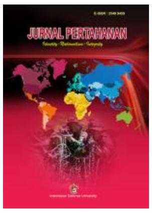
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



THE CHALLENGES OF THE TECHNOLOGY 4.0 AND INFORMATION TECHNOLOGY WITHIN TOTAL WAR STRATEGY STRUCTURE

Ruslan Arief[1], Helda Risman[2], Rudy Sutanto[3]
Indonesia Defense University
Salemba Raya Street 14, Central Jakarta, DKI Jakarta, Indonesia 10430
ruslaarief01@gmail.com[1], rismancan@gmail.com[2], rudi.sutanto071@gmail.com[3]

Article Info

Article history:
Received : December 17, 2020
Revised : April 26, 2021
Accepted : April 26, 2021

Keywords:
Information Technology,
Technology 4.0,
Total War Strategy,
Strategic Environmental

DOI:
http://dx.doi.org/10.33172/jp.v7i1.1099

Abstract

The development of information technology has a significant impact on various important aspects of life. Apart from positive impacts, there are also negative impacts that are important to know and anticipate to prevent major damage and losses. On a broad scale, namely at the national level, the development of information technology can also affect the development of national defense as it is known that the nature of Indonesia's defense is total defense, which is prepared to face the total war. Based on the explanation above, the purpose of this study is to examine the impact of the development of information technology on the implementation of Indonesia's total war strategy. The approach used is qualitative phenomenology with research data in the form of secondary data collected using literature studies. The data is then analyzed using qualitative analysis techniques. The results of the study indicate that the development of information technology has both positive and negative impacts. These impacts encourage the need for changes and adjustments to the total war strategy implemented by Indonesia. This is important to do so that Indonesia can have a stronger defense in preparation for a total war that may occur in the future.

INTRODUCTION

The development of information technology is something that cannot be avoided because it occurs along with changes in human wants and needs. However, information technology which is increasingly advanced and developing has various impacts, which are not only positive but also negative.

Information technology enables access to information in a much more effective and efficient manner than before. This is one of the positive impacts of advanced information technology that encourages easier implementation of various human jobs. Besides, technology also facilitates social interaction between people, which makes time and distance no longer an obstacle to building a relationship (Ngafifi, 2014).

The negative impact of the development of information technology is no less significant than the positive impact felt by humans. First, information technology is said to be the main factor causing the breakdown of relationships between family members because each member is busy with his virtual world, thus ignoring closeness to family. Second, the occurrence of moral decline in the nation's generation is also indicated due to the misuse of information technology (Yusuf, 2016). Third, there are various types of security threats launched using increasingly advanced information technology (Arianto & Anggraini, 2019).

Threats that arise from the misuse of information technology are classified into types of cyber threats, which underlie the emergence of various types of crimes in cyberspace that are intangible or invisible. Nonetheless, the losses caused by the crime proved to be enormous (Arianto & Anggraini, 2019). To overcome potential crimes through misuse of information technology, the government has enacted a law regulating the use of information technology in Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT Law). Although there is no specific explanation regarding cybercrime, the law describes its anatomy, which can be used as a basis for categorizing the types of cybercrime.

The first category is crimes that target internet systems, computers, and networks. These crimes can be in the form of illegal activities as follows (Prahassacitta, 2019):

Table 1. First Category of Cyber Crime

Article	Types of Crime
30	*Hacking*
31	Illegal interception
32	*Defacing*
33	*Interference*
34	Facilitating criminal acts
35	Identity theft

Source: Processed by Authors, 2021

The second category of cybercrime is the activity of using the internet, computers, and networks as a means of committing crimes, namely by uploading destructive illegal content. The types of content according to the EIT Law, among others:

Table 2. Types of Illegal Content in Second Category of Cyber Crime

Article	Types of Illegal Content
27 (act 1)	Pornography
27 (act 2)	Gambling
27 (act 3)	Slander
27 (act 4)	Blackmail
28 (act 1)	Fraud
28 (act 2)	Hate speech
29	Threats of violence to others

Source: Processed by Authors, 2021

The misuse of information technology is increasingly dangerous so that the scale is not only at the level of ordinary cybercrime but has escalated and has the potential to create a global scale cyberwar. Thus, it is not only individual interests that will be affected due to the misuse of increasingly advanced information technology, but also interests and security at the national level. (Rahmawati, 2017).

The echo of cyberwar has been buzzing for the past decade. However, the real damage caused by cybercrime which became the origin of cyberwar has only been felt massively in recent years. However, the Indonesian government has recognized the dangerous seeds of misuse of information technology for a long time. This is as stated by Soewardi (2013) that Indonesia needs to immediately build a formidable cyber defense due to the development of information technology that has the potential to be used as a tool for global scale crimes.

As it is known that the Indonesian defense system is total in nature, namely by involving the roles of all defense components, starting from the human resource component which includes the Indonesian National Armed Forces (*Tentara Nasional Indonesia* or TNI) to the entire Indonesian people; regional components, as well as other resource components that can be empowered to defend the country's sovereignty. It can also be said that total defense is a combination of military and non-military defense. The main purpose of total defense is to support a war that is also total in nature (Lebo & Anwar, 2020). Thus a line can be drawn connecting the development of information technology and Indonesia's total war. Increasingly sophisticated information technology will have an impact, either directly or indirectly, positively or negatively, on how Indonesia arranges its defenses to prepare itself for total war.

Based on the overall explanation above, this study is conducted to examine the influence of the development of information technology on the implementation of Indonesia's total war strategy. The analysis is carried out to find and describe the various positive and negative impacts of the development of information technology that need to be considered in the formulation and implementation of strategies to prepare Indonesia for a total war that might occur in the future.

METHODS

This study is a qualitative phenomenology type. Qualitative research can be understood as research that examines natural phenomena to be interpreted narratively by referring to the researcher's point of view as the main research instrument (Anggito & Setiawan, 2018). A phenomenological approach is a research approach that offers procedural implications to be able to get the correct interpretation of the phenomena studied in the research. Through this approach, the reality that is the natural background of research can be understood as it is (Farid & Adib, 2018). This type of phenomenological qualitative research was chosen by the author to be able to understand and narrate the development of information technology and its influence on the total war strategy adopted by Indonesia.

The data used in this study is secondary data, which is data that has been documented so that researchers can collect it without directly interviewing research informants (Siyoto & Sodik, 2015). The secondary data of this research is all information related to the development of information technology and Indonesia's total war strategy.

The research data were collected using literature studies, namely by tracing information, whether it is published in books, journals, or news reports. The data were then analyzed using qualitative techniques, which consist of five stages, namely reviewing the entire data, data reduction, data categorization, checking the validity of the data, and interpreting the data (Moleong, 2018).

National Defense

Etymologically, the word defense comes from the original word ‘resilient’, which according to the Big Indonesian Dictionary, means “remains in its state (position and so on) despite experiencing various things (influenced by many factors); does not change quickly; or strong or able to endure something”. Based on the meaning of the original word, defense means to defense; defense of one thing (country or other matter); a place (in the form of a fort or stronghold) that is used to defend oneself or against attacks coming from outside. Furthermore, from the meaning of defense, by the context of this study, the meaning of national defense is obtained as all efforts to prevent and fend off opponents, protect and defend national interests against all kinds of coercion by force and attacks from other parties.

Based on the etymological meaning above, it can be concluded that defense includes efforts, methods, capabilities, and systems and structures that allow self-protection from attacks and prevent negative impacts from the result of aggressive actions from other parties. In the national context, defense is not only sufficient in the actions taken to defend the country but must achieve a state of being able to realize these actions effectively so that the national interest is truly protected from various potential threats.

The definition of national defense according to Article 1 act 1 of Law of the Republic of Indonesia Number 3 of 2002 concerning State Defense (hereinafter referred to as the Law on 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 threats. Disturbance to the integrity of the nation and state. Furthermore, Article 2 also explains that the nature of national defense is the total defense which is implemented based on awareness of the rights and obligations of citizens as well as confidence in their strength.

National defense can also be interpreted as the dynamic condition of a country that has national capabilities and strength based on the overall integration of all aspects of the nation, which can be empowered to protect all the interests of the nation from various threats that come from within or from abroad, which are launched directly or indirectly. With the existence of national defense, state security can be protected so that various important processes can be carried out optimally to achieve the nation's goals (Pranowo, 2010).

By its meaning, the purpose of national defense is basically to protect the security of the interests of all parts of the nation. This protection can be in the form of anticipatory efforts to prevent the realization of potential threats becoming real threats, as well as efforts in the form of handling to overcome threats that already have a perceived damage impact (Pranowo, 2010). If referring to the Law on National Defense, the objectives of national defense can be categorized into several points as follows:

1. We are ensuring the integrity and upholding of the Unitary State of the Republic of Indonesia based on Pancasila and the 1945 Constitution.
2. Supporting the implementation of the functions of the state government to realize one national defense unit to achieve national goals, namely to protect the entire nation and the entire territory of Indonesia, promote public welfare, educate the nation's life and participate in implementing world order based on independence, eternal peace, and social justice.
3. They are providing opportunities for every citizen to exercise their rights and obligations to defend the state as a reflection of national life which guarantees the rights of citizens to live in an equal, just, safe, peaceful, and prosperous manner.
4. Build, maintain, develop and use the national defense force based on the principles of democracy, human rights, public welfare, the environment, the provisions of national law, international law and international customs, and the principle of peaceful coexistence.
5. Maintain 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.
6. Realizing and maintaining the entire territory of the Unitary State of the Republic of Indonesia as one defense unit.

Following the Law on National Defense, the components of national defense are divided into three categories, namely the main component, the reserve component, and the supporting component.

1. The main component of national defense is the Indonesian National Army which is a special unit prepared to carry out defense tasks. According to Law Number 34 of 2004 concerning the Indonesian National Armed Forces (*Tentara Nasional Indonesia* or TNI), hereinafter referred to as the TNI Law, the TNI is a defense tool of the Unitary State of the Republic of Indonesia, serving as executor of state defense policy to uphold state sovereignty, maintain territorial integrity, and protect the safety of the nation, carry out

military operations for war and military operations other than war, and participate actively in regional and international peacekeeping tasks.

2. The reserve components of national defense are national resources that have been prepared to be mobilized to enlarge and strengthen the main components. The existence of this reserve component is very important because it is a component that will be a substitute for the main component if needed in certain circumstances. However, the specific stipulation has not been realized by the state. Guidelines that explain the reserve components are still in the form of the State Defense Reserve Components Bill, which was proposed as a mandate of the State Defense Law.
3. The supporting components of national defense are national resources that can be used to increase the strength and capability of the main components and reserve components. The definition of national resources, in this case, includes human resources, natural resources, and man-made resources. Natural resources include all the potentials contained in the earth, water, and aerospace, which in their original form can be utilized for the benefit of national defense, while artificial resources include natural resources whose usability has been increased for the benefit of national defense.

Total Defense System and Total War

The national defense system is the first dimension of national defense which consists of territorial and resource aspects. According to the territorial aspect, the national defense system includes a series of defenses that are developed in layers, namely defense in the Exclusive Economic Zone (EEZ), defense in jurisdictions (territorial waters), and defense in the deepest islands (Hikam, 2014).

1. Defense in the Exclusive Economic Zone (EEZ)

   Following international regulations governing state sovereignty in the sea area, namely the United Nations Convention for the Law of the Sea (UNCLOS), every country that has maritime boundaries is given the right to control natural resources in the sea area as far as 200 miles. From the baseline of the sea to the furthest region. This right is not a territorial right, but rather a right based on interests, so that countries that have an EEZ basically cannot claim the sea area in the EEZ as their territory, but have the right to defend the area to fulfill their interests. Given the richness of natural resources in the EEZ, the sovereignty of the state to control these natural resources needs to be maintained through safeguards carried out sustainably.
2. Defense in the Territory of Jurisdiction

   Jurisdiction or territorial waters is a benchmark used to measure the territory that becomes the sovereignty of a country. This area is measured from a distance of 12 miles from the outer point of the islands at low tide towards the sea. Territorial sovereignty applies from that point, starting from the sovereignty of the airspace above it, the seabed, and the land below, which is absolutely the property of the country concerned. Violation of these boundaries is considered a real threat to the country's sovereignty, which must be anticipated and overcome through the development of a strong defense.
3. Defense in the Territory of the Deepest Islands

   Defense in the deepest islands is the core of national defense because the region is located at the center of government and is a place for various important activities to take place that contribute to the sustainability and development of a nation. The deepest island area extends from the coastline to the entire land area owned by a country. Efforts to maintain security in this central region are a top priority that must be upheld to maintain the sovereignty of the state.

According to the resource aspect, the national defense system includes human resources, natural and artificial resources, and defense infrastructure. The three resources can be categorized into two components, namely the main component that refers to military forces, both land, sea, and air forces, which are specifically developed and empowered to defend the country; as well as supporting components including reserve forces, defense infrastructure, and militia obligations. All of these components form a total defense system of Indonesia, which is built and improved on an ongoing basis to deal with wars that are also total in nature (Lebo & Anwar, 2020).

RESULT AND DISCUSSION

Development of Information Technology and Its Use in Various Fields

Information technology was not created in prehistoric times, but the seeds of communication have begun to be etched at that time. As noted by historians, humans began carving on cave walls as a form of communication in 3,000 BC. Carvings made using animal horns form pictograph symbols that function like letters in the language of communication.

In the next period, humans began to create symbols that symbolized letters, and the media used to write these letters. The written media, which was originally in the form of rocks, was further refined in 500 BC by China in paper form. Writing equipment that became a form of early new technology was created around 1400 by Gutenberg in the form of a printing press for letter plates. In the following years, various other, more sophisticated equipment were made by engineers, ranging from telephones, televisions, computers to the internet (Lubis & Safii, 2018).

Along with the development of information technology, the benefits that can be obtained by humans are also increasing. It can even be said that information technology is one of the main facilities that humans need to carry out various important jobs. Without the existence of information technology, humans will certainly experience many difficulties in fulfilling their needs and desires (Rusydi, 2017).

The tangible form of the benefits of information technology can be felt by humans in various fields, starting from the fields of education, social, economy to supporting efforts to strengthen national defense. In the field of education, there are at least five fundamental changes in the implementation of teaching and learning activities through the application of the latest information technology, among others (Rusydi, 2017):

1. Change from teaching model from training to performance
2. Changing the place of teaching from classrooms to classrooms without rooms
3. Change from using paper to networking or online
4. Change from physical facilities to network facilities
5. Change from cycle time to real-time

Information technology provides means, such as telephones, computers, e-mail, the internet, and others, to increase the effectiveness and efficiency of the implementation of communication and interaction between teachers and students. By optimally empowering information technology, the interaction between parties involved in the learning process can be changed from a conventional model in the form of face-to-face to an online model, where teachers and students can be in far different places but can still carry out their respective roles. Besides, the need to obtain complete and easy information and knowledge is also facilitated by information technology which can become a very large information storage medium, which can be accessed easily and cheaply (Rosenberg, 2001).

The efficiency of the learning process makes the costs for learning activities much cheaper. Study materials that are stored and accessed online reduce the cost of printing books or study modules. Implementation of online learning reduces transportation costs that must be incurred by teachers and students, such as when doing face-to-face learning (Zulfah, 2018).

It can also be stated that the use of increasingly sophisticated information technology can encourage the increase in the quality of education evenly. Specifically, an information technology product in the form of the internet that can remove space and time limitations in learning activities becomes a medium that allows the subject matter to be shared with students who are in different places at the same time. Thus, it is not only students who are in areas with a complete educational infrastructure who can get quality learning. Students who are in areas with incomplete educational facilities can also get quality education by utilizing the existence of information technology (Husaini, 2014).

There are at least four forms of utilization of information technology for the development of the education sector, among others (Husaini, 2014):

1. Improved information management
   Information technology enables massive storage of information, as well as access to information easily and cheaply. This is very beneficial for the implementation of learning activities that require large amounts of educational information. Besides, information technology also enables information exchange to create equitable quality education. Broadly speaking, it can be stated that information technology allows easier management of information and can meet educational needs as a whole.
2. Online learning design
   As stated earlier, the existence of information technology enables distance learning via the internet, otherwise known as online learning. Apart from having a learning model that is far different from traditional learning, online learning also has enormous flexibility for both teachers and students in terms of knowledge exploration. Teachers no longer have limitations in terms of teaching materials to be delivered due to the availability of a large database that can be accessed online. Likewise with students who are no longer fixated on accepting the material presented by the teacher only but can freely explore various learning sources on the internet. Thus, information technology is not only used in the formation of new learning models but also in a more active and exploratory learning system.
3. Development of new learning media
   Learning media has a very important role in achieving the success of learning activities. Therefore, along with the increasingly intense use of information technology in learning, there is a development of learning media used, namely by integrating aspects of information technology in the form of learning media. The results obtained are in the form of new learning media that are more attractive and offer various advantages over conventional learning media. Broadly speaking, there are three forms of utilizing information technology in the development of learning media. First, information technology is used as a medium for delivering teaching materials to students, which is generally referred to as computer-based training or computer-assisted instructional.

   Teachers package teaching materials in a program that can be accessed by students using computer devices. In addition to delivering teaching materials, the program can also produce information on the development of student learning activities that are used as a basis for evaluating and assessing learning outcomes. Second, information technology is used as a medium for distributing teaching materials. This second utilization model is the same as the first model, which aims to facilitate the transfer of teaching materials from teachers to students. However, the procedure for the two models is different, where the first model uses a program that is run on a computer, while the second model uses the internet network. Teaching materials are uploaded to the website, then accessed by students via a web browser. Third, communication technology is used to facilitate teleconferences between related parties, namely teachers, students, and resource persons who become speakers in learning activities. This third model emphasizes the use of information technology in an effective and efficient communication process, which not only allows the delivery of teaching materials directly but also obtains feedback following the results of the teleconferences conducted.

4. Teaching life skills

   Along with the rapid use of information technology in all fields, almost every job requires the ability to operate information technology products. Therefore, mastery of information technology can be said to have become a very important life skill. The integration of information technology in learning activities has the potential to become a means of teaching life skills comprehensively and sustainably.

The benefits of the development of information technology in the social field are mainly in increasing the speed of information distribution needed to solve various existing social problems. The lack of clarity of information is the root of many social problems so that with the advancement of information technology, efforts to clarify and update information can be carried out very easily and quickly. This is the basis for the ease in solving social problems caused by errors in receiving information (Setiawan, 2018).

Besides, information technology is also an important factor that determines the increase in ease and speed of social interaction. Before the existence of information technology, the interaction between individuals could only be done in traditional ways, such as face to face or by sending letters. However, after the existence of increasingly sophisticated information technology products, interactions can be established more freely and flexibly (Setiawan, 2018).

Social changes due to the development of information technology can be broadly classified into three. First, changes in the structural dimension, namely changes that occur in the structure of society in the form of the emergence of new social roles, social class, and social institutions. Second, changes in the cultural dimension, namely changes in cultural matters that prevail in society in the form of innovation, diffusion, and cultural integration. Third, changes in the interactional dimension, namely change in the relationships that occur between individuals who are members of social society. Interactional changes can occur in terms of frequency of interactions, social distance formed in society, social intermediaries, rules and patterns of social interaction, and changes in the form of interactions (Martono, 2012).

The benefits of the development of information technology in the economic field are enormous. First, all economic activities require a flow of information that can meet development needs to achieve higher productivity over time. The existence of various information technology products facilitates this need so that the economic process can run much faster. Business actors can find out various changes in market demand quickly based on information accessed through various information technology products so that they can formulate the right production strategies (Burhan, 2018).

Another benefit of the development of information technology for the economic sector is in terms of developing the quality of Human Resources (HR) that can be carried out better. The transfer of science and technology becomes easier by utilizing information technology products to encourage the higher knowledge and ability of the community in carrying out various activities of economic value (Radhi, 2010).

The distribution of information that is getting cheaper, easier and faster has also become a big capital in the implementation of infrastructure development that supports economic activity. The existence of this infrastructure makes people more productive and can freely carry out economic activities to improve the quality of their lives. This is correlated with the increasing economy in line with the smooth running of activities in the economic sector carried out by the community (Wardhana et al., 2020).

The development of information technology not only brings changes on a small scale but also on a very broad scale. Apart from actually causing changes in the educational, social, and economic fields, the government can also use information technology that is increasingly developing to strengthen efforts to protect national defense from threats originating from within and outside the country (Susdarwono et al., 2020).

Threats to state sovereignty are currently monitored not only based on the source but also the form of threats which can be in the form of military or non-military threats. The dominant threats during non-war times like today are threats that are non-military in nature, mainly in the form of cyberattacks by utilizing the latest information technology products. Therefore, strengthening defense is also carried out by these types of threats, namely through the establishment of a cyber defense agency supported by policies and regulations regarding cyber defense.

According to the Regulation of the Minister of Defense of the Republic of Indonesia Number 82 of 2014 concerning Guidelines for Cyber Defense (Cyber Defense Law), the definition of cyber defense is an effort to tackle cyber attacks that disrupt the implementation of national defense. It also states that cyber-attacks are all forms of deeds, words, thoughts, whether done intentionally or unintentionally by any party, with any motive and purpose, which are based on electronic systems or their content (information) or equipment that is highly dependent on technology and networks on any scale, against vital and non-vital objects in the military and non-military spheres, which threaten the sovereignty of the state, territorial integrity and the safety of the nation.

Following those forms of cyber attack, there are several cyber defense targets set by the government, among others:

1. Increase understanding of the latest situation related to cyber threats
2. Formulate the most appropriate handling of existing cyber threats
3. Raising awareness about the importance of cyber defense as part of national defense
4. Increase the active participation of all elements of national defense in defending the country from cyber threats
5. Increasing the empowerment of all national resources in increasing cyber defense power
6. Formulate the most appropriate strategy to deter, act against and restore the cyber defense sector
7. Establishment of comprehensive cyber defense implementation guidelines

To achieve these goals, the use of various new information technology products is a necessity. Thus, the increasingly rapid development of information technology encourages the rapid development and strengthening of national cyber defense to respond to cyber challenges and threats.

Positive and Negative Impacts of Information Technology Development on the Implementation of the Total War Strategy

As it is known, the Indonesian defense system is known as a total defense system, which focuses on the involvement of all defense components, including human resources, territory, and various other types of resources owned by the state. The concept of a total defense system is also explained in Article 30 act 2 of the 1945 Constitution, namely:

> National defense and security efforts are carried out through the total people's defense and security system by the Indonesian National Army and the Indonesian National Police, as the main force, and the people, as the supporting force.

It is also explained in the Defense Law, that total defense is enforced by three components consisting of main components, reserve components, and supporting components. The empowerment of these three components to form total defense is basically a preparation for facing total war (Lebo & Anwar, 2020). The essence of total war is a war that occurs in all possible domains at a scale appropriate to the development of the existing situation. Total war can be in the form of war in the military or non-military realms so that it demands total defense power in these two domains (Putra et al., 2018). Concerning the development of information technology, the biggest threat that has the potential to be faced in a total war comes from cyber threats launched to destroy Indonesia's total defense force.

It can be said that the increasing cyber threat is a negative impact of the development of information technology on Indonesia's defense. Thus, the existence of cyber threats demands that a fundamental adjustment be made to the total war strategy adopted by Indonesia. The adjustment is meant by integrating aspects of information technology in all the forces forming the total defense.

Apart from having a negative impact, the development of information technology also has positive impacts on Indonesia's total war strategy. As mentioned by Lebo & Anwar (2020), that many parties master information technology, which can be used as executors of total defense, especially in the cyber domain. These parties can come from the community, which is the supporting component of total defense, as well as from the main defense component that is directed to become the implementer of cyber defense. In this case, it can be said that the empowerment of the main and supporting components is more optimal than before.

The existence of a cyber community originating from civil society, which has the potential to increase the power of total defense and become the vanguard in cyber warfare, shows an increase in the role and position of society from the supporting components that are behind the ranks of the main components in war, to being aligned with the main components in the cyberwar. As it is known, in open warfare, civil society is not directly involved but only becomes a supporting component of the TNI (Indrawan, 2015). However, in the realm of total war that is military but also non-military in nature, society can increase its position and role to be not only a supporter but also an important actor in open warfare in the cyber realm.

Optimization of this empowerment is based on the existence of a new threat model which is dominated by the cyber domain, which changes the defense paradigm from initially placing the main component as the main defense operator to empowering the community from the supporting components to participate in becoming one of the main defense forces.

The next positive impact is the presence of an event which is a strong reason to increase the integration of information technology into national defense. It can be said that this integration is a form of strengthening national defense in the context of facing total war because of the development of information technology which is the basis for the emergence of various new threats. Following the nature of the new threat which is dominated by the cyber realm, there is no better solution than to increase the integration of information technology into Indonesia's total defense system. This needs to be a major priority considering that the potential for cyber warfare is greater than armed warfare (Meiliyanti et al., 2019).

The integration of information technology in total defense can be done through several methods. First, by increasing the portion of the material on applicable information technology into the learning of the community or prospective TNI personnel at formal schools. This method can encourage the deepening of public knowledge and abilities related to information technology, which can be empowered by the state to strengthen total defense. Second, providing information technology training to TNI personnel who specifically handle cyber threats. This training is directed at achieving goals in the form of mastery of appropriate information technology by the development of cyber threats that are currently being faced and which could potentially arise in the future.

Third, build state education facilities that specifically deepen knowledge about information technology. The public can register at this facility, but on the condition that they will use their knowledge for the benefit of the state. Fourth, collaborating with private institutions engaged in information technology to transfer technology to defense personnel. This effort aims to increase the knowledge and ability of information technology management of defense personnel, as well as to build a network of information technology institutions that can strengthen the total defense, particularly against cyber threats.

The existence of cyber threats with the potential for widespread damage makes all defense components strive to strengthen the total defense. These efforts are carried out in the form of cross-sector cooperation based on full awareness of the potential dangers of cyber attacks. This aspect of cross-sector cooperation is one of the important capitals needed to strengthen total defense to face total wars that have the potential to occur in the future.

Cross-sectoral cooperation is not limited to one government agency and other government agencies, for example, between the Ministry of Defense and the Ministry of Communication and Information Technology (Siagian et al., 2018), but it can also be implemented between government agencies and private institutions that have business fields related to information technology applications; or between government agencies and educational providers. Besides, the existence of high capital requirements to finance information technology experiments can also be used as an excuse for the procurement of cooperation between state institutions in the defense sector and financial institutions capable of supporting this aspect of capital.

Overall, it can be stated that the development of information technology has had a significant impact on the total war strategy. The impact, which can be positive or negative, is the basis for the formulation and implementation of a total war strategy that has a fundamental difference from the previous one.

The total war is a war that involves all components of defense by prioritizing the role and position of the main component of defense, namely the TNI. Following the development of information technology, this formation has the potential to undergo significant changes. Total defense to prepare for the total war, which is no longer only open war with the deployment of military power but also in the form of war in the cyber realm, can be carried out by empowering civil society to strengthen the front line of defense in this cyberwar.

The development of information technology is the basis for the need to change the total war strategy to be more flexible in determining and mobilizing parties who are components of defense. Besides, the aspect of integrating information technology into the defense component needs to be prioritized because it is the main key to the success of strengthening total defense to face total war.

An important thing that also needs to be considered in the formulation of a total war strategy is the nature of cyber threats, which tends to change from time to time and the development of information technology. These changes can occur in the source, aspect, form, or type of cyber threat. As stated in Cyber Defense Law, there are nine sources of cyber threats, namely internal and external sources; intelligence activities; disappointment; investigation; extremist organizations; hacktivists; organized crime groups; competition, enmity and conflict; and technology. The development of information technology can produce many sources of new threats in addition to those nine sources, which need to be explored in-depth as a measure to anticipate and prepare for total war.

Regarding the cyber threat aspect, it is also stated in Cyber Defense Law that cyber threats can occur in ideological, political, economic, social, cultural, national, military, science and technology aspects, and other important aspects. The development of information technology has the potential to increase the scale of threats in these aspects so that the damage and losses that occur can be even greater.

According to Cyber Defense Law, there are seven forms of cyber threats that generally frequently occur, namely attacks from Advanced persistent threats (APT), denial of service (DoS), and distributed denial of service (DDoS); defacement, phishing, malware, cyber intrusion, spam, and misuse of communication protocols. These forms of cyber threats can change their level of impact and increase in variety and number according to the increasing number of uses and new products from existing information technology.

Finally, concerning the types of cyber threats, which consist of hardware threats, software threats, and data/information threats, along with the increasingly sophisticated information technology, more and more products are emerging, both in the form of programs/applications or use hardware that can be used to launch a cyberattack.

Based on the potential changes in cyber threats above, it is necessary to anticipate efforts in the form of adjustments to the existing total war strategy to the development of information technology. The adjustment is primarily aimed at ensuring that national defense can ward off and overcome various potential threats that arise, especially threats from the cyber domain so that they can have high readiness in the event of total war in the future.

CONCLUSIONS, RECOMMENDATION, AND LIMITATION

The development of information technology has a significant impact on various aspects of life. These impacts can be in the form of positive or negative impacts according to how humans place and empower information technology.

In general, the development of information technology can be used to increase achievements in various important fields, starting from the fields of education, social, economy, and national defense. In the economic field, the development of information technology can be used to improve information management, design online learning, develop new learning media, and teach life skills. In the social field, the continued use of information technology encourages changes in three social dimensions, namely the structural dimension, the cultural dimension, and the interactional dimension.

In the economic sector, developments in information technology have significantly increased productivity, accelerated the development of the quality of human resources, and accelerated the development of infrastructure required for economic activity. The development of information technology can also be used to strengthen national defense, especially to prepare for threats that come from the cyber domain.

Following statutory provisions, total state defense is applied to prepare for total war. Thus, a fundamental change in the formation of total defense due to the impact of the development of information technology will automatically lead to changes in the total war strategy implemented by Indonesia. These changes are basically due to the positive and negative impacts of the development of information technology. The negative impact is in the form of increasing threats to state security and sovereignty originating from the cyber domain. The positive impacts consist of increasing empowerment of the community in implementing total defense, having events to increase the integration of information technology into national defense, and increasing cross-sector cooperation to strengthen total defense.

The findings of this study can be used as a consideration for the government to formulate a total war strategy by prioritizing the development of defense forces, especially in the cyber domain. On the other hand, the findings of this research can also add insight to the public regarding the importance of using information technology wisely, which is not only beneficial for the fulfillment of personal interests but also the interests of the wider community and national interests.

This research can be used as a reference for further research that wants to re-examine the impact of the development of information technology on Indonesia's total war strategy. However, further research may use a different approach than this research, namely a quantitative approach, to produce findings by empirical data that describes the realities in the field.

REFERENCES

Anggito, A., & Setiawan, J. (2018). *Metodologi penelitian kualitatif*. CV Jejak.

Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siber global melalui Indonesia security incident response team on internet infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13–29.

Burhan, A. B. (2018). Pemanfaatan teknologi informasi dan komunikasi untuk pengembangan ekonomi pertanian dan pengentasan kemiskinan. *Jurnal Komunikasi Pembangunan*, *16*(2), 233–247.

Farid, M., & Adib, M. (2018). *Fenomenologi dalam penelitian ilmu sosial*. Prenadamedia Group.

Hikam, M. A. (2014). *Menyongsong 2014-2019 memperkuat Indonesia dalam dunia yang berubah*. CV Rumah Buku.

Husaini, M. (2014). Pemanfaatan teknologi informasi dalam bidang pendidikan (e-education). *Jurnal Mikrotik*, *2*(1).

Indrawan, J. (2015). Perubahan paradigma pertahanan Indonesia dari pertahanan teritorial menjadi pertahanan maritim: sebuah usulan. *Jurnal Pertahanan*, *5*(2), 93–114.

Lebo, D., & Anwar, S. (2020). Pemerdayaan komunitas siber oleh pemerintah Republik Indonesia dari perspektif strategi perang semesta. *Jurnal Strategi Pertahanan Semesta*, *6*(1), 101–127.

Lubis, I., & Safii, M. (2018). *Smart economy*. PT karya abadi mitra indo.

Martono, N. (2012). *Sosiologi perubah-an sosial: perspektif klasik, modern, postmodern, dan postkolonial*. Raja Grafindo Persada.

Meiliyanti, Y. T., Setiyono, J., & Supriyadhie, K. (2019). Kajian hukum humaniter internasional mengenai cyber warfare dalam konflik bersenjata internasional antara Israel dan Palestina atas Gaza. *Diponegoro Law Journal*, *8*(2), 1581–1600.

Moleong, L. J. (2018). *Metodologi Penelitian Kualitatif* (revisi). Remaja Rosda Karya.

Ngafifi, M. (2014). Kemajuan teknologi dan pola hidup manusia dalam perspektif sosial budaya. *Jurnal Pembangunan Pendidikan*, *2*(1), 33–47.

Prahassacitta, V. (2019). *Konsep kejahatan siber dalam sistem hukum Indonesia*. https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Pranowo, M. B. (2010). *Multidimensi ketahanan nasional*. Pustaka Alpabet.

Putra, R. D., Supartono, & Deni, D. A. R. (2018). Ancaman siber dalam perspektif pertahanan semesta (studi kasus sistem pertahanan semesta). *Jurnal Prodi Perang Asimetris*, *4*(2), 99–120.

Radhi, F. (2010). Pengembangan appropriate technology sebagai upaya membangun perekonomian Indonesia secara mandiri. *Jurnal Ekonomi Bisnis*, *1*(15), 1–8.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber dalam peningkatan cyber defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66.

Rosenberg, M. J. (2001). *E-Learning : Strategies For Delivering Knowledge In The Digital Age*. McGraw-Hill Book Company.

Rusydi, I. (2017). Peranan perkembangan teknologi informasi dan komunikasi dalam kegiatan pembelajaran dan perkembangan dunia pendidikan. *Jurnal Warta*, *53*.

Setiawan, D. (2018). Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya. *Simbolika*, *4*(1), 62–72.

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran keamanan siber dalam mengatasi konten negatif guna mewujudkan ketahanan informasi nasional. *Jurnal Prodi Perang Asimetris*, *4*(3), 1–18.

Siyoto, S., & Sodik, A. (2015). *Dasar Metodologi Penelitian*. Literasi Media Publishing. https://books.google.co.id/books?id=QPhFDwAAQBAJ&pg=PA28&dq=sumber+data+penelitian+kualitatif&hl=en&sa=X&ved=0ahUKEwiEvfrcpvXbAhXGWisKHT97AesQ6AEIXzAH#v=onepage&q=sumber data penelitian kualitatif&f=false

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Kemhan*, 31–35.

Susdarwono, E. T., Setiawan, A., & Husna, Y. N. (2020). Kebijakan negara terkait perkembangan dan revitalisasi industri pertahanan Indonesia dari masa ke masa. *Jurnal USM Law Review*, *3*(1), 155–181.

Wardhana, A., Kharisma, B., & Lisdiyanti, T. (2020). Teknologi informasi komunikasi dan pertumbuhan ekonomi wilayah barat dan timur Indonesia periode 2014-2018. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, *9*(11), 1103–1116.

Yusuf, I. (2016). Analisis penggunaan teknologi informasi (internet) terhadap masyarakat di Kecamatan Sigi Biromaru Kabupaten Sigi. *EJurnal Katalogis*, *4*(9), 125–136.

Zulfah, S. (2018). Pengaruh perkembangan teknologi informasi lingkungan (studi kasus kelurahan Siti Rejo I Medan). *Jurnal Ilmu Administrasi UISU*.

Anggito, A., & Setiawan, J. (2018). *Metodologi penelitian kualitatif*. CV Jejak.

Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siber global melalui Indonesia security incident response team on internet infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13–29.

Burhan, A. B. (2018). Pemanfaatan teknologi informasi dan komunikasi untuk pengembangan ekonomi pertanian dan pengentasan kemiskinan. *Jurnal Komunikasi Pembangunan*, *16*(2), 233–247.

Farid, M., & Adib, M. (2018). *Fenomenologi dalam penelitian ilmu sosial*. Prenadamedia Group.

Hikam, M. A. (2014). *Menyongsong 2014-*

2019 memperkuat Indonesia dalam dunia yang berubah. CV Rumah Buku.

Husaini, M. (2014). Pemanfaatan teknologi informasi dalam bidang pendidikan (e-education). *Jurnal Mikrotik*, *2*(1).

Indrawan, J. (2015). Perubahan paradigma pertahanan Indonesia dari pertahanan teritorial menjadi pertahanan maritim: sebuah usulan. *Jurnal Pertahanan*, *5*(2), 93–114.

Lebo, D., & Anwar, S. (2020). Pemerdayaan komunitas siber oleh pemerintah Republik Indonesia dari perspektif strategi perang semesta. *Jurnal Strategi Pertahanan Semesta*, *6*(1), 101–127.

Lubis, I., & Safii, M. (2018). *Smart economy*. PT karya abadi mitra indo.

Martono, N. (2012). *Sosiologi perubah-an sosial: perspektif klasik, modern, postmodern, dan postkolonial*. Raja Grafindo Persada.

Meiliyanti, Y. T., Setiyono, J., & Supriyadhie, K. (2019). Kajian hukum humaniter internasional mengenai cyber warfare dalam konflik bersenjata internasional antara Israel dan Palestina atas Gaza. *Diponegoro Law Journal*, *8*(2), 1581–1600.

Moleong, L. J. (2018). *Metodologi Penelitian Kualitatif* (revisi). Remaja Rosda Karya.

Ngafifi, M. (2014). Kemajuan teknologi dan pola hidup manusia dalam perspektif sosial budaya. *Jurnal Pembangunan Pendidikan*, *2*(1), 33–47.

Prahassacitta, V. (2019). *Konsep kejahatan siber dalam sistem hukum Indonesia*. https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Pranowo, M. B. (2010). *Multidimensi ketahanan nasional*. Pustaka Alpabet.

Putra, R. D., Supartono, & Deni, D. A. R. (2018). Ancaman siber dalam perspektif pertahanan semesta (studi kasus sistem pertahanan semesta). *Jurnal Prodi Perang Asimetris*, *4*(2), 99–120.

Radhi, F. (2010). Pengembangan appropriate technology sebagai upaya membangun perekonomian Indonesia secara mandiri. *Jurnal Ekonomi Bisnis*, *1*(15), 1–8.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber dalam peningkatan cyber defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66.

Rosenberg, M. J. (2001). *E-Learning : Strategies For Delivering Knowledge In The Digital Age*. McGraw-Hill Book Company.

Rusydi, I. (2017). Peranan perkembangan teknologi informasi dan komunikasi dalam kegiatan pembelajaran dan perkembangan dunia pendidikan. *Jurnal Warta*, *53*.

Setiawan, D. (2018). Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya. *Simbolika*, *4*(1), 62–72.

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran keamanan siber dalam mengatasi konten negatif guna mewujudkan ketahanan informasi nasional. *Jurnal Prodi Perang Asimetris*, *4*(3), 1–18.

Siyoto, S., & Sodik, A. (2015). *Dasar Metodologi Penelitian*. Literasi Media Publishing. https://books.google.co.id/books?id=QPhFDwAAQBAJ&pg=PA28&dq=sumber+data+penelitian+kualitatif&hl=en&sa=X&ved=0ahUKEwiEvfrcpvXbAhXGWisKHT97AesQ6AEIXzAH#v=onepage&q=sumber data penelitian kualitatif&f=false

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Kemhan*, 31–35.

Susdarwono, E. T., Setiawan, A., & Husna, Y. N. (2020). Kebijakan negara terkait perkembangan dan revitalisasi industri pertahanan Indonesia dari masa ke masa. *Jurnal USM Law Review*, *3*(1), 155–181.

Wardhana, A., Kharisma, B., & Lisdiyanti, T. (2020). Teknologi informasi komunikasi dan pertumbuhan ekonomi wilayah barat dan timur Indonesia periode 2014-2018. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, *9*(11), 1103–1116.

Yusuf, I. (2016). Analisis penggunaan teknologi informasi (internet) terhadap masyarakat di Kecamatan Sigi Biromaru Kabupaten Sigi. *EJurnal Katalogis*, *4*(9), 125–136.

Zulfah, S. (2018). Pengaruh perkembangan teknologi informasi lingkungan (studi kasus kelurahan Siti Rejo I Medan). *Jurnal Ilmu Administrasi UISU*.