Network Centric Operations In Supporting Tni Operations To Dealing With Irregular Warfare

Zulfikar Fabri[1], Djayeng Tirto[2], Achmed Sukendro[3], Dyah Tribuwana Tungga Dewi[4]

[123] Peace and Conflict Resolution Study Program, National Security Faculty, Republic of Indonesia Defense University

[4]Defense Management Study Program, Defense Management Faculty, Republic Of Indonesia Defense University

Email : zulfikarfabri6@gmail.com

Abstract— Irregular warfare requires a special strategy for handling it, one of which is through network-centric warfare where NCW is a concept of a command and control system applied in modern military operations, with interoperability capabilities for elements of military power that optimizes the use of defense-based computer network systems. this is done in the context of supporting war military operations and military operations other than war by taking into account aspects of support or availability of intelligence data and information (SIGINT, GEOINT MASINT, OSINT, HUMINT. This writing uses the literature study method by looking at several previous studies, books, and academic papers on existing laws and theoretical foundations to create new analytical results.

Keywords—Irregular; Interoperability; Network ; Warfare

I. INTRODUCTION

War in the present and the future has a wide spectrum. Even troops with the most advanced weapons and technology do not guarantee victory. Civilian tools such as the media, cyberspace, and the internet essentially have a decisive monopoly in current and future wars. This irregular phenomenon gave rise to the term Irregular Warfare.

The war strategy has changed to a new war strategy aimed at targeted attacks and the violent displacement of civilian populations. The effect of this new war is even more devastating than the traditional cross-border war. The new war hit the core of the country's social order, threatening its political and economic development. These wars are carried out either through ethnic cleansing, through the violent displacement of populations, or through the systematic killing of people who have different opinions and identities in politics, religion, or ethnic groups (Malantowicz, 2013).

The current conditions have brought the world no longer to VUCA which is characterized by its complexity but to BANI which brings disorientation, unpredictability, and chaos. BANI as an acronym for Brittle, Anxious, Nonlinear, and Incomprehensible was proposed in early 2020 by Cascio (2020). Furthermore according to Cascio that articulating an increasingly common situation with simple volatility or complexity is not enough to understand the situation that occurs. The existing conditions were not only unstable but also chaotic. The outlook for the future is not only difficult to predict but downright unpredictable. The last one is that what happened is not only ambiguous but also completely incomprehensible.

The development of the strategic environment and the influence of technological developments as a consequence of technological advances has resulted in a shift like threats originating from states (state threats) with certain ideologies, with the power of weapons switching to groups (non-state threats) with the paradigm of modern warfare in the future. including hybrid warfare and unrestricted warfare that rely on the sophistication of information and communication technology, military

elements, and non-military aspects. In dealing with it, the Indonesian National Armed Forces (TNI) has the task of upholding state sovereignty, maintaining the territorial integrity of the Unitary State of the Republic of Indonesia based on Pancasila and the 1945 Constitution of the Republic of Indonesia, and protecting the entire nation and all of Indonesia's bloodshed from threats and disturbances to the integrity of the nation and state organized by War Military Operations (OMP) and Military Operations Other Than War (OMSP), must be able to adapt to developing strengths and capabilities as well as deploying strengths, both centralized and regional units (smaller, lighter, more mobile forces) (Harkavy, 2006). The defense system is a national interest that is considered a core value or something that is considered the most vital for the country and concerns the existence of a country. (Kalevi, 1981)

Along with the development of information and communication technology, the demands for the implementation of TNI operations are increasingly complex where assurance of interoperability, security, and reliability is a must. The deployment of the Communication and Electronics System (Siskomlek) within the TNI aims to support the smooth running of the TNI's main tasks, particularly in ensuring the smooth running and security of the TNI's Kodal (command and control) comprehensively.

Interoperability is the ability of a system, unit, or force to provide and receive services to and from other systems, units, or forces and to use the services exchanged in a way that enables them to work together effectively. Meanwhile, technical interoperability can be interpreted as a condition that can be achieved between electronic communication systems or electronic communication devices, when information or services can be exchanged directly and satisfactorily between them and/or their users (Kasih Prihantoro et al, 2019).

Following national defense policy, one of which is the development of a technology-based Tri Matra operating system which includes Network Centric Warfare (NCW), Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR), and Cyber Warfare to deal with threats that are "Irregular Warfare".

II. THEORETICAL BASIS

2.1. Network Centric Warfare

Network Centric Warfare is a command and control system concept that is applied in modern military operations, with interoperability capabilities for elements of military force that optimize the use of defense-based computer network systems. In the aspect of operational control, NCO (Network Centric Operation) can be operated in the operational area, which is capable of being integrated across all dimensions and military platforms, systems, and devices (Sweet, 2004). The NCO will carry out an information management system related to monitoring, controlling, and recording ongoing network activities to ensure that everything goes according to the operational plan, with a command and control center (Puskodal), a communication system, or satellite network that functions to carry out control, monitoring network conditions and performance including military intelligence, to monitor network security systems and produce documentation and data related to services provided by a Puskodal.

NCO is a theory that proposes that applying information age concepts to speed up communications and increase situational awareness through networking will improve both the efficiency and effectiveness of military operations. Proponents argue that this would allow combat forces to become smaller, operate more independently and effectively, and perform a different range of missions than non-networked forces (Wilson, 2007).).

A leading network-centric advocate describes the impact of network-centric warfare as follows: In traditional military operations, missions are assigned and planned, forces are organized, and operations are conducted to focus forces on objectives. This is a highly coordinated "step-by-step" cycle :periods of relative inactivity (the flat portion of the stride) where force is generated and action is coordinated alternate with periods of action (the vertical portion) where combat power is applied. However, when the forces are linked to create near-real-time situational awareness (see Figure 1), it can act continuously. No more pausing before deciding to take further action. The necessary information and adjustments are already available. Moreover, shared consciousness allows for a flattened and decentralized command structure, with decision making occurring at the lowest level of actual command (Smith, 2001).

2.2. Irregular Warfare

The new wars of the 21st century are manifested in irregular warfare, also known as unconventional warfare, asymmetric

warfare, low-intensity conflict, or civil tyranny. The term irregular warfare is used to describe forms of warfare in which the enemy may use non-traditional means, such as g. guerrilla attacks, terrorist attacks, subversion in the struggle for state power, and rebellion to control the local population (Hrnčiar, 2017). Irregular warfare prefers an indirect approach, although it may use various military forces and other capabilities to weaken the enemy. Irregular warfare, also known as irregular warfare, is defined as a violent conflict between states and non-state actors to gain legitimacy and influence from the surrounding community (Endo, 2017).

The geopolitical changes in the world that occurred at the end of the 20th century fundamentally changed the security environment and forced Western countries to engage in a new type of asymmetric military conflict with non-state actors, terrorist organizations, and criminal syndicates. New types of threats, multiple military conflicts, and the search for an effective response require reconsideration, generalization, and assessment of the latest military experience and the formulation of theoretical concepts that will help prepare for and operate effectively in zones of military conflict. This condition led to the formulation and formation of new military theories, including the theory of hybrid warfare. The hybrid war theory developed by Hoffman covers four aspects: conventional power, non-regular tactics, terrorism, and criminal acts in one battle space (Kilinskas, 2016).

III. METHODOLOGY

Literature research is a form of qualitative research that is usually carried out by searching for sources of information without going into the field. Library research can also be interpreted as research that is only based on written works, which include both published and unpublished research results.

The research used in this research is library research or library research, namely research conducted by collecting information or scientific writing aimed at research objects or collections of library materials, or research conducted to solve a problem basically based on critical review and thoroughly to the relevant library materials. Before conducting a literature search, researchers must first know exactly where the source of scientific information comes from. Some of the sources used are e.g. textbooks, scientific journals, statistical references, research results in the form of theses, dissertations, theses, and the internet and other relevant sources. (Anwar, 2016)

IV. RESULT AND DISCUSSION

4.1. Defense Information System Policy according to Minister of Defense Regulation No. 38 of 2011 concerning National Defense Information System Policy

Regulation of the Minister of Defense of the Republic of Indonesia Number 38 of 2011 concerning National Defense Information System Policies has accommodated and regulated the roles and duties of the Data and Information Center for each Matra in the TNI. In the appendix it is explained that the level of the national defense information system is following the authorities, interests, duties, and responsibilities as well as the functions carried out by each organizational stratum as follows:

1. Ministry of Defense level. Carry out the development and implementation of the National Defense Information System to support the main tasks and functions of the Ministry of Defense as well as the National Information System with the technical supervisor being the Ministry of Defense Data and Information Center, hereinafter abbreviated as the Ministry of Defense Data and Information Center.

2. TNI Headquarters Level. Carry out development and implementation of the National Defense Information System to support the main tasks and functions of the Indonesian National Armed Forces as well as information systems at the Ministry of Defense level with the technical supervisor being the Information Center and Data Processing of the Indonesian Armed Forces, hereinafter abbreviated as Information and Data Processing Center for the TNI.

3. Force Headquarters Level. Carry out development and implementation of the National Defense Information System within the Forces to support the main tasks and functions of the forces, as well as information systems at the TNI Headquarters level and the Ministry of Defence. The technical advisor for information systems in the Forces organizational unit is the Forces Information and Data Processing Service, hereinafter abbreviated as Forces Disinfolahta.

4. Main Command Level and Central Executing Agency. Carry out the development and implementation of the National Defense Information System within the Main Command and Central Executive Agency to support the main tasks and

functions of the Main Command and Central Implementing Agency, information systems at the Forces level, TNI Headquarters and the Ministry of Defense.

4.2. The Network Centric Warfare concept in the TNI's Integrated Three Dimensional Operations system

The synergy of the strengths of the three dimensions of the TNI in the ability to carry out Irregular Warfare, which is implemented in the integration of planning, operations, and training, organizing support to deploying the TNI's Defense Equipment System, in supporting implementation requires several supporting components including:

1. Modern and smart Command and Control System (Kodal). The Integrated Tri Matra Operation involves all three dimensions in which there are various elements of supporting units that have different operating patterns. Therefore, in its command and control function, a modern and intelligent support system is needed that can ensure that these supporting elements can be integrated and synergized with each other, so as to streamline operations to achieve the goals and objectives to be achieved. By using the Kodal system which is smart in processing various kinds of data and parameters about friendly troops, enemies, terrain, and weather in an operation as input for the system, so that output is visualized in the form of an information dashboard (semantic web) that is used by leaders and employees. staff in making the right decisions.

2. Communication is interoperable and runs on the right backbone. Integrated Tri Matra Operations must be supported by a communication backbone (Satellite, Microwave, Tactical Broadband, Radio Frequency, Fiber Optic) according to the operating field and communication equipment according to various settings and characteristics of each of these must be interoperable, so that it will optimize the information system. Hura, et al (2000) stated that at the strategic level, interoperability creates possibility for the development of integrated work between dimensions. At this level, the main issue in interoperability is the harmonization of the views, strategies, doctrines and power structures of each dimension. Interoperability is considered as the willingness of each dimension to work together for a long period of time in order to achieve and maintain common interests in facing threats. At the tactical level, Hura et.al (2000) stated that interoperability strategies must go hand in hand with interoperability technologies to shape environments, manage crises, and win wars. Interoperability gains at the tactical level obtained from the equivalence/fitness/compatibility between the system and data owned from each dimension/unit (Kusuma et al, 2021).

3. Digitalization and data computing. This Command and Control System application has the ability to manage and present data and parameters about its own troops, opponents, weather, and the field of operations that are represented in digital form in order to integrate all Alutsista that support operations. Data and parameters in digital form will be easier and faster to be computed by the operating Kodal system so that the Command and Control System will facilitate the deployment of forces, it will produce Command and control based on data and facts in the field (data/fact-based decisions).

4. Intelligence data integration system with an analysis system that is close to reality. One of the determining factors for the success of an operation is the support or availability of valid and accurate intelligence data and information (SIGINT, GEOINT MASINT, OSINT, HUMINT) (U.S. Intelligence Community). Raw data consisting of various formats, such as images, text, videos, and so on, is inputted into the intelligence database system which is integrated into the analysis system. So that the analysis obtained becomes supporting data for leaders in making decisions, through:

   a. SIGINT (Signals Intelligence). Is a method of collecting intelligence information that is carried out through analysis of trajectories and intercepted signal data, both communication signals between people or called Communications Intelligence (COMINT) or from electronic signals that are indirectly used in communication or called Electronic Intelligence (ELINT) (Lee, 2018)

   b. GEOINT (Geospatial Intelligence). Contains a series of data collection activities about human activities on Earth originating from the exploitation and analysis of geospatial images and information that describe, assess, and visually describe physical features and activities that are geographically referenced on Earth. Imaging can be obtained from visual photography, radar sensors, infrared sensors, lasers, and electrooptics (aerial photography). Broadly speaking, geospatial intelligence can be defined more simply as data, information, and information collected from entities that can be associated with specific locations above or below the earth's surface. Information collection methods can be in the form of pictures, signals, measurements, signatures, and human

resources, namely IMINT, SIGINT, MASINT, and HUMINT, as long as the geographic location can be associated with the information. Geospatial intelligence can synthesize information or other data that can be conceptualized in a geospatial context. Geospatial Intelligence can be derived completely independently from satellite or aerial imagery and can be clearly distinguished from IMINT (Imagery Intelligence). Geospatial Intelligence can be described as a product made at the time of delivery, i.e. based on the amount of analysis performed to solve a particular problem, not based on the type of data used. (Hotroiman, 2017)

c. HUMINT (Human Intelligence). Is an espionage activity or information gathering activity, both open and closed, in which the source of the information is provided by humans. In terms of the type of information collected, there are various kinds. If during a war, the information collected is about Weather, Terrain and the Enemy or abbreviated as CU-MEMU (strategic intelligence), which is needed in War Military Operations (OMP), and information on aspects such as Ideology, Politics, Economics, Social Culture and Defense Security (Ipoleksosbudhankam) versus (Strategic Intelligence) are used in Military Operations Other Than War (OMSP).

d. OSINT (Open Source Information) is an activity of collecting data from publicly available sources (open sources) for use in intelligence contexts where available information is collected, exploited, and disseminated promptly.

e. MASINT (Measurement and Signature Intelligence) is a technique of gathering intelligence, which functions to detect, track, identify, or describe the unique characteristics of fixed or dynamic target sources. The form integration between data, intelligence systems, and analysis systems is a form of an integrated system of systems, which in the end will be able to support the TNI's Three Dimensional Integrated Operations more optimally.

5. The Integration of Sensor Systems. To be able to optimally support the operation of the TNI's Three Dimensions Integrated, then all sensor systems (radar, surveillance system), integration of these sensor systems, it is hoped that the surveillance and reconnaissance functions will have Link-Data as input to the TNI's Alutsista sensor system in a joint operation. The NCW war concept is a fighting concept using integrated information technology, which integrates all layers of data information by adhering to the PAID principle (Procedure, Application, Infrastructure, and Data)

V. CONCLUSION

The realization of the interoperability of the Integrated Three Dimensional Operations, carried out by the TNI, is a necessity in the development of defense posture, especially the improvement of the Electronic Warfare aspect in dealing with Irregular Warfare with the availability of intelligence data and information (SIGINT, GEOINT MASINT, OSINT, HUMINT), as well as surveillance capabilities and reconnaissance has Link-Data. Where the concept of TNI force operations implementing Joint Operations requires the capabilities of the elements/units of the TNI AD, TNI AL, and TNI AU as well as involving assets/capabilities of reserve/support components related to Electronic Warfare capabilities, with an integrated and synergized system to streamline operations to achieve goals and the goals to be achieved. The progress and development of combat information technology are directly proportional to the budget requirements and the needs of Human Resources (HR) in the field of information technology, including organizational/institutional systems at TNI Headquarters. The concept of Network Centric Operation in the TNI's Three Dimensional Integrated Operations is urgently needed as an effort to overcome the problems that occur in the field of operations involving all dimensions of the TNI with all existing systems within the internal dimensions, in the implementation of War Military Operations And Military Operations Other Than War.

REFERENCES

[1] Cascio, J. (2020) *Facing the Age of Chaos*. Available at: https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d (Accessed: 13 April 2023).

[2] Endo, T. (2017) *The Conceptual Definition of "Irregular Warfare" and the Today's International Security Environment, International Forum on War History: Proceedings*. Available at: http://www.nids.mod.go.jp/english/event/forum/pdf/2017/04_endo.pdf

[3] Harkavy, Robert E, "Thinking About Basing", dalam Lord, Carness (et.all), Reposturing the Force: U.S. Overseas Presence in the Twenty First Century, Naval War College Newport Papers 26. Newport, Rhode Island: Naval War College Press, 2006, hal.19

[4] Hotroiman, Seweit. 2017. Penggunaan Geospatial Intelligence (Geoint) Pada Program Nationwide Operational Assessment Of Hazard (Noah) Di Filipina Dalam Studi Peperangan Asimetris. *Jurnal Prodi Peperangan Asimetris*. Vol 3 no 3 pp 1-16

[5] Hrnčiar, M. 2017. Keystones of irregular warfare. *International Conference*

[6] Hura, M. 2000. A Broad Definition of Interoperability. Dalam M. Hura, Interoperability: A Continuing Challenge in Coalition Air Operations (hal. 7-15). California: Rand Corporation.

[7] Kalevi J. Holsti, International Politics: A Framework of Analysis, (New Delhi: Prentice Hall, 1981), hal. 200

[8] Kasih Prihantoro Zakariya, Lukman Yudho Prakoso, Ratna Damayanti, A. D. (2019). Public Policy Analysis of Defense Areas and Defense Area Plan In Grati Pasuruan. The 3th Indonesia International Defense Sciense Seminar, 2(Universitas Pertahanan), 483–490

[9] Kilinskas, K. (2016) 'Hybrid Warfare: An Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine?', *Lithuanian Annual Strategic Review*, 14(1), pp. 139–158. doi: 10.1515/lasr-2016-0006.

[10] *Knowledge-Based Organization*, *23*(1), 150-154.

[11] Lee, Bartholomew. "Radio Spies – Episodes in the Ether Wars" (PDF). Diarsipkan dari versi asli (PDF) tanggal 2018-10-06.

[12] *LF*, *5*, 52

[13] Malantowicz, A. 2013. Civil war in Syria and the new wars debate. *Amsterdam*

[14] Peraturan Menteri Pertahanan Nomor 38 Tahun 2011 Tentang Kebijakan Sistem Informasi Pertahanan

[15] Sanusi, Anwar Metodologi Penelitian Bisnis,(Jakarta : Salemba Empat,2016), h.32

[16] Smith, Edward. 2001. Network-centric Warfare. Naval War College Review. Vol 54 no 1 p. 2

[17] Sweet,Norman. Command and Control Research and Technology Symposium The Power of Information Age Concepts and Technologies : Network Centric Applications and C4ISR Architecture, (Massachusetts, Hanscom Air Force Base, 2004, Standard Form 298), hal. 5

[18] Wilson, Clay. 2007. Network Centric Operations: Background and Oversight Issues for Congress. American Military University, p 2