Identification of Positive Clandestine Intelligence Threats In Cyber Terrorism For National Security

Yudha Fernando[1], Mohammad Amin Soetomo[2]

[1]Sekolah Tinggi Intelijen Negara, Bogor, Indonesia, [2]Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:

Accepted:

Published:

DOI: 10.33555/ejaict.v…

Corresponding Author:

Mohammad Soetomo

Email: mohammad.soetomo@sgu.ac.id

ISSN 2355-1771

ABSTRACT

This study is motivated by the vigilance towards the development of cyberspace technology that is so fast that it causes dependence on it in almost all fields. This condition poses a potential threat to our national resilience in various fields, especially in the national security sector. Researchers try to identify the threat of Positive Clandestin Intelligence (PCI) in the form of cyber terrorism on national security, so that it can bring stakeholders to a better level of knowledge. Theories and concepts used are related to threats, national security, positive clandestine intelligence, terrorism and cyber terrorism (CT). This study is a qualitative method and the type of research is descriptive qualitative. Interview and literature review are used in primary and secondary data collection. Data is evaluated and analyzed with an interactive analysis model. Researchers also validate by measuring the degree of accuracy between the data that occurs in the object of research with data that can be reported by researchers. This study succeeded in identifying the types of PCI CT targets, forms of PCI CT attacks, psychological motivations of PCI CT perpetrators and the position of PCI CT threats in the taxonomy of Rogers M.K.'s cybercrime behavior.

Keywords: *Cyber Terrorism, Nasional Ressiliance, Terrorism, Positive Clandestine Intelligence, PCI*

1. Introduction

Discussions on national security threats that are created in cyber space is something that cannot be avoided for parties dealing with issues of national security. This study tries to provide a picture in the form of identification related to the threat of cyber terrorism from the perspective of national security intelligence. The results of this study are expected to provide vigilance related to cyber terrorism as a PCI for stakeholders in the field of national security, particularly intelligence related to national security. In Article 1 paragraph 1, Law no.17/2011, mentioned that intelligence is knowledge, organization, and activities related to policy formulation, national strategies, and decisions based on the analysis of the information and facts gathered through working methods for the detection and early warning in the context of prevention, deterrence, and response to any threats to national security.[6]

In the era of industrial revolution 4.0 today, a threat to national security has found new forms, including threats of positive manifold PCI. Conceptually, PCI has various forms, one of which is terror, the activity by the opposing agent with the negative intentions. The method has been successfully dialectic of terror with their external environment in order to create fear.[3] Dynamic development of technology and globalization cannot avoid and become supporting factors for the existence of this terror threat; the terror threat in question is the threat of terror in cyberspace or cyber terrorism.[1]

Below what PCI, terorism definition, threats according to Indonesian law, roles of intelligence in national security, and how cyber techniques formed and developed for terrorism acts are reviewed.

1.1. PCI

Intelligence in a country is defined in three appearances, namely appearance as an organization, appearance as an activity, and appearance as knowledge.[12] Intelligence as an activity means a closed activity, either in the form of clandestine activities or covert action; these activities include activities that are routine in nature and intelligence operations that are temporary and time-limited.[9][11] The output of intelligence activities is called PCI, which can take the form of espionage, propaganda, social conflict or terror [12].

1.2. Terrorism

Whittaker, citing several definitions of terrorism, including Walter Reich who stated that terrorism is a strategy of violence designed to promote desired outcomes by instilling fear in the public at large. Terrorism is the use or threat of using violence, which aims to achieve political change.[2]

1.3. Threat

Law no.17/2011 of National Intelligence states that a threat is any effort, job, activity and action, both from within the country and abroad, which are assessed and/or proven to endanger the safety of the nation, security, sovereignty, territorial integrity of the Unitary State of the Republic of Indonesia, and national interests in various aspects whether ideological, political, economic, socio-cultural, or defense and security.[6] A threat is a thing, a situation, an event, an action that can endanger, complicate, disturb, cause pain, harm, etc.[3]

Basically, threats have goals and interests, namely as follows:

1) State: the threat interests are the sovereignty and independence of the state and territorial integrity.
2) Nation: the threat interest is national unity and the noble values of the nation.
3) Government: the interests of the threat are government policies and actions and government legitimacy.
4) Society: the interest of the threat is the life of the community and the interests of the community groups.
5) Individual: the threat is the security of one's soul and family and assets.[13]

1.4. National Security

As part of the national security system, intelligence acts as an early warning system and a strategic system to prevent strategic incidents that threaten national security.[12] National security is generally defined as a basic need to protect and safeguard the national interests of a nation which states by using political, economic and military power to face various threats both from outside and from within the country; national security can also be interpreted as a condition that is national in nature and describes the freedom of the state, society, and citizens from all forms of threats and/or actions, whether influenced by external or internal factors; and national security is defined as a basic need to protect and safeguard the national interest of a nation by using political, military and economic power to face threats both from within and outside the country.[10] This view supports the argument that national security in a democratic country generally includes state security, public security and human security.

1.5. Cyber Terrorism

Cyber craft can be defined as any type of intelligence activity that uses telematics technology as the media; the forms of cyber craft range from propaganda in the form of defamation through social media, hoax, hate speech to 'high tech' such as cyber terrorism by using dos attach, malware and ransomware.[4][8]

The definition of cyber terrorism can be defined as the use of computer network techniques to make the main infrastructure of a computer network malfunctioning, with the aim of intimidating or coercing the government and community groups.[2] Meanwhile, the main infrastructure for computer networks is

systems and assets which, if destroyed, will have an impact on infrastructure security, economic security and the security of the public health system; this includes the energy industry, food, transportation, banking, communications, government and cyberspace itself.[2][4] The perpetrators of cyber terrorism can be state actors (SA) and nonstate actors (NSA).[8] It depends on the motivation of the intelligence organization user who uses PCI cyber terrorism as an intelligence activity in cyberspace.

This study attempts to identify the shape, type and psychological motivations of terrorists, so that it can be input for the country's national security system in finding a solution.

2. Methods

This is a qualitative study. The study used a qualitative approach. The qualitative approach chose, because this study aims to identify the threat of PCI cyber terrorism to national security through social phenomena, that occur from the subject's point of view, where the researcher is the key instrument.

This qualitative research process involves important efforts, such as asking questions and procedures, gathering specific data from informants, inductively analyzing data ranging from specific themes to general themes, and interpreting the meaning of the data.[5] The qualitative approach was considered by researchers as appropriate to identify the threat of PCI cyber terrorism to national security as a social phenomenon that tends to be described in descriptions in the form of words rather than numbers.

The research method used is a qualitative description method by studying the forms of PCI cyber terrorism threats to national security. Qualitative descriptive research seeks to describe, record, analyze and interpret the forms of PCI cyber terrorism threat to national security. In other words, this study aims to obtain information about the existing situation. This descriptive research uses a case study model, where the researcher tries to identify the form of PCI cyber terrorism threat to national security. The final report for this study has a flexible structure or framework. Anyone involved in this form of research must apply an inductive research perspective, focus on individual meanings, and translate the complexity of a problem [14].

2.1. Data Validation

This study uses triangulation techniques in the data validation stage. Triangulation technique is checking data by matching it with something outside the data for comparison; triangulation techniques are carried out through interviews, direct observation and indirect observation [5][14].

2.2. Data Collecting Method

The main data sources obtained by researchers in this study are words, actions and additional data such as other documents. This study uses data collection techniques to obtain primary and additional data sources.[14] The types of data obtained in this data collection consist of primary data and secondary data. Primary data were obtained through in-depth interviews with informants (practitioners, academics and researchers); meanwhile, secondary data obtained from observation and study of documents related to the research objectives [5].

2.3. Data Evaluation

Evaluating information is an integral step in the analysis process, and in general, evaluation is carried out when the information is obtained. Data is evaluated according to the level of confidence in the data source as well as the accuracy of the actual information.[14] When evaluating information, analysts ask questions such as:

1) What is the level of trust in information sources?
2) Has the source of information supported by the previous information?
3) How accurate is this information?
4) How is that information status at this point?

The evaluation process is needed, because deception is something that is commonly encountered in the intelligence world. To create levels or levels of information, analysts can use information accuracy codes and information reliability codes.[9]

3. Result & Discussion

This study succeeded in collecting primary data and secondary data to be used as material for further analysis.[5][14] The primary data that the researchers succeeded in obtaining came from in-depth interviews with intelligence researchers, academics and intelligence practitioners. In order to increase the quality of the analysis results, researchers also collected secondary data using observation techniques and document study. The primary and secondary data are then evaluated according to the level of confidence and accuracy of the actual information. The evaluated data is then reduced by summarizing, selecting main points, focusing on important things related to the identification of the threat of PCI in the form of cyber terrorism against national security.

Primary data obtained from interviews with intelligence practitioners (resource person A) explained that intelligence activities in the form of PCI cyber terrorism have indeed occurred in Indonesia. This can be seen from the wannaCry virus incident which attacked a number of hospitals in 2017. The attack is classified as cyber terrorism using the Ransomware method. In addition to these examples, the resource person also added several examples of cyber terrorism attacks such as cyber terrorism attacks on the General Election Commission (KPU) servers in 2004 and 2005. The form of cyber terrorism attacks in 2004 took the form of defacing the display of the national tabulation page of the KPU's voting results. Meanwhile, the form of cyber terrorism attack in 2005 was in the form of KPU takedown server, so that the internet network at the KPU national tabulation center could not function. According to the informant, the objectives of cyber terrorism (CT) attacks are divided into three types of attacks, namely data confidentiality, data integrity and finally data availability.

The next primary data, researchers obtained from the results of in-depth interviews with terrorism lecturers at the State Intelligence College (STIN), DR. Supriyadi, SE., M.Si. In the in-depth interview, he explained that the form, form of cyber terrorism attack can be in the form of a virus outbreak, which is a virus attack that enters our computers; Spam mail/mailbomb is an attack that usually occurs in someone's email sent by irresponsible people; Dos Attack is an attack that can paralyze a person's computer system if they are sent a dos attack; Unauthorized Access is an infiltration of our computers without our knowledge and without our permission.

Primary data for the three researchers obtained from interviews with the Executive Director of the Center of Intelligence and Strategic Studies, DR (Candidate) Ngasiman Djoyonegoro. According to him, the phenomenon of cyber terrorism is in accordance with one of the books he wrote, namely Intelligence in the Digital Age. Terrorism attacks are no longer conventional, but will use cyber media. This is related to the increasing difficulty of the terrorist movement in carrying out conventional threats.

In addition to the primary data, the researchers also succeeded in obtaining secondary data with engineering studies documents. Researchers obtained data in the form of the Taxonomic Continuum of cybercriminals ranging from new people (novice) and amateurs in the form of ordinary delinquency to major acts of terrorism. This taxonomy researcher got from the book The Psyche of Cybercriminals: A Psycho-Social Perspective by Roger M.K.[15] The explanation of the taxonomy of cybercrime can be explained as follows:

1) Script Kiddies (SK), are individuals with limited technical abilities, without really understanding what the impact of their behavior is.
2) Cyber-punks (CP), namely groups that "expand" the punk mentality into cyberspace. This group has no respect and no care for authority, symbols and social norms.
3) Hacktivist (H), which is a term used for individuals or groups who perform deviant behavior, but with semantic camouflage to disguise their actions.

4) Thieves (T) are criminal in general. His main motivations are financial gain and greed.
5) Virus Writers (VW), starting from adolescence and developing into a category of ex-writers in line with their cognitive and chronological development and maturity. There is a sensation of mental challenges and academic practice (learning) in the viral creation process.
6) Professional (P) is the most elite category group in cyber criminals, who have competitive intelligence and gray activity. These P individuals can engage in high-profile scams to corporate espionage.
7) Cyber-terrorists (CT) can be part of the military or paramilitary of a country and are positioned as soldiers or vice versa as liberation fighters in cyberspace warfare. Their goal is the same as in traditional military, which is to win battles or wars. CT carries out two functions, namely attacking the enemy's defense system and society and protecting its own system from similar attacks from the opposing side.

Furthermore, researchers also obtained data related to the motivation of cybercriminals [15], namely:

1) Social Learning Theory. The social learning process works in the context of social structures, interactions and situations. Criminal behavior is a function of the variables of the social learning process, especially reinforcement. The main mechanisms in social learning include differential reinforcement and imitation. Definitions in one's social environment are achieved by imitation and observational learning. Reinforcement can be in the form of tangible and intangible rewards in the form of the activity itself, money, or social rewards including increased status in social interactions. Over time, imitation is no longer important because it is the reinforcement or consequences that determine the next behavior.
2) Moral Disengagement-moral justification. Cyber criminals are generally described as modern Robin Hoods, who carry a valuable function in society.
3) Anonymity and Social Control Theory. Research on online behavior has found that people behave differently in cyberspace than in the real world. Individuals tend to be more aggressive, less tolerant, more indiscriminate, and their opinions tend to be more polarized to extreme points on the continuum. In simple terms we can understand that online behavior reflects the actual individual self in conditions without self-control and without social norms or pressure.

From the secondary data from literature study, it can be seen that cyber terrorism is the most dangerous level in the cybercrime taxonomy. This can be seen from the perpetrators, methods and targets that can be categorized as threats to the national security of a nation. Meanwhile, in terms of psychological motivation, cyber terrorism is motivated by the Moral Disengagement - moral justification and Anonymity and Social Control Theory variables. This can be seen from the behavior of terrorists who are generally described as modern Robin Hoods, who carry a valuable function in society so as to produce an act of moral justification. Radical thinkers tend to be more aggressive, less tolerant, more indiscriminate. Their actions and opinions tend to be more polarized to extremes on the continuum. In simple terms Rogers [15] argues that online behavior reflects the actual individual self in conditions without self-control and without social norms or pressure.

3.1. Data Evaluation

Prunckun, 2014 [16] the evaluation process firstly assesses the source's reliability and, secondly, the information's accuracy. In theory, this process is performed on each piece of information collected. However, in agencies collecting large volumes of data, this may be an automated process where a generic rating is assigned if the data are merely stored, but if used in an intelligence research project, it is reevaluated on an individual basis. Each piece of data is assigned an alphanumeric rating indicating the degree of confidence the analyst has in that piece of information. This system is universally known as the *admiralty ratings.*

After the primary and secondary data have been collected, the next step is the researcher evaluates the accuracy and confidence level of the data source. The results of this evaluation can be seen in table 1 below.

Table 1. Data Accuracy & Trustworthiness

No.	Type of Data	Sources	Trust	Accuracy
1	*Books*	*Library*	*A*	*1*
2	*Interview*	*Practitioner*	*B*	*2*
		Researchers	*B*	*2*
		Academics	*A*	*2*

3.2. Data Visualization

After data cleansing from data collection method the researchers present several tables such as the goal table of cyber terrorism, the form of cyber terrorism attacks, the position of cyber terrorism attacks in the taxology of cybercrime and the psychological motivation of cyber terrorism perpetrators. Here is how it looks.

1) PCI threats in the form of CT to national security have three types of targets, namely:
   - Confidentiality: Disclosure of confidential target data belongs to the government that may cause fear; this is similar to typical terrorist activities. An example is seen in the case of Snowden and several groups of democracy activists in western countries who disclose confidential government and company data to the public due to differences in political attitudes.
   - Integrity: Manipulate the integrity of an application/network system, so that it did not work normally. For example, an unauthorized data changed incident during the KPU's tabulation process by cyber terrorists in 2004 and 2005.
   - Availability: Terminate authorized users' access to the computer network, so that the application was unavailable. This happened in 2017 in several hospitals in Indonesia that were affected by the wannaCry virus. The indication of inaccessible networks at related hospitals was devastated.

Figure 1. Types of Cyber Terrorism Target

2) From the research findings based on threats of PCI Cyber Terrorism to national security: the forms of attacks used are shown at Figure 2. Forms of Cyber Terorrism Attacks.

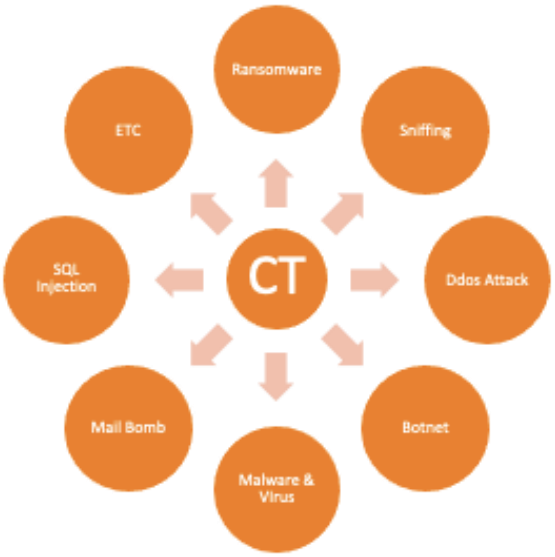

Figure 2. Forms of Cyber Terrorism Attacks

3) Moreover, the study has found types of cybercrime perpetrators' motivation, CT actors fall into the Moral Disengagement/moral justification and Anonymity & Social Control Theory groups. Motivation can arise from one of these types or a combination of the two. See figure 3 venn diagram upon the results of CT perpetrators' motivation in carrying out acts of terrors.

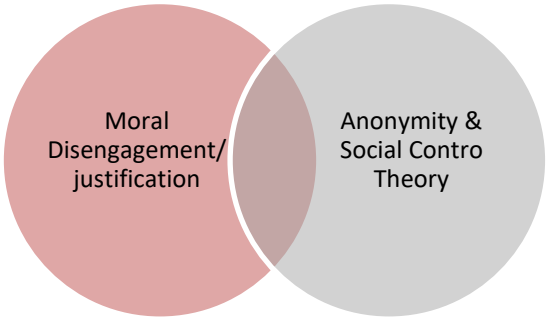

Figure 3. Motivation of CT Actors

4) This study also succeeded in finding the threat level of CT in the Taxonomy Continuum of cybercrime behavior, which ranges from new people (novice) to major acts of terrorism. Here is how it looks taken from the book The Psyche of Cybercriminals: A Psycho-Social Perspective by Roger M.K [15].

In the taxonomy of Rogers' cybercrime behavior[15], it appears that the position of CT is on the far right. This shows that the level of cyber terrorism threat is the highest compared to other forms of cybercrime. This is because the impact generated by the threat of cyber terrorism is very large and can disrupt national resilience in the security sector.

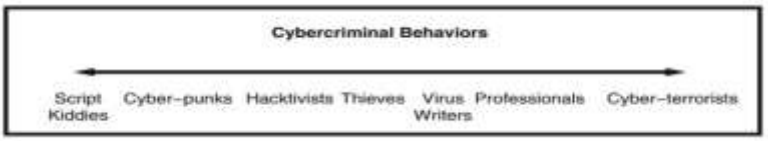

Figure 4. Cyber Crime Rogers' Taxonomy of Behavior [15]

4. Conclusion

PCI has undergone a dialectical process along with the changing environment in which PCI is used. Terrorism, as a form of PCI, also experiences this dialectical process. Terror is no longer just a form of bomb

and bullets, but has metamorphosed into bits and bytes. Perpetrators of terror acts no longer need to come out of their hiding places, because they can carry out acts of terror with only a computer. The threat of PCI in the form of CT against national security needs special attention for stakeholders in the field of national security, so that national resilience does not become disrupted.

In this study, researchers have succeeded in producing knowledge to identify the threat of PCI cyber terrorism against national security. The knowledge that the researchers generated is in the form of PCI CT target types, forms of PCI CT attacks, psychological motivation of perpetrators of PCI CT action and PCI CT threat position in Rogers M.K's taxonomy of cybercrime behavior[15].

5. References

[1] Benjamin, Cole. "*Conflict, Terrorism and the Media in Asia*". Routledge. 2006.
[2] Whittaker, David J. "*Terrorist and Terrorism in the Contemporary World*". Routledge. 2004.
[3] Barry Buzan, People. *States and Fear: an Agenda for International Security Studies in the Post-Cold War.* (Boulder: Lynne Rienner Publisher, 1991).
[4] Mutimer, David. *Beyond Strategy: Critical Thinking and the New Security Studies, In Contemporary Security and Strategy*. Craig A Snyder (ed). (London: Macmillan Press Ltd, 1999).
[5] Sugiyono. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Alfabeta. Bandung. 2009.
[6] Law No.17/2011 of National Inteliigence states.
[7] Brian, Jenkins. *International Terrorism: A New Kind of Warfare*. Santa Monica: CA: Rand Corporation. 1974.
[8] Sederberg, Peter C. *Terrorist uths: Illusions, Rhetoric, and Reality Change*. Harpercollins College Div, 1993.
[9] Irawan Sukarno. *"Ilmu Intelijen".* Puslitbang BIN & STIN. STIN PRESS. 2014.
[10] Wahyono S.K. "*Pengertian dan Lingkup Keamanan Nasional*". Program Pasca Sarjana UI, Kajian Stratejik Ketahanan Nasional. 2003.
[11] Saronto, Yohanes Wahyu. "*Intelijen Teori, Aplikasi dan Modernisasi*". PT Ekalaya Saputra. 2004
[12] Widjajanto, Andi. Wardhani, Artanti, "*Hubungan Intelijen-Negara*". Jakarta. 2010.
[13] Darmono, Bambang. "*Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan bagi Bangsa Indonesia*". Sekretariat Dewan Ketahanan Nasional. 2010.
[14] Suharsaputra, Uhar. DR, M.pd. *Metode Penelitian.* PT. Refika Aditama. Bandung. 2014.
[15] Rogers. M.K. 2010. *The Psyche of Cybercriminals: A Psycho-Social Perspective* in Ghosh. S. & Turrini. E. (Ed). Cybercrimes: A Multidisciplinary Analysis. New York: Springer.
[16] Prunckun, H., "Scientific Methods of Inquiry for Intelligence Analysis (Security and Professional Intelligence Education Series)", 2nd. ed., Rowman & Littlefield, 2015