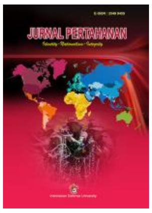
Jurnal Pertahanan

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 STRUCTURING OF ORGANIZATIONAL AND DOCTRINE OF STATE DEFENSE IN FACING HYBRID WARFARE

Novky Asmoro[1], Andi Sutomo[2], Teguh Haryono[3], Rizki Putri[4]
Republic of Indonesia Defense University
IPSC Area, Sentul, Bogor, West Java, Indonesia 16810
novky.asmoro@idu.ac.id[1], andi.sutomo@idu.ac.id[2]
teguh.haryono@idu.ac.id[3], rizki.putri@idu.ac.id[4]

Article Info

Article history:
Received : April 25, 2021
Revised : June 30, 2021
Accepted : August 15, 2021

Keywords:
Conventional and Unconventional Warfare,
Defense Strategy,
Hybrid Warfare,
Military and Non-Military Components,
National Defense Doctrine

Abstract

Defense Doctrine and Strategy are designed to be able to synergize the performance of military and non-military components to protect and maintain Indonesia's national interests. The current doctrine of the Indonesian Armed Forces (TNI) Military Campaign is still dominant in dealing with military threats, even though based on the 2018 Indonesian Defense White Paper, the TNI must also be able to deal with hybrid threats. With its adaptive nature to changing threats, problems will arise if the military campaign doctrine has not accommodated the TNI's strategy and way of acting in dealing with hybrid threats. The defense doctrine must be able to accommodate the integration of military and non-military components is facing various types of warfare and threats such as military threats, non-military threats, and hybrid threats. Especially for the kind of hybrid threats namely cyber threats, terrorism, and other unconventional threats. Through an analytical descriptive analysis based on qualitative methods, it is hoped that the proper organization and doctrine will be disentangled in the face of this model war. Indonesian Armed Forces (TNI) as the war organizations that prioritize a modern universal perspective are a necessity as one of the efforts offered. This needs to be supported by the doctrine of national defense which accurately defines how an effort against hybrid warfare can transform from conventional to unconventional warfare and the actors involved. Military or TNI organizations that prioritize a modern universal perspective are supported by the doctrine of national defense which accurately maps how an effort against hybrid warfare could transform from conventional warfare to unconventional.

DOI:
http://dx.doi.org/10.33172/jp.v7i2.1220

INTRODUCTION

The essence of hybrid warfare is a mixed war which is a combination of conventional warfare and unconventional forms of war. Hybrid warfare, among others, combines missions and operations of conventional warfare, asymmetric, terrorist, and cyber warfare, as well as diverse and dynamic crimes (Nyagudi, 2020). In addition to these various war combinations, hybrid warfare can also be in the form of integrated attacks by utilizing the use of chemical, biological, nuclear, and explosive weapons (Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE), and information warfare (Defense Ministry of The Republic of Indonesia, 2019).

In the face of hybrid warfare, applying a military defense pattern by placing the Indonesian Armed Forces (TNI) as the main component supported by related ministries or nation agencies and other elements of the nation's power including the Indonesian National Police (Polri), Paramilitary and Regional Governments which are informed based on the professional and proportional capabilities. Based on the Government Regulation instead of Law Number 23, 1959, TNI as Main Component and Reserve Component have to conduct mobilization after the President declaring both Mobilization and War Situation to deal with military threats only. There is a problem for TNI especially for facing Hybrid Threats with a military defense pattern that requires the mobilization of TNI and other defense components proportionally according to the level of authority. The rules or doctrine which stipulated deployment of TNI to deal with hybrid threats is none currently even though these provisions have been regulated in Government Regulation instead of Law, number 23, 1959, revocation of law no. 74 the year 1957 state-magazine No. 160 the year 1957 and establishment of danger (Amendement to Law Number. 74 of 1957 (State Gazette NO. 160 of 1957) and Determination of the State of Danger, 1959). Furthermore, the analysis will also relate some interesting phenomena that this hybrid threat trend occurred until it was determined by the Ministry of Defense through a defense white paper that must be faced with military operations. This is carried out based on the escalation of both kinds of threats, military, and hybrid threats as well as encouraging the mobilization of related ministries/national agencies and Local Governments to jointly face hybrid warfare by paying attention to capabilities professionally and proportionally. This study aims to analyze the structuring development of organizational and doctrine of state defense in facing hybrid warfare.

METHODS

Hybrid warfare is a new challenge in the information environment. The nature of the military threat environment has changed as our adversaries and potential adversaries increasingly use nonmilitary and paramilitary means to achieve strategic and operational objectives that were previously considered purely military duties. The trend towards using nonmilitary capabilities and operations to replace military force, as well as the convergence of conventional and irregular approaches, have been recognized over the years by military writers and experts. These tactics employed during peacetime competition can have lasting negative outcomes that directly affect international security, economics, and law.

Military organizations must deal with very high levels of uncertainty (Posen, 2016). To get a complete understanding of organizational arrangements and defense doctrine in the face of hybrid threats as research subjects, it is necessary to review them based on a research model. There needs to be a study and theory that identifies the impact of an organizing and defense doctrine on efforts to resolve conflict. According to the Theoretical Framework (Figure 1), the specifics of each research will be indicated from how the

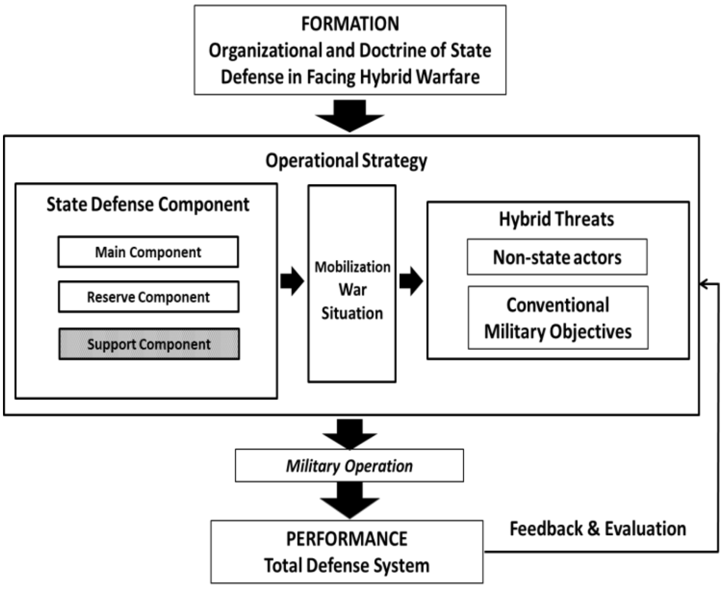


Figure 1. Theoretical Framework
Source: Wahyuni, 2016

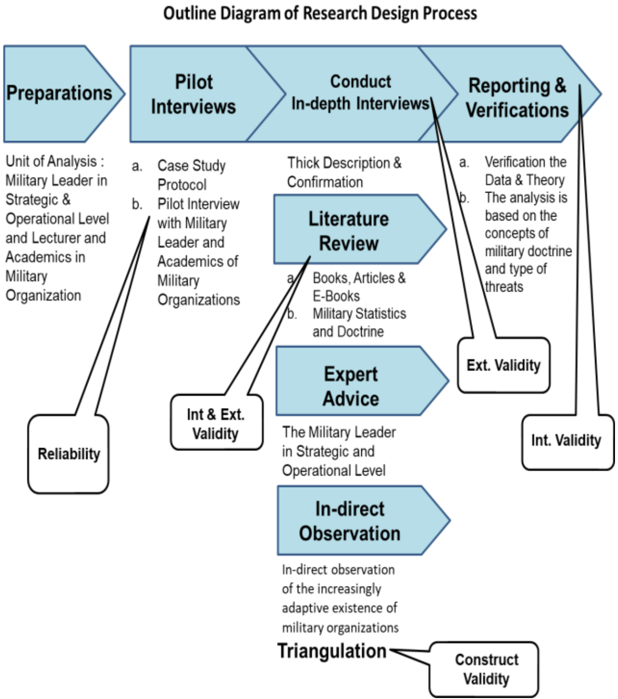

Outline Diagram of Research Design Process
Preparations
Pilot Interviews
Conduct In-depth Interviews
Reporting & Verifications
Unit of Analysis : Military Leader in Strategic & Operational Level and Lecturer and Academics in Military Organization
a. Case Study Protocol
b. Pilot Interview with Military Leader and Academics of Military Organizations
Thick Description & Confirmation
a. Verification the Data & Theory
b. The analysis is based on the concepts of military doctrine and type of threats
Literature Review
a. Books, Articles & E-Books
b. Military Statistics and Doctrine
Expert Advice
The Military Leader in Strategic and Operational Level
In-direct Observation
In-direct observation of the increasingly adaptive existence of military organizations
Triangulation
Reliability
Int & Ext. Validity
Ext. Validity
Int. Validity
Construct Validity

Figure 2. Research Design
Source: Wahyuni, 2016

researcher's point of view is in determining a military operation as the operating model that will be conducted in facing some hybrid threats. The reliability of qualitative research is very much determined by how the perspective is attributed to the research topic because this is a controlling tool so that the process of investigation, deepening of material, and extracting data will be following the theoretical basis that has been determined (Wahyuni, 2016).

The Formation Organizational Doctrine of State Defense in Facing Hybrid Warfare is related to the fact that the determination of organizations and doctrines that strictly regulate military organizations in dealing with hybrid threats requires an analytical effort that departs from the history of the formation of the TNI. Through this approach, it is hoped that data will be collected systematically and relevant to the object of research so that several related hypotheses, impacts, and trends will be analyzed so that they can assist in describing the problems that occur today as anticipatory efforts in the future (Gay, Mills, & Airasian, 2012).

A qualitative research method approach is also needed which is considered quite effective in discussing how the phenomenon of every military operation is required to be able to deal with these mixed threats. To get the right understanding according to the process of the research design including the attribution of the approach used, it will be shown in Figure 2. This trend has recently accelerated as the superpowers try to achieve military objectives without sparking open conflict between nations. The mixed approach to modern warfare has been given many names, including new generation warfare, asymmetric warfare, compound warfare, hybrid warfare, and has recently been described as acts committed in a gray zone between classical diplomacy and open military conflict. Within the North Atlantic Treaty Organization (NATO), this term is used to describe the new operational attributes of the Russian attack on Ukraine. Russia's use of military equipment and troops under the guise of indigenous and separatist forces in Ukraine is a tricky example of hybrid warfare that includes the use of lethal force (Brown, 2018).

Hybrid warfare uses a combination of military and nonmilitary methods in peacetime to achieve traditional military objectives (for example, territorial control or conquest), and thereby alter facts on the ground without triggering an actual conflict. Peacetime hybrid warfare achieves military objectives, namely control of the battlefield (Mazarr, 2015). Hybrid warfare is a challenge that is likely to persist. The contemporary strategic environment presents potential adversaries with an array of new, more cost-effective means to employ in combination, ranging from information operations in cyberspace to the proliferation of cheap air defense and missile technology (Mälksoo, 2018).

As hybrid warfare is primarily well-equipped and designed to exploit national vulnerabilities across the political, military, economic, social, informational, and infrastructural spectra, it virtually means that it comprises war against nation-states. India continues to be vulnerable to hybrid threats, being a large, pluralistic, democratic nation, with a huge diversity in geography, demographic profile, socio-economic disparity, and other forms and manifestations (Ahluwalia, 2019). Scramble for land through hybrid warfare in peacetime can be seen as shaping the field of future military operations by extending military control over contested land or operational space to make better use of offensive and defensive capabilities in the event of an actual conflict.

The Russian and Chinese version of hybrid warfare uses measures without triggering direct military confrontations between countries that would violate the boundaries of the treaty. The Russian version features unusual and varied techniques combining a mix of special forces, information campaigns, third-party forces, and criminal activity (Ripley, 2014). Because Russia and China have developed state-of-the-art cyber capabilities and strategies. The plausible denial of cyber-attacks has made it a practical and preferred component of hybrid warfare. Russia’s approach can rightly be called hybrid warfare and argues not only that the hybrid label is unhelpful and misleading but also that it gives an entirely misplaced impression of novelty (Giles, 2016). A common feature of this new form of war is the accurate strategic management of force and operations, down to the tactical level, to achieve ambiguity about whether the troops and methods used are actually under the authority of national command, and to achieve the desired effect of influence and delivery strategic communication messages messages across all media.

China now fully regards cyberspace as a component of military operations, as revealed in the 2015 Defense White Paper, which stated that China will accelerate the development of its cyber force, the Stars and Stripes newspaper reported in May 2015. More recently, In October 2015, Bloomberg News broadcast the PLA announcement that the PLA was consolidating China's various cyber warfare units and capabilities into a single military command under the Central Military Commission. The PLA's actions in establishing a cyber command come more than a year after the Russian military's announcement in February 2014 of its cyber command. Russia once again acted in a way that utilized the potential of the hybrid threat as a military strategy and modus operandi, this time in the Crimea (Bachmann, 2015). The hybrid approach is visualized and explained in the Gerasimov doctrine and the capabilities are available. The challenge is how long those capabilities can be preserved due to economic reasons. In the short term. It is viable until 2020 or 2022, but in the long term the Russian economic situation must be improved to avoid the implosion of the current system (Śliwa, Veebel, & Lebrun, 2018).

RESULT AND DISCUSSION

Structuring the Doctrine of National Defense in Response to Hybrid Warfare

The doctrine of State Defense has a position as a basic instrument in the development of various doctrines related to State defense. Thus, the doctrine of State Defense is referred to in the document component as the basic doctrine in doctrine stratification. Another level form is the main doctrine, namely the military defense doctrine which is described by the TNI as the *Tridharma Eka Karma* Doctrine, and the non-military defense doctrine which is carried out through the function of the Ministry of Defense which oversees non-military defense. While the executing doctrine level consists of military defense doctrine in each dimension such as the land dimension, *Kartika Eka Paksi* as Indonesian Army’s Doctrine, *Jalasveva Jayamahe* as Indonesian Naval's Doctrine, and *Swa Bhuwana Pakca* as the Indonesian Air force’s doctrine (Defense Ministry of The Republic of Indonesia, 2019).

Doctrinal stratification in the document on National Resilience of the Republic of Indonesia has differences with doctrinal categorization. Doctrine of the dimensions is more of an environmental doctrine because it is the nature of how to use force in a certain operation (Drew & Snow, 2006). Meanwhile, in the documents of the Republic of Indonesia's national defense, it is determined as the main doctrine, namely the TNI doctrine on military defense. Furthermore, the implementation doctrine in the Indonesian state defense doctrine is the doctrine of each dimension of military defense, while in the Drew and Snow categorization, the dimension doctrine is the environmental doctrine. Practical doctrines are known as organizational doctrines. The similarity of doctrinal stratification in the doctrine of the Republic of Indonesia defense doctrine with the categorization of the doctrine of Drew and Snow's version is the fundamental doctrine. The TNI’s doctrine is the dedication of three TNI dimensions for one National Goal.

It has been previously explained that the position of doctrine is very important in accommodating how organizations or institutions move in carrying out their operations. Environmental and organizational, the doctrine that is required to be adaptive needs to be able to be properly structured, including in responding to the phenomenon of hybrid warfare. Several steps in preparing doctrine, especially at the level of strategic doctrine (Buzan, 2008). First, the perfection of doctrine. Doctrine is not something dogmatic and irrefutable, on the contrary, the good military doctrine will adapt to the actual operating environment, be adaptive to all forms of the situation, and can be understood and implemented starting from the leadership of the TNI to executing soldiers in the field and the doctrine must be applied according to the nature of warfare. So that to support the readiness of the TNI in facing the phenomenon of hybrid warfare, the TNI doctrine must be able to adapt to the development of warfare which applies to the tactics that are operational in the field. The tactics must adapt to the operating environment and the nature of the enemy to be faced, lest the war tactics used by the TNI be out of sync with the hybrid warfare pattern which tends to penetrate space and time.

The Army as the foundation in carrying out TNI operations should be leading sector changes in war doctrine leading to hybrid warfare going forward. An example of success in making doctrine is like that carried out by the United States military where the formulation of doctrine was initiated by the army, while other forces will adjust it in the form of a joint publication containing basic principles that direct the use of the military in coordinated activities for the same goal. Second, increasing human resources through education and training at home and abroad. TNI personnel from now on must begin to understand what is meant by hybrid warfare, how to maneuver Major Weapon Systems for hybrid warfare, how to deal with cyber warfare and information warfare. The demands of war progress have forced the TNI to have non-military skills. Apart from that civil relations and military relations need to be trained in the form of integrated training, wherein the pattern of operations carried out, non-military agencies will provide support in the form of personnel, expertise, and equipment that the TNI does not have in the face of hybrid warfare (Buzan, 2008).

Hybrid Warfare and a Universal Perspective

Indonesian national defense is carried out by the government which is prepared early in the Total Defense System (*Sishankamrata*) through efforts to manage national resources which include all human resources, natural resources, artificial resources, as well as national facilities and infrastructure, throughout the region. The Republic of Indonesia is a unit of defense in overcoming threats. The management of the national defense system is one of the functions of government aimed at protecting national interests and supporting national policies in the defense sector. The Ministry of Defense as the bearer of government functions in the defense sector strives to achieve the stated national defense policy targets, following the national development paradigm.

The strategic process for dealing with hybrid warfare is to determine national security objectives as the basis for the strategy process. Formulating a grand strategy, better known as a policy developing a military strategy, designing an operational strategy, and formulating a battlefield strategy, is better known as tactics. The TNI, *Tri Dharma Eka Karma* doctrine emphasizes that the essence of the TNI is to be formed to carry out state duties in the defense sector is facing various threats and disturbances to the integrity of the nation and state. Apart from carrying out these defense duties, the TNI is also prepared to carry out tasks to support national interests following statutory regulations. The TNI doctrine, especially concerning the concept of dealing with the threat of hybrid warfare carried out by non-state actors, needs to be immediately compiled so that it can serve as a guide for all TNI forces in conducting guidance and in using force in dealing with cyber warfare threats.

As it is known that Indonesia's defense

system is the Total Defense System, where the main component is the TNI and the supporting component is the people. In this context, the universal defense system as stipulated in Law No. 3 of 2002 about the National Defense System must be able to be interpreted as a universe that is not only physical but non-physical, especially digital and cyberspace. This means that all efforts are made including empowering all the potential of the virtual world that exists in the face of hybrid warfare. TNI Readiness Hybrid warfare is a military strategy that combines conventional warfare, irregular warfare, and cyber warfare threats, both in the form of nuclear attacks, biological and chemical weapons, improvised explosive devices, and information warfare. Therefore, facing the possibility of the threat of hybrid warfare, the TNI must be able to respond and immediately adapt to the developing situation to anticipate and overcome it more quickly and precisely.

Thinkers from both the military, defense analysts, and members of the Indonesian parliament explained that the Ministry of Defense and the Indonesian National Army (TNI) had anticipated the possibility of strengthening what was termed the hybrid war. It is proper for the TNI to be aware of the threat of hybrid warfare, apart from the threat of conventional warfare. From a land, sea, and air perspective, the TNI must be aware of all forms of threats, be it conventional warfare or non-conventional war such as hybrid warfare (Sa'diyah & Vinata, 2016). The situations where hybrid threats evolve are hybrid conflicts or hybrid wars. Pawlak describes the hybrid conflict as a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives (Vaczi, 2016).

Preparing TNI with Artificial Intelligence Capability

Symptoms of hybrid warfare are not the same as conventional warfare where the threat or enemy that comes can look real because the threat in hybrid warfare will appear in the form of symptoms or the opposite effect after it occurs (MCDC, 2017). To respond to this, a coordinating body under the ministry of defense is needed, whose membership comes from the military and non-military agencies. Both members of the military and non-military are people who have special abilities in hybrid warfare, such as software experts, anti-hackers, information experts, telematics experts, explosives experts, atomic physicists, biologists, and military tactics.

Currently, Big Data is needed that is strong, accurate, with an integrated architecture to support strategic decisions for national defense. The ideal Big Data for national defense must be able to present accurate, real-time, complete data, to be able to do profiling with strong analytical support. The key is analytical capabilities as the forward projection of a lot of artificial intelligence is used for cyber attacks. So, in addition to the power of Alusista, you must also have cyber power. Examples of things that have been done by Cyber Defense Center of Ministry of Defense RI (Pushansiber Kemhan RI) to search information systems. Testing one of the government's web or information systems. After the inspection, several vulnerabilities were found, such as SQL (Standard Query Language) Injection, XSS (Cross-Site Scripting), and CSRF (Cross-Site Request Forgery), which of course hackers can change HTML (HyperText Markup Language) code to exploit their information system database. From their recent search results, for example, there were 4 findings from 4 different domains. Such as critical severity that can be used to steal databases. Luckily, the National

Cyber and Crypto Agency of Indonesia (BSSN) responded quickly to these findings. The collaboration between Pushansiber Kemhan RI-BSSN is very positive. There are mutually reinforcing functions. Both are committed to maintaining cyber 'sovereignty'.

Indonesian National Armed Forces Cyber Unit (Satsiber TNI) is tasked with protecting and maintaining critical TNI infrastructure that is connected. Cyber War Becomes a New Battle Arena. The threat of cyberwar whose presence as cyberspace, cyber threat, cybercrime in today's global life has given rise to cyber defense or cyber defense in various countries in the world. Many countries in the world have formed various special units such as the cyber army, cyber naval, cyber air force, cyber military, cyber troops, and cyber force. Organically, national security and defense are built by the organizers of the electronic system universally and continuously. In line with this, cybersecurity can be a form of cyber defense. The functions that must be possessed by Cyber TNI are detection, protection, recovery, and ensuring that the cyber system that is running does not have holes or defense weaknesses that malware or backdoors can enter.

This agency is tasked with coordinating the actions that will be taken against all forms of potential threats to the country's sovereignty when faced with hybrid warfare. Once it is time for the TNI to have military satellites to support operations, especially in anticipation of hybrid warfare. By having satellites, the TNI will be more integrated in terms of command control, information dissemination, and early detection to find out upcoming threats. Things that are known to be threats will be more quickly informed to all elements so that each unit will prepare its operational unit to act in a coordinated manner.

The relevance of dealing with hybrid warfare with Artificial Intelligence technology cannot be separated from one type of hybrid war, namely cyber warfare. This type of war is classified as a hybrid war departing from the main actors who come from non-state actors although in its development the military is increasingly dominant as the actor. The use of cyberspace as a medium for AI technology is very crucial so that cyber-attacks can cripple national forces and even control them by the center of gravity using AI technology.

There are 14 Artificial Intelligence (AI) implementations in the defense sector the fastest working and developing technology in the world is the military. After that, technology will enter the industrial sector and other sectors. Based on President Joko Widodo's direction in early July 2020 regarding the application of Artificial Intelligence (AI) in the defense sector, the latest military technology has been able to combine weaponry instruments with the use of Artificial Intelligence.

The 14 implementations of Artificial Intelligence in the defense sector include (Kurniawan, 2020), namely (1) Autonomous Machine System that capable in seeing patterns of hybrid warfare, (2) Artificial Intelligence which is a collaboration between Humans– Machines, (3) Artificial Intelligence which assists human operations/soldiers (Assisted human operations), (4) Advanced Human-Machine which combines humans with machines in a more advanced and intensive manne, for example, AI that combines the human brain with a processor (Combat-Teaming), (5) Artificial Intelligence for Network-enabled semi-autonomous weapons, (6) Artificial Intelligence for image understanding, (7) Artificial Intelligence for Face Recognition or recognizing and understanding humans, (8) Cognitive C41SR or Artificial Intelligence to support decision making, (9) Cognitive command decision making or Artificial Intelligence which was developed to make decisions more quickly, precisely, and accurately, (10) Artificial Intelligence for cognitive processors implemented in Unmanned Combat Aerial Vehicle (UCAV) vehicles, (11) Artificial

Intelligence for cognitive countermeasure or protecting information, (12) Artificial Intelligence to predict cyber attacks (predictive system cyber attack), (13) Artificial Intelligence to assist force in the field (energy usage predictive system), (14) Artificial Intelligence to monitor electronic devices in a war (Health Condition Predictive System).

Some examples of applications of AI technology in the implementation of hybrid or cyber warfare include the use of UAV technology from Azerbaijan when repelling Armenian troops in the war between the two countries at the end of 2020. In the war theater, it was proven that Azerbaijani Kamikaze Drones played an active role in defeating Armenia because of the support from Azerbaijan's Electronic Warfare technology is superior.

Another example of the development of AI technology by Russia is in terms of military modernization featuring the mastery of autonomous or robotic weapons platforms. In a report entitled Artificial Intelligence and Autonomy in Russia, the Kremlin government shows its seriousness by calling AI mastery Information Domination on the Battlefield. The Human Resources factor to develop Artificial Intelligence (AI) remains the most important. Even though Indonesia currently has lacks the quantity and quality of human resources of Artificial Intelligence development. The key to Artificial Intelligence is in Human Resources because no matter how sophisticated the technology is, humans still play an important role (Kurniawan, 2020).

The threats facing Indonesia will become increasingly complex. In various war events that have occurred in various parts of the world lately, we cannot easily judge who the real actors/actors of war are, whether they are on behalf of a country or state actor or not a state or non-state actor. The background of the war was mixed between interests that were political, ideological, economic, or social aspects and others. Systems and methods of warfare are also complex because war is carried out by applying the concepts of conventional warfare and modern warfare.

The dimensions of warfare that occur have also penetrated the dimensions of the virtual world or the cyber world as facilities/means/media of cyber warfare or cyber warfare. The warfare that is complex, the mix of various interests that become the background of the conflict, the unclear who is the real perpetrator of the war, the mix of methods, methods, techniques, and tactics of war is what is then referred to as Hybrid Warfare. Hybrid Warfare as a method of war is not new. Hybrid Warfare as a method of warfare has its roots in methods of warfighting of past conflicts; while not necessarily new as a category of conflict, it has the potential to change the future conceptualization of conflict (Mosquera & Bachmann, 2016).

CONCLUSIONS, RECOMMENDATION AND LIMITATION

Military or TNI organizations that prioritize a modern universal perspective are a necessity as one of the efforts offered. This needs to be supported by the doctrine of national defense which accurately maps how an effort against hybrid warfare can transform from conventional forms of war to unconventional warfare and the actors involved. So, the key to Artificial Intelligence is in Human Resources because no matter how sophisticated the technology is, humans still play an important role. After all, Artificial Intelligence in the use of detection system technology and modern weapons requires high academic competence and skills on TNI soldiers guarding them.

Regulating defense organizations and doctrines in the face of hybrid threats can be pursued in two ways. Firstly, structuring the doctrine of national defense in response to hybrid warfare. This effort was pursued by redefining the TNI's doctrine to be more flexible, especially in guiding military operations in the face of hybrid war attacks.

Secondly, that way above needs to be supported by the preparation of reliable human resources in terms of mastery of AI-based weapon systems used in military operations against hybrid threats including their effectiveness when supporting non-military elements with various elements. To achieve this, it is necessary to prepare the TNI with Artificial Intelligence Capability including the ability to organize and fight information operations by utilizing military satellite technology.

REFERENCES

Ahluwalia, V. K. (2019). Hybrid Warfare: Battlegrounds of the Future. *CLAWS Journal*, *12*(2), 15–34.

Amendement to Law Number. 74 of 1957 (State Gazette NO. 160 of 1957) and Determination of the State of Danger. , Pub. L. No. 23 Tahun 1959 (1959). Indonesia: JDIH BPK RI.

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

Brown, J. (2018). An Alternative War: The Development, Impact, and Legality of Hybrid Warfare Conducted by the Nation State. *Journal of Global Faultlines*, *5*(1–2), 58–82. https://doi.org/10.13169/jglobfaul.5.1-2.0058

Buzan, B. (2008). *People, states & fear: an agenda for international security studies in the post-cold war era* (2nd ed.; E. Egar, Ed.). Brighton: Jhon Spiers.

Defense Ministry of The Republic of Indonesia. *Law No 15 of 2019 on Amendement to law Number 12 Year 2011 Regarding Establishment of laws and Regulations.* , Pub. L. No. 19 Tahun 2015 (2019). Indonesia.

Drew, D. M., & Snow, D. M. (2006). *Making Twenty First Century Strategy: An Introduction To Modern National Security Processes And Problems*. Alabama: Air University Press. Retrieved from https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0104_drew_snow_twentyfirst_century_strategy.pdf

Gay, L. R., Mills, G. E., & Airasian, P. (2012). *Educational Research: Competencies for Analysis and pplication* (10th ed.). New Jersey: Pearson Education. Retrieved from https://yuli-elearning.com/pluginfile.php/4831/mod_resource/content/1/Gay-E Book Educational Research-2012.pdf

Giles, K. (2016). Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power. In *Russia and Eurasia Programme*. Retrieved from https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

Kurniawan, A. (2020, December). Perwira TNI AU Paparkan 14 Implementasi AI di Bidang Pertahanan - Cobisnis.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European Security*, *27*(3), 374–392. https://doi.org/10.1080/09662839.2018.1497984

Mazarr, M. J. (2015). *Mastering the gray zone: understanding a changing era of conflict*. Fort Belvoir: US Army War College Carlisle.

MCDC. (2017). MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. In *Multinational Capability Development Campaign*.

Mosquera, A. B. M., & Bachmann, S. D. (2016). Lawfare in hybrid wars: The 21st century warfare. *Journal of International Humanitarian Legal Studies*, *7*(1), 63–87. https://doi.org/10.1163/18781527-00701008

Nyagudi, N. (2020). *Election Shenanigans - Kenyan Hybrid Warfare*. Amazon

Digital Services LLC - KDP Print US.

Posen, B. R. (2016). Foreword: Military doctrine and the management of uncertainty. *Journal of Strategic Studies*, *39*(2), 159–173. https://doi.org/10.1080/01402390.2015.1115042

Ripley, T. (2014). *IHS Jane's Defence Weekly* (No. 35; P. Felstead, Ed.). Jamaica.

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif: Kajian Masalah Hukum Dan Pembangunan*, *21*(3), 168–187.

Śliwa, Z., Veebel, V., & Lebrun, M. (2018). Russian Ambitions and Hybrid Modes of Warfare. *Estonian Journal of Military Studies*, *2018*(7).

Vaczi, N. (2016). *Hybrid Warfare: How to Shape Special Operations Forces*. Károly Eszterházy College.

Wahyuni, S. (2016). *Qualitative research method: Theory and practice 2nd edition*.