

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Dalam operasi militer baik operasi militer perang maupun operasi militer selain perang membutuhkan informasi dan koordinasi yang tepat dan aktual dalam satu matra maupun antar matra agar jalannya unsur tugas operasi dapat berjalan secara efektif dan efisien dalam mencapai tujuan operasi. Sehingga proses manajemen operasi dapat dilaksanakan dengan maksimal karena integrasi dan operabilitas alutsista serta keamanan informasi dan komunikasi dalam pengambilan keputusan strategis dapat tercapai dengan cepat dan tepat. Pelaksanaan operasi militer perang maupun operasi militer selain perang mengacu pada konsep trimatra terpadu. (Kementerian Pertahanan Republik Indonesia, 2015)

Pada suatu operasi khususnya operasi militer perang, informasi penting yang dibutuhkan adalah mengenai cuaca, medan dan musuh. Cuaca tempat tujuan harus diketahui agar dalam mengirimkan pasukan ke daerah tujuan dapat tercapai tanpa kendala cuaca buruk atau yang merugikan pasukan sendiri karena terlihat oleh lawan. Berikutnya mengenai medan operasi, kondisi medan operasi menentukan logistik dan peralatan yang sesuai untuk digunakan di daerah tersebut. Kemudian musuh yang akan dihadapi, sebaiknya kita mengetahui ataupun memperoleh informasi sebanyak-banyaknya terkait dengan musuh yang akan dihadapi, baik jumlah kekuatannya, peralatannya, posisinya, kemampuannya dan sebagainya.

Peperangan digolongkan dalam empat generasi yaitu peperangan generasi pertama yang mengandalkan kekuatan sumber daya manusia; peperangan generasi kedua mengandalkan senapan dan meriam; peperangan generasi ketiga mengandalkan keunggulan teknologi senjata dan teknologi informatika; peperangan generasi keempat berupa perang asimetris dan

non-linier yang mengandalkan seluruh sarana prasarana dan sistem senjata. Perang generasi keempat merupakan konsep baru yang berdasarkan pada *networked, transnational* dan *information based*. Bentuk peperangan generasi ke empat tidak hanya sebatas persenjataan modern namun juga menggunakan kemajuan ilmu pengetahuan dan teknologi, diantaranya adalah teknologi sensor yang dapat monitoring situasi wilayah darat, laut, udara serta angkasa secara terintegrasi yang diimplementasikan melalui kemampuan K4IPP (Komando, Kendali, Komunikasi, Komputer, Intelijen, Pengawasan dan Pengintaian).(Sebastian, 2015)

Penggunaan teknologi informasi dan komunikasi yang canggih, peluru kendali yang presisi, penggunaan pesawat pengintai nirawak telah mengubah konsep peperangan bahwa perang dapat dimenangkan oleh negara yang memiliki keunggulan teknologi pertahanan. Sehingga konsep *Revolution in Military Affairs (RMA)* untuk mencapai kemenangan dengan penggunaan pasukan dan waktu yang minimal untuk memperoleh hasil yang maksimal dengan mengutamakan teknologi pertahanan. *RMA* ditandai dengan perubahan yang mempengaruhi karakter konflik pada periode waktu yang singkat. Perubahan tersebut menyebabkan terjadinya perubahan pada doktrin militer dan organisasinya.(Luthfi, 2012)

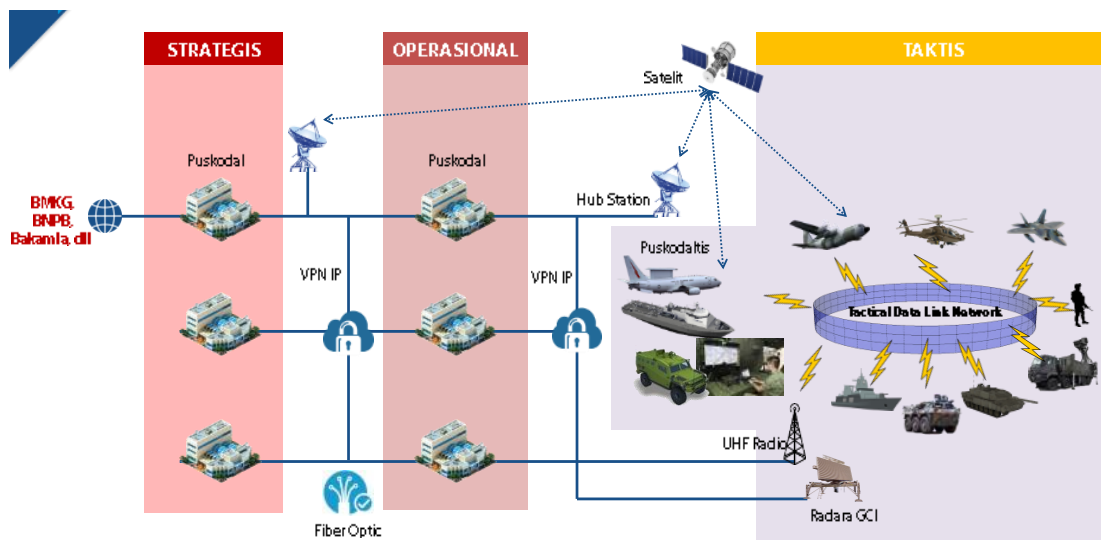
	1980-an	1990-1994	1995-2000	2001-2005	2005-xxxx
Gelombang	Penemuan intelektual	Adaptasi awal di negara-negara barat	RMA "teknofilia"	Perubahan ke Transformasi Pertahanan	Pemikiran kedua dan ketiga
Konsep	Revolusi Teknis Militer Uni Soviet	Revolusi Militer vs RMA	<i>Revolution in Military Affairs</i>	Transformasi Pertahanan	Modernisasi "plus"
Fokus	Perubahan paradigma teknologi,	RMA dalam sejarah;	Sistem dari peperangan berpusat	Operasi berbasis akibat;	Dari paradigma RMA

	inovasi doktrin Uni Soviet	sumber inovasi militer	pada jaringan (NCW)	peperangan berpusat pada jaringan	berubah kepada "penekanan perubahan"
--	----------------------------	------------------------	---------------------	-----------------------------------	--------------------------------------

Tabel 1.1 Lima "Gelombang" RMA

Sumber: (Raska, 2011)

Sistem pertempuran saat ini lebih mengutamakan pada peperangan informasi dengan menggunakan konsep *Network Centrix Warfare (NCW)*, dimana seluruh sistem peralatan utama sistem senjata terintegrasi dan teroperabilitas dalam satu kesatuan kendali yang memudahkan pimpinan dalam memberikan komando pertempuran. *NCW* merupakan konsep operasi yang berbasis jaringan internet untuk mengumpulkan serta pengolahan data di pusat komando secara *real time* dan koordinasi dengan seluruh unsur terkait sehingga pasukan di lapangan dapat menyelesaikan tugas operasinya secara lebih efektif sesuai dengan fungsi K4IPP (Komando, Kendali, Komunikasi, Komputer, Intelijen, Pengawasan dan Pengintaian). (Ferris, 2004)



Gambar 1.1 Interkoneksi Antar Komponen NCW

Sumber : Materi Kuliah *Radar Modern and Cyber Sensing for Defense* pada

24 Mei 2021

Sistem *NCW* tersebut berbasiskan pada jaringan komunikasi dan informasi, sehingga untuk mengamankan sistem jaringan tersebut digunakan *cyber security* yang dapat mendeteksi dan menangkal serangan siber tersebut bahkan juga dapat menyerang balik.

Di Indonesia dalam monitoring aktivitas serangan siber dilaksanakan oleh BSSN (Badan Siber dan Sandi Negara). Dalam laporan tahunan 2020 terlihat bahwa serangan siber berupa *malware* masih menjadi *tools* yang digunakan oleh para penyerang. Selain itu hal ini memberi gambaran bahwa Indonesia masih menjadi target penyerangan.



Gambar 1.2 Negara Sumber Serangan Tertinggi  
Sumber: (BSSN, 2020)

Dalam peperangan informasi, diperlukan kemampuan intelijen untuk memperoleh data-data strategis/rahasia lawan. Kemampuan yang harus dimiliki yaitu berupa *Human Intelligence (Humint)*, *Signal Intelligence (Sigint)*, *Communication Intelligence (Commint)*, *Electronic Intelligence (Elint)*, *Geospatial Intelligence (Geoint)*, *Open Source Intelligence (Osint)*, dan *Imagery Intelligence (Imint)* yang kemudian informasi intelijen tersebut diolah dan dianalisa untuk mendukung pengambilan keputusan strategis. (Ferris, 2004)

Sistem NCW pada K4IPP dalam operasionalnya bertumpu pada sistem jaringan yang terintegrasi dengan berbagai platform. Jaringan komunikasi data taktis tersebut dikenal sebagai *Tactical Data Link (TDL)* yang digunakan pada komunikasi data melalui gelombang radio atau kabel untuk mengirimkan dan menerima data taktis. Indonesia memiliki wilayah lautan yang luas sehingga dalam pelaksanaan patroli wilayah maritim, TNI AL perlu dukungan dari TNI AU untuk pengintaian dan pengamatan tersebut. Data dan informasi yang diperoleh pada saat operasi pengintaian dan pengamatan diolah dan dianalisa oleh Pusat Komando dan Pengendali (Puskodal) untuk kemudian diambil tindakan. Sehingga sistem TDL harus aman dari berbagai gangguan dan serangan siber agar informasi yang diperoleh merupakan data yang valid serta *real time*. Dalam pelaksanaannya, penggunaan TDL pada K4IPP dapat diterapkan pada operasi militer perang maupun operasi militer selain perang. Pada operasi militer selain perang dapat digunakan untuk monitoring wilayah strategis diantaranya ALKI (Alur Laut Kepulauan Indonesia) I, ALKI II, ALKI III serta wilayah strategis lainnya. Dalam hal ini, PT. LEN tengah mengembangkan *Combat Tactical Data Link System (CTDLS)* untuk mendukung misi strategis tersebut. (Hutomo, 2021)

Pada K4IPP arsitekturnya meliputi struktur pengorganisasian yang dibuat dan digunakan untuk mengidentifikasi, memverifikasi, memvisualisasikan, dan membahas komponen sistem K4IPP yang dibutuhkan



yang semakin kompleks dan multidimensional, yaitu berupa ancaman militer, ancaman non militer serta ancaman hibrida yang dapat dikategorikan dalam bentuk ancaman aktual dan ancaman potensial. Bentuk ancaman tersebut diantaranya terorisme, radikalisme, separatisme, pemberontakan bersenjata, pelanggaran, wilayah perbatasan, spionase, serangan siber dan sebagainya. (I. N. Putra & Hakim, 2016)

Kemampuan pertahanan negara dalam mengantisipasi ancaman dapat dilakukan dengan penggunaan teknologi informasi dan komunikasi yaitu dengan mengembangkan konsep Sistem Komando, Kontrol, Komunikasi, Komputasi, Intelijen, Pengawasan, Pengintaian (K4IPP) yang dapat mengatur berbagai fungsi komando dan kendali, peringatan dini, komunikasi, pengendalian senjata, dan keamanan informasi dalam operasi militer. Dalam konteks K4IPP, sistem informasi digital adalah sistem utama untuk memperoleh / memproses / meneruskan informasi militer sehingga keputusan, komando dan kendali, dan manajemen medan pertempuran dapat tercapai.

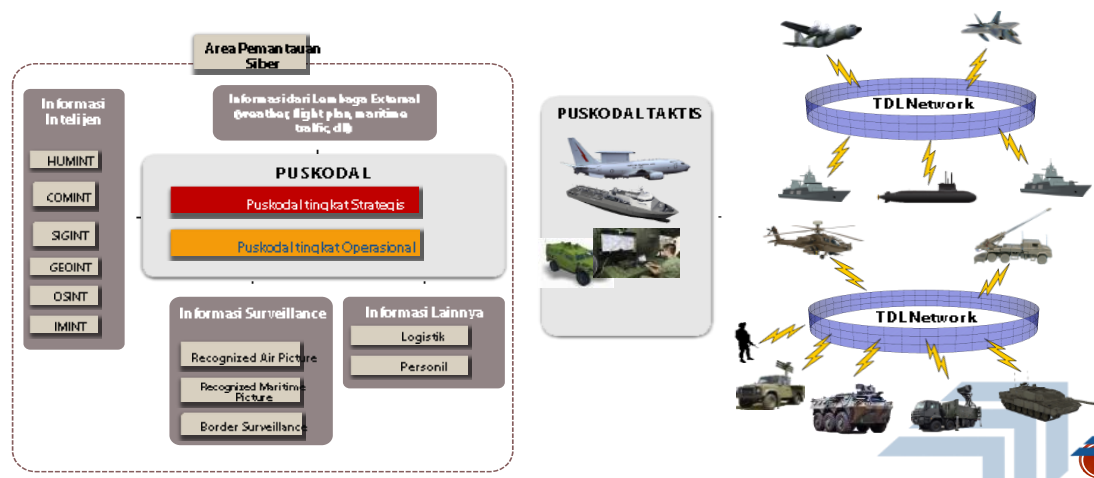
Dengan memperhatikan dan mempertimbangkan kebijakan pemerintah, kepentingan sinkronisasi pembangunan gelar kekuatan TNI dengan pembangunan nasional maupun dengan visi misi Panglima TNI yang akan dihadapkan dengan tugas TNI maka ditetapkan 11 (sebelas) program prioritas dalam rangka pembangunan TNI yang meliputi: (1) revitalisasi program-program didalam *Minimum Essential Force (MEF)*; (2) penyempurnaan doktrin TNI dan doktrin Angkatan; (3) penyempurnaan organisasi TNI; (4) pengembangan sistem pengelolaan SDM TNI yang berbasis kompetensi; (5) pembangunan TNI AD menjadi kekuatan terpusat, kewilayahan, dan pendukung; (6) pembangunan TNI AL melalui penyusunan Sistem Senjata Armada Terpadu (SSAT) terdiri atas kapal perang, pesawat udara, marinir dan pangkalan; (7) pembangunan TNI AU untuk mencapai *air supremacy* atau *air superiority*; (8) pembangunan unit khusus yang terdiri dari pasukan-pasukan khusus Tri Matra; (9) pengembangan sistem operasi Tri Matra yang

berbasis teknologi yang meliputi *Network Centrix Warfare*, K4IPP, dan *Cyber Warfare*; (10) penguatan diplomasi militer dan peningkatan kontribusi dalam rangka memenangkan kepentingan nasional; (11) mewujudkan sistem pengadaan Alutsista yang berpedoman pada *effect based* dan interoperabilitas yang dilakukan secara transparan dan akuntabel serta bebas KKN. (Kompas, 2018)

## 1.2 Identifikasi Masalah

Dengan menggunakan konsep K4IPP, TNI diharapkan dapat memperoleh informasi yang cepat, tepat dan *real time* sehingga dapat memudahkan pimpinan dalam mengambil keputusan strategis.

Sistem K4IPP bertumpu pada sistem jaringan serta data yang terintegrasi, sehingga bila sistem jaringannya terkena serangan siber akan melumpuhkan sistem K4IPP tersebut.

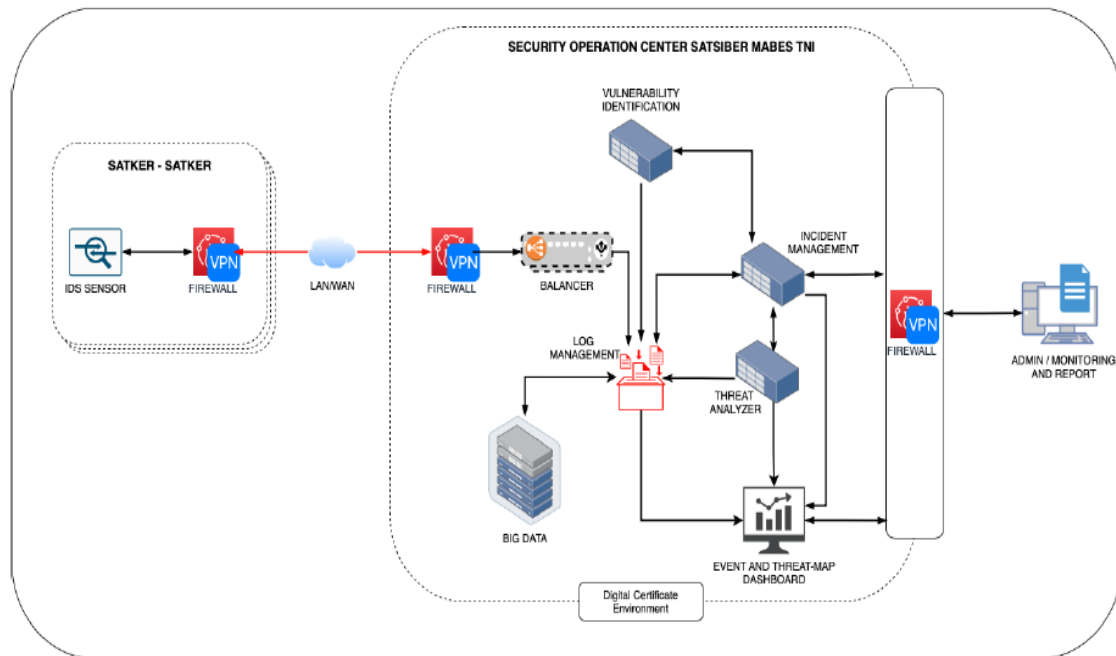


Gambar 1.4 Fungsi Sistem Pemantauan Siber Pada K4IPP

Sumber : Materi Kuliah *Radar Modern and Cyber Sensing for Defense* pada 12 juli 2021

## 1.3 Pembatasan Masalah

Penelitian ini dibatasi pada keamanan data dan informasi di Kemhan dan Mabes TNI serta K4IPP dari serangan siber.



Gambar 1.5 Topologi Sistem Keamanan Siber

Sumber : Materi Kuliah *Radar Modern and Cyber Sensing for Defense* pada 12 juli 2021

#### 1.4 Rumusan Masalah

Perkembangan lingkungan strategis dikawasan Asia Pasifik yang penuh dengan dinamika dapat berdampak pada masalah ekonomi dan keamanan. Untuk itu perlu implementasi dalam melaksanakan komando, kontrol, komunikasi, komputer, intelijen, pengawasan dan pengintaian (K4IPP) dan sistem pertahanan siber dalam menghadapi dinamika lingkungan strategis.

Pada operasi militer perang dan operasi militer selain perang, dibutuhkan informasi yang *real time*, terpercaya, dan tidak ada kebocoran informasi agar memudahkan pimpinan dalam mengambil keputusan strategis secara tepat, efektif dan efisien serta dapat memberikan komando yang terintegrasi antar matra dan antar platform alutsista.

Dalam menghadapi masalah tersebut, dapat dirumuskan masalah penelitian ke dalam pertanyaan penelitian berikut:

- a. Bagaimana keamanan data K4IPP dalam pertahanan siber Kemhan dan TNI
- b. Bagaimana indeks pertahanan siber Kemhan dan K4IPP TNI yang diharapkan

### **1.5 Tujuan Penelitian**

Tujuan penelitian ini adalah sebagai berikut :

- a. Menganalisis keamanan data K4IPP dalam pertahanan siber Kemhan dan TNI
- b. Memberi masukan indeks pertahanan siber Kemhan dan K4IPP TNI yang diharapkan

### **1.6 Manfaat Penelitian**

Manfaat penelitian ini adalah :

- a. Dari sisi teoritis sebagai bahan kajian akademis dalam menganalisa ancaman siber pada sistem K4IPP
- b. Dari sisi praktis sebagai bahan masukan bagi TNI dalam merumuskan kebijakan terkait keamanan data K4IPP dalam menghadapi ancaman siber.