Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/9059
DOI URL: http://dx.doi.org/10.21474/IJAR01/9059

RESEARCH ARTICLE

SWOT ANALYSIS OF NATIONAL DEFENCE SYSTEM TO FACE INFROMATION WAR IN DIGITAL ERA.

Heriyadi[1], Z. Fanani[2], Setyo Widagdo[2] and Alfi Hariswanto[2].

1. Postgraduate Student Of Brawijaya University.
2. Postgraduate Lecturer Of Brawijaya University.

Manuscript Info

Manuscript History
Received: 13 March 2019
Final Accepted: 15 April 2019
Published: May 2019

Key words:-
Swot Analysis, Information War, Digital, National Defence.

Abstract

The purposes of this study are 1) analyzing the current state defence in face of the threath of information warfare in the digital era, and 2) analyzing the current strengths, weakness, opportunities, and threats of the national defence system in the face of information warfare in the digital era. This research was conducted at the Office of the Commission 1 of the Republic of Indonesia, the Ministry of Defence of the Republic of Indonesia (*Kemhan RI*) specifically the Directorate General of Defence Strategy (Directorate General of Strahan), Directorate General of Defence Potential, data and information centre as well as cyber defence centres and at the Central Information and Communication Republic of Indonesia Ministry of Defence. In addition, the location of the study was also determined at the TNI information centre (*Puspen TNI*) and the Military Cyber Unit Office (*Satsiber*), the TNI Staff Commander's Office and the Indonesian Army Territorial Centre which had been tasked with preparing the region or region as the basis of the universal defence. This research is conducted in November 2018 until March 2019. This study uses a qualitative descriptive method. The result of this study are that the issue of national defence is not the duty and responsibility of the government and its devices but is the duty and responsibility of all components of the nation.

Introduction:-

Strategic environmental developments in the past two decades show how important science and technology is including those related to information technology. The development of information technology has changed the life order and communication patterns of the world community and even has an effect on the dimensions of threats and security of both human and state security. The issue of security is no longer only related to military and ideological issues, but also has penetrated far into the economic, political, religious, and cultural domains as a result of information exchange. This of course will also affect the determination of how people and countries act in addressing various forms of new threats that are plural or hybrid.

One potential threat that is currently engulfing a number of countries in the world is information attacks. This attack was designed in an information war scenario using digital media as the main tool. This new form of battle plate is

Corresponding Author:-Heriyadi.
Address:-Postgraduate Student Of Brawijaya University.

actually inseparable from the development of cyber war (cyber war / cyber-attack) and proxy war. Cyber warfare is generally known as a form of warfare that uses information technology systems to attack opponents, creates political, economic and security instability through information engineering, agitation, propaganda, damaging information installations or stealing important information possessed by opponents or operating targets.

Carling (2016) explains that even though the United States has prepared a strong cyber defence but it is proven that US cyber security is still very weak and impenetrable. This was based on a statement from CIA Director Leon Panetta regarding the weakness of US cyber defence before the attack, which called 9/11. Carling also wrote that less than two years after the attack, the US was surrounded by instructors from various parts of the world and even the attackers who were branded as US enemies were also able to carry out cyber-attacks (hacking) in a number of other countries such as China, North Korea , Syria, Iran and others. They (terrorists) steal sensitive information from government databases, dismantle and destroy computer systems including those of private company even personal information from targeted individuals to benefit terrorist organizations.

The development of the increasingly rapid and modern production of ICT equipment accompanied by the increasing interest of digital media users is one of the academic reasons that the threat of information war will continue to grow. The practical reason is the impact of information war that is not less powerful, cheaper at a cost that is relatively much smaller than when compared to conventional war which costs a lot with the risk of greater losses for both parties.

Research purposes: -

Based on the above background, the research objectives are as follows;

1. What is the current state defence system in the face of the threat of information warfare in the digital era?
2. What are the current strengths, weaknesses, opportunities and threats of the national defence system in the face of information warfare in the digital era?

Research Methods: -

Time and Location of Research: -

This research was conducted at the Office of the Commission 1 of the Republic of Indonesia, the Ministry of Defence of the Republic of Indonesia (*Kemhan RI*) specifically the Directorate General of Defence Strategy (Directorate General of Strahan), Directorate General of Defence Potential, data and information centre as well as cyber defence centres and at the Central Information and Communication Republic of Indonesia Ministry of Defence. In addition, the location of the study was also determined at the TNI information centre (*Puspen TNI*) and the Military Cyber Unit Office (*Satsiber*), the TNI Staff Commander's Office and the Indonesian Army Territorial Centre which had been tasked with preparing the region or region as the basis of the universal defence. This research is conducted in November 2018 until March 2019.

Research methods: -

This study uses a qualitative descriptive method with observation and deepening of the material for quite a long time. In addition, this study will seek more systematic depiction of data systematically, factually and accurately about the facts of an event and certain traits.

Sampling technique: -

Respondents in this study were 1 of national defence expert, 1 of legislative official involved in the formulation of national defence policy, 5 of related officials in the Ministry of Defence, 5 people from military and civilian who were in charge of information, 1 person from a digital media practitioner or online media and 5 people from the cyber community.

Data Retrieval Techniques: -

The technique used to collect the data needed is: primary data obtained through in-depth interviews with predetermined respondents and several respondents who were randomly selected. Secondary data is obtained through documentation from relevant agencies and from various other relevant reference materials. Researchers will also make direct observations in the field to examine how millennial generations, especially cyber or IT communities, use digital media both personally and in their groups.

Data analysis technique: -
The data obtained in this qualitative study will be interpreted and analysed using Descriptive-Qualitative analysis techniques. Data analysis will be carried out by referring to Sudjarwo's opinion (2001), descriptive research is a research pattern that describes what is in the field and seeks to delineate data, regardless of whether the data is qualitative or quantitative. Then it will be analysed using SWOT analysis. According to Rangkuti (2003) the SWOT analysis identifies each factor systematically to determine the strategy to be pursued, based on logic that can maximize strengths and opportunities, and minimize weaknesses and threats.

Research Result And Discussion:-

Data Analysis: -

Indonesia's national defence system is currently facing information warfare: -
The Act No. 3 of 2002 concerning National Defence, Indonesia's national defence system is universal, involving all citizens, regions and other national resources. This system must be prepared early by the government and carried out in a total, integrated, directed and continuing manner to uphold national sovereignty, territorial integrity and the safety of all nations from all threats. The law is outlined in more detail in the national defence doctrine (The ministry of defence, 2014), which essentially states that Indonesian national defence is based on the rights and obligations of all citizens to help maintain the survival of the nation and state of Indonesia. Compensation implies the involvement of all people and all national resources, as a whole and comprehensive defence unit.

The State Defence Regulation has not specifically regulated the potential threat of information war even though the threat has been predicted for a long time. This can be seen in the national defence system white paper (Kemhan, 2008) and in the book on synchronizing the development of the title of TNI force with national development up to 2024 (TNI Headquarters, 2017). In CHAPTER III the book describes the most dangerous threats to watch out for are hybrid threats, namely the combination of various strengths, both regular and irregular, including cyber by mobilizing state and non-state actors (TNI Headquarters, 2017). Related to this, the TNI needs a hybrid power, namely combined arms that are able to overcome military and non-military threats in the long term (Protracted) and involve the people as part of the universal defence system.

In general, the conditions and weaknesses of the current state defence system in the face of information warfare in the digital era can be seen from 5 (five) aspects, they are:

a. Policy Aspects: -
The rule of law at the operational level in the face of information warfare in the digital era is indeed very important considering that the implementation of universal state defence is highly dependent on the support of national resources as a defence resource. Operational rules are also needed to ensure the implementation of efficient and effective human resource management tailored to specific needs facing information warfare. Management of defence resources in the field of information is very complex, including planning, organizing, using, monitoring and communicating all defence resources from the policy level to the operational level. Therefore, it is necessary to formulate a regulation that regulates the synchronization of national forces in the face of information warfare in the digital era by involving all national potential in accordance with the principles of universal defence. However, this is difficult to realize considering that there is no law that specifically regulates the involvement of national components in defending the country.

Opportunities that can be used to fix defence sector regulations include the plan to reconsider the Reserve Component Act or called as national resource management and Presidential Regulation Number 97 of 2015 concerning the 2015-2019 National Defence Policy that must be replaced immediately with the formulation of the 2020 strategic plan -2024.

Various weaknesses in the regulation of the national defence sector face new threats today, also responded by the Head of the TNI Information Centre Major General TNI Sisriadi. According to the *Kapuspen TNI* in an interview with the author on April 4, 2019, national defence policies have not specifically accommodated the development of potential threats today, especially information warfare. Within the TNI itself, there is no doctrine of information war even though the doctrine is very important as a guideline for every soldier and TNI unit in carrying out information war operations. The current joint operation doctrine still uses conventional war operation patterns so it must be revised again. Regarding the existence of the ITE Law, Sisriadi argues that the Act has accommodated the legal aspects of the misuse of ICTs, but it is very important to know that in the operation of information, there are times

when special information dissemination steps must be taken so that the Act must provide space for that purpose. That is, regulations related to information warfare must not be too rigid or must be able to provide certain space for the operation of information. Do not let the existing law actually make the state defence apparatus in the field of ICT unable to do anything because they are bound by the Act.

b. Aspects of Human Resources (HR): -

Human resources are the key success factors facing the threat of information war in addition to legal aspects and information technology. In the roadmap for developing Cyber Defence HR capabilities (The Minister of Defence, 2014), the Ministry of Defence of the Republic of Indonesia has begun efforts to prepare Human Recouses in support of cyber defence systems. However, this effort is more as an internal effort of the Ministry of Defence and the TNI, more about awareness and improvement of information security skills and knowledge for pre-existing personnel. The State Civil Servants (ASN) recruitment with cyber qualifications has also been started by the Ministry of Defence, but the number is still very limited.

The Indonesian nation can actually take advantage in the midst of the limitations of the country's ability to build an integrated cyber defence system, namely with the many potentials of millennial young people who have the skills and abilities specifically in the field of information technology. Based on the search results of the author during the study, the number of cyber communities in Indonesia grew and developed in various environments with various specifications of information technology expertise. The IT Communities of Depok, Bekasi, Bogor, Tangerang and Cibubur with personnel who are under 25 years old are some of the cyber communities that the author had met. Even though these communities tend to be closed to parties outside their community but some of them in person can be invited to communicate and cooperate. Some of the reasons why they do hacking activities include fad, wanting to earn income in an easy way or because they want to test the knowledge and expertise they get. According to Ahmed, testing new knowledge is necessary because applications in IT continue to grow, as well as applications for security installations, virus development and anti-virus. In fact, the potential of Human resource from the millennial generation with special cyber capabilities, has not been well empowered by the state to support integrated cyber defence systems. It is true, that state-owned institutions such as the ranks of the TNI, the Intelligence Agency and the Ministry of Defence have established informal cooperative contacts with a number of cyber communities in the country. However, the Collaboration is not yet structured, does not have strong legality with a limited scope of cooperation in efforts to secure information installations and knowledge transfer.

c. Institutional Aspects: -

Building strong and integrated Institutions is an important factor in realizing an integrated and solid cyber defence system. So far, institutions related to the use of information technology have tended to move on their own. In the future, the urgency of the rules at the operational level must be immediately realized including the development of the organizational structure of ministries or government-owned institutions, the development of integrated strategies, the division of tasks and authorities, work mechanisms, information and communication systems and supervision. This institution needs to be realized through a special study of the development of work unit organizations within the government so as to enable the synergy of roles between institutions and community components in accordance with the required expertise specifications. In the universal defence system, the development of TNI and Intelligence Institutions is directed at empowering the millennial generation that has information technology expertise as a backup component or supporting component of national defence in information warfare. State institutions engaged in information and communication technology such as the Ministry of communication and information, the Ministry of defence, the State Intelligence Agency, the TNI, the National Police, the State Cyber and Code Body (BSSN), Immigration, customs, BNN, BNPT, BAKAMLA and so on, must be integrated into a connected cyber technology system. These special institutions can also be integrated with the early detection system of the TNI and Indonesian Police in the regions and related institutions according to the principles of equality in the effort to defend the country. The early detection system of the Indonesian Intelligence and Territorial range in particular the existence of intelligence and territorial nets can be developed through military operations other than war (OMSP). In the details of the tasks of the TNI for CSOs, the defence area empowerment operation (*Opsdayawilhan*) is regulated which gives the opportunity to involve experts in the information field.

d. Technology and Support Infrastructure Aspects: -

Technology and supporting infrastructure are needed as facilities and equipment for integrated defence activities facing information warfare in the digital era. A fundamental weakness in the aspect of national cyber defence technology is the limited number and quality of technological equipment and the difference in quality as a result of

the presence of the manufacturer and the origin of the product being purchased. According to the Commander of the TNI Cyber Unit, Rear Admiral TNI *Markos* in a follow-up interview with the author on 12 January 2019, that the procurement of TNI military equipment is still being developed in accordance with technological advances and the country's financial capacity. In addition, the procurement process must also be more careful because differences in manufacturers and national origin can also affect the interconnection ability between all other equipment. In the midst of the condition of national information technology capabilities which are still weak, every relevant state institution and non-state institutions that have high information security risks need to place the development of aspects of information technology as a priority. However, the development of technological aspects itself does not guarantee the realization of the ability of the state to face information warfare. Infra support structures such as integrated operation control centres and connected information networks are also needed. In the Presidential Regulation Number 97 of 2015 concerning national defence policies, it is explained that the form of threats that develops must be the main basis in the preparation of the design of the national defence system. In the presidential regulation the current and future forms of threats are classified into 3 (three) types, namely (a) military threats both armed and unarmed, (b) non-military threats and (c) hybrid threats. A hybrid threat is a mixed threat that is integration between military and non-military threats. Hybrid threats include combining conventional, asymmetric, terrorist and cyber warfare threats, as well as criminals. Hybrid threats can also be in the form of integration of attacks between the use of chemical weapons, biology, nuclear and explosives (Chemical, Biological, Radiological, Nuclear and Explosive / CBRNE), with information warfare through information media. Therefore, the development of information technology as a means of national defence must also be followed by the development of legal aspects, HR and operational strategies. Realizing this, the Ministry of Defence of the Republic of Indonesia has compiled a 2004 military non-military defence manual.

e. Strategy Aspect of Defence Operation: -

Information war in the digital era has a broad spectrum of threats and multi-dimensional impacts. Knowledge of the dangers of information war actually has been widely known to the public but integrated efforts to deal with the threat of war have not become a real national awareness and initiative. The national strategy for cyber defence is still in the stage of reviewing and formulating policies so that the state does not yet have a standard strategy to deal with the threat of information war that can come suddenly. This is reflected in the non-military defence strategy manual (Ministry of Defence, 2016) which basically explains defence strategies in general facing non-military threats but has not yet studied specific strategies for dealing with information war or cyber war. Faced with a threat perspective in the era of information technology with its multidimensional patterns and impacts, the need for the implementation of a universal defence system is actually increasingly needed. Therefore, it is necessary to immediately formulate an appropriate strategy to deal with any possible threat of information warfare adapted to the national defence system, namely the universal defence system.

Access to information war covers aspects of political, economic, socio-cultural, national security and defence. Therefore, strategies to deal with information warfare must also be based on the concept of integrated operations. The integrated operation strategy in question is an integrated information operation which is a form of resistance based on mobilizing all national potential for information warfare. Operations against information warfare are realized through the involvement of all national potential and resources, both technological aspects and legal, political and human resources (HR) aspects. This was justified by the Director of Components of Support for the Ministry of Defence Tristan Soemardjono in a repeat interview with the author on March 28, 2019 that in the future, the empowerment of human resource potential should be extended to areas of expertise that are in line with the needs and interests of national defence. The same thing was also conveyed by the Head of the TNI Headquarters Maj. Gen. Sisriadi who stated that the empowerment of the millennial generation of ICT experts was the right strategy because as previously explained that when talking about information warfare it was related to information and information. Informatics concerns the network and information technology while the information itself is the content or content of the message delivered.

SWOT Analysis Defence Strategy to Face Information War: -

a. Strength Analysis: -

1. The development of information and communication technology resources in Indonesia is quite rapid and supported by the development of human resources sources that have the ability of information and communication technology have become a distinctive force for Indonesia in the framework of implementing integrated strategies to face information warfare in the digital era.

2. Information and electronic transactions (ITE) acts. With the enactment of the Act and other supporting regulations, it will become a legal basis and is expected to facilitate the implementation of integrated cyber defence. Even though it hasn't completely fulfilled all aspects needed in cyber defence, at least it has become a first step and gives significant strength.
3. The concept of national defence. Through the current national defence doctrine and strategy that is owned by the universal defence system, it will become a guideline and basis that directs or facilitates the development and development of integrated cyber defence systems.
4. The existence of government institutions such as the military, police and law, regulators, intelligence elements, elements of technology users, academics, business elements and community elements, both organized and talented individuals, are potential strengths that can be relied upon.

b. Weaknesses Analysis

1. Low awareness of the need for strong national cyber defence.
2. Initiatives to handle threats of uninformed information attacks.
3. Lack of budget or financial support.

c. Opportunity Analysis

1. International cooperation. Good relations with friendly countries are supported by the active involvement of Indonesian government institutions in the activities of the world's cyber organizations to provide opportunities to support the development of cyber defence in Indonesia.
2. The development of information security technology is also quite rapid in Indonesia so that it can be empowered in the face of information attacks.
3. The policies and steps of the Indonesian Ministry of Defence which have prepared state defence cadres through recruitment, training and briefing awareness of defending the state from various components of society.

d. Threat Analysis or constraints

1. Countries that have conflicting interests with Indonesia. A country like this must be wary because it does not close the possibility directly or indirectly, openly or closed, it will support an organization or individual to foil strategic plans for the interests of Indonesia. Examples of espionage disorders.
2. Terrorists are traditional enemies of all nations and countries.
3. Industry spies and organized crime groups
4. *Hacktivists*. usually forming small populations, including foreign hackers who participate in politics with anti-government motives.
5. Hackers (Hacker), if the existence of these hackers is ignored, it can be a serious threat to the interests of the community, nation and state.

Conclusions And Suggestions:-

Conclusions: -

1. The policy or regulation also shows that the issue of national defence is not the duty and responsibility of the government and its devices but is the duty and responsibility of all components of the nation. However, this system has not run optimally due to the lack of strong national initiatives to build integrated defence systems and the weak regulatory aspects at the operational level. The act derived from Act Number 3 of 2002 has not even been made entirely as a law on the components of reserves and defence support, so that the mandate of the law on universal defence cannot be realized.
2. The current national defence strategy that prepared by the Ministry of Defence has been designed to deal with military threats and non-military threats (physical and non-physical threats). However, the defence strategy facing the non-military threat that is currently seen as more dominant is still general, not yet accompanied by the determination of the standard strategy to face information warfare in the digital era. Gradual efforts have indeed begun to be compiled and implemented in stages by certain ministries and institutions such as the Ministry of Communication and Information, Ministry of Defence, TNI and Police, but these efforts are still sectorial, have not been coordinated and have not accommodated all defence needs in the information war era. Real efforts that have been implemented by relevant ministries and institutions are still in the level of internal efforts such as the development of technological aspects followed by the development of awareness-based Human Resource capabilities

Suggestion: -

The strategy of cyber defence operations developed by the Ministry of Defence as well as being the basis for the development of TNI cyber units needs to be formulated more specifically integrated with the role of the Indonesian Public Relations and Information Agency and all providers of information media services to accommodate all modern defence needs while referring to the universal defence system. up to now. The national defence doctrine facing information warfare is suggested to be immediately realized by the TNI as a guideline for all levels of the TNI in carrying out information operations while still referring to the universal defence system.

Bibliography:-

1] Carling,P. 2016. Detect, Distrut, Deter : Whole of Goverment Approch to National Security Cyber Threats. Journal.
2] Kemhan RI. 2008. Buku Putih Pertahanan Negara. Kemhan Jakarta.
3] Kemhan RI. 2014. Peta Jalan Pembinaan Kemampuan Sumber Daya Manusia Pertahanan Siber.Kemhan Jakarta.
4] Naskah Akademik Grand Design Satuan Siber TNI; Satsiber TNI; 2017.
5] Peraturan Menteri Pertahanan RI nomor 32 tahun 2016 tentang pedoman pembinaan kesadaran bela negara.
6] Rangkuti,F. 2003. Analisis SWOT, Teknik Membedah Kasus Bisnis. Gramedia Pustaka Utama. Jakarta.
7] Sudjarwo,MS. 2001. Metode Penelitian Sosial. Mandar Maju. Bandung.