International Journal of Social Science (IJSS)
Vol.2 Issue.6 April 2023, pp: 2351-2356
ISSN: 2798-3463 (Printed) | 2798-4079 (Online)
DOI: https://doi.org/10.53625/ijss.v2i6.5363

THE ROLE OF THE KOPASSUS 81 UNIT IN DEALING WITH CYBER TERRORISM: A CONFLICT RESOLUTION EFFORT IN INDONESIA

By
Arifuddin Uksan[1], Pujo Widodo[2], Herlina Saragi[3]
[1,2,3]Universitas Pertahanan RI
Email: [1]arifuddinuksan123@gmail.com, [2]pujowidodo78@gmail.com, [3]herlinsara897@gmail.com

Article Info

Article history:
Received Jan 12, 2023
Revised Feb 24, 2023
Accepted Mar 21, 2023

Keywords:

ABSTRACT

Facing the current developments in the global environment, terrorist groups have been able to utilize cyberspace to carry out acts of terrorism against vital national installations and national information infrastructure. The rise of cyber crimes in the form of identity fraud, child pornography, fraud, and digital-based terrorism are threats that must be faced by all components of the nation. If this problem is not prevented from developing immediately, then a series of other problems will surface and more and more individuals will be affected by terrorism via cyberspace, so that cyberterrorist groups will be free to carry out their actions. In an effort to prevent the threat of cyber terrorism in Indonesia, the role of the 81 anti-terror Special Forces Unit is needed which specifically handles the threat of terrorism in an offensive and optimal manner. This study aims to analyze the role of the Kopassus Unit 81 in preventing the threat of terrorism, by choosing a qualitative research method. From the results of the research it was found that the development of cyber terrorism threats in Indonesia is very advanced and dangerous, for this reason an optimal role is needed from the Kopassus unit in dealing with cyber terrorism threats to support national defense. This study concludes that progress in the field of science, especially Information and Communication Technology can have a negative impact in creating contemporary crimes known as cybercrimes so that this condition has the potential to increase the spectrum of threats to National Defense.Keywords: optimizatioan; kopassus; cyber terrorism; national defense.

Corresponding Author:
Arifuddin Uksan
Universitas Pertahanan RI
Email: [1]arifuddinuksan123@gmail.com

1. INTRODUCTION

National Defense is a fundamental and very important aspect to be built in the context of national and state life, in order to ensure the survival of a country. Based on this need, it is important for national defense to be known by every component of the nation throughout the world. Defense science emerges and develops in military circles as well as knowledge about war. Defense science can be used for organizational interests, military tactics and strategies in order to achieve goals for a country. In order to anticipate drastic developments in the strategic environment in a country, region and globally, defense science can be used as a reference and conceptual foundation in interacting with countries in the world [1]

Observing the condition of the development of the strategic environment, the Indonesian state is currently dealing with the hegemony of western civilization as well as dealing directly with the domination of China as a super power in Asia, especially in the case of control of the South China Sea-North Natuna Sea. This provides insight in building a paradigm of thinking for the nation's children that it is time for the national defense force to be increased in line with the advances in science and technology of the superpower countries. If we look at some time ago, when

Indonesia experienced a blackout on August 4 2019, even though this problem was quickly recognized and could be anticipated, the negative impact on people's lives was enormous. [2]

At present the spectrum of threats to state sovereignty is always rolling so fiercely in line with the progress of information and communication technology aspects which are very fast from time to time. The various conveniences provided by technology have also brought people to face new dangers. The presence of new media, in this case communication media, also creates new types of threats which are often referred to as cyber threats or cyber threats. Threats of this type include fraud, child pornography, identity forgery, to digital-based terrorism (cyber terrorism). In fact, the President of the Republic of Indonesia, Joko Widodo, in his directive, emphasized that the spectrum of threats is getting wider, from radicalism to terrorism.[3]

In simple terms, cyber terrorism as a crime that is classified as extraordinary crime in this case the impact of the crime is more massive and is also accompanied by the fulfillment of extreme political and ideological desires. The data and facts obtained regarding cyber attacks come from the ISIS terrorist group, in which the terrorist group has a cyber unit called the ISIS Cyber Caliphate.

From a demographic perspective, Indonesia's population of 264 million (2019 data) is around 171.17 million (64.8%) people connected to the internet, which has the potential to directly increase threats in the form of cyber crimes. The existence of a cyber security development movement from policy makers is the right solution in solving problems in the life of society and the nation.[4]

In a geographical view, the data and facts obtained regarding cyber attacks come from the ISIS terrorist group, in which the terrorist group has a cyber unit called the ISIS Cyber Caliphate Army, which has succeeded in destabilizing countries that have the most advanced science and technology, namely the United States and several other countries.[5]

Indonesia's very strategic position coupled with the condition of diversity in ethnicity, culture, customs, religion and language as a multi-cultural country, makes Indonesia very vulnerable to the growth and proliferation of cyber terrorism crimes. From this explanation, it can be seen that the threat of terrorism, especially in the realm of cyber radicalization and cyber terrorism attacks, is a serious threat, even the sovereignty of a country can be torn apart, the life of society, which has now entered the digitalization era, will certainly be disrupted. Various vital national objects that have been digitally integrated will of course also be vulnerable to cyber terrorism attacks. The threat of terrorism is a real threat to state sovereignty, this was emphasized in the Indonesian defense white paper which states that the threat of terrorism is classified as a real threat [6]

2. METHODE AND THEORY

The chosen research method is descriptive qualitative where the researcher is the key instrument. The research procedure was used to compile a research paper as well as a description of Optimizing the Role of the 81 Kopassus Unit in dealing with cyberterrorism to Support National Defence. Data sources obtained from interviews, observations and documentation studies in the field. To maintain the immutability of the assessment process and prevent and overcome miss information, data triangulation is carried out both data sources, techniques, time and place, so that data is obtained validly.The data analysis uses the Miles and Huberman model with stages namely data condensation, data presentation, verification, and drawing conclusions.[7]

According to Syarifuddin Tippe, in the context of national and state life, defense is an important thing to build in order to guarantee its national interests. For this need, defense is important to be studied and understood by every country in the world. Defense science was born in the military environment and the science of war. Defense science is used for the development of military organizations, strategies and tactics to achieve its national goals. Defense science has developed into a defense concept to anticipate the rapid development of the strategic environment in the national, regional and global areas.[8]

In terms of countering terror, Kopassus has an anti-terror unit, hereinafter known as the 81st Terror Countermeasures Unit. This unit consists of Battalion 811, Battalion 812 and the Assistance Detachment. In the assignment of Kopassus to combating acts of terror, Kopassus has Unit 81 Counter Terror, which is a unit in Kopassus that is at the same level as the Group and is the best Soldier out of all TNI Soldiers, headquartered in Cijantung, East Jakarta. The strength of this unit is not publicly published regarding the number of personnel or the type of weapons it has, all of which are kept secret.[9]

3. DISCUSSION

Advances in the field of information and communication technology, of course, will produce positive and negative impacts, with improvements and ease of obtaining various information offered via the internet. Progress in this field can also be used by some unscrupulous criminals in carrying out their goals, so that cybersecurity becomes a strategic issue in various countries, including Indonesia. An example of cyber security issues is cyber terrorism, in

DOI: https://doi.org/10.53625/ijss.v2i6.5363

which terrorist groups see good opportunities in the development of this technological advancement, so they carry out acts of terror by planning to attack targets by utilizing the internet and computer networks.

In the era of globalization 4.0, which has produced innovations in the field of technology and information, such as internet media, communication media and actions used by terrorist groups are growing. They try to adjust their abilities and patterns of action with the existing developments in information and communication technology. The transformation from the use of conventional media to new media, namely the internet, which gave rise to the phenomenon of cyber terrorism, especially in the future terrorist groups will also utilize artificial intelligence technology[10] The more rapid the development of new media technology, the more sophisticated the media used by terrorists and the greater the acts of terrorism. The benefits of advances in information and communication technology, especially the internet, have touched all lines of life in modern society, this positive side also seems to be followed by the dark side of internet use [11]. Supporting this statement, based on data and facts from the National Cyber and Crypto Agency (BSSN) it is explained that, the higher the level of utilization of Information and Communication technology, will be directly proportional/parallel to the level of security risks and threats.

Based on the development of war from time to time, that the first to third generation wars are wars that use the military as the main force so that the penetration power is physical. The fourth generation war began to penetrate the non-physical realm, namely the economy and was continued with an information war that penetrated social, cultural and ideological boundaries through cyber warfare.[12]

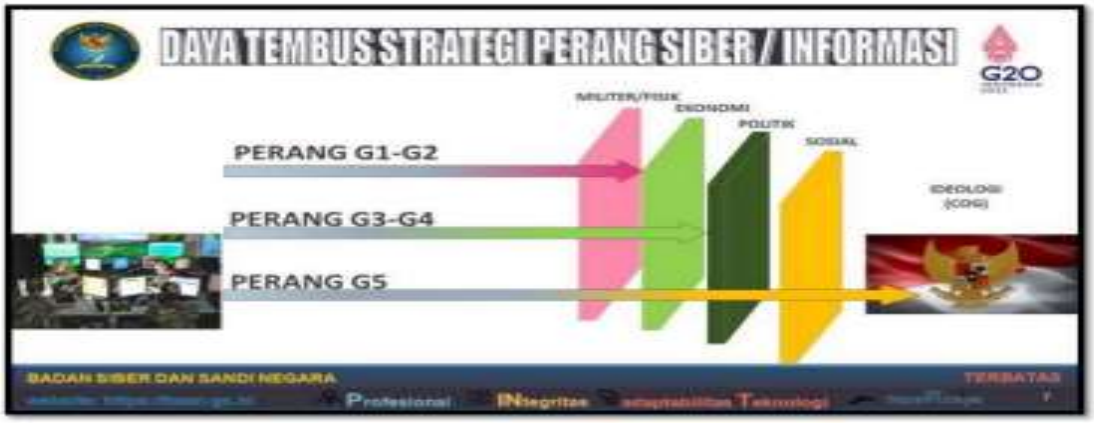

Figure 1. Cyber/Information Warfare Strategy Penetration Illustration
Source: BSSN, 2022

The role of Unit 81 Kopassus in preventing Cyber Terrorism attacks.

a. **Special Operations Development.**
The development of this special operation will later involve various related institutions specifically in handling cyber terrorism, these various institutions will be in a structured coordination, so that handling cyber terrorism will be much more effective, because it contains elements of preventive, defensive and offensive. The Kopassus Special Operations Unit will be developed by utilizing qualified cyber technology. In terms of anti-cyber terrorism operations, what must be developed is how cyber operations can support the anti-cyber terrorism operation itself. In practice, this special operation is basically focused on being a direct action or a special physical action. At present, special operating conditions have been created in such a way as to deal with physical threats, so that the Kopassus personnel themselves have the ability to deal with these threats. Therefore, it is necessary to develop a physical operation that can also adapt to operations in cyberspace. For example, there is a special reconnaissance operation that currently exists and can then be developed by carrying out a special cyber reconnaissance operation, in this case means reconnaissance in cyber anti-terrorism operations. The point in the development of the Kopassus Special Operations Unit is "Cyber Operations can reduce a risky to friendly forces".[13]

b. **Formulation of the Pattern and Doctrine of the Special Operations Unit of Kopassus in dealing with the threat of cyber terrorism.**
In formulating the strategy in the form of the pattern and doctrine of the Special Operations Unit of the Kopassus, this is based on the pattern of the threat trend itself. The formulation of this pattern and doctrine is also flexible in nature, following the development of attack patterns and extreme propaganda dissemination by perpetrators of cyber terrorism.[14]

The formulation of these patterns and doctrines is formulated into Cyber Anti-Terrorism Operations which include:[15]

1) Cyber Deterrence. Cyber deterrence in the implementation of cyber terrorism Special Operations is carried out in a planned and systematic manner which includes monitoring, detection, observation and mitigation of cyber awareness on cyber terrorism attacks to protect critical infrastructure. The operations carried out in the deterrence function are Information Cyber Patrol Operations (Patsi), Infrastructure Incident Monitoring Operations (Moninsi), and Critical Information System and Data Security Operations.
2) Cyber Recovery. Efforts to carry out cyber incident recovery as a result of various forms of cyber attacks which include digital forensics, maintenance and installation, as well as the Military Computer Emergency Team. The operations carried out in the recovery function are Cyber Exploitation Operations and Condition Creation Operations.
3) Cyber Assistance. Cyber assistance in the implementation of cyber is carried out in a planned and systematic manner in carrying out cyber assistance including system development and operational support, both from technical and non-technical aspects related to cyber operations and activities.
4) Cyber Counterattack. Cyber counter attack efforts are carried out in a planned and systematic manner in carrying out cyber counter attacks utilizing all physical strength and also collaborating with cyber capabilities to be able to carry out counter attacks against cyber terrorists (cyber terrorism). The operation carried out in the counterattack function is the Counter Cyber Terrorism Attack Special Operation.

c. Formulation of appropriate training for personnel in Special Operations.

The training can be started with education and training as well as courses on cyber security in which there is material on cyber terrorism, counter cyber attacks, cyber intelligence, and digital forensics for personnel who will join cyber organizations, especially within the scope of Kopassus itself. Training for personnel who will join the cyber organization in Kopassus can use the curriculum from the National Cyber and Crypto Polytechnic as well as the National Cyber and Crypto Agency itself. Then, training can also be carried out by involving various related institutions, namely carrying out routine joint exercises in stages, stages and continuing from the level of Subject Matter Expert Exchange (SMEE), Table Top Exercise (TTX), to Field Training Exercise (FTX) involving personnel from institutions related to handling cyber terrorism by covering training materials for Intelligence Operations, Special Operations on Countering Cyber Terrorism Actions and also Law Enforcement in the framework of Countering Terrorism Actions.[16]

The joint exercise will carry out information exchange and information development, equalizing operating standards (who and what to do) in the implementation of Intelligence Operations and Law Enforcement. Furthermore, in dealing with cyber attacks, various countries have cyber defense institutions or organizations. For example, the United States has the United States Cyber Command (USACYBERCOM), North Korea with Unit 180 capable of overwhelming the US military, China with a cyber force called the "Blue Army" which is in command of the Army, Israel with Unit 8200 under the command the Armed Forces, as well as Singapore with the Digital Intelligence Unit (Digital Unit Service) which is under the command of the Singapore Armed Forces.[17]

In Indonesia itself, on a national scale, it has BSSN as the front guard in national cyber defense, then various institutions also have it. Within the scope of the Indonesian Armed Forces itself, there is a Pussansiad, but Pussansiad in terms of its main duties and functions and capabilities has not been able to tackle the threat of cyber terrorism. Furthermore, the existence of cyber organizations such as USCYBERCOM and Pussansiad are a reference for researchers to be able to propose the formation of cyber organizations in Kopassus as pioneers within the TNI to be able to deal with cyber-dimensional threats, especially cyber terrorism.

The capability currently possessed by Kopassus is terror countermeasures which can be considered as the basic capital in the context of concept preparation and initial development or a comprehensive Backbone Cyber Defense against Cyber Terrorism, bearing in mind that so far the development of the Cyber Defense concept is still sectoral or not comprehensive, it is necessary to have establishment of a cyber organization in Kopassus with reference to USCYBERCOM and BSSN. The formation of a cyber organization in Kopassus must first carry out the development of cyber strength and infrastructure in coordination with relevant agencies such as BSSN, BNPT, BIN, Pussensiad and also other state cyber defense agencies such as USCYBERCOM, Unit 180, "Blue Army", Digital Intelligence Service. , as well as Unit 8200.

In implementing it, several indicators must be met, namely as follows:[18]

1) Facilities and Infrastructure. Fulfillment of qualified facilities and infrastructure is very necessary in building an organization, especially in cyber organizations which must get more attention by adapting to the development of information technology. The implementation that can be done is that Headquarters can facilitate the fulfillment of facilities and infrastructure that support the handling of the threat of cyber terrorism.

2) Budget. Budget support largely determines the performance and performance carried out in the conception of the Special Operations developer, which is then formed by the Kopassus Cyber Unit. The implementation that can be done is to formulate ideal budget requirements in the face of the workload to be carried out. The allocation of the budget portion to the Kopassus Unit must be based on realistic calculations taking into account operational needs, dynamics on the ground and the level of threats that the unit will face. The aim is to support operational needs, strengthen personnel, and increase the capability of the Kopassus Unit towards optimal performance and professionalism.
3) Legitimacy. Support and legitimacy will help the performance of the Kopassus Unit to be more optimal in handling cyber terrorism. The community and all components of the nation can also provide support in efforts to tackle terrorist activities in cyberspace, such as empowering the potential of community organizations that have special attention in the field of cyber, social and cyber media activists, traditional leaders, religious leaders, and community leaders. This is to support terrorism prevention activities in the form of early prevention, early detection and quick reporting to the authorities.

4. CLOSING.

This research concludes that the threat of cyber terrorism has grown quite alarming and will certainly threaten state sovereignty. If this problem is left unchecked then a series of other problems will surface, the potential problem that will arise is when many individuals in society are affected by radical understanding through cyberspace (cyber radicalism), and in the end cyber terrorist groups will be free to carry out their acts of terror. in cyberspace, which can threaten the National Vital Objects (Obvitnas) and the National Vital Information Infrastructure (IIVN). Therefore, in order to overcome these problems, it is necessary to play the role of Kopassus in dealing with the threat of cyber terrorism in order to support national security, namely, Kopassus personnel who will later join the Kopassus Cyber Unit as the main element can be used anytime and anywhere, which can combine physical and military operations. online to carry out an offensive strategy to deal with the threat of cyber terrorism, including the threat of cyber radicalization and cyber attacks.

Formation of a cyber organization in Kopassus as a pioneer within the scope of the TNI to be able to deal with threats with cyber dimensions, especially cyber terrorism. Current capabilities in Kopassus such as countering terror can be considered as basic capital in the context of concept preparation and initial development or a comprehensive Backbone Cyber Defense against Cyber Terrorism, bearing in mind that so far the development of the Cyber Defense concept is still sectoral or not comprehensive, it is necessary to have establishment of a cyber organization in Kopassus with reference to USCYBERCOM and BSSN.

Support and legitimacy will help the performance of the Kopassus Unit to be more optimal in handling cyber terrorism. The community and all components of the nation can also provide support in efforts to tackle terrorist activities in cyberspace, such as empowering the potential of community organizations that have special attention in the field of cyber, social and cyber media activists, traditional leaders, religious leaders, and community leaders. This is to support terrorism prevention activities in the form of early prevention, early detection and quick reporting to the authorities.

REFERENCES

[1] Supriyatno., M. (2014). Tentang Ilmu Pertahanan. Jakarta: Pustaka Obor Indonesia.
[2] Cross, R. 2013. Radicalism. Dalam Snow, D., della Porta, D., Klandermans, B., dan McAdam, D. (eds.). The Wiley-Blackwell Encyclopedia of Social and Political Movements. Doi: 10.1002/9781405198431.wbespm175.
[3] BSSN melalui Kumparan, 2021. Waspada Ransomware dan Teror Rampok Siber di Internet, diakses melalui: https://kumparan.com/kumparantech/waspada-ransomware-danteror-rampok-siber-di-internet-1wfrj19dTzM/1
[4] Tempo, 2021. Jokowi: Spektrum Ancaman TNI Semakin Luas, dari Radikalisme hingga Terorisme, diakses melalui: https://nasional.tempo.co/read/1513888/jokowi-spektrum-ancamantni-semakin-luas-dari-radikalisme-hingga-terorisme
[5] Christina Schori Liang, 2017. Unveiling "United Cyber Caliphate" and the birth ot the E-Terrorist, Georgetown University Press
[6] Kementerian Pertahanan Republik Indonesia, Buku Putih Pertahanan Indonesia tahun 2015
[7] Miles,M.B, Huberman,A.M, dan Saldana,J. 2014. Qualitative Data Analysis, A. Methods Sourcebook, Edition 3. USA: Sage Publications. Terjemahan.
[8] Tippe,S. (2016), Ilmu pertahanan : sejarah, konsep ,teori dan implementasi, Publisher: Jakarta: Salemba Humanika.
[9] Data Internal Kopassus, Arsip Sejarah Perkembangan Kopassus

[10] Rahman, R. A., & Habibulah, R. (2019). The Criminal Liability of Artificial Intelligence: Is It Plausible To Hitherto Indonesian Criminal System? Legality : Jurnal Ilmiah Hukum, 27(2), 147.

[11] Trisa, U. (2014). Kebijakan Anstisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism. Masalah-Masalah Hukum, 43, 1– 10. https://media.neliti.com/media/publications/158219-ID-none.pdf)

[12] Luthfi Ghifariz dan Endri Ahmadi, 2021. ISIS Returnees: A Potential Treats to the National Security in the Disruptive Era, Politika : Jurnal Ilmu Politik. Vol.12, No.2, 2021. DOI : 10.14710/politika.12.1.202.297-309

[13] BNPT, 2022. Kerjasama Penanggulangan Terorisme di ASEAN, diakses melalui: https://bnpt.go.id/pimpin-somtc-wg-on-ct-ke-18-deputibidang-kerjasama-internasional-bnpt-bahas-kerjasamapenanggulangan-terorisme-di-asean

[14] Yunanto, D. S. (2017). Ancaman dan Strategi Penanggulangan Terorisme di Dunia dan Indonesia. Jakarta: Institute For Peace and Security Studies (IPSS)

[15] KEP/ 12/ VI/ 2001 Terjadi perubahan organisasi dari GRUP-5/ Anti Teror Kopassus menjadi SAT-81 GULTOR KOPASSUS, dan kini menjadi Satuan 81 Kopassus.

[16] Bagus Artiadi Soewardi, 2013. Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh bagi Indonesia, Jurnal Potensi Pertahanan : Ditjen Pothan Kemhan RI. Hlm: 31-35

[17] Cross, R. 2013. Radicalism. Dalam Snow, D., della Porta, D., Klandermans, B., dan McAdam, D. (eds.). The Wiley-Blackwell Encyclopedia of Social and Political Movements. Doi: 10.1002/9781405198431.wbespm175.

[18] Dorothy Denning, 2000. Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University, diakses melalui: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.htm