



NETWORK CENTRIC WARFARE (NCW): KONSEP PEPERANGAN MODERN TNI

Gita Wisnuwardhana¹, Priyanto², Dudik Purwanto³

¹Universitas Pertahanan Republik Indonesia

²Universitas Pertahanan Republik Indonesia

³Sekolah Staf dan Komando TNI

*¹ gita_avionic98@yahoo.com, priyanto@idu.ac.id

Korespondensi penulis: gita_avionic98@yahoo.com

Abstract. *The national defense system must undergo transformation in line with the rapid and sophisticated advancement of technology, particularly in adapting military doctrines to remain responsive to emerging challenges. The adoption of defense technology within the framework of modern warfare is embodied in the implementation of the Network Centric Warfare (NCW) system within the Indonesian National Armed Forces (TNI). This aims to obtain real-time and accurate data and information through integration and interoperability across TNI weapon systems to support both Military Operations for War (OMP) and Military Operations Other Than War (OMSP). Despite encountering several obstacles in the development of NCW, the TNI continues to pursue innovative breakthroughs to overcome these challenges. This study employs a descriptive method, drawing upon both primary and secondary sources to identify key issues and formulate strategic recommendations for the development of TNI's Network Centric Warfare (NCW).*

Keywords: *TNI Network Centric Warfare, Concept, Modern Warfare, TNI*

Abstrak. Sistem pertahanan nasional harus melakukan transformasi seiring perkembangan teknologi yang sangat cepat dan canggih dalam melakukan perubahan doktrin perang agar menjadi adaptif terhadap tantangan baru. Adopsi teknologi pertahanan dalam konsep peperangan modern ini diimplementasikan dalam sistem Network Centric Warfare (NCW) di lingkungan TNI untuk mendapatkan data dan informasi secara cepat dan akurat melalui integrasi maupun interoperability pada sistem alutsista TNI dalam rangka mendukung tugas OMP maupun OMSP. Walaupun dalam pelaksanaan Pembangunan NCW mengalami beberapa hambatan, namun TNI terus melakukan terobosan-terobosan dalam mengatasi hambatan tersebut. Dalam penulisan kajian ini, penulis menggunakan metode deskriptif serta pengumpulan data yang berasal dari berbagai sumber primer dan sekunder untuk mengidentifikasi permasalahan dan merumuskan strategi pembangunan Network Centric Warfare (NCW) TNI.

Kata kunci: Network Centric Warfare TNI, Konsep, Peperangan Modern, TNI

1. LATAR BELAKANG

Perkembangan teknologi telah membawa dampak terhadap doktrin perang yang terus berubah, sehingga keunggulan teknologi yang dikuasai dapat meningkatkan kemampuan berperang baik kemampuan menyerang maupun bertahan. Keunggulan dalam penggunaan teknologi canggih dapat merubah strategi dan taktik pertempuran secara efektif dan efisien. Salah satu teknologi yang memiliki dampak besar dalam doktrin perang adalah teknologi



informasi dan komunikasi (TIK) yang memiliki keunggulan dalam kecepatan dan keakuratan yang memungkinkan untuk memperoleh keunggulan dalam peperangan.

TNI (Tentara Nasional Indonesia) saat ini telah melakukan adopsi teknologi berupa transformasi digital sebagai upaya untuk memperbarui dan meningkatkan efektivitas kinerja TNI dengan memanfaatkan kemajuan teknologi informasi dan komunikasi (TIK). Kelebihan penggunaan teknologi digital pada sektor pertahanan tidak hanya untuk efisiensi tetapi juga akurasi dalam memproses dan menganalisis data dengan cepat. Teknologi digital juga diharapkan dapat meningkatkan kemampuan pengawasan dan pengendalian dalam operasi militer yang akan memberikan manfaat lebih besar di medan tempur dengan kecepatan dan keakuratan komunikasi data dan pertukaran informasi yang saling terhubung di antara satuan yang terlibat dalam operasi serta pengambilan keputusan yang lebih akurat oleh komando pengendali.

Seiring dengan kemajuan teknologi, pertahanan nasional harus mengikuti perubahan yang terjadi agar menjadi adaptif terhadap tantangan baru. Sebaran geografis unit militer Indonesia yang luas dengan kondisi geografis yang sangat beragam memiliki tantangan kesulitan yang tinggi dalam mengembangkan sistem komunikasi digital yang dapat menjamin alur informasi dan komunikasi yang dapat saling terhubung dengan efektif dan efisien. Pada lingkup pertahanan terdapat beberapa sistem informasi antara lain C4ISR (Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance) istilah dalam militer Indonesia lebih dikenal dengan K4IPP (Komando, Kontrol, Komunikasi, Komputer, Intelijen, Pengawasan, dan Pengintaian). Kebijakan C4ISR tertuang di dalam Permenhan Nomor 8 Tahun 2016. Pada pasal 18 ayat 1e dinyatakan bahwa pembinaan sistem komunikasi dan teknologi komunikasi diarahkan untuk dapat terselenggaranya sistem K4IPP (Komando, Kendali, Komunikasi, Komputer, Intelijen, Pengawasan, dan Pengintaian) yang aman dan dapat diandalkan.

kebijakan Kementerian Pertahanan RI yang tertuang dalam Permenhan Nomor 12 Tahun 2021 tentang Kebijakan Pertahanan Negara Tahun 2020-2024 yang memuat tentang sistem komunikasi dengan teknologi Network Centric Warfare (NCW). Kebijakan pembangunan menyatakan : "Mengintegrasikan jaringan sistem Trimatra terpadu (tiga mata secara terpusat) atau Network Centric Warfare (NCW) dalam rangka meningkatkan interoperabilitas operasi antara kekuatan darat, laut, udara, serta antariksa dan siber.

Implementasi NCW menjadi salah satu fokus utama dalam strategi pertahanan modern di seluruh dunia, termasuk Indonesia. Beberapa contoh implementasi NCW di TNI yaitu pengembangan Sistem Komunikasi Taktis Terpadu (SKTT) pada TNI AD, TNI AL dan TNI AU yang memungkinkan pertukaran informasi secara real time dalam situasi perang. Penerapan NCW sistem pertahanan udara yang terintegrasi pada tahun 2018, implementasi teknologi Unmanned Aerial Vehicle (UAV) pada TNI AD dan TNI AU sebagai sarana pengintai dan pengawasan yang memungkinkan pengumpulan data informasi secara real time untuk mendukung pengambilan keputusan yang tepat.



Saat ini Mabes TNI sedang membangun sistem NCW berupa Sistem Interoperability Kodal (SIK) TNI yang diharapkan dapat mewujudkan interoperability Tri Matra Terpadu dengan tiap-tiap Puskodal Mabes Angkatan melalui kerjasama dengan salah satu penyedia teknologi dari Yunani (Scytalys) yang bekerjasama dengan beberapa industri pertahanan Indonesia.

Dalam mengembangkan Sistem Operasi Tri Matra Terpadu, TNI masih belum mampu menyediakan segala kebutuhan secara mandiri sehingga tetap membutuhkan kerjasama dan kolaborasi dengan berbagai pihak yang berkompeten di bidang komunikasi dan elektronika lainnya. Seperti Kerjasama dengan BSSN terkait dengan keamanan jaringan dari serangan siber, PT. Telkom yang berhubungan dengan ketersediaan jaringan komunikasi serta dengan PT. LEN untuk mengembangkan peralatan elektronika. Kerjasama dengan pihak lain sangat memungkinkan namun soliditas di dalam internal TNI sendiri mutlak diperlukan. Tahun 2021 Kepala Staf Angkatan Darat (KASAD) Jenderal TNI Andika Perkasa menyatakan bahwa saat ini di lingkungan TNI sendiri masih terdapat adanya ketidakseragaman/ego sektoral dari masing-masing Angkatan dalam mm mengembangkan infrastruktur interoperability komunikasi, sensor elektronika dan komunikasi data. Permasalahan lainnya yang harus dihadapi dalam pembangunan NCW tersebut adalah kebutuhan jaringan komunikasi yang dapat menjangkau seluruh wilayah Indonesia yang demikian luas, sementara teknologi yang dimiliki untuk menyediakan komunikasi bagi unit militer yang mobile seperti pesawat udara TNI AU dan kapal perang TNI AL masih terbatas.

Teknologi Network Centric Warfare (NCW) yang berhubungan dengan peperangan yang melibatkan seluruh simpul yang saling terhubung dalam jaringan kerja tunggal menghadapi tantangan lain seperti pembiayaan yang besar dalam membangun infrastruktur untuk menyediakan hardware dan software yang handal sesuai kebutuhan. Pada Upacara HUT Ke-75 TNI yang dilaksanakan pada tanggal 5 Oktober 2020 di Istana Negara, dalam amanatnya Presiden meminta agar TNI terus melakukan transformasi teknologi. Transformasi teknologi tersebut diharapkan agar seluruh prajurit TNI mampu memahami dan memanfaatkan kemajuan teknologi yang demikian pesat, terutama teknologi informasi dan teknologi artificial intelligence, sehingga mampu mengantisipasi perubahan karakter pertempuran masa depan yang memiliki daya hancur sangat besar atau high level destruction. Untuk itu, diperlukan adanya perubahan kebijakan yang semula dari kebijakan belanja pertahanan, menjadi kebijakan investasi pertahanan yang dirancang secara terukur, sistematis, dan dilaksanakan secara konsisten serta berkesinambungan agar TNI memiliki kekuatan modern sejalan dengan perkembangan teknologi.

Tantangan lainnya terkait komponen yang tercakup di dalam sistem informasi adalah transmisi data, proses analisa data dan keamanan data. Tantangan software dalam sistem program input dan akses data rentan terhadap peretasan dan penyalahgunaan data yang mengarah pada kejahatan siber. Oleh karena itu keamanan sistem NCW juga menjadi perhatian penting melalui penggunaan teknologi yang canggih seperti artifisial inteligen serta penerapan standar keamanan seperti penerapan enkripsi, firewall, antivirus dan tindakan keamanan lainnya. Sehingga kerjasama dengan Lembaga keamanan siber seperti BSSN sangat diperlukan untuk meningkatkan kemampuan dan daya tangkal sistem informasi milik TNI untuk kepentingan pertahanan nasional.

2. TINJAUAN PUSTAKA

Teori Strategi Pertahanan Negara. Strategi pertahanan negara dapat didefinisikan sebagai rancangan tindakan yang melibatkan sasaran serta kebijakan untuk mencegah, melindungi, dan membela kepentingan nasional dari berbagai macam kekerasan dan serangan pihak lain (La Ode et al, 2021).

Teori Network Centric Warfare (NCW). *Network centric operation* atau Network Centric Warfare merupakan penggabungan sistem dari ketiga matra (Darat, Laut dan Udara) yang didukung oleh sarana komunikasi satelit. Pada perkembangannya, NCW menetapkan sistem pertahanan udara yang terintegrasi dalam suatu jaringan bertempur atau Network Centric Warfare serta mengembangkan sistem operasi Trimatra yang berbasis teknologi C4ISR dan Cyber Warfare. NCW secara spesifik merupakan Interface yang dirancang dengan memenuhi karakteristik hardware (perangkat keras), software (perangkat lunak), network (jaring komunikasi) dan brainware (sumber daya manusia / pengawak alat komunikasi / pengguna / operator alat komunikasi) agar interface yang dirancang baik itu perancangan interface inter modular, rancangan eksternal maupun rancangan manusia – computer dapat menghubungkan antar protocol yang digunakan dalam pengiriman data untuk diproses menjadi informasi.

Teori Sistem. McLeod dan Schell (2007) dalam merumuskan teori tentang sistem, membaginya dalam 5 jenis sistem, yaitu antara lain:

- a. *Transaction Processing System (TPS).* Transaction processing system adalah sebuah sistem komputer yang didesain untuk mengolah transaksi yang tidak hanya didesain untuk mengolah transaksi yang tidak hanya terbatas pada database atau file system namun juga melakukan pengolahan beberapa operasi transaksi dimana semua transaksi harus berhasil atau semua transaksi harus dibatalkan.
- b. *Management Information System (MIS).* Management information system adalah sebuah sistem yang sudah terkomputerisasi yang melakukan pengolahan data agar bisa digunakan oleh orang yang membutuhkannya.
- c. *Virtual Office System.* *Virtual office system* merupakan pengembangan dari Office Automation System, yaitu mesin komputer (hardware) dan software yang digunakan untuk membuat, mengumpulkan, menyimpan, memanipulasi dan menyebarkan informasi untuk kebutuhan perkantoran (perusahaan) secara digital untuk mengerjakan tugas-tugas perusahaan guna mencapai tujuan yang telah ditetapkan.
- d. *Decision Support System (DSS).* *Decision support system* merupakan sebuah sistem yang membantu seorang manajer atau sekelompok kecil manajer untuk memecahkan sebuah permasalahan.
- e. *Enterprise Resource Planning System (ERP).* *Enterprise resource planning system* merupakan sistem yang terkomputerisasi yang melibatkan seluruh resource manajemen dalam sebuah perusahaan.



Teori Interoperability. Michael S. McBeth (2003) dalam artikel ilmiah yang berjudul “*A Theory of Interoperability Failures*” menyatakan bahwa Institute of Electrical and Electronics Engineers (IEEE) mendefinisikan interoperability yaitu: “*the ability of two or more systems to exchange information and to mutually use the information that has been exchanged.*” Penggunaan teori interoperability pada penelitian ini adalah sebagai penunjang dalam perancangan interface yang digunakan untuk mengintegrasikan data dari sensor yang diterima. Perancangan interoperability data link pada peralatan elektronika alutsista Hanud menjadi tuntutan mendesak. Hal ini disebabkan oleh kebutuhan data dalam rangka pengambilan kebijakan untuk mengatasi problem yang ada khususnya pada pengamanan wilayah udara NKRI yang dilakukan oleh TNI AU.

3. METODE PENELITIAN

Kajian terkait Network Centric Warfare (NCW) TNI ini menggunakan metode penelitian deskriptif kualitatif serta pengumpulan data yang berasal dari berbagai sumber primer dan sekunder, yang selanjutnya dianalisis untuk mendapatkan hasil kajian terkait korelasi antara Network Centric Warfare (NCW) dengan konsep peperangan modern di lingkungan TNI.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian.

Pembangunan NCW memerlukan waktu dan biaya yang tidak sedikit, selain itu diperlukan kesinambungan dalam rangka terwujudnya NCW TNI. Konsep pembangunan NCW TNI telah di canangkan pada tahun 2018 melalui Kebijakan Panglima TNI yang tertuang dalam Keputusan Panglima TNI Nomor Kep/27/1/2018 tanggal 15 Januari 2018 tentang Pokok-pokok Kebijakan Panglima TNI Tahun 2018, diantaranya pembangunan Network Centric Warfare, yang pelaksanaannya akan dibangun berdasarkan beberapa fase yaitu : fase pertama, membangun tingkat pusat (Pusdalops TNI) berupa kemampuan sistem berikut infrastruktur guna mendukung C4ISR, data/ink, multi data/ink gateway, integrasi Puskodal Angkatan serta pilot project sensor maritim; fase kedua, melanjutkan pencapaian pembangunan fase pertama berupa pembangunan tingkat Kotama Operasional agar dapat terhubung dengan Pusdalops TNI dan Puskodal Angkatan; fase ketiga, melanjutkan pencapaian pembangunan fase-fase sebelumnya berupa pembangunan pada tingkat taktis alutsista serta sensor-sensor; dan fase keempat, menyempurnakan pencapaian pembangunan fase-fase sebelumnya dengan proof of concept dalam konteks operasi gabungan yang diberdayakan pada OMP maupun OMSP.

Adapun Perkembangan kemajuan pembangunan NCW TNI sampai dengan saat ini adalah sebagai berikut:

a. **Tingkat Mabes TNI.** Saat ini Mabes TNI telah memasuki tahap kedua pada pembangunan NCW, yang mana tahap pertama telah diawali pada tahun 2015 sampai dengan 2019 dengan sasaran capaian antara lain : pertama, Pembangunan Pusdalops TNI yang memiliki kemampuan memberikan Common Operational Picture (COP) yang terintegrasi secara nasional melalui interkoneksi Puskodal Angkatan untuk menjalankan kodalops yang efisien; kedua, pembangunan data link nasional; ketiga, pembangunan multi data/link gateway guna memudahkan sistem yang sudah tergelar agar tetap dapat diberdayakan hingga batas akhir usia pakai karena pada kenyataannya populasi existing system lebih dominan dibandingkan dengan sistem yang baru; keempat, pembangunan Integrated Surveillance Maritime System (ISMS) di Natuna yang dapat dioperasikan maupun dikendalikan jarak jauh dari Mabes TNI.

b. **Unsur Darat.** Saat ini TNI AD telah mengembangkan Integrated Command and Control System (ICCS) dengan menggunakan protokol komunikasi CY-16H/Kartika Link yang diharapkan untuk menjamin sistem yang telah digelar akan kompatibel dengan sistem baru yang akan diadakan. Dengan terimplementasinya sistem ICCS tersebut, TNI AD saat ini telah menerapkan peperangan berbasis jaringan yang mana segenap elemen taktis yang beroperasi akan dapat memberikan informasi yang dimiliki kepada elemen taktis lainnya bahkan kepada elemen strategis. Sensor-sensor yang berada pada elemen taktis seperti kamera, pengukur jarak berbasis laser (Laser Range Finder), pengukur suhu setempat, parameter kendaraan tempur dan posisi masing-masing elemen dapat diketahui oleh elemen pengendali yang berada di Puskodal tanpa melakukan plotting secara manual di peta sesuai dengan tingkatan operasionalnya.

Untuk mengoperasikan ICCS tersebut, TNI AD sampai dengan saat ini masih belum memiliki infrastruktur backbone jaringan komunikasi data yang mampu menghubungkan antar elemen dengan jarak yang jauh serta kapasitas komunikasi data yang besar. Untuk memenuhi kebutuhan jaringan tersebut TNI AD masih mengandalkan alokasi bandwidth dari pihak ketiga berupa komunikasi satelit sebesar 8 MHz dan jalur VPN-IP PT. Telkom.

Berkaitan dengan keamanan jaringan yang dibutuhkan untuk menjamin keamanan komunikasi data yang dilaksanakan oleh TNI AD, saat ini telah dibentuk sebuah satuan pelaksana Pusat Sandi dan Siber AD (Pussansiad) pada tanggal 21 April 2020 dengan tugas pokok menyelenggarakan pembinaan personel serta fungsi sandi dan siber. Dengan usia yang masih relatif muda tersebut, saat ini Pussansiad masih banyak melakukan penataan dan pemenuhan organisasi baik personel dan materiel serta pembenahan prosedur operasional. Disamping itu, saat ini TNI AD telah memiliki Laboratorium Siber yang berkedudukan di bawah Pusdikhub Kodiklat TNI AD dengan fungsi sebagai tempat pendidikan siber di lingkungan TNI AD.

c. **Unsur Laut** Pembangunan NCW pada matra laut saat ini terus menerus dilaksanakan dengan sasaran utamanya adalah kemampuan TNI AL dalam melaksanakan komando pengendalian terhadap seluruh unsur Angkatan Laut yang terintegrasi dalam Sistem Senjata Armada Terpadu (SSAT) melalui sebuah sistem Command and Control Management System (C2MS) yang berfungsi sebagai kodal antara unsur operasional dan pimpinan. Sistem ini bekerja dengan memasukkan data yang diperoleh secara manual dengan basis komunikasi data yang digunakan adalah transmisi satelit dan radio, dimana basis satelit diperoleh dari tracking AIS (Automatic Identification System).

Saat ini Puskodal Mabes TNI AL sedang dalam pelaksanaan revitalisasi yang mulai dilaksanakan pada Oktober 2021 dengan melakukan pengembangan sebuah sistem baru yaitu Spartan (System Performance Readiness and Tactical Analysis). Program revitalisasi Puskodal tersebut terdiri dari revitalisasi hardware, software, organisasi dan sumber daya manusia. Adapun target dari revitalisasi Puskodal tersebut diharapkan nantinya Puskodal akan memiliki beberapa fitur aplikasi yang terdiri dari; monitoring laut Indonesia, tracking KRI untuk analisa efektifitas operasi dan keamanan navigasi, analisis kapal yang dicurigai melakukan pelanggaran di laut Indonesia, distress signal mandiri TNI AL, komunikasi real time dari unsur SSAT, dan akses surveillance system dengan IMSS dan KRI.

Untuk mendukung kebutuhan komunikasi data dalam mengoperasikan sistem C2MS maupun Spartan, secara umum TNI AL banyak memanfaatkan jaringan komunikasi satelit dikarenakan operasional yang dilaksanakan lebih dominan pada basis perairan dibandingkan dengan daratan. Terdapat infrastruktur komunikasi satelit pada beberapa KRI maupun instalasi yang berada di pinggir pantai, yang mana membutuhkan alokasi bandwidth yang lebih besar dibandingkan dengan TNI AD dan TNI AU sehingga saat ini TNI AL telah memiliki alokasi bandwidth Ku Band sebesar 18 MHz untuk mendukung operasional KRI yang dilaksanakan di seluruh perairan Indonesia.

d. **Unsur Udara.** Saat ini TNI AU belum menggelar secara permanen jaringan komunikasi Kodal yang digunakan sebagai sarana bagi Panglima/Komandan dalam mengendalikan dan memonitor pelaksanaan operasi sesuai dengan rentang kendali yang dimilikinya dengan memanfaatkan backbone Link VPN-IP dan VSat yang telah tersedia. Kedepan jaringan ini sangat penting untuk dibangun secara permanen guna tercapainya K4IPP TNI AU yang akan digunakan di seluruh Pangkalan Udara, Puskodal Koopsudnas dan Puskodal Mabes AU. Untuk mewujudkan hal tersebut, TNI AU telah membangun beberapa sistem diantaranya Voice Data Communication System (VDCS) yang digunakan untuk menyelenggarakan operasi penegakan hukum dan pengamanan wilayah udara. VDCS dikembangkan untuk menghubungkan jaringan komunikasi secara terus menerus dan real time berupa layanan komunikasi data, suara, video maupun file digital lainnya yang mempunyai fleksibilitas tinggi namun tetap bersifat rahasia. Melalui VDCS ini memungkinkan terjalinnya komunikasi antara pilot pesawat dengan satuan radar di darat dalam rangka koordinasi maupun pemberian instruksi antara kedua pihak dengan jarak jangkauan yang semakin jauh.

Sistem lain yang dibangun TNI AU adalah Communication Tactical Data Link System (CTDL) yaitu jaringan yang dibangun untuk melakukan sharing informasi dan pertukaran tactical data atau combat information secara real time, aman dan lengkap antara pesawat Patmar dengan Pangkalan Udara dan kapal laut untuk kepentingan taktis. Sedangkan untuk kepentingan strategis dilakukan komunikasi data dari pesawat ke ground station (Puskodal) dengan melakukan integrasi jaringan dengan Base Tranceiver Star menggunakan jaringan VPN-IP yang tergelar di setiap Pangkalan Udara.

Untuk menjamin keberlangsungan sistem VDCS maupun CTDLs diperlukan jaringan komunikasi yang dapat diandalkan. Secara umum penggunaan backbone komunikasi TNI AU hampir sama dengan TNI AL, dimana didominasi pada infrastruktur komunikasi satelit. Hal ini disebabkan banyaknya instalasi TNI AU yang berada pada lokasi yang cukup jauh dari lokasi strategis pertimbangan penempatan sensor yang berada di perkotaan. TNI AU menggunakan komunikasi satelit pada infrastruktur permanen, seperti Satuan Radar untuk menghubungkan radar dan pelaporan ke tingkat yang lebih tinggi sesuai struktural hirarkinya. Meskipun demikian, seiring dengan pertumbuhan di berbagai daerah, maka infrastruktur yang berkaitan dengan telekomunikasi ikut tumbuh di daerah tersebut. Hal ini memberikan implikasi pada beberapa Satuan Radar sehingga memungkinkan untuk terhubung melalui jasa telekomunikasi tertentu sebagai poros ganda selain komsat. Adapun alokasi frekuensi komsat C Band yang dimiliki oleh TNI AU sebesar 10 MHz, sedangkan untuk Koopsudnas sebesar 37 MHz.

4.1 Pembahasan

Dalam mengoptimalkan pembangunan *Network Centric Warfare* (NCW) TNI, maka diperlukan beberapa strategi dan upaya yang merupakan bagian penting dalam mengatasi permasalahan yang dihadapi.

a. Bidang Personel. Jumlah personel yang memiliki kualifikasi Teknologi Informasi dan Komunikasi (TIK) sebagai pengawak NCW TNI yang dibutuhkan oleh Mabes TNI dan Mabes Angkatan pada semua tingkatan baik operator, teknisi dan manajer masih mengalami kekurangan. Untuk mengatasi hal tersebut, TNI telah melakukan beberapa terobosan yakni dengan melakukan rekrutmen untuk level operator dan teknisi pada strata Bintara dari SMK jurusan IT. Akan tetapi pada level manajer (Perwira) masih mengalami kendala diakarenakan minimnya rekrutmen yang berasal dari sarjana IT.

Oleh karena itu, perlu dilakukan rekrutmen secara internal personel TNI yang sudah aktif berdinamika tetapi memiliki minat dan kemampuan talenta digital meskipun selama ini tidak berdinamika di bidang TIK. Disamping itu perlu juga dilakukan rekrutmen secara khusus untuk tenaga profesional di bidang siber yang masih sangat langka dan sulit untuk didapatkan dari internal personel TNI. Para tenaga ahli bidang siber tersebut dapat diperoleh dari komunitas siber/hacker yang selama ini belum banyak di dekati

dan dilibatkan dalam bela negara. Hal ini perlu mendapatkan dukungan kebijakan dari Kementerian Pertahanan dalam hal ini Dirjen Potensi Pertahanan.

Mabes TNI perlu menyiapkan Lembaga Pendidikan dan Pelatihan khususnya untuk menyiapkan SDM yang berkompeten di bidang TIK agar dapat menghasilkan personel TNI yang profesional pada semua tingkatan baik operator, teknisi maupun manajer sebagai pengawak NCW agar dapat menjamin tercapainya interoperabilitas

b. Ketersediaan infrastruktur dan jaringan komunikasi. Persoalan mengatasi infrastruktur dan jaringan komunikasi di daerah yang sulit dijangkau serta integrasinya menjadi persoalan yang cukup rumit di lingkungan TNI. Hal ini disebabkan karakteristik yang sangat khas dan berbeda-beda oleh masing-masing matra. Beberapa variabel atau faktor yang bisa diukur untuk melihat tercapainya interoperabilitas Kodal TNI adalah tersedianya infrastruktur dan jaringan komunikasi yang dapat memenuhi kebutuhan konektivitas yang handal. Upaya yang dapat dilakukan diantaranya adalah melanjutkan pembangunan infrastruktur jaringan terrestrial seperti pengembangan kabel serat optik. Sedangkan jaringan nirkabel dapat dikembangkan jaringan sambungan data langsung (SDL) VPN jaringan GSM, dan gelombang radio. Disamping itu perlu pula dikembangkan jaringan satelit dengan kapasitas bandwidth yang lebih besar serta jangkauan yang lebih luas untuk dapat menjamin konektivitas operasional alutsista yang mobile dan tidak terjangkau jaringan terrestrial seperti operasional KRI dan Pesawat Udara. Untuk mengembangkan jaringan tersebut Kementerian Pertahanan dan TNI dapat berkolaborasi dengan Kementerian Kominfo untuk dapat bersama-sama memanfaatkan Satelit Satria-1 yang diluncurkan pada tanggal 19 Juni 2023 di Amerika Serikat. Ketersediaan komunikasi satelit dengan bandwidth yang cukup besar tersebut diharapkan dapat memastikan konektivitas digital yang handal di seluruh wilayah Indonesia.

Selain itu, pengembangan data link TNI dalam bentuk Indonesia National Data Link yang saat ini sedang dikerjakan oleh PT. LEN perlu untuk didukung dan didorong agar dapat segera diwujudkan. Pemerintah dalam hal ini Kementerian Pertahanan bersama dengan TNI harus memiliki komitmen yang kuat untuk menuntaskan program tersebut secara konsisten dengan dukungan kebijakan dan anggaran yang memadai.

Selanjutnya pengembangan multi data link gateway tetap harus dilanjutkan untuk dapat menghubungkan sistem-sistem yang beragam dan menggunakan varian data link yang sudah existing saat ini. Gateway ini akan memungkinkan pertukaran informasi antara sistem-sistem yang berbeda dan memastikan kompatibilitas dan interoperability antara mereka serta mengintegrasikan berbagai platform dan sistem yang berbeda dalam NCW TNI saat ini. Oleh karena itu, perlu adanya dukungan dari setiap matra untuk bekerjasama dan menghilangkan ego masing masing satuan yang saat ini telah memiliki sistem informasi dan komunikasi dengan kesediaannya untuk membuka protokolnya sehingga dapat terintegrasi dengan multi datalink gateway tersebut.

c. Keamanan jaringan NCW dalam menghadapi ancaman serangan siber. Dalam pengamanan jaringan NCW, TNI menghadapi beberapa tantangan antara lain meningkatnya konektivitas jaringan yang membuat jaringan tersebut rentan terhadap serangan dan ancaman siber. Untuk mengatasi permasalahan ini, TNI perlu melakukan beberapa upaya, antara lain ;

Pertama, Keamanan berbasis alat. TNI harus menjaga keamanan jaringan dengan menggunakan perangkat jaringan yang dilengkapi dengan metode pengamanan dari manufaktur. Misalnya, perangkat jaringan sudah dilengkapi dengan enkripsi standar internasional setara 128 bit atau lebih. Selain itu, TNI juga dapat menambahkan alat keamanan khusus seperti alat enkripsi/deskripsi untuk menyandi atau menerjemahkan transmisi yang keluar atau masuk pada peralatan. Hal ini memastikan bahwa keamanan jaringan sudah terjamin melalui peralatan itu sendiri.

Kedua, Pengawasan keamanan siber (cyber security). TNI mengimplementasikan pengawasan keamanan jaringan melalui Security Operation Center (SOC). SOC merupakan bagian dari pendukung keamanan teknologi informasi dan komunikasi (TIK) dalam jaringan. Di dalam SOC, dilakukan pemantauan dan analisis ancaman dan insiden serta tanggung jawab manajemen dalam mengatasi insiden. Tujuan utama dari SOC adalah meningkatkan keamanan TIK dengan mendeteksi dan merespon ancaman dan serangan sebelum berdampak pada jaringan operasional.

Ketiga, Kebijakan sistem pengamanan dan akses pengguna. TNI memberikan perhatian pada kebijakan sistem pengamanan, termasuk tata laksana akses bagi pengguna jaringan NCW. Hal ini bertujuan untuk memastikan bahwa pengguna jaringan memperhatikan aspek keamanan informasi dan sistem telekomunikasi, melindungi informasi rahasia negara, informasi pribadi, dan informasi yang dianggap penting oleh Kementerian Pertahanan dan TNI. Selanjutnya TNI juga menyusun dan menerapkan Buku Petunjuk Operasional NCW yang akan memuat ketentuan keamanan jaringan yang ketat, termasuk penggunaan password yang kuat.

5. KESIMPULAN DAN SARAN

Doktrin perang akan terus berubah seiring perkembangan teknologi khususnya di bidang pertahanan sehingga keunggulan teknologi yang dikuasai dapat meningkatkan kemampuan berperang baik kemampuan menyerang maupun bertahan. Keunggulan dalam penggunaan teknologi canggih juga akan merubah strategi dan taktik pertempuran secara efektif dan efisien. Salah satu teknologi yang memiliki dampak besar dalam doktrin perang adalah teknologi informasi dan komunikasi (TIK) yang diaplikasikan dalam konsep Network Centric Warfare (NCW). Keunggulan konsep NCW ini terutama dalam kecepatan dan keakuratan yang memungkinkan untuk memperoleh data secara real time sehingga akan berdampak pada keunggulan dalam peperangan.



Saat ini TNI sedang melakukan pembangunan NCW sebagai konsep peperangan modern sesuai Peraturan Menteri Pertahanan RI Nomor 12 Tahun 2021 tentang Kebijakan Pertahanan Negara Tahun 2020-2024 yang memuat tentang sistem komunikasi dengan teknologi seperti Network Centric Warfare (NCW). Kebijakan ini merkaait pengintegrasian jaringan sistem Trimatra terpadu atau Network Centric Warfare (NCW) guna meningkatkan interoperabilitas operasi antara kekuatan darat, laut, udara, serta antariksa dan siber.

DAFTAR PUSTAKA

- Alberts, D., S., et.al., (1999), “*Network Centric Warfare: Developing and Leveraging. Information Superiority*,” US Department of Defense.
- Amanat Presiden Jokowi pada Upacara HUT Ke-75 TNI tanggal 5 Oktober 2020 di Istana Negara. <https://www.setneg.go.id/baca/index/presiden-jokowi-pimpin-upacara-peringatan-ke-75-hari-tni> (diakses 27/08/2024 pk. 07.12 wib)
- Amrulloh, M. H., Purwanto, S., Hutajulu, B., & Siagian, F. (2025). STRATEGI KODAM XVII/CENDERAWASIH DALAM PEMENUHAN PERSONEL GUNA MENDUKUNG KESIAPAN OPERASI DI PAPUA. *Sparta Multidisciplinary Journal*, 1(1), 16-32.
- Andrew, T., (2021), “*Network Centrik Warfare sebagai upaya Transformasi Perang TN*,” *Defense Indonesia*,” h. 35-45.
- Bermana, S., Prakoso, L. Y., Patmi, S., Al-Mujaddid, T. F., Habibie, S. Y., Susmoro, H., ... & Gunawan, R. (2025). UNDERWATER SURVEILLANCE PERTAHANAN LAUT INDONESIA.
- Cushman, J. H., (1985), “*Command and Control of Theater Forces: The Korea Command and Other Cases*,” Harvard University, Center for Information Policy.
- Deputi Bidang Politik, Hukum, dan Hankam, Kementerian PPN/Bappenas, *Materi Ceramah kepada PPRA LXV Tahun 2023*, Tanggal 5 Juli 2023.
- Firmansyah, D., (2018), “*Implementasi Kebijakan Breakthrough Project : Pemisahan Dan Penyaluran Perwira Dalam Rangka Pembinaan Sumber Daya Manusia Prajurit TNI AD*,” *Strategi Pertahanan*, (J.SP.D), 4(1).
- I Nengah Putra Aprianto, M.Si.Han., (2018), “*Information Technology Design TNI AL Guna Mendukung Strategi Pertahanan Laut Nusantara*,” Kartika Mulya Surabaya
- Kremers, W., (2003), “*Network Centric Warfare and Information Operations: The New Paradigm*,” *Journal of Electronic Defense*.
- Mabes TNI AL, Puskodal (2023), Slide paparan Laporan Perkembangan Program Revitalisasi Puskodal 2021-2022.
- Pernyataan KASAD disampaikan pada acara Rakornis Teknologi dan Industri Pertahanan TNI AD pada tanggal 24-26 Februari 2021.



-
- Purwanto, S., Purnomo, M. R., & Budiman, H. (2025). Power Dynamics in Decision Making: a Qualitative Analysis. , 2(1), 80-86.
- Perpres Nomor 95 Tahun 2017 Tentang Sistem Elektronik Nasional
- Purwanto, S., & Siagian, F. (2025). Strategic Human Resources Management in the Global Era: Navigating Opportunities and Challenges. *Centurion MSPD Journal*, 1(1).
- Purwanto, S., & Ilhamsyah, I. (2025). Army Human Resources Development Strategy through Human Capital Approach. *Indonesian Journal of Social Science and Education (IJOSSE)*, 1(1), 1-22.
- Undang-Undang Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara
- Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.
- Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber Nasional.
- Peraturan Menteri Pertahanan Nomor 12 Tahun 2021 Tentang Kebijakan Penyelenggaraan Pertahanan Negara Tahun 2020-2024.
- Sakari Ahvenainen, (2023), “*Backgrounds and Principles of Network-Centric Warfare.*” National Defence College.
- Skomlek Mabes TNI, *Laporan Desk NCW*, Sistem Interoperabiliy Kodal TNI, Slide Paparan.
- Skomlek Mabes TNI (2021), *Konsep Network Centric Warfare Dalam Rangka Mendukung Sisops Trimatra Terpadu*. H.26