Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/9061
DOI URL: http://dx.doi.org/10.21474/IJAR01/9061

RESEARCH ARTICLE

THE STRATEGY MODEL OF ALTERNATIVE STATE DEFENSE SYSTEM FOR FACING 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:-
Strategy model, alternative, state defense syste, war, digital era.

Abstract

The purposes of this study is arrage alternative strategies for national defense systems that can be applied today to deal with 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 Defense of the Republic of Indonesia (*Kemhan RI*) specifically the General Director of Defense Strategy (Directorate General of *Strahan*), Directorate General of Defense Potential, data and information centers as well as cyber defense centers and at the Central Information and Communication Republic of Indonesia Ministry of Defense. In addition, the location of the study was also determined at the TNI information center (*Puspen TNI*) and the Military Cyber Unit Office (*Satsiber*), the TNI Staff Commander's Office and the Indonesian Army Territorial Center which had been tasked with preparing the region or region as the basis of the universal defense. This research is conducted in November 2018 until March 2019. This study uses a qualitative descriptive method with observation and deepening of the material for quite a long time. The result of this study are the formation of augmentation strategy.

……………………………………………………………………………………………………....

Introduction:-

Cyber space which supported by digital information media has now become a new arena of war between countries and non-countries. The choice of such a way of war is influenced by the level of risk of smaller losses for the attacker with the risk of heavy losses to the party being attacked. With a broad and fast spectrum of attacks, information warfare in the digital era can attack two targets at once, such as the installation of information and the joints of the life of the nation and state. The operation of information through message engineering, agitation and propaganda and war of opinion, is an old strategy in the history of war, but with the rapid advancement of information technology in the present, information operations are increasingly effective in destroying the national security of a country. Information warfare in the digital era with its multidimensional impact cannot be faced by one party or just one strategy but requires an integrated approach that includes technological aspects, political and legal aspects, as well as integrated deployment of national resources.

Indonesia's national defense system has actually been referring to the principles of integration in the national defense strategy as stipulated in Act No. 3 of 2002 concerning the Universal State Defense System. This system requires the

Corresponding Author:-Heriyadi.
Address:-Postgraduate student of brawijaya university.

support of all national potential and resources in the effort of national defense. However, the universal defense system has not been able to run optimally. Based on the SWOT analysis, Indonesia has a superior factor that can be developed to deal with information warfare in the digital era, including Act No. 3 of 2002 concerning the universal state defense system and Act No. 34 of 2004 concerning the TNI (Indonesian National Army). In the TNI Law it is specifically regulated by the task of Military Operations Other Than War (OMSP) in which the defense area empowerment operations are listed. In addition, the Electronic Information and Transaction Act (ITE) has also been implemented as well as several regulations regarding the development of cyber defense systems issued by the Ministry of Defense. Another advantage that can be developed is the development of information technology in Indonesia which is quite rapid accompanied by a very large number of digital media users that can be developed as part of integrated Human resource of cyber defense. However, Indonesia also has a number of obstacles or weaknesses that must be eliminated including the lack of encouragement or public pressure to trigger national initiatives to develop integrated cyber defense systems. In addition, the Act related to the national defense system has not been followed by strong regulations at the operational level so that the principle of integrated defense cannot be realized optimally. The weak awareness or understanding of some citizens towards the importance of information security in the digital era is also an obstacle that must be immediately found a solution.

Efforts to develop the potential for excellence and eliminate weaknesses or obstacles in the face of information warfare in the digital era have been initiated by the Ministry of Defense of the Republic of Indonesia, but these efforts are certainly not effective enough if they are not supported by stronger regulations at the operational level. For this reason, this study examines and formulates alternative strategies that can be taken to deal with information warfare in the digital era in the midst of still weak regulations and still a lack of state capabilities in the field of information technology. The alternative strategy in question is an augmentation strategy or power multiplication that is realized through the involvement of all potential Indonesian Human Resources who have special expertise in information technology as an agent of national defense in information warfare. This strategy can be realized through several patterns; through personnel recruitment for cyber and Ministry of defense and TNI units, strengthening military cooperation with digital social media service providers or through involving cyber communities as intelligence information networks and TNI territorial units. In addition to this pattern, millennial generation with special cyber capabilities can also be placed as agents who move independently in an integrated information operations management. All of that certainly requires strong regulation to support the realization of an integrated and integrated defense system in the face of information warfare in the digital era.

Research purposes:-

Based on the above background, the research objectives are as follows;
What alternative strategies for national defense systems that can be applied today to deal with 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 Defense of the Republic of Indonesia (Kemhan RI) specifically the General Director of Defense Strategy (Directorate General of Strahan), Directorate General of Defense Potential, data and information centers as well as cyber defense centers and at the Central Information and Communication Republic of Indonesia Ministry of Defense. In addition, the location of the study was also determined at the TNI information center (Puspen TNI) and the Military Cyber Unit Office (Satsiber), the TNI Staff Commander's Office and the Indonesian Army Territorial Center which had been tasked with preparing the region or region as the basis of the universal defense. 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 defense expert, 1 of legislative official involved in the formulation of national defense policy, 5 of related officials in the Ministry of Defense, 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 analyzed using Descriptive-Qualitative analysis techniques. Data analysis will be carried out by referring to Sudjarwo's (2001) opinion, 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.

Research Result And Discussion:-

Data Analysis: -

Steps to Develop Information War Capabilities that have been achieved by the Indonesian Ministry of Defense at this time: -

The development of national defense capabilities in the face of information warfare in the digital era has not yet become a coordinated national initiative. The implementation steps are still sectorial based on their respective interests and abilities. In addition, capacity and deterrence and countermeasures from each of the stakeholder institutions in the field of information and communication are still weak, making them very vulnerable to massive attacks. The Minister of Defense's policies, especially those related to strategies to deal with information warfare, basically refer to the 5 (five) cyber security policy agenda of the Ministry of Communication and Informatics, namely Capacity Building, Policy and Operational Framework, Organizational Structure, Technical and Operational Measures, and International Cooperation.

In the roadmap of Human Resource defense capabilities development (Kemhan 2014), several targets will be achieved from the formulation of a Human research cyber defense capability development roadmap, including awareness about the importance of developing human research defense capabilities, establishing partnerships with all stakeholders. Cyber defense, the willingness of all parties involved in the preparation of Human research cyber defense and the human resource capacity of as a part of the national defense system. Conceptually, the design of national defense strategy in the face of information war has been formulated by the Indonesian Ministry of Defense since 2014, but factually policies or regulations that specifically regulate the empowerment of national resource potential as part of supporting components of national defense have not been regulated by the government. The limitation of the regulatory aspect is an obstacle for the Ministry of Defense to realize an integrated defense strategic plan into a defense system capable of facing the threat of information warfare from various aspects. However, the initiative towards the realization of cyber defense strategies has been carried out by a number of agencies, institutions and business entities including the Ministry of Communication and Informatics established the Indonesia Security Incident Response Team Ion Internet Infrastructure (ID-SIRTII) since 2007, then the country's password institutions have ICT unit specializing in Human Resource development related to Signal Intelligence. Furthermore, the State Intelligence Agency and the Strategic Intelligence Agency also have special units in ICT security related to Signal Intelligence, and the Ministry of Defense and the TNI have also had the initiative to build cyber power even though it is still in the process of developing gradually from the equipment and HR aspects. Some ICT communities outside government institutions have also been established including Indonesia Computer Emergency Response Team (ID-CERT) which was established by the Indonesian ICT community in collaboration with CERT in several Universities, such as ITB, UI, UGM and ITS. In addition, several Business Entities also began to implement information and communication network security standards in accordance with SNI 27001 standards including PT. Telkom, Bank Indonesia and the Oil and Gas Industry. (Study of cyber defense organizations; Ministry of Defense 2013)

The steps of organizational development have been initiated by the Ministry of Defense by empowering data and information centers and Cyber Defense Centers, as well as TNI institutions that have established new organizations called TNI cyber units which are the development of information technology installations that were previously owned by the information center and data processing of TNI Headquarters. But the cyber institutions are still in the form of adding cyber defense tasks and functions into the existing organizational structure of the Ministry of Defense and the TNI. Institutionally, cyber defense organizations have not supported the specific needs of cyber defense strategies. In this regard, the Ministry of Defense will try to put in place a larger and substantive human resource improvement program in the cyber defense capacity building program in the coming years as stated in the roadmap for developing Human Resource defense capabilities (Ministry of defense, 2014).

Looking at various policies at the ministry of defense, it is seen that the direction of human resource development is more on increasing internal capacity of Human resource or employees who already exist in the Ministry of defense and TNI work units. The strategy of multiplying power through the empowerment of cyber communities and other young people who have information technology expertise, has not been specifically described in the policy. In fact, in the strategic arena, the empowerment of the millennial generation in the efforts of national defense has actually been accommodated in general in Act number 3 of 2002 concerning national defense.

Priorities for Developing Defense Capabilities of Facing the Information Wars in the Digital Era: -

1. Encouraging the Government and Parliament to formulate and ratify regulations at the operational level of the universal defense system as a basis for formulating strategies to deal with information warfare in the digital era.
2. Encouraging the realization of interoperability Cyber Defense Operations as part of an alternative strategy to face information warfare in the digital era.
3. Develop security systems for installations in the national cyber space through the transfer of knowledge and information technology as well as strengthening the role of government and private public relations and information to ensure the availability of information for the community, nation and state.
4. Building an organization or institution that enables the realization of information security system governance in an integrated manner.
5. Encourage media literacy education and training programs, cyber security awareness and the initial ability to defend the country.
6. Establish international cyberspace security cooperation.

Technical Steps for Developing Capabilities and the Integrated Strength of Facing Information War in the Digital Era: -

The technical steps for developing alternative strategies as part of the national defense strategy can be taken through the following steps:

1. Realizing the legal protection of national resource reserves or management components, the legal protection of the National Cyber and Cyber Code Agency, as well as regulation on the involvement of digital media service providers in efforts to defend the country against information warfare.
2. Formulate and alternative strategies to deal with information warfare in order to strengthen weaknesses in technological aspects and law enforcement, along with the preparation of standard operating procedures (SOPs), recruitment and human resource development including involvement of media service providers.
3. Socialize all existing regulations and operational strategies including the rules of engagement to all relevant parties.
4. Ensure the realization of information installation security capabilities through professional HR recruitment, preparation of implementation instructions and operating technical instructions and installation security, as well as determining alternative ways of acting to ensure that the information supply for the community continues to flow in the event of an installation disruption.
5. Establishing a national cyber committee that acts as a coordinator or leading sector of all government institutions and private institutions, develops standard operating procedures and rules for involving supporting components of national cyber operations.
6. Realizing the synergy of the role of related institutions in order to increase internal capacity and responsibility for compiling digital media literacy materials, developing media literacy skills, developing information security awareness in digital media and developing awareness of defending the state in the community including cyber communities and information technology experts.
7. Realizing international cooperation in order to increase internal capacity to face threats and strengthen cooperation in detecting, eliminating and long-term cooperation in facing threats in the cyber space.

The Urgency of Alternative Strategies for the State Defense System Proposed in the Face of Information War in the Digital Age: -

a. The concept of alternative strategies (augmentation strategies): -

This alternative strategy proposed is an elaboration of integrated defense doctrine, called the strategy of multiplying strength (augmentation), will play an important role when the country is faced with threats that are proxy or hybrid, which emphasize non-military threats. The development of this strategy is needed in view of the non-military threat, which has characteristics that are different from traditional threats so that it requires a pattern of handling and approach in accordance with the nature and form of threats. Especially in the era of globalization where the practices of hegemony, economic pressure, epidemics, natural disasters, cultural penetration and information attacks are tangible forms of non-military threats that can endanger the sovereignty and safety of the state.

The augmentation strategy developed was a form of defense operation against information warfare. The strategy of "Opposing information warfare operation" is essentially a multiplication of forces, intended to cover weaknesses in technology-based defense strategies and law enforcement. The augmentation strategy will focus on efforts to deal with the threat of information warfare in the digital era by involving human resources with special expertise in information technology or cyberspace. It is important to understand as also explained earlier that information warfare is not always purely a non-military threat but can be a combination of military threats and non-military threats so that augmentation strategies should be positioned as strengthening aspects of military defense and legal, political and international cooperation approaches.

b. Implementation of the Augmentation Strategy Facing Information War in the Digital Age: -

The augmentation strategy is based on the results of a study of the development of the use of digital information media as a tool to fight with all its multidimensional excesses. The Augmentation Strategy (Strength Multiplication) means that in the face of threats and attacks of information, it means that in addition to being needed an implementing agency that is the spearhead of cyber defense also requires coordination and cooperation with other parties, both between government agencies and cyber agencies or collaboration with Quadruple Helix such as Government, Academics, Industry (companies), and cyber communities. Coordination and close collaboration with other parties is called the augmentation strategy or the multiplication of forces in the face of threats and cyber-attacks. The augmentation strategy can be coordinated by the Ministry of Defense, TNI and POLICE ranks, realized by means of interconnection and interoperability. Interconnection has the meaning of connection between one implementing agency and other bodies and with the entire community engaged in the same field. In order to guarantee the interconnection and interoperability of various critical information infrastructures, it is necessary to standardize devices or protocols and HR expertise used by each element or component.

The implementation of augmentation strategies, especially in the development of standardization towards interconnection and interoperability of operations against information warfare, is the party that needs to be involved, including:

1. Cyber agency and country code, Ministry of Defense, Ministry of Communication and Information, TNI, Police, BIN and BAIS.
2. Higher education, industry / private companies / BUMN and other strategic industries.
3. Cyber communities, independent hackers and other young people who have cyber expertise.

Augmentation strategies can also be carried out through the development of Military Cooperation with Digital Media. This strategy is limited to collaboration between digital media operators and digital information media service providers with Military Public Relations institutions. That is, the augmentation strategy includes 2 (two) engagement targets, that are cyber community or individuals who have special expertise in cyber and digital information media actors including social media operators and social media service owners who work professionally. The efforts developed include national policies related to the involvement of millennial generation (cyber communities and individual cyber experts) and steps of military cooperation with managers of digital media services. Military cooperation with digital media service providers can be in the form of rapid information reports if there is content or messages circulating through digital media that are considered to threaten the interests of the state and society.

c. Targets to be achieved in the Development of an Augmentation Strategy for Information War: -

1. Ensure the availability of correct, accurate and fast information.
2. Increase national resilience to attacks in cyberspace or cyberspace.

3. Ensure that the implementation of government information systems is safe and resistant to attacks on cyber shutter so as to reduce the impact.
4. Increasingly strong understanding of all parties to the current situation and conditions related to the threat of information attacks or cyber warfare, especially in the national defense sector, including how to handle it.
5. Awareness of the importance of integrated cyber defense systems in the context of securing information resources in both the defense sector and national critical infrastructure.
6. The involvement of all parties involved fully and integrated in a defense initiative facing information warfare in the digital era.

d. Method Used: -

The information operation method that can be done by each component involved in this augmentation strategy is to prepare defensive and offensive methods (attack or counterattack). In implementing a defensive strategy involving scattered resistance agents, the establishment of a Security Operation Center (SOC) is required, namely an information network as one of the critical infrastructure for information exchange pathways to recognize all kinds of illegal activities such as hacking attacks, malware, spyware, trojan and so on. Offensive methods implemented in the augmentation strategy can also be done through patterns of exploitation operations, Special Cyber operations, Operations support for Intelligence and operations Information both statically and mobile, involves elements inherent in the government as the main component and millennial generation cyber community as a supporting component of offensive action. However, the implementation of an offensive strategy is an option that must be thoroughly considered, both in terms of law and diplomacy and the whole process is clandestine (closed and confidential) activities using unique encryption that is not owned by other entities.

e. Outcome Development of Alternative Strategies to Face Information War in the Digital Age: -

It is widely known, the expected outflows from the implementation of the augmentation strategy include:

1. National resilience from aspects of information or cyber material is more resilient, able to detect sources of threats before passing a critical point and capable of counterattacking.
2. National defense and critical infrastructure information resources are protected from cyber-attacks.
3. Integrated operations against information warfare capable of deterrence, prosecution and recovery.
4. Able to strengthen the resilience and national resilience of the Indonesian nation from the possible threat of opinion war which divides unity. False information (hoax), agitation and propaganda through digital social media can be eliminated within the boundaries that do not disrupt the national security of the Indochinese nation.
5. Realized the basis of integrated and connected information war defense and based on digital media users so as to be able to address the threat of multidimensional information attacks.

Conclusions And Suggestions:-

Conclusions: -

The implementation of this augmentation strategy is carried out through the empowerment of cyber communities and other millennial generations who are specifically capable of information technology and the involvement of digital media service providers as agents of resistance to information warfare. Military cooperation with the media, especially the manager of digital media services, is also part of an augmentation strategy to multiply the power to face information warfare. However, this alternative strategy can only be realized if it is supported by strong regulations, especially the rules for involving citizens in efforts to defend the country both as the main component and as a supporting component and reserve component. The involvement of cyber communities and the millennial generation with special capabilities in information technology can be done through a pattern of recruitment as an employee or cyber soldier (main component), or placed as an information and communication network for the intelligence and territorial units of the TNI, can also be positioned as experts / consultants in ministries and institutions related countries, or made as freelance agents who move independently under the control of a cyber-operations management and information operation in the TNI and State Intelligence (supporting and reserve components).

Suggestion: -

In order to realize an integrated defense pattern (Augmentation) it is recommended that the government and the House of Representatives immediately formulate and ratify the Act that concerning reserve components and supporting components as part of a universal state defense system. Plans for submitting the PSDN Bill are suggested to be able to accommodate backup and support components, so that they become a strong basis for the implementation of augmentation strategies in the efforts of national defense in the digital era. The involvement of the millennial generation that has expertise in information technology, either directly or indirectly in integrated defense systems, will provide an outcome in the form of resilient national endurance support.

Bibliography:-

1] Kemhan RI. 2013. Kajian Organisasi Pertahanan Siber. Ditjen Pothan. Jakarta.

2] Kemhan RI. 2014. Peta Jalan Pembinaan Kemampuan Sumber Daya Manusia Pertahanan Siber.Kemhan Jakarta.

3] Sudjarwo,MS. 2001. Metode Penelitian Sosial. Mandar Maju. Bandung.