

Koto, I. (2021). Perlindungan Hukum Terhadap Korban Tindak Pidana Terorisme. *Prosiding Seminar Nasional Kewirausahaan*, *2*(1), 1052–1059.

Leong,Angela Veng Mei.2007.The Disruption of international organised crimed

LEMHANNAS RI, & Daihani, D. U. (2019). Sistem Pengukuran Ketahanan Nasional dan Simulasi Kebijakan Publik Berbasis GIS. *Laboratorium Pengukuran Ketahanan Nasional Republik Indonesia*.

Managhan, T. (2020). *Unknowing the "War on Terror": The Pleasures of Risk*. Routledge.

Microsoft Word - POLICY PAPER 4 - Cyber Security (wantiknas.go.id)

Moulds, S. (2019). Parliamentary Rights Scrutiny and Counter-Terrorism Lawmaking in Australia: A Framework for Evaluating Legislative Scrutiny in Modern Democracies. *JSEAHR*, *3*, 185.

Munhanif, A., Jahroni, J., & Makruf, J. (n.d.). *Memahami Terorisme: Sejarah, Konsep dan Model*.

Soekanto, S. (1981). *Pengantar penelitian hukum*. Universitas Indonesia. https://books.google.co.id/books?id=C4iHHAAACAAJ

Subrahmanian, V. S., Pulice, C., Brown, J. F., Bonen-Clark, J., & Kuiper, G. (2020). *A Machine Learning Based Model of Boko Haram*. Springer.

Sumpter, C., Wardhani, Y. K., & Priyanto, S. (2021a). Testing transitions: Extremist prisoners re-entering Indonesian society. *Studies in Conflict & Terrorism*, *44*(6), 473–494.

Sumpter, C., Wardhani, Y. K., & Priyanto, S. (2021b). Testing Transitions: Extremist Prisoners Re-Entering Indonesian Society. *Studies in Conflict and Terrorism*, *44*(6), 473–494. https://doi.org/10.1080/1057610X.2018.1560666

Wiener, H. B. and M. (2019). *Religious*

Freedom Under Scrutiny. Pennsylvania Studies in Human Rights.

Yehoshua, S. (2020). *TERRORIST MINDS: From Social-Psychological Profiling to Assessing the Risk* (Vol. 13). World Scientific.

Zubaidi, A., & Sutarmanto, H. (2019). Indeks Ketahanan Ideologi Pancasila. *Jurnal Ketahanan Nasional*, *25*(2), 277–294.