JOURNAL OF SOCIAL SCIENCE
Printed ISSN: 2720-9938
Electronic ISSN: 2721-5202
jsss.co.id

The Empowerment of The Cyber Communities By The Indonesian Goverment From The Perspective of Total War Strategy

Devis Lebo[1*], Syaiful Anwar[2]
[1*] Student of the Faculty of Defense Strategy, University of Defense, Sentul, Jakarta and Indonesia, Indonesia
[2] Lecturer at the Faculty of Defense Strategy, University of Defense, Sentul, Jakarta and Indonesia, Indonesia
Email: devislebo@ymail.com

Keywords:
Empowering, Cyber Communities, Indonesian Government, Total War Strategy

ABSTRACT

The development of Information Technology and Computers (ICT) has made changes that affect the concept of security. The impact of these ICT developments poses a cyber threat to the National Critical Information Infrastructure (IIKN). The cyber community empowerment effort aims to help the government, institutions and private parties related to the ICT sector in safeguarding and securing IIKN from cyber attacks whose impact can collapse a country if it is not anticipated earlier. For that we need a strategy that is able to support the empowerment of the cyber community by the government in the perspective of universal war. In writing this article, the author uses a method by collecting data and information through the help of various materials contained in the literature (books) or also known as the type of phenomological research associated with qualitative descriptive. From the results of the literature research that the authors get, it is known that the cyber community has not fully helped the government in national defense, there are some cyber communities that have not been involved, it takes the role of government, institutions and private parties related to ICT to be able to realize cyber community empowerment by the Government in the perspective of Total war.

INTRODUCTION

Indonesia's national defense system is universal by involving all citizens, territories and other national resources. Therefore, the universal defense system is prepared early by the government and is carried out in a total, integrated, directed and continuous manner to uphold state sovereignty, territorial integrity and the safety of the entire nation from all threats (Pariyatman et al., 2023).

Integrity refers to the power elements built into the universal defense system, which combines military defense forces and non-military defense forces (Rahman et al., 2021). The concept of universal defense which always involves all the capabilities possessed by this nation should be data, processed and used as well as possible to support total war.

In Law No.29 / 1954 "for the first time" states that total war is a universal people's war.

In the book Lt. Gen. JS.Prabowo is shortened to "total war" (Prabowo, 2009). According to Prabowo, the future Total War is also uncertain, it can be literally equated with guerrilla warfare and and is not entirely the same as the independence war of the Republic of Indonesia (1945-1950).

Total war is by no means something simple, and can be described in simple terms. Any notion of Total War that uses military means to resolve conflicts as far as possible should be avoided. According to Sun Tzu: "Why are we busy debating whether the enemy will attack or not, we better be prepared to welcome him".

In the grouping of war generations, in this era, fourth generation warfare (4GW) has entered, which is an asymmetrical and non-linear warfare that uses all facilities and infrastructure and weapon systems aimed primarily at destroying the enemy's 'will' to fight. In asymmetric and non-linear warfare, non-military defense forces are part of the warfare. One of the threats to non-filter defense forces is ICT (information and communication technology).

The development of ICT, especially in the cyber realm, has been developing so fast until now and seems unstoppable, especially since the use of ICT has entered all aspects of community life such as: ideology, politics, economy, social, culture, law, education, defense and security. The need for ICT is absolute at this time, both at home, office, industry, business and anywhere will not be separated from ICT.

Its activities in the form of communication, interaction and movement through social media are already very massive, so they are very important and become a concern in every country. The development of ICT, if linked in industry, has entered a stage commonly called the industrial revolution 4.0 This has created an increasingly complex form of threat, so that the enemy's way of acting will be more varied and accurate This can also be a threat to Indonesia's non-military defense (Siahaan & Risman, 2021). In the 4.0 industrial revolution, the problem of non-military threats has caught the attention of various groups both abroad as well as inside domestically. As a result of the Industrial Revolution 4.0, a new threat emerged, namely cyber threats. This cyber threat is very serious, because it does not use a lot of troops to carry out attacks but the impact is very large to destroy a target and its recovery takes a very long time.

ICT is increasingly sophisticated and modern, this affects the tactics used by people who are classified as wanting to commit cybercrime. The current condition of cybercrime has hit Indonesia, they attack banks, power plants, e-commerce business centers (Bukalapak, Tokopedia), e-style, transportation, hospitals, regional elections and even in the defense and security sector. This proves that cyber attacks are very serious and very dangerous to our national critical information infrastructure (IIKN).

Based on information from The Global cyber security 2017 released by the UN International Telecommunication Union (ITU), Indonesia is one of the countries with the weakest cyber security (Union, 2017). The situation experienced by Indonesia is not much different from countries in South America such as Brazil and also countries in Africa which are vulnerable to cyber attacks. This weak cybersecurity has resulted in an increase in cyber attacks. Indonesia is ranked 70th out of 195 countries, with a suspension of 0.424. Singapore ranks first, followed by the United States in second place with the best cybersecurity system (Goode et al., 2023).

According to Sigit Kurniawan, the head of the sub-directorate for vulnerability identification and risk assessment of the national critical information infrastructure III of the National Cyber and Crypto Agency (BSSN) that "according to the data in the assessment of 76 countries, in the 2019 assessment Indonesia was ranked second worst after Algeria, but soon improved in 2020, at number 21 (Achi, 2023).

By looking at this situation, in order to protect Indonesia's sovereign territory, especially in the cyber realm, it requires the involvement of all existing resources in maintaining the country's sovereignty which is carried out through the defense and security system of the people of all (sishankamrata), which places the TNI as the main force and the people as a reserve and supporting component, where every citizen has the obligation to participate in national defense efforts in accordance with the contents of the 1945 Constitution article 30 paragraphs 1 and 2.

The involvement of citizens in facing Total War is a responsibility that needs to be

shared together so that the problems faced can be prevented as early as possible. Since the development of technology, all activities in society always use technology such as the availability of tools or other supporting things, such as computers, internet connections, gadgets, providers, and others (Mineraud et al., 2016). This community of ICT users is what is commonly called the cyber community. Initially, the cyber community was small and developed using a spider web pattern, thus forming a large society. Cyber community involves all people who use gadgets, computers and networks.

When doing virtual work, they never meet face to face and do not have territorial boundaries, they interact by using the technology and internet networks they have. The existence of the cyber community in communicating is very important to research. The author sees that there are many cyber communities in Indonesia, often gathering to exchange information, but they are closed and do not want to be known by people or are often called underground / anonymous. Their existence plays a very important role in cyberspace (virtual).

The cyber community has reliable capabilities to prevent destruction from cyberattacks. The cyber community is a part of society that is currently untouched and is a priority for the state to be involved in national defense efforts. The cyber community needs to take part in protecting IIKN, which is an asset of the nation. Regarding the formation of a cyber community to date is still being debated, some circles still see the cyber community in a real form in a regional bond, although not everyone who is in the same environment can be said to be a community, it can be said to be a community if members of the existing members in it have the same experience and a sense of being a community "sense of community" (Mankowski & Rappaport, 2014).

A strategy is needed so that the empowerment of the cyber community is considered as an activity in preventing and securing telematics resources so that crime does not occur in the cyber world. It should be noted that defending the state in facing Total War is not only a legal obligation, but also a right and honor as a citizen. Strategies in researching cyber community empowerment are needed so that the empowerment of cyber communities in the midst of technological developments can be appropriately involved in supporting Total War, This is in accordance with Law Number 20 of 1982 concerning Basic Provisions for the Defense and Security of the Republic of Indonesia, articles 17 to article 25 (Wahyuningsih et al., 2020).

The condition of the cyber community is still busy with their own world, they are only concerned with their own individual or group. Sometimes there are cyber communities who carry out illegal activities, this happens because of the absence of clear control and guidance from the government. The condition of character and spirit to help the state is a right and obligation for every cyber community which is carried out through state defense efforts to uphold the country's sovereignty, maintain the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation. Cyber community empowerment is carried out on the basis of awareness and belief in one's own strength which is grown and developed through efforts to defend the country.

The existence of this extraordinary cyber community is so that it can be more useful for the country in facing Total War. Therefore, in this paper, the author intends to explain how the empowerment of cyber communities can be carried out by the Indonesian government in the perspective of Total Warfare so that the cyber community can take part as a supporting component that will assist the government in maintaining state sovereignty in the field of defense with its ICT capabilities.

In the book Art of War, Sun Tzu (403-221) says "The supreme art of war is to subdue the enemy without fighting." This means that "War is an art, conquering the enemy without fighting is the highest art of war." From this opinion, it is very relevant to current cyber activities, where in destroying the enemy, it is hidden, it is not necessary to bring a large army, it is enough to use the capabilities and skills possessed, but the impact of the damage is very large and can even collapse a country and to recover it takes a long time.

According to Thomas Rid & Peter McBurney, who defines as follows: "Cyberspace is a part of weapons designed to threaten or endanger the physical, functional or mental structure or systems or living systems." (Netolická & Mareš, 2018). This theory is very relevant because cyber attacks have a very large impact on information and culture prevailing in society today

such as the 'Arab Spring', where the collapse of a country due to cyber attacks through hoaxes, FOF, and Post Truth which is very reliable, shaping public opinion so that it occurs. polarization in society which results in the disintegration of the nation, chaos and the state collapsing.

Cyber attacks against physical and logical targets are no less intense, such as what happened in Estonia in May 2007, Ukraine in December 2017, because it happened in winter, blackouts and malfunctioning heating devices caused casualties. From this incident, it is very possible that it could happen in Indonesia. Therefore, the empowerment of the cyber community in this country is highly anticipated to be able to help the government solve problems in the cyber world.

As it is known that the word "empowerment" is a translation from English "Empowerment", empowerment comes from the root word "power" which means the power to do, achieve, do or make it possible. The prefix "em" for empowerment can mean strength in humans, a source of creativity. Empowerment emphasizes that people acquire sufficient skills, knowledge and power to influence their lives and the lives of others they care about. According to 'person', empowerment is a process by which a person is strong enough to participate in controlling and influencing events and institutions that affect his life.

If it is associated with the cyber community, it means that an activity is carried out by the cyber community to show its capabilities in carrying out activities that can affect his life in a better way and benefit others. In Law Number 23 of 2019 concerning Management of National Resources for State Defense (PSDN), it can be used as a basis for recruiting the cyber community to be educated to become countrymen. According to Lt. General JS TNI. Prabowo said that the present and future Total War should not be carried out by mobilizing the population "all out" to be played as combatants in combat.

In Law no. 3 of 2002 concerning State Defense, national defense is all efforts to defend the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from threats and disturbances to the integrity of the nation and state. The Indonesian state defense system is a universal defense system, which involves all citizens, territories and other national resources, and is prepared early by the government and is carried out in a total, integrated, directed, and continuous manner to uphold state sovereignty, territorial integrity and the safety of the entire nation from all threats.

In the 2015 Indonesian defense white paper p.22, it is stated that current and future threats can be classified into three types, namely military threats, both armed and unarmed, non-military threats, and hybrid threats. Sources of threats can come from within and outside the country, and be carried out by state and non-state actors, which are national, regional and international in nature. Cyber threats are non-military threats that can come from within and outside the country and can be categorized as real threats both now and in the future (Bachmann, 2015).

METHOD

This research is a type of research by collecting data and information through the help of various materials found in literature (books) or also known as phenomological research. This type of research is a study aimed at describing the phenomenon of society that uses online, events, social activities, attitudes, beliefs, perceptions, thoughts of people individually or in groups. To describe the phenomenon of cyber community empowerment in depth, Then the research uses literature study associated with qualitative descriptive fenomonologis. With literature study, empirical findings can be described in detail, more clearly and more accurately, especially various matters relating to the cyber community. For this reason, through this paper, it is hoped that literature studies can help research in thinking and imagining, abstractly.

Phenomenological research can be started by observing and examining the focus of the phenomenon to be studied, which looks at various subjective aspects of object behavior. Then, the researcher conducted data mining in the form of how the object interpreted in giving meaning to the related phenomenon. This data mining is carried out by collecting secondary data from the literature that has been read, this information will be carried out in literature research that refers to Hammersley & Atkinson (2019) who studied the data obtained for the development of concepts related to social conflict in social media (Triantoro, 2019).

The focus in this research is on cyber community empowerment in the perspective of Total Warfare, the goal is to prepare the cyber community to face Total War. In order to explore this focus, this research will use qualitative methods. Qualitative research was chosen because the observed phenomenon needed observation through literature study, because it was easier to deal with reality, so that in-depth secondary data was obtained. This qualitative research is used with the aim of exploring the peculiarities of a person or group's experience whose data is taken from a literature study when experiencing a phenomenon so that the phenomenon can be opened and selected to achieve an existing understanding.As previously stated, the strategy used in this qualitative research is phenomenology. According to Creswell, phenomenology was chosen because in it the researcher will identify a certain phenomenon, and requires researchers to study the subject by being directly involved in developing meaningful patterns and relationships.

In the context of the research that will be studied, the main focus in this research is to carry out data searches through literature studies on cyber communities because in general they are closed, all activities are carried out in cyberspace (virtual) and very little face-to-face. The author will explore the activities carried out by the cyber community at this time, their social status both work and educational background, as well as the spirit of the cyber community in protecting IIKN from cyber attacks in order to realize national defense which I will associate with the Total War strategy. Meanwhile, the research location is the place where the research will be carried out.

Determining the research location is a very important stage in qualitative research, making it easier for writers to conduct research. This location can be in a certain area or a certain institution in society. To obtain secondary data, the research location is based on data obtained through books, journals and other electronic media.

RESULTS AND DISCUSSION

Research Result

It should be noted that based on data obtained in 2019, there are 56% or 150 million internet users in Indonesia, all without cybersecurity where the risks to be faced will be very large, because of the many security threats (Sutrisna et al., 2019). In avoiding attempts to steal personal data about online transactions through cyber threats, the cyber community can be relied on to be at the forefront (Ghelani et al., 2022). The cyber community in their daily activities when interacting always uses gadgets, computers and networks, so the cyber community is a new study which is currently the center of attention for ICT users. This virtual world becomes a new reality, which has become the second community world after the real world itself.

Based on the results of research on the existence of the cyber community, this cyber community is divided into two groups, the first is the millennial group or young people, whose education starts from elementary school, junior high school, high school and college. Millennial interest in cyberspace (cyberspace) is getting higher because it is supported by various types of chat applications on social media such as WhatsApp, BlackBerry Messenger (BBM), Facebook. Currently on social media there is one feature that is most in demand by millennials, this feature is the WhatsApp group. Whatsapp groups are the prima donna among teenagers in social interaction with peers.

Millennials use whatsapp groups, to be able to meet and gather to exchange ideas, greet/ground coffee, share information and even joke together. Second, other cyber community groups come from both working and non-working adults. Millennial and adult groups have different knowledge of the cyber world, some are just interacting to carry out communication among gadget users, issuing all aspirations both in assessing, responding to or criticizing information provided by other members (Sadler, 2014).

Some are used to carry out business activities so that they can make profits, some are even used to support work in the office or to support their reputation, even if there are those who use this technology to commit crimes, such as anonymous groups. Anonymous tends to be closed and does not want to be identified with his identity. They are hacker activists formed in

2003. Their trademark is the Guy Fawkes mask or commonly known as V for Vendetta. Activists like this have been widely spread in Indonesia.

In everyday life, most people in expressing opinions are usually reluctant to express them directly because they feel cared for by those around them or in short they have a mental burden, whereas through the cyber community someone is more free to give their opinion because it is not seen directly by other members.

Sometimes members of the cyber community can share experiences and enjoy content provided on cyber media. If the community in the real world requires face-to-face meetings to establish communication, however, in the cyber community, face-to-face meetings are not required, they even tend to close themselves and do not know each other. The existence of formal and non-formal cyber communities, where formal ones have representative offices or places of interaction such as the Ministry of Defense cyber community, BSSN cyber, National Police cyber community, cyber military community at universities, TNI cyber, cyber Angkatan, cyber in other institutions and and cyber in private agencies that have an interest in the ICT sector.

Usually this formal cyber community facility is very complete, because they generally have a duty as a cyber defense which aims to protect and protect data on computers from cyber attacks, while non-formal cyber community is where they are, can be at home, in a cafe, in a park. etc. They have no purpose to protect important data, they only need gadgets, computers and an internet network connection to carry out the interaction.

The ability of the formal cyber community is mostly obtained from education and courses, especially regarding ICT science, while the non-formal ones are mostly obtained from independent learning, through available applications such as Youtube, Google is then applied in the field. They do not have special duties like the formal cyber community, they are mostly anonymous, as we have previously explained. Anonymous is usually active according to their respective wishes. Anonymous is usually against scientology, homophobia and corruption.

Whereas in the beginning, this cyber community group was created for the purpose of joking, greeting each other and exchanging ideas. Today's scattered anonymous are only small groups and not an organization, but are more likely to be groups of people who have the same interests. They always fight for the right to internet freedom besides that they also have various missions, one of which is against the existence of censorship in the internet world and also the supervision of the internet world by the government.

Anonymous in action will supervise the government by taking action, launching protests by storming government websites. Another ability that Anonymous has is as a hacker or in Indonesia it is called peretas (Nasyiah, 2021). Hackers are people who are very interested in studying, analyzing, modifying, breaking into computers and computer networks, either for profit or motivated by challenges. Hackers or hackers are a desire to know in depth about the work of a system, computer or computer network, so that they become an expert in the field of mastery of systems, computers or computer networks.

Hackers are people who are very interested in studying, analyzing, modifying, breaking into computers and computer networks, either for profit or motivated by challenges. Hackers or hackers are a desire to know in depth about the work of a system, computer or computer network, so that they become an expert in the field of mastery of systems, computers or computer networks.

It is known that the activities carried out by hackers and crackers have certain plans so as to produce the results they want, therefore based on the data obtained, it is clear that the nature of the hackers themselves are still willing to share knowledge, notifying system administrators of vulnerabilities in security which is seen, does not take unfair advantages from hacks, does not distribute and collect pirated software and never takes stupid risks while the nature of a cracker is that it is able to make a program for its own benefit and is destructive or destructive and makes it an advantage. example: sending viruses, theft of credit cards, burglary bank accounts, theft of E-mail / Web Server passwords and so on.

Crackers can stand alone or in groups in action, have a website or channel in IRC that is hidden, only certain people can access it, Internet Relay Chat or IRC is a form of communication on the Internet that was created for interpersonal communication, especially

group communication in a discussion area. is called a channel (channel), but can also be for private line communication (Moedjahedy, 2016). Crackers also have IP addresses that cannot be traced, the most frequent cases are Carding, namely credit card theft, then breaching the site and turning everything in to a mess. In the world of e-commerce, hackers help many companies to find vulnerabilities in their applications.

From the explanation above about hackers and crackers, it is known that Hackers are people who know what they are doing, are aware of all the consequences of what they are doing, and are responsible for what they are doing. While Cracker is a person who knows what he is doing, but often does not realize the consequences of his actions, and he does not want to be responsible for what he has known and done (Fadjar, 2014).

Discussion

Indonesia, is a country with the fourth largest growth in internet users in the world, so this is an opportunity and at the same time can be a big threat with the development of digital technology and the internet, there is even a consulting company, McKinsey, who argues that Indonesia can increase its economic growth to US $ 150 billion, or equivalent to 10% of Gross Domestic Product (GDP), by 2025 if digital technology can be embraced (Das et al., 2018). From these benefits, there will be other challenges that will be faced with technological developments, namely in the form of cyber threats.

In facing cyber threats to the national critical information infrastructure (IIKN) owned by this nation, the cyber community is expected to be a reliable tool for the state to participate in maintaining the IIKN that the Indonesian nation currently has, such as the law enforcement sector, the energy sector and mineral resources (including in it electricity), the transportation sector, the financial and banking sector, the health sector, the information and communication technology sector, the agricultural sector, the defense sector and strategic industries as well as the emergency services sector and the water resources sector. According to the National Cyber and Crypto Agency (BSSN), the 10 IIKNs above are considered to be the most vulnerable sectors to cyber attacks in the future so BSSN needs to map the IIKNs that need to be protected.

a. The Essence of Cyber Community Empowerment

The blackout incident that had been experienced by Jakarta, Banten, West Java and its surroundings on Sunday (4 August 2019) again reminded Indonesians of the importance of cybersecurity in the digital era. Electricity is one of the primary needs in the ICT era which is all computerized to facilitate human life (Liu et al., 2021).

The protection of IIKN should have begun to be given more serious attention by the Government, especially since the condition of this country has just been tidying up and started to build all the infrastructure that has been outlined in the nine priority agendas or Nawacita by President Jokowi. All of which need to be protected from cyber attacks. According to the theory of empowerment, involving the cyber community to take part in protecting this country from cyber attacks is something that must be done because this cyber community has power within each of them and this is a source of creativity. According to the empowerment theory, by empowering the cyber community, they will gain sufficient skills, knowledge and power to influence their lives and the lives of others they care about.

The cyber community must feel that it belongs to this country, because the founders of this nation have struggled to gain freedom from the shackles of the colonialists for a very long time. The cyber community is expected to have the awareness to protect and build this nation according to its talents, don't think about destroying this nation with its capabilities and intelligence.

At present, as previously explained, the development of ICT has been so fast, that cyber threats to IIKN will run in a balanced manner following these developments. BSSN, related institutions, TNI Headquarters, Police Force Headquarters which has a Cyber Operation Center and also private parties engaged in ICT have carried out daily monitoring of their critical information infrastructure, but the observation and reporting of the results of these operations have not been well integrated and have not there is cooperation and

collaborating with each other. The tasks are carried out in accordance with the rules issued by each of these institutions or units.

At present and in the future, cyber attacks will always increase, war on cyber needs to be well planned between the government, related institutions and the private sector in the field of ICT. The increase in cyber attacks lately cannot be overcome by official government institutions alone, but the involvement of the cyber community is very much needed. There is a need for collaboration between governments, the private sector and the cyber community.

In the statement of Lt. Gen. TNI JS. Prabowo said that the present and future Total War should not be carried out by mobilizing the population "all out" to be played as combatants in combat. . This statement is very relevant to current cyber activities, that the cyber community is not a combatant, but can weaken the ICT system which has an impact on government and society (Prabowo, 2009). Cyber communities that are spread both in formal channels such as official government agencies, including in BSSN, Institutions, Satsiber TNI, Force, Polri, private parties and also cyber communities that are on non-formal channels, can jointly unite to prevent and mitigate cyberattack.

From the previously stated "Sun Tzu" statement that war is an art, the highest art is without fighting. This theory is an illustration that in order to achieve victory, you do not have to fight, but by means of diplomacy or attack without using weapons and do not involve many soldiers. This if seen is very relevant to the existence of cyber attacks that do not require weapons but can take human lives, like the events in Ukraine 2017 (Reuter, 2017).

During this Covid pandemic, not only the Covid virus can kill humans, but ransomware attacks on hospital computer systems that can take control of computers so that users cannot access these computers. like an attack on a hospital in Germany that cost a woman her life (Nasution, 2020).

Indonesian history has proven that the independence obtained at this time was the struggle of all Indonesian people at that time. All citizens of the country fought to help each other and were involved in the struggle to help TKR against the invaders. General Soedirman along with his troops and the people entered the forest to carry out a guerrilla war to attack the Dutch troops.

The general attack on March 1, 1949 was an event that raised the name of the Indonesian nation in the eyes of the world at that time and had proven that this nation still had an army. An event that led to a round table conference (KMB) in the Netherlands on 23 August-2 November 1949, one of which was The contents of the agreement were: The Netherlands recognized sovereignty to the Republic of the United States of Indonesia in December 1949. Thanks to the struggle of all citizens, what had been waiting for a long time was finally achieved. The guerrilla war that was carried out at that time was a collaboration (People's Security Army) TKR now TNI with the people. General A.H Nasution had a great hand in providing input to General Soedirman to carry out guerrilla war tactics. The position of General A.H Nasution at that time was as the representative of the TKR Commander who was appointed in February 1948 (Rusman, 2019).

The success of the guerrilla war has become a strong basis for Indonesia today in making laws and regulations so that in facing all threats it can involve all its resources. The existing law and contains the involvement of all components of the nation in Total War, starting from the 1945 Constitution article 30 paragraph 1, which reads "Every citizen has the right and obligation to participate in national defense and security efforts." This means that every Indonesian citizen has the same rights and obligations to participate in national defense efforts (Serafica Gischa, 2020).

In article 30 paragraph 2 it reads: "National defense and security efforts are carried out through the defense and security system of the total people by the Indonesian National Army and the Indonesian National Police, as the main force, and the people, as the supporting force." Then in Law No. 3 of 2002 concerning State Defense, in CHAPTER I, Article I, paragraph 2, it reads: "The national defense system is a comprehensive defense system that involves all citizens, territories and other national resources, and is prepared in a

comprehensive manner. early by the government and carried out in a total, integrated, directed, and continuous manner to uphold state sovereignty, territorial integrity, and the safety of the entire nation from all threats".

Furthermore, in the 2015 Indonesian defense white paper p. 28 states that: the defense of the Indonesian state is carried out in a universal defense system. The form of defense that has been developed involves all citizens, all resources, areas and national infrastructure, which have been prepared early by the Government, and are carried out in a total, integrated, directed and sustainable manner.

The universal defense system integrates military defense and non-military defense, through efforts to build a strong and respected national defense force and capability with high deterrence. Being prepared early means that the universal defense system is built sustainably and continuously, to deal with various types of threats, both military, non-military, and hybrid threats. Accumulatively, these various types of threats can be grouped into real and non-real threats (Ryacudu, 2015).

From several theories and laws currently held regarding the involvement of citizens to participate in Total War, it is an absolute obligation, because history has proven it. The cyber community is part of the citizens, who should be obliged to be involved in Total War in order to uphold the sovereignty and dignity of this nation from all threats to the integrity of the unitary state of the Republic of Indonesia.

National defense policy is implemented through various efforts in the management of resources and facilities national infrastructure to overcome various forms of threats. Therefore, the empowerment of the cyber community in national defense is directed at maintaining and developing all the strength and potential of national defense in an integrated and directed manner by involving all citizens, as well as utilizing all national resources and infrastructure as well as the entire territory of the country to always be ready to be part of the system. National Defense. Empowerment of the cyber community in national defense also aims to improve integrated preparedness to deal with contingent situations and escalation of threats as a result of the dynamics of strategic environmental developments (Ryacudu, 2015).

In the context of the current increasing cyber threat, the reason for the empowerment of the cyber community should be the main focus of the government, institutions and private parties related to the ICT sector which has not been a priority to be empowered in the midst of current cyber attacks. This priority for the empowerment of the cyber community aims to be able to take part in safeguarding and securing IIKN from cyber attacks which have a very devastating impact and can tear down a country if not anticipated earlier.

b. Cyber Community Empowerment

Cyber Community Empowerment aims to form independent human beings, improve living standards and provide awareness of the freedom of everyone. The orientation is towards a powerless community. Empowerment of the cyber community is an effort so that the cyber community can benefit the state in preventing and protecting IIKN from cyber attacks.

In law no. 23 of 2019 concerning PSDN, article 1 paragraph 4 states that human resources are citizens who provide their resources and efforts for the benefit of the nation and state. The cyber community is a citizen who has the ability in the field of ICT which can be used for the national interest.

The government, in this case the ministry of defense, should take preventive steps quickly to be able to manage, direct and accommodate the cyber community so that it can be formed as a supporting component that is ready to be used in the interests of national defense in the face of Total War (Saltzman, 2013).

In order for cyber community empowerment to run as expected, it is necessary to intervene both the government and the private sector related to the ICT sector to carry out coaching activities in increasing the ability of the cyber community to protect IIKN from cyber attacks.

This cyber community empowerment according to 'Talcott Parsons' is an effort for people to get skills, knowledge and power that are sufficient to affect their lives and the lives of others (Popay et al., 2021).

By empowering the cyber community, the capabilities that are owned can develop with the activities that are followed, besides that, it will get benefits that can affect the life of the cyber community itself.

In empowering the cyber community, the first steps taken by the Government and the private sector include conducting cyber competitions. This competition is an effort to minimize negative cyber exploitation activities by hackers. This competition is a cybersecurity competition that specifically focuses on the operational aspects of the management and protection of information system services and infrastructure.

Another goal obtained from this cyber competition is that later the government will have authentic data about the existence of the cyber community, so that it will be easier to build this cyber community.

The organizer of the activity representing the government and the participants had met face to face and interacted directly with the cyber community, which seemed always closed. This competition is a positive forum for cyber enthusiasts in the country. This is because the cyber community, which is mostly young people, is very smart and has potential in terms of system security. If not directed, it can get out of control.

They mostly carry out hacking activities just to show their existence that they exist and have the ability such as taking money in the bank and some even can make a country collapse and take a long time to recover. Cyber competition activities are expected to be carried out more frequently and provide appropriate rewards / incentives for winners so that they can support their lives and become a challenge for those who have not won.

The hope is that by participating in this cyber competition, all communities will be challenged to study harder and develop themselves to face the next competition. This will make the cyber community more useful for himself and society.

For the winners of the competition, the government can provide proper facilities by taking advantage of their ability to work together in protecting IIKN from cyber attacks. For the cyber community who wants to cooperate with the government, they are given a take home that is suitable for their work. However, before collaborating with the government, cyber communities that have not carried out national training are required to carry out national training, so that their nationalism spirit can be fully formed to defend the country.

They will be educated to become supporting components in this country both in peacetime and wartime. Another activity carried out by the government and the private sector is conducting a group discuss forum (FGD) as has been implemented by BSSN. BSSN invites the cyber community to work together and collaborate to create national resilience in the cyber realm. What was conveyed in the FGD was that information has now become a very important commodity.

Communities who are already in the level of "information-based society", a community that is able to access and provide information quickly and accurately, so that the need for cyber resilience for national resilience of the cyber community is very much needed (Hukum & Masyarakat, 2018). FGD activities other than in BSSN, have also been carried out at Pushansiber Kemhan, Satsiber TNI. All of this is done to exchange information about cyber developments, threats to IIKN and human resource capabilities and development plans.

When viewed from the collaboration and collaboration, cyber communities with formal backgrounds already have a place to interact with each other, but cyber communities with non-formal backgrounds do not yet have such a forum. Attention to the informal cyber community should not be ignored, because they will be very dangerous for this nation. This is very relevant to the theory of Thomas Rid & Peter McBurney which states that "cyber is a part of weapons designed to threaten or endanger the physical, functional or mental structure or systems or systems of life".

This has led to the idea that the activities of the non-formal cyber community can be controlled and can have a positive impact on this nation. If necessary, with their abilities,

they can be specially trained to join Command units, whose job is only to penetrate enemy areas, so that enemy command lines, computer-based communication devices but not connected to the internet can be paralyzed before the main troops come in. This may be a way for them to do what is best for this nation.

This coaching must be clear, directed and measured and need more attention from the government towards the cyber community that has not been accommodated. If coaching goes well, this cyber community will feel more valued than just running competitions, and this cyber community can be easily mobilized at any time to support the government both in times of peace and during wartime as a component of the nation's support.

This shows that empowering the cyber community in protecting the country's territory from cyber attacks is an obligation that must be carried out consciously and with a full sense of responsibility.

c. Cyber Community, Government and Private Roles.

The cyber community is human resources who have formal and non-formal educational backgrounds in the field of ICT, carry out interaction activities in the realm of cyber (cyberspace) with the aim of supporting something desired.

The existence of the cyber community is spread everywhere and the numbers are very large, they are all gadget users, computers connected to the internet network. The formal cyber community is at BSSN, Pushansiber Kemhan, TNI Headquarters, Force Headquarters, Institutions, Police Headquarters, Universities, professional associations and private parties engaged in ICT such as: telecommunications service provider associations, satellite associations throughout Indonesia, telephone associations, association of data center operation of Indonesia, association of Indonesian internet services. Meanwhile, the existence of non-formal cyber communities cannot be predicted, they can be in homes, cafes, parks, trains, airports and anywhere they want. In the real world they are very closed and keep their abilities secret, but if they can interact with them in cyberspace, they will be open but only in their community.

It is known that there are cyber communities capable of being hackers and crackers who work as security guards, online motorcycle taxis and so on to just show their status in the real world. The role of the government and institutions as well as the private sector related to the ICT sector in fostering, guiding and directing the cyber community to take part in national defense as a supporting component that can be realized through defense programs in the Ministry of Defense or they can be used as a computer emergency response team (CERT) to deal with local, regional and international problems even if necessary they are made easier to be recruited as Civil Servants (PNS) and placed throughout the Ministry / Institution, TNI and Polri and if needed the opportunity to be trained as agents of penetration into enemy areas with commandos can be implemented through special recruitment.

Increasing competition activities between formal and non-formal cyber communities, increasing FGD program activities, providing rewards / incentives on a regular basis for communities that assist the government in maintaining IIKN. This cyber community empowerment regulation has actually been included in the May 2019 version of the Cyber Security and Resilience Act, in articles 7 and 8 which state that the administrators of cyber security and security (KKS) consist of state institutions, central and local governments , as well as the community consisting of internal organizations and provision of KKS services.

Furthermore, Article 35 states that every KKS organizer must make efforts to cultivate KKS so that the quality of risk management increases. These cultural efforts include the implementation of promotional activities, technical guidance and / or scientific activities to increase literacy and public awareness of KKS (Wuryasti, 2020). It is hoped that with the presence of the KKS Law in the future, both central and regional governments, communities, institutions and the private sector related to the ICT sector can work together and collaborate in supporting the development of the cyber community.

CONCLUSION

The current state of rapid development of ICT has an impact on the concept of national defense in the face of non-military threats, in which there are cyber threats. The government, institutions and private parties related to the ICT sector have tried to implement safeguards against IIKN which are frequently attacked.

The current state of rapid development of ICT has an impact on the concept of national defense in the face of non-military threats, in which there are cyber threats. The government, institutions and private parties related to the ICT sector have tried to implement safeguards against IIKN which are frequently attacked.

The government, institutions, the private sector related to ICT have tried to implement empowerment of cyber communities in the perspective of Total Warfare to deal with cyber attacks. Empowerment is carried out for all cyber communities through competitions between cyber communities as well as organizing and collecting data to be used as a supporting component, other activities are increasing the discussion group forum (FGD) activities, increasing the national education program carried out by the Ministry of Defense, providing rewards / incentives for communities involved in collaboration with government, institutions, private parties related to ICT on a regular basis. The government's cyber community empowerment activities in the perspective of Total War have found several advantages and disadvantages, as follows:

REFERENCES

Achi, A. (2023). Efficiency and its determinants in the Algerian banks: network data envelopment analysis and partial least squares regression. *International Journal of Productivity and Performance Management*, *72*(5), 1479–1508.

Bachmann, S. (2015). Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*, *43*(1), 77–98.

Das, K., Tamhane, T., Vatterott, B., Wibowo, P., & Wintels, S. (2018). *The digital archipelago*.

Fadjar, A. (2014). *Acceptancy of Application an Innovative Management Accounting System, User Satisfaction and Corporate Soundness Level*.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

Goode, K., Kim, H. M., & Deng, M. (2023). Examining Singapore's AI Progress. *Center for Security and Emerging Technology*, 19.

Hammersley, M., & Atkinson, P. (2019). *Ethnography: Principles in practice*. Routledge.

Hukum, B., & Masyarakat, H. (2018). *Program PTSL Pastikan Penyelesaian Sertipikasi Tanah Akan Sesuai Target, dilihat pada 13 Januari 2020*.

Liu, L., Guo, X., & Lee, C. (2021). Promoting smart cities into the 5G era with multi-field Internet of Things (IoT) applications powered with advanced mechanical energy harvesters. *Nano Energy*, *88*, 106304.

Mankowski, E., & Rappaport, J. (2014). Stories, identity, and the psychological sense of community. In *Knowledge and memory: The real story* (pp. 211–226). Psychology Press.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications*, *89*, 5–16.

Moedjahedy, J. (2016). Implementasi Point to Point Jaringan Internet Nirkabel di SMA Universitas Klabat. *Cogito Smart Journal*, *2*(2), 240–249.

Nasution, M. (2020). Smart-Design Instalasi Digester Biogas Skala Komunal Pesantren High Temperature. *AGREGAT*, *5*(2).

Nasyiah, I. (2021). Potential Criminal Action in Shadow Banking Practice. *International Conference on Engineering, Technology and Social Science (ICONETOS 2020)*, 128–133.

Netolická, V., & Mareš, M. (2018). Arms race "in cyberspace"–A case study of Iran and Israel. *Comparative Strategy*, *37*(5), 414–429.

Pariyatman, M. H., Madjid, A., Santoso, P., & Saragih, H. (2023). Defense Strategy in Dealing With Threats of National Security. *International Journal Of Humanities Education and Social Sciences (IJHESS)*, *2*(6).

Popay, J., Whitehead, M., Ponsford, R., Egan, M., & Mead, R. (2021). Power, control,

communities and health inequalities I: theories, concepts and analytical frameworks. *Health Promotion International*, *36*(5), 1253–1263.
Prabowo, J. S. (2009). *Pokok-pokok Pemikiran Tentang Perang Semesta*.
Rahman, A., Mufida, S., Handayani, D., & Kuntanaka, W. N. (2021). Strengthening National Defence: Coordinating Waters and Air Territory Security under the Indonesian National Police. *Journal of Maritime Studies and National Integration*, *5*(1), 48–56.
Reuter, Y. (2017). *Le Roman policier-3e éd.* Armand Colin.
Rusman, E. (2019). Ensuring learning continuity everywhere: Seamless learning in the Netherlands. *World Conference on Mobile and Contextual Learning*, 132–140.
Ryacudu, R. (2015). Buku Putih Pertahanan Indonesia. *Jakarta: Kementerian Pertahanan RI*.
Sadler, D. R. (2014). Beyond feedback: Developing student capability in complex appraisal. In *Approaches to assessment that enhance learning in higher education* (pp. 45–60). Routledge.
Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1), 40–63.
Serafica Gischa. (2020). *Jumlah Penduduk Indonesia 2020*. https://www.kompas.com
Siahaan, S., & Risman, H. (2021). Contemporary Irregular Warfare: Defense Strategy. *Journal of Social and Political Sciences*, *4*(1).
Sutrisna, P. D., Candrawan, J., & Tangguh, W. W. (2019). Microfiltration of oily waste water: a study of flux decline and feed types. *IOP Conference Series: Materials Science and Engineering*, *543*(1), 12079.
Triantoro, D. A. (2019). Konflik Sosial Dalam Komunitas Virtual di Kalangan Remaja. *Jurnal Komunikasi*, *13*(2), 135–150.
Union, I. T. (2017). *Global Cybersecurity Index (GCI) 2018*. ITU Geneva.
Wahyuningsih, Y. Y., Satino, S., & Sulastri, S. (2020). Legal Arrangements of Law Enforcement in the Defense of the State to Strengthen the Defense of the Unitary Republic of Indonesia. *International Journal of Multicultural and Multireligious Understanding*, *7*(9), 201–225.