

BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

Teori mengandung suatu konsep teoritis abstrak yang dapat memberikan gambaran realitas dunia sebagaimana hasil dari pengamatan. Dalam sebuah kajian ilmiah, landasan teori ini dapat membuat ruang lingkup variabel pembahasan menjadi lebih jelas dan runcing, serta dalam penelitian kuantitatif teori dapat membantu peneliti dalam membuat rumusan hipotesis dan sebagai landasan dalam penyusunan instrumen penelitian (Ziauddin, 1996). Dengan demikian teori berperan sebagai kontrol pembahasan dalam suatu kajian atau penelitian sehingga dapat menghasilkan suatu rekomendasi akademis. Untuk itu, penulis perlu mengidentifikasi terlebih dahulu *Grand-Theory*, *Middle-Theory*, dan *Applied-Theory* yang dapat diterapkan sebagai dasar kajian akademis tersebut.

Dalam hal ini, untuk membangun penelitian terkait konsep optimalisasi interoperabilitas berbasis satelit ini dapat diidentifikasi teori-teori yang digunakan sebagai berikut.



Gambar 2.1 Tingkatan Teori yang Digunakan

Sumber: Diolah oleh Peneliti (2022)

2.1.1 Teori Keamanan Nasional

Keamanan nasional (*national security*) adalah keadaan aktual suatu negara tanpa adanya ancaman apapun yang tercermin dari terciptanya stabilitas internal dan kedaulatan suatu negara (Dworecki, 1994; Kitler, 2021). Dengan demikian, keamanan dapat diartikan sebagai kemampuan suatu negara dalam melindungi nilai-nilai internalnya dari ancaman luar. Namun tidak selalu mengarah pada keamanan secara nasional dan totalitas, melainkan berfokus pada ancaman terhadap kepentingan dan tujuan vital nasional.

Sehubungan dengan hal tersebut, keamanan nasional dapat dimaknai sebagai keadaan aman suatu negara sebagai satu kesatuan (entitas). Darmono (2010) menjelaskan bahwa keamanan nasional dapat diartikan sebagai kondisi maupun sebagai fungsi. Keamanan nasional sebagai fungsi artinya upaya untuk menciptakan rasa aman sebagai wujud kebutuhan dasar umat manusia selain kesejahteraan. Keamanan nasional tidak lagi dipandang sebagai bebas akan ancaman militer saja, melainkan kondisi dimana suatu bangsa terlindungi keamanan dan keselamatannya dari situasi *insecurity* oleh faktor-faktor atau ancaman non militer.

Waldemar Kitler (2021) memberikan pandangannya terkait domain keamanan nasional yang tertuang dalam Buku *National Security: Theory and Practice*. Keamanan militer termasuk dalam domain keamanan nasional, yang memiliki tujuan utama untuk menangkal ancaman eksternal maupun internal yang mengarah pada penggunaan kekuatan militer. Upaya yang dilakukan diantaranya meliputi tindakan membatasi kedaulatan suatu negara dengan menciptakan perlindungan dan pertahanan yang terorganisir terhadap ancaman-ancaman tersebut.

Dalam materi paparan mantan Menteri Pertahanan Prof. Juwono Sudarsono mengemukakan bahwa pertahanan negara merupakan salah satu fungsi ideal pemerintahan yang menjadi tumpuan suatu sistem

keamanan nasional. Hal ini berkaitan dengan peran pemerintah negara dalam menghadapi ancaman dari luar negeri untuk melindungi kedaulatan negara, keselamatan, dan keutuhan NKRI (Mukhtar, 2011). Waldemar Kitler (2021) juga menjelaskan bahwa pertahanan negara merupakan bagian dari keamanan nasional yang meliputi upaya sipil dan militer untuk melawan ancaman baik secara langsung maupun tidak langsung. Artinya, perlawanan terhadap ancaman tidak hanya tentang penggunaan senjata, melainkan dapat dengan upaya pertahanann diplomatik dan pertahanan di berbagai bidang lainnya, seperti ekonomi, infrastruktur, komunikasi, transportasi, *cyberspace*, dan sebagainya. Oleh karena itu, untuk mewujudkan keamanan nasional dalam suatu bangsa perlu adanya strategi pertahanan negara yang mengoptimalkan kekuatan bersama (militer dan sipil).

2.1.2 Strategi Pertahanan Negara

Strategi merupakan suatu proses dan upaya dalam menemukan konsep, sarana dan tujuan yang menguntungkan sehingga dapat membawa pada keberhasilan (Bowdish, 2006). Secara sederhana, strategi merupakan suatu pendekatan yang dilakukan untuk mewujudkan suatu tujuan tertentu. Dalam konteks negara, Liddle Hart mendefinisikan strategi sebagai cara dalam pendistribusian dan penggunaan kekuatan militer dalam mewujudkan tujuan politik (Prayuda & Sundari, 2019). Pencapaian tujuan tersebut erat kaitannya dengan manajemen sistem dan kebijakan negara yang penataannya dilaksanakan secara bertahap, yakni dimulai dari merencanakan, melaksanakan, dan mengevaluasi penerapan strategi tersebut (Rusdiana et al., 2021). Dengan demikian, apabila berbicara mengenai strategi pada level pertahanan negara maka akan mengarah pada pendekatan yang digunakan suatu negara dalam menjalan 3 tahap (perencanaan, pelaksanaan, dan pengevaluasian) tersebut untuk mencapai tujuan nasional.

Dalam militer internasional, strategi pertahanan negara merupakan turunan dari strategi keamanan nasional sehingga dapat didefinisikan tingkat strategi yang berhubungan dengan elemen kekuatan militer dalam negara sebagai berikut (Bowdish, 2006):

1. *Grand strategy*, yaitu suatu rencana menyeluruh yang merangkum visi nasional dalam penerapan, pengembangan dan pengkoordinasian semua instrument kekuatan nasional untuk mencapai tujuan strategis, meliputi menjaga keamanan nasional, meningkatkan kesejateraan ekonomi, dan memajukan nilai-nilai kebangsaan.
2. *National Security Strategy*, yaitu ilmu dan seni yang mengembangkan, menerapkan, dan mengkoordinasikan diplomatic, ekonomi, militer, dan informasi untuk mencapai tujuan keamanan nasional.
3. *National Military Strategy*, yaitu ilmu dan seni pendistribusian dan penerapan kekuatan militer untuk mencapai tujuan nasional dalam damai maupun perang.
4. *Theater Strategy*, yaitu ilmu dan seni yang mengembangkan konsep strategis terpadu dan tindakan yang mengarah pada tujuan kebijakan dan strategi keamanan nasional dan koalisi dengan penggunaan kekuatan, maupun operasi yang tidak melibatkan kekuatan.

Sehubungan dengan strategi dalam level pertahanan, dalam Buku Putih Pertahanan Negara Republik Indonesia, telah ditegaskan bahwa pertahanan negara diselenggarakan agar dapat mendukung pelaksanaan kebijakan pertahanan sesuai dengan Pasal 1 Ayat (3) Undang-Undang Nomor 3 tahun 2002 (Kemhan, 2015). Untuk itu, perumusan strategi pertahanan negara ini dapat dilakukan berdasarkan 3 substansi berikut ini.



Gambar 2.2 Tiga Substansi Dasar dalam Strategi Pertahanan Negara Republik Indonesia

Mengacu pada tiga substansi tersebut, *Ends* bermakna tujuan dengan pertanyaan “*apa yang dipertahankan?*” Maka jawabannya selaras dengan tujuan negara Indonesia, yakni untuk menjaga kedaulatan negara dan keutuhan wilayah NKRI, serta melindungi segenap bangsa Indonesia. Pada hakekatnya, tujuan ini pulalah yang menjadi alasan fundamental pentingnya membangun sistem pertahanan negara. Substansi selanjutnya, negara perlu mempersiapkan komponen-komponen pertahanan sehingga tujuan tersebut dapat terwujud. Dalam hal ini, pertahanan negara dapat terwujud dengan mengerahkan sumber daya nasional dengan strategi pertahanan berlapis (militer dan nirmiliter) sesuai dengan UU No 3 tahun 2002 pasal 7 dan 8. Substansi terakhir adalah *Ways* bermakna cara sehingga muncul pertanyaan “*bagaimana cara mempertahankannya?*” Dengan dikerahkannya komponen pertahanan berlapis, maka yang diperlukan adalah perencanaan strategis untuk membangun kekuatan nasional sehingga dapat mempersiapkan SDN secara optimal. Dengan demikian, negara akan mampu melaksanakan pertahanan negara yang dapat membentengi NKRI melalui strategi yang tangguh dan berdaya tinggi.

Apabila dikaitkan dengan doktrin TNI Tri Dharma Eka Karma (Tridek), dapat dikatakan bahwa strategi pertahanan negara selaras dengan doktrin tersebut yang bertujuan untuk melakukan pencegahan, penangkalan, dan penanganan ancaman maupun gangguan terhadap keutuhan bangsa dan negara (Puspen, 2007). Adanya doktrin ini menegaskan bahwa pertahanan negara secara konsep dirancang berdasarkan analisis potensi ancaman multidimensional. Maka dapat disimpulkan bahwa strategi pertahanan negara merupakan pendekatan yang dilakukan suatu negara dalam menyusun perencanaan hingga terjadinya pelaksanaan pertahanan negara dengan memanfaatkan *national source* (SDN) menjadi *national power* (kekuatan nasional) sehingga dapat menjaga keutuhan wilayah NKRI, menjaga kedaulatan, dan melindungi segenap bangsa dari berbagai potensi ancaman.

Berbicara mengenai strategi pertahanan negara, dalam Buku Putih Pertahanan Negara telah disebutkan bahwa strategi pertahanan dalam mencapai tujuan tersebut memiliki 5 sasaran strategis, yaitu:

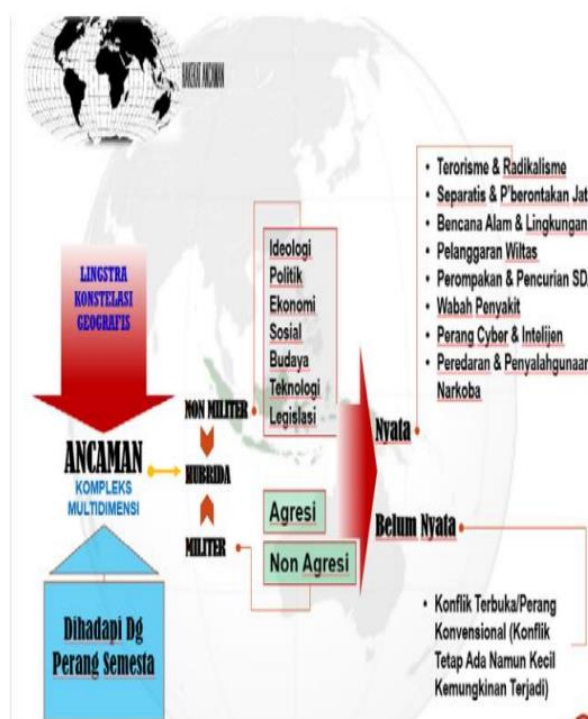
1. Mewujudkan pertahanan negara yang mampu menghadapi ancaman.
2. Mewujudkan pertahanan negara yang mampu menangani keamanan wilayah maritim, keamanan wilayah daratan dan keamanan wilayah dirgantara.
3. Mewujudkan pertahanan negara yang mampu berperan dalam menciptakan perdamaian dunia berdasarkan politik bebas aktif.
4. Mewujudkan industri pertahanan yang kuat, mandiri dan berdaya saing.
5. Mewujudkan warga negara Indonesia yang memiliki kesadaran bela negara.

Apabila dikaitkan dengan tujuan penelitian, maka sasaran strategis dari strategi pertahanan negara ini (terutama pada poin 1 dan 2) menjadi

dasar urgensi penguatan pertahanan kawasan perbatasan Laut Natuna Utara dalam rangka menghadapi ancaman terhadap keamanan wilayah maritim.

2.1.3 Teori Ancaman Nasional

Perubahan lingkungan strategis sangat mempengaruhi keamanan nasional. Oleh karena itu, negara perlu untuk mempertahankan keamanan nasional yang stabil melalui perumusan strategi besar (*grand strategy*) yang mempertimbangkan adanya potensi ancaman. Penjelasan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara menyebutkan bahwa ancaman merupakan segala usaha dan kegiatan, baik dari dalam maupun luar negeri yang dinilai dapat membahayakan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa. Untuk lebih jelasnya, hakekat ancaman nasional dapat dilihat melalui Gambar 2.3.



Gambar 2.3 Hakekat Ancaman Nasional

Sumber: Kemhan (2017)

Perkembangan lingstra yang begitu pesat mendatangkan isu-isu strategis dengan intensitas yang semakin dinamis menjadi perhatian dunia, salah satunya terkait isu perbatasan antar negara. Hingga saat ini masih banyak masalah perbatasan yang belum selesai sepenuhnya. Sehingga dapat dikatakan bahwa lingstra dapat mendatangkan ancaman yang kompleks dan multidimensi bagi suatu negara. Ancaman tersebut baik ancaman nyata maupun potensi ancaman yang belum nyata. Saat ini memang, ancaman nyata lebih merujuk pada ancaman-ancaman non militer. Seperti halnya yang sering terjadi di kawasan perbatasan Laut Natuna Utara meliputi pelanggaran batas wilayah, serta perompakan dan pencurian sumber daya alam. Namun tak dapat dipungkiri bahwa fakta empiris menunjukkan bahwa persoalan batas wilayah menjadi salah satu penyebab terjadinya perang. Paling tidak, isu perbatasan di ini berpotensi menyebabkan ketegangan dan konflik antar negara yang dapat mengganggu stabilitas keamanan nasional (Kemhan, 2015).

Dalam menghadapi ancaman di wilayah maritim, maka dapat mengacu pada arsitektur pertahanan militer untuk postur pertahanan dalam mewujudkan Poros Maritim Dunia sebagai berikut.



Gambar 2.4 Arsitektur Pertahanan Militer dalam Postur Pertahanan

Sumber: Kemhan 2016

Arsitektur pertahanan ini menggambarkan perpaduan dinamis fungsi-fungsi peperangan antar matra sehingga dapat menghasilkan satu kekuatan militer yang solid untuk menghadapi ancaman. Apabila mengacu pada Gambar 2.4 fungsi-fungsi yang dimaksud setidaknya meliputi fungsi sensor, fungsi mobilitas, fungsi dukungan, fungsi pemukul, fungsi proyeksi kekuatan, dan fungsi kodal. Dalam hal ini fungsi sensor akan memadukan tiap sensor dari Tri Matra dan sensor sipil sesuai dengan perundang-undangan yang berlaku. Selama ini pengembangan sensor militer berfokus di bawah Komando Pertahanan Udara Nasional saja namun kurang menjawab kebutuhan satuan matra lainnya. Untuk menjamin keterpaduan antar matra memerlukan sistem sensor *remote sensing* yang mutakhir dan mumpuni. Dalam hal ini penggunaan satelit dalam mendukung postur pertahanan sangat mendesak guna memperluas cakupan informasi dengan tingkat kerahasiaan yang tinggi (Kemhan, 2016).

2.1.4 Pengelolaan dan Pengamanan Perbatasan

Sehubungan dengan ancaman yang telah dijelaskan sebelumnya, ancaman dan gangguan dari pihak asing terhadap suatu negara sangat rentan masuk melalui titik-titik lemah perbatasan. Hal ini memunculkan urgensi pengelolaan dan pengamanan perbatasan yang tepat dan sesuai kebutuhan. Kawasan perbatasan yang secara geografis terletak di bagian dalam dari garis batas suatu negara ini memegang peran krusial yang mencerminkan aspek yuridiksi, ekonomi, politik, sosial budaya, serta pertahanan dan keamanan. Dengan adanya dimensi yang begitu kompleks, dapat dikatakan bahwa kawasan perbatasan mencerminkan manifestasi utama kedaulatan suatu negara (Bangun, 2017).

Hadiwijoyo (2009) membagi definisi perbatasan dari sudut pandang ahli geografi politik, yaitu perbatasan sebagai *boundary* dan perbatasan sebagai *frontier*. Sebagai *boundary* perbatasan suatu negara dimaknai sebagai fungsi untuk memberi batas suatu unit spasial politik yang

berdaulat. Sementara sebagai *frontier* perbatasan dimaknai sebagai posisi terdepan dari wilayah suatu negara. Baik sebagai *boundary* maupun sebagai *frontier* perbatasan tetap memiliki nilai strategis bagi suatu negara yang berdaulat. Oleh karena itu, kawasan perbatasan perlu ditopang dengan pengelolaan pengamanan perbatasan yang efektif dan berkesinambungan.

Muradi (2009) mengidentifikasi upaya yang dapat dilakukan dalam pengelolaan perbatasan. Dalam hal ini upaya-upaya yang relevan terhadap pengelolaan kawasan perbatasan laut dapat diidentifikasi sebagai berikut.

1. Peningkatan pengawasan terhadap berbagai pelanggaran atau tindak ilegal di kawasan perbatasan. Hal ini dapat didukung dengan memanfaatkan informasi geospasial yang mampu memetakan jalur tindak ilegal oleh pihak asing dan mengintegrasikannya dengan *database* pengamanan perbatasan.
2. Peningkatan koordinasi antar instansi sipil dan militer yang bertanggungjawab dalam pengamanan perbatasan melalui operasi gabungan.
3. Peningkatan jaringan dan peran intelijen yang dibangun secara terpadu di kawasan perbatasan. Upaya ini merupakan langkah pendeteksi dini melalui pendekatan militer yang dapat mencegah masuknya ancaman yang mengganggu kedaulatan melalui pintu-pintu perbatasan.
4. Pembinaan masyarakat di kawasan perbatasan maritim juga perlu dilakukan meliputi pembinaan wilayah dan pembinaan teritorial. Hal ini akan menjadi dasar terciptanya koordinasi antar masyarakat sipil dan militer dalam memperkuat pertahanan di perbatasan.
5. Peningkatan kualitas dan frekuensi patroli perbatasan pada setiap jengkal wilayah kedaulatan Indonesia.

6. Melakukan *upgrade* terhadap infrastruktur, peralatan pertahanan dan keamanan, serta alutsista yang dibutuhkan sehingga dapat mengoptimalkan operasi pengamanan perbatasan.
7. Pengalokasian anggaran pengamanan daerah perbatasan yang dapat memaksimalkan pengelolaan terhadap kawasan perbatasan.
8. Melakukan revisi terhadap regulasi yang berhubungan dengan pengamanan daerah perbatasan, meliputi sanksi tegas bagi pelaku IUUF dan tindak ilegal lainnya, adanya kepastian hukum di kawasan tersebut baik bersifat regional maupun berdasarkan kesepakatan dengan negara tetangga.

Dalam hal pengamanan terhadap wilayah laut di kawasan perbatasan Laut Natuna Utara terdapat peraturan perundang-undangan yang menjadi dasar bagi Indonesia dalam menetapkan batas sekaligus mengelola kawasan perbatasan LNU tersebut. Peraturan perundang-undangan tersebut meliputi Undang Undang Republik Indonesia Nomor 17 tahun 1985 tentang Ratifikasi UNCLOS 1982, Undang-Undang Nomor 6 Tahun 1996 tentang Perairan Indonesia, serta Undang-Undang Nomor 43 Tahun 2008 tentang Wilayah Negara. Regulasi ini tidak hanya mengikat ke dalam, melainkan juga menjadi dasar bagi Indonesia dalam mempertahankan kedaulatan wilayah lautnya di ruang internasional.

Mengingat adanya isu perbatasan yang berpotensi mendatangkan berbagai ancaman, Bakamla RI telah membentuk IMIC (*Indonesia Maritime Information Center*) sebagai tindak lanjut dari amanat Undang Undang Nomor 32 tahun 2014 tentang Kelautan. Merujuk pada kebijakan Joko Widodo tentang Poris Maritim Dunia, maka IMIC dibentuk untuk mendukung kewaspadaan maritim bagi pengguna laut yang mana pada saat ini pelaksanaannya menekankan pada sinergitas antara TNI AL dan Bakamla RI.

2.1.5 Komando dan Pengendalian

Komando dan Pengendalian atau yang dikenal dengan *Command and Control* (C2) adalah serangkaian proses secara teknis penyampaian informasi untuk pemecahan masalah atau untuk penyelesaian misi yang melibatkan kemampuan intelijen pengambil keputusan. Dalam bidang militer dapat didefinisikan sebagai suatu sistem kompleks terkait pengambilan keputusan dalam bidang pertahanan. Berbagai perkembangan teknologi diperluas untuk memenuhi tantangan multidisiplin dalam sistem C2 yang dapat mengoptimalkan pengambilan keputusan.

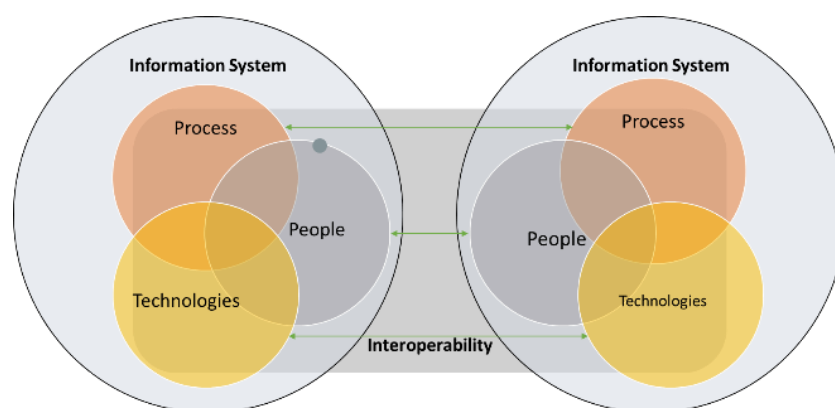
Dalam menjalankan misi operasi di perbatasan, Pusat Komando Pengendalian (Puskodal) masing-masing matra menggunakan saluran yang berbeda dan perangkat teknologi yang berbeda pula. Hal inilah yang menjadi tantangan bagi penguatan pengamanan di kawasan perbatasan, yaitu terwujudnya interoperabilitas antar sistem komunikasi antar instansi yang beroperasi. Pengintegrasian sistem komando kendali antar instansi yang terlibat dalam pengamanan kawasan perbatasan maritim merupakan upaya yang dapat dilakukan untuk mengirimkan data pemantauan.

2.1.6 Konsep Interoperabilitas

Seiring dengan pemanfaatan teknologi yang semakin berkembang, kemudahan mengakses data dan memperoleh informasi menjadi suatu kebutuhan bagi berbagai bidang kehidupan. Berkaitan dengan kebutuhan untuk memenuhi pertukaran informasi yang terkoodinasi bagi suatu organisasi maupun antara organisasi, memunculkan istilah interoperability atau interoperabilitas. Kata interoperabilitas yang merupakan serapan dari bahasa Inggris, *interoperability*, terdiri dari tiga kata dasar, yaitu *inter*, *operate*, dan *ability*. *Inter* menggambarkan interaksi antara sistem, aplikasi, atau antar organisasi. *Operate* artinya beroperasi, sedangkan *ability* berarti kemampuan.

Teori interoperability dalam penelitian ini terkait dengan desain interoperabilitas berbasis satelit untuk keperluan pertahanan tersebut. Berdasarkan IEEE *dictionary*, interoperabilitas dapat dikatakan sebagai kapasitas dari dua atau lebih sistem atau komponen dalam rangka bertukar informasi dan menggunakan data dari pertukaran informasi tersebut. Dalam hal ini, kapasitas untuk bertukar dan menggunakan data tersebut menggambarkan kemampuan satu entitas untuk menggunakan fungsionalitas dari entitas lainnya.

Kemudian Interoperabilitas juga dapat dijelaskan sebagai suatu prosedur peralatan, doktrin dan pelatihan, serta kemampuan orang, organisasi, dan peralatan atau perangkat dapat beroperasi bersama-sama secara efektif dan efisien (Greenbaum et al., 1991). Lebih lanjut John Kim & McDaniel (2020) memaparkan konsep interoperabilitas yang didefinisikan oleh Federal Research Division sebagai suatu kemampuan dalam melakukan pertukaran informasi antara, lintas proses, maupun berkaitan dengan negosiasi dengan kunci adanya pemahaman yang sama terkait informasi tersebut. Pelaksanaannya bergantung pada ketersediaan sumber daya yang terpadu dan prosedur hasil kesepakatan yang terdokumentasi sehingga dapat menyeleraskan motivasi antar pihak terlibat.



Gambar 2. 5. Interoperability: A Sociotechnical Perspective

Sumber: Soares & Amaral, 2014

Secara sederhana Soares & Amaral (2014) menjelaskan bahwa dalam perspektif *sociotechnical*, interoperabilitas berhubungan dengan sistem informasi yang dapat diilustrasikan pada Gambar 2.2. Sistem informasi dapat didefinisikan sebagai suatu desain penyampaian, penggunaan, dan sebagai dampak teknologi informasi yang efektif dalam organisasi maupun masyarakat (Avison & Wood-Harper, 1990). Sistem informasi suatu organisasi merupakan fitur induk untuk menjalankan interoperabilitas dalam lingkungan organisasi tersebut.

Secara teknis, kemampuan berinteraksi antar aplikasi atau sistem tersebut memerlukan suatu protokol yang disepakati bersama. Macam-macam jalur komunikasi yang biasa digunakan adalah jaringan TCP/IP dan protokol HTTP dengan memanfaatkan file XML. Dengan kata lain, dalam rangka mencapai interoperabilitas yang benar dan efektif antara sistem informasi bukan hanya memerlukan koneksi saja, melainkan pemahaman dan kapasitas operasi dari elemen-elemen teknologi sistem informasi yang mengisyaratkan relevansi sistem informasi antara proses, orang, dan teknologi (Soares & Amaral, 2014). Hal tersebut merujuk pada tiga komponen utama dalam interoperabilitas, yaitu:

1. *Hardware*, meliputi perangkat genggam, gadget, laptop, komputer, printer, handphone, kendaraan, pengontrol, usb, *hard disk*, maupun perangkat sejenis lainnya (Pernin et al., 2019).
2. *Software*, meliputi *software application*, aplikasi antarmuka, program pemantauan, gadget, sistem operasi (OS), dan *security software*.
3. *Brainware*, meliputi manusia, pengguna, personel, programmer, analis, petugas, manajer, kepala, kolaborator, peneliti, perencana, maupun pengambil keputusan (Ahmad et al., 2021).

Selanjutnya *hardware* dapat diartikan sebagai *physical compute* dan peripheral, *software* didefinisikan sebagai OS dan aplikasi, sedangkan *brainware* merupakan *human factor* (Gultom et al., 2018). Dalam hal ini,

komponen *Brainware* memang memegang peran paling dominan diantara semua komponen interoperabilitas. Sebab dapat dikatakan bahwa interoperabilitas merupakan hasil kesepakatan antar manusia yang mana teknologi akan membantu dalam mengimplementasikan kesepakatan itu. Oleh karena itu, tanpa adanya kesepakatan manusia maka tidak akan ada suatu teknologi yang dapat mencapai interoperabilitas sejati (Reach, 2004).

Jenis interoperabilitas dapat diklasifikasikan sebagai interoperabilitas teknis atau nonteknis. Jenis interoperabilitas teknis meliputi interoperabilitas komunikasi, elektronik, aplikasi, dan interoperabilitas multi-basis data. Sedangkan jenis interoperabilitas non-teknis meliputi interoperabilitas organisasi, operasional, proses, budaya dan koalisi. Klasifikasi interoperabilitas ini bergantung pada sudut pandangnya. Artinya suatu interoperabilitas dapat dipandang sebagai teknis namun disisi lain dapat dipandang sebagai non teknis.

Namun pada intinya, interoperabilitas bermakna pertukaran layanan untuk menciptakan operasi sistem, unit, atau kekuatan yang efektif (Ford et al., 1980). Mengacu pada hal tersebut dapat dikatakan bahwa interoperabilitas yang konseptual dirancang dalam penelitian ini merupakan interoperabilitas sistem informasi TNI AL, TNI AU, dan Bakamla RI. Sehingga dapat dikatakan bahwa dari segi non-teknis meliputi interoperabilitas antar organisasi dan operasional. Namun tentunya interoperabilitas sistem informasi ini juga termasuk interoperabilitas teknis yang memuat komunikasi, elektronik, aplikasi, dan multi database.

Interoperabilitas sangat erat hubungannya dengan perangkat Internet of Things (IoT). Interoperabilitas antar perangkat tersebut sangat terbatas karena banyaknya komponen, lapisan data, bahasa, dan *hardware* maupun *software* pendukung yang terlibat pada pengembangan perangkat IoT tersebut. Namun perangkat tersebut dapat dengan mudah bekerja sama melalui konektivitas dan pertukaran informasi atau pengetahuan apabila

dalam *framework* yang ideal. Tantangan utama dari interoperabilitas komunikasi pada perangkat IoT adalah interaksi tanpa batas antara *multi-devices*. Dalam mewujudkan hal itu dibutuhkan adanya standar yang mencakup kemampuan interoper tersebut.

2.1.7 Interoperabilitas dalam Militer

Dalam dunia militer, NATO (2006) mendefinisikan interoperabilitas sebagai suatu kemampuan yang mengacu pada pengoperasian bersama oleh organisasi militer yang berbeda maupun angkatan bersenjata berbeda (AD, AU, dan AL) sehingga memungkinkan terbentuknya peningkatan kekuatan antar unit atau sistem untuk menjalankan operasi secara bersamaan (dikenal dengan *Joint Operation*). Department of Defense Directive (2004) menjelaskan bahwa tingkat interoperabilitas dalam militer bergantung pada kondisi yang dicapai di antara sistem komunikasi-elektronik. Tingkat interoperabilitas dapat ditentukan ketika informasi atau layanan dipertukarkan secara langsung yang menghasilkan kepuasan antara organisasi terkait dan/atau user. Dalam hal ini interoperabilitas menekankan pada sistem dan peralatan yang direncanakan dari suatu pasukan gabungan dan koalisi. Lebih lanjut dalam buku tersebut dijelaskan bahwa kebutuhan interoperabilitas harus diturunkan menggunakan arsitektur terintegrasi, harus diperbarui sepanjang masa pakai sistem, dan harus berfokus pada kemampuan.

Sehubungan dengan kaitan inteoperabilitas degan IoT yang telah dipaparkan sebelumnya, maka dalam ruang lingkup militer muncul konsep baru yang dikenal denga IoMT. IoMT (*Internet of Military Things*) adalah kelas IoT yang diimplementasikan pada operasi tempur dan berperangan. Konsep ini pada dasarnya didorong oleh pemikiran bahwa pertempuran militer di masa depan akan didominasi oleh *machine* inteliigence dan *cyberwarfare*. Oleh karena itu, IoMT dirancang untuk menciptakan lingkungan teknologi cerdas yang mampu menyaring informasi sensorik

dan mengatur banyak tugas secara mandiri, misalnya perang tanpa awak. Untuk itu dalam hal ini interoperabilitas adalah tantangan besar bagi IoMT yang mengharuskan akses, pemrosesan dan pertukaran data terkumpul dan terintegrasi untuk menghasilkan informasi yang efektif dan tepat waktu.

Konsep interoperabilitas dalam militer digunakan sebagai dasar dari penelitian ini sehubungan dengan Kebijakan pembangunan pertahanan negara dalam Perpres No.97 tahun 2015 yang menjelaskan bahwa pembangunan pertahanan daerah dapat dilakukan melalui pembangunan kawasan perbatasan dan pulau-pulau kecil terluar/terdepan, serta pembangunan teknologi, sistem informasi dan komunikasi bidang pertahanan. Dalam hal ini bertujuan untuk memperkuat pertahanan perbatasan Laut Natuna Utara yang merupakan bagian dari Kepulauan Natuna Provinsi Kepulauan Riau yang terdiri dari pulau-pulau kecil terluar atau terdepan.

Untuk itu, optimalisasi interoperabilitas menjadi wujud pembangunan TIK dalam rangka memperkuat pertahanan di kawasan terdepan tersebut. Kusumah (2022) menyebutkan bahwa interoperabilitas yang diterapkan dalam operasi pengamanan perbatasan wilayah kedaulatan NKRI untuk mendukung peran kodal merupakan kolaborasi antara *software*, *hardware*, dan *brainware*. Dengan adanya interoperabilitas tersebut, maka instansi militer maupun sipil dapat bekerja sama melalui penyampaian informasi yang cepat dan akurat tanpa mengurangi nilai dari informasi tersebut. Dalam menjamin transfer data (Supartono, 2017) interoperabilitas TNI terdiri dari 3 model, yaitu:

1. Interoperabilitas (tutup buka) tergantung pada situasi
2. Interoperabilitas (tutup buka) tergantung pada urgensi.
3. Interoperabilitas dengan data yang bersifat operasional dan taktis nonstruktural yang bersifat integrasi.

Supartono (2017) menegaskan bahwa dalam mewujudkan efektivitas pembangunan interoperabilitas dan integrasi sistem informasi antar matra maupun dengan pihak eksternal yang bersangkutan, perlu didukung dengan adanya Undang-Undang yang mengatur secara khusus mengenai sistem informasi Hanneg. Sebab apabila meninjau dari budaya organisasi TNI saat ini telah mengkombinasikan sistem konvensional dengan penggunaan teknologi mutakhir. Hal tersebut didukung dengan pemanfaatan satelit BRISAT oleh TNI meskipun penggunaan satelit tersebut memang belum setara dengan konsep asli *information warfare* atau *information operation*.

Interoperabilitas militer saat ini sangat penting untuk mempertimbangkan karakteristik-karakteristik dalam *Network Centric Warfare*, diantaranya:

1. *Systems of Systems*, dalam hal ini interoperabilitas seiring dengan paradigma peperangan NCW yaitu menghubungkan basis sistem satu ke sistem lainnya. Hal yang perlu digarisbawahi adalah, setiap sistem yang dihubungkan ke jaringan sangat mungkin berasal dari karakteristik sistem yang berbeda dan disinilah interoperabilitas secara teknis dibutuhkan.
2. *Networked*, jaringan sangat diperlukan dalam NCW dan merupakan kunci dari keberhasilan pencapaian suatu misi. Jaringan ini (baik bersifat *wired* maupun *wireless*) menjadi fitur dominan yang memerlukan konektivitas, untuk itulah interoperabilitas diperlukan.
3. *Information Sharing*, masih berhubungan dengan komponen jaringan. Jaringan yang sebelumnya telah dibahas tak lain adalah untuk melakukan pertukaran informasi dari satu sistem ke sistem lainnya. Dengan terbentuknya interoperabilitas jaringan antar sistem yang bersangkutan akan mendukung kecepatan dan keamanan data informasi tersebut.

4. *Collaboration*, hal ini ditujukan untuk mencapai tujuan bersama lebih cepat dan lebih presisi dengan memberdayakan sistem masing-masing. Sehingga interoperabilitas diperlukan untuk memadukan sistem-sistem tersebut.
5. *Shared Situation Awareness*, melalui fitur *information sharing* dalam sebuah jaringan komputer dan adanya kolaborasi yang memungkinkan komunikasi lebih cepat dan presisi. Maka kewaspadaan situasi dari dinamika lapangan dapat diperoleh informasi secara serencak, cepat dan presisi apabila interoperabilitas telah terbentuk.

2.1.8 Peran Satelit dalam Interoperabilitas

Satelit adalah pesawat ruang angkasa yang mengorbit Bumi yang dikembangkan untuk mengirim dan menerima data dari satelit atau stasiun bumi lainnya. Informasi yang dibawa dapat berupa suara, audio, video, atau data lainnya (Hoffman, 2007). Pada dasarnya, satelit di orbit untuk melayani tujuan tertentu sepanjang masa pakainya. Dalam operasi militer, kemampuannya untuk memfasilitasi pengumpulan, transmisi, dan penyebaran informasi yang cepat membuat satelit pertahanan dianggap sebagai 'Pengganda Daya'. Cakupan global, kesiapan tinggi, respons cepat, dan fleksibilitas yang melekat adalah beberapa manfaat satelit yang dapat dimanfaatkan. Kemampuan ini memungkinkan untuk menawarkan dukungan distribusi informasi *real-time* untuk operasi militer selama masa damai, darurat, dan berbagai jenis konflik. Satelit dapat memberikan rincian tentang rencana pertempuran musuh, koordinat geografis yang tepat, dan lokasi ancaman selama tahap perencanaan operasi militer (Maini & Agrawal, 2011). Sistem C4ISR (Komando, Kendali, Komputer, Komunikasi, Intelijen, Pengawasan, dan Pengintaian) dalam militer dapat secara efektif menggunakan teknologi satelit militer.

Komunikasi satelit militer yang menggunakan teknologi internet berkaitan dengan inefisiensi dan latensi dalam TCP dan protokol aplikasi. Dalam hal ini, faktor lingkungan dapat mengganggu kinerja jaringan, keandalan, dan pemanfaatan *bandwidth*. Untuk memastikan interoperabilitas protokol antara jaringan militer yang berbeda perlu adanya suatu standar yang bersifat terbuka. Lalu lintas non esensial melalui WAN (*wide-area network*) perlu dikurangi secara signifikan melalui optimalisasi WAN dan solusi akseleris SCPS (*Space Communications Protocol Standards*). Solusi ini dapat memberikan akses cepat, andal dan aman terhadap informasi penting suatu misi bagi personel militer yang bertugas (Dorworth, 2010).

Penerimaan informasi akurat yang tepat waktu akan mempengaruhi keberhasilan bagi suatu operasi militer. Oleh karena itu perlu adanya sistem komunikasi taktis yang membantu penyediaan data berkecepatan tinggi dan secara *real-time*. Hal ini menyangkut tentang penerimaan data sensor, pemrosesan informasi dan komunikasi (Ryan & Frater, 2000). Puskodal tidak akan dapat membaca sinyal ancaman tanpa adanya komunikasi yang memenuhi kebutuhan tersebut. Dalam hal ini sinyal satelit dan layanan berbeda yang dirancang untuk pengguna yang bersifat kompatibel dan terbuka dapat memungkinkan untuk melakukan interops sistem informasi yang semaksimal mungkin (Januszewski, 2011). Untuk itu dengan adanya interoperabilitas berbasis satelit diharapkan mampu mengoptimalkan desain interops antar matra dalam rangka memperkuat pertahanan di Perbatasan Laut Natuna Utara. Meskipun demikian, hal ini akan berjalan lebih optimal apabila Indonesia memiliki satelit militer sehingga keamanan yang lebih terjamin dan dapat meminimalisir resiko gangguan layanan.

Sistem komunikasi satelit merupakan komponen penting dalam suatu sistem komunikasi taktis. Melalui teknologi ini memungkinkan penerimaan informasi berkecepatan tinggi ke pos komando dan mengkomunikasikan pengambilan keputusan jarak jauh (Andrew, 2017). Sehubungan dengan

hal tersebut, Sistem Komunikasi Satelit (Siskomsat) sendiri telah diterapkan oleh TNI AL dan TNI AU. Sebelumnya sistem komunikasi TNI ini menggunakan radio HF, VHF, dan UHF namun data rate yang rendah menjadikan keterbatasan pada sistem komunikasi ini. Pada tahun 2015, siskomsat telah digunakan oleh TNI AL yang bekerja sama dengan PT Telkom dan PT LEN dalam rangka mengembangkan *software* dan pengadaan *hardware*. Namun siskomsat TNI yang digelar di bawah Kodal Panglima TNI ini masih belum optimal.

Terkait dengan interoperabilitas yang dikaji dalam penelitian ini, tentunya satelit komunikasi berperan besar dalam membangun teknologi interoperabilitas. Namun, teknologi satelit untuk pertahanan juga bisa diterapkan pada misi lain. Salah satunya adalah satelitintai atau satelit mata-mata yang dapat memberikan berbagai informasi intelijen, seperti GEOINT, IMINT, dan SIGINT. Keberadaan satelit ini juga dapat mendukung sistem peringatan dini. Untuk dapat mewujudkan penguatan pertahanan berbasis satelit, setidaknya negara tersebut harus memiliki satelit yang meliputi satelit komunikasi, satelit ISR (*Intelligence, Surveillance Reconnaissance*), dan satelit navigasi.

2.2 Hasil Penelitian Terdahulu

Penelitian terdahulu merupakan cara bagi peneliti untuk menemukan ide baru dalam penelitian melalui perbandingan dengan penelitian yang pernah dilakukan sebelumnya. Adanya hal ini dapat mengarahkan peneliti kepada orisinalitas dari penelitian yang dilakukannya. Oleh karena itu, untuk mendukung tulisan dan mempertajam analisis dalam penelitian ini, berikut pada Tabel 2.2 disajikan beberapa penelitian terdahulu yang relevan sebagai daftar rujukan dalam melakukan penelitian.

Tabel 2.1 Penelitian Terdahulu

No	Peneliti, Tahun, Judul	Tujuan Penelitian	Ringkasan Penelitian	
			Persamaan	Perbedaan
1.	<p>Muhammad Iwan Kusumah, Ikhwan Syahtaria, Dohar Sianturi, Lukman, Yudho P, Herlina Juni Risma Saragih (2022)</p> <p>Strategi Interoperabilitas Sistem Informasi TNI Guna Mendukung Komando dan Pengendalian Operasi Pengamanan Perbatasan di Laut Natuna Utara</p> <p>Jurnal Inovasi Penelitian Vol. 2 No. 8</p>	<p>Menganalisis interoperabilitas sistem informasi TNI serta strategi interoperabilitas tersebut dalam mendukung kodal Operasi Pengamanan Perbatasan di LNU</p>	<p>Melakukan analisis interoperabilitas sistem informasi antar institusi pada lokus yang sama.</p>	<p>Perspektif Metode penelitian</p>
2.	<p>Mahasiswa & Dosen Prodi Teknologi Penginderaan (2019)</p> <p>Konsep Pemanfaatan Pesawat Terbang Tanpa Awak (PTTA) Skadron 51 Lanud Supadio Pontianak dalam Mendukung Interoperabilitas Operasi Gabungan Tri Matra TNI di Wilayah Kalimantan Barat</p>	<p>Menganalisis dan membangun teknologi <i>information sharing</i> dan <i>information integration</i> dalam Operasi Gabungan TNI di Perbatasan Kalimantan Barat.</p>	<p>Hasil berupa konsep desain sistem interoperabilitas antar institusi di kawasan perbatasan.</p>	<ul style="list-style-type: none"> - Instansi yang terlibat dalam interoperabilitas - Obyek penelitian - Menekankan pada peran PTTA sementara penelitian ini

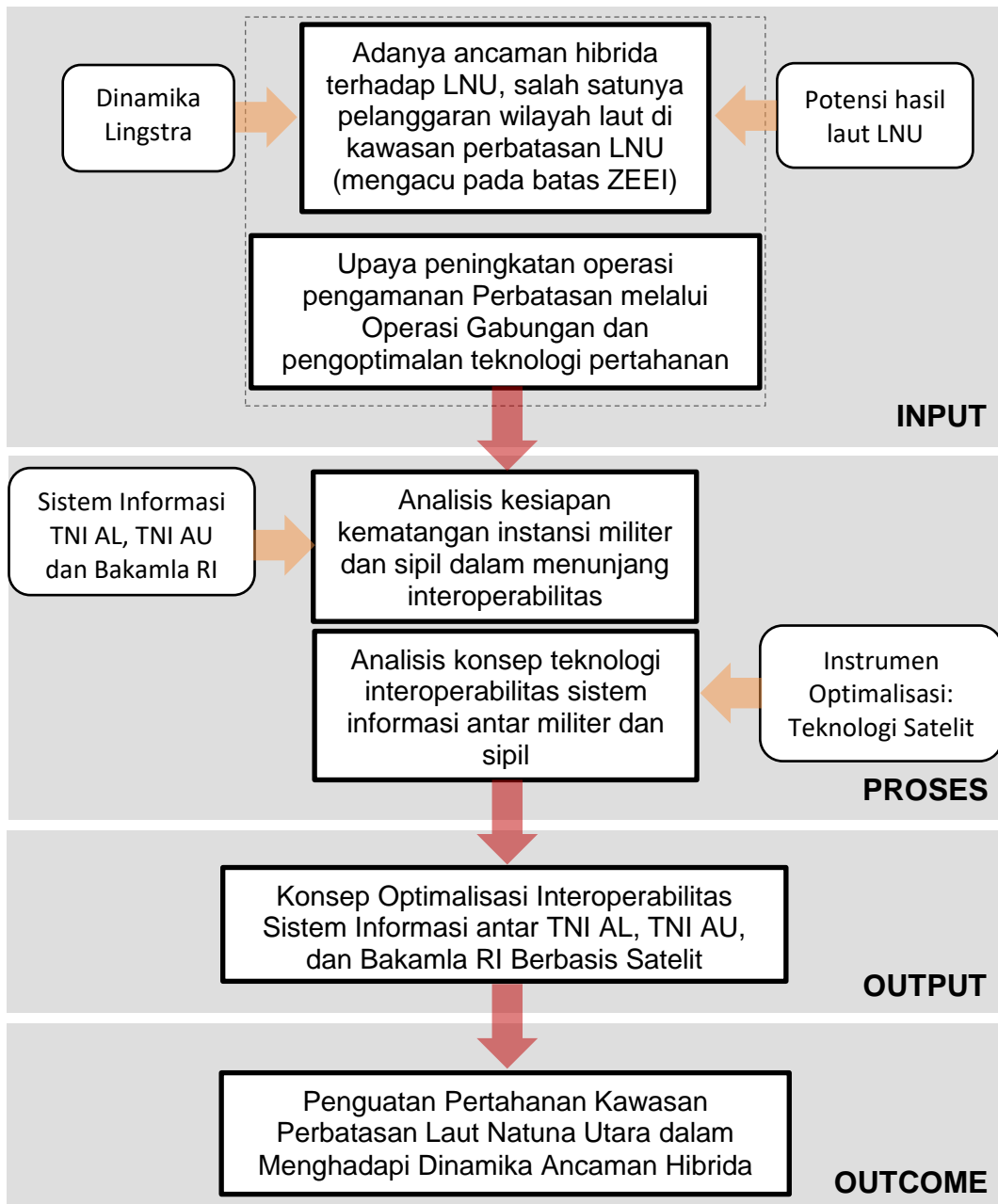
	Hasil Penelitian KKDN Prodi Teknologi Penginderaan Unhan RI			menekankan pada peran satelit.
3.	<p>Agus Priyanto, Arry Bainus, R. Widya Setiabudi Sumadinata, Wawan Budi Darmawan (2022)</p> <p><i>Indonesia Maritime Security (Study on Interoperability Inter Institution Indonesia Sea Border Security in Mallaca Strait)</i></p> <p>Specialusis Ugdymas Vol.1 No.43</p>	<p>Melakukan kajian pemanfaatan teknologi informasi institusi keamanan perbatasan laut yang bertugas di Selat Malaka untuk menemukan konsep baru dalam konteks interoperabilitas antar institusi tersebut.</p>	<p>Mengkaji teknologi untuk perbatasan maritim</p> <p>Menganalisis interoperabilitas inter institusi</p>	<p>Perspektif Lokus Penelitian</p>
4.	<p>Firmandes Pasaribu, Syaiful Anwar, Tatar Bonar (2017)</p> <p>Penggunaan Sistem Unmanned Aerial Vehicle dalam Pengamanan Wilayah Perbatasan Indonesia-Malaysia (Studi Interoperabilitas Skadron Udara 51 TNI AU dan Direktorat Topografi TNI AD)</p> <p>Jurnal Prodi Strategi Pertahanan Udara Vol.3 No.2</p>	<p>Melakukan kajian efektivitas penggunaan pesawat UAV melalui analisis kesiapan UAV Skadron Udara 51 TNI AU untuk mendukung inteoperabilitas pada operasi perbatasan Indonesia-Malaysia</p>	<p>Metode pengukuran interoperabilitas LISI dan OIM</p> <p>Mengkaji interoperabilitas TNI dalam pengamanan kawasan maritim</p>	<ul style="list-style-type: none"> - Metode penelitian - Instansi yang diinteroperabel - Lokasi penelitian - Menekankan pada peran sistem UAV sementara penelitian ini berfokus pada peran satelit.

5.	<p>Undang Rohana (2022)</p> <p>Interoperabilitas TNI AL dan Bakamla RI dalam Melaksanakan Kegiatan Pengawasan terhadap Pelanggaran di Wilayah Laut Natuna Utara</p> <p><i>Journal of Industrial Engineering and Management Research Vol.3 No.4</i></p>	<p>Melakukan kajian interoperabilitas dan komunikasi-koordinasi antar lembaga, serta kendala dan hambatan dalam menjalankan interoperabilitas tersebut.</p>	<p>Kajian inteoperable instansi yang sama dan lokus yang sama</p>	<ul style="list-style-type: none"> - Perspektif - Metode penelitian - Instansi yang diinteoperabel
6.	<p>Budima, Touran, dan Rayanda Barnas (2020)</p> <p>Penguatan Peran Sistem Komunikasi Satelit dalam Mendukung Pelaksanaan Operasi dan Latihan TNI</p> <p>Jurnal Strategi Pertahanan Udara</p>	<p>Menganalisis peran, kendala serta upaya untuk meningkatkan siskomsat TNI AU yang dapat mendukung sistem Komando dan Kendali</p>	<p>Mengkaji peran satelit Teori yang digunakan</p>	<ul style="list-style-type: none"> - Perspektif - Hanya diperuntukkan untuk Matra Udara saja, sementara penelitian yang akan dilakukan mengarah pada sistem komunikasi satelit antar matra udara dan laut, serta instansi sipil.

Sumber: Diolah oleh peneliti, 2023

2.3 Kerangka Berpikir

Berdasarkan landasan teori dan penelitian terdahulu yang telah dikumpulkan, peneliti membuat kerangka berpikir (Gambar 2.6) sebagai panduan dalam menyusun metode penelitian dan kerangka kerja.



Gambar 2.6 Kerangka Berpikir

Sumber: Data Olahan Peneliti, 2023