UNIVERSITAS PERTAHANAN

IMPLEMENTASI SISTEM PENGAMANAN INFORMASI DALAM APLIKASI *INAPORTNET* UNTUK *MARITIME CYBER SECURITY*

ASMAUL MUFIDASARI
NIM: 120170302004

Tesis yang Ditulis untuk Memenuhi Sebagian Persyaratan dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS KEAMANAN NASIONAL
PROGRAM STUDI KEAMANAN MARITIM

BOGOR

Januari 2019

UNIVERSITAS PERTAHANAN

IMPLEMENTASI SISTEM PENGAMANAN INFORMASI DALAM APLIKASI *INAPORTNET* UNTUK *MARITIME CYBER SECURITY*

ASMAUL MUFIDASARI
NIM: 120170302004

Tesis yang Ditulis untuk Memenuhi Sebagian Persyaratan dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS KEAMANAN NASIONAL
PROGRAM STUDI KEAMANAN MARITIM

BOGOR

Januari 2019

LEMBAR PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	Asmaul Mufidasari
NIM	:	120170302004
Program Studi	:	Keamanan Maritim
Judul	:	Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk *Maritime Cyber Security*

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Magister dalam Ilmu Pertahanan pada Program Studi Keamanan Maritim, Fakultas Keamanan Nasional Universitas Pertahanan.

DEWAN PENGUJI

Pembimbing I	:	Laksamana Muda TNI Dr. A.Octavian, ST., M.Sc., D.E.S.D	( )
Pembimbing II	:	Dr. Herlina Juni Saragih	( )
Reviewer I	:	Laksamana Madya TNI (Purn) Dr. Moch. Yurianto S.E., M.M	( )
Reviewer II	:	Kolonel Laut (KH) Dr. Abdul Rivai Ras, M.M., M.Si	( )
Reviewer III	:	Kolonel Laut (P) Purwanto, M.M., M.Si (Han)	( )

Ditetapkan di : Bogor

Tanggal : Januari 2019

PERNYATAAN ORISIONALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragrat, subbab atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dandisebutkan dalam Daftar Referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai ketentuan peraturan/undang-undang yang berlaku.

Bogor, Januari 2019

Asmaul Mufidasari

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH
UNTUK KEPENTINGAN AKADEMIS

Tesis ini diajukan oleh:

Nama : Asmaul Mufidasari

NIM : 120170302004

Program Studi : Keamanan Maritim

Fakultas : Keamanan Nasional

Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pertahanan Hak Bebas Royalty Noneksklusif (*Non-exclusive Royalty-Free Right*) atas ilmiah saya berjudul:

Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk *Maritime Cyber Security*

Beserta perangkat yang ada jika diperlukan. Dengan Hak Bebas Royalty Noneksklusif ini Universitas Pertahanan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tesis saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta/Karya Intelektual dari tesis ini.

Demikian pernyataan ini saya buat dengan kesadaran penuh tanpa paksaan dari pihak manapun.

Bogor, Januari 2019

Asmaul Mufidasari

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya penyusunan tesis dengan judul: “Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk *Maritime Cyber Security*” dapat diselesaikan.

Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister pada Program Studi Keamanan Maritim, Fakultas Keamanan Nasional, Universitas Pertahanan.

Penyusunan tesis ini dapat diselesaikan berkat bantuan dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Rektor Universitas Pertahanan Letnan Jenderal TNI Dr. Tri Legionosuko, S.IP., M.AP
2. Dekan Fakultas Keamanan Nasional Laksamana Muda TNI Dr. Siswo Hadi Sumantri, S.T., M.MT
3. Laksamana Muda TNI Dr. A.Octavian, ST., M.Sc., D.E.S.D dan Dr. Herlina Juni Saragih selaku Pembimbing 1 dan 2 untuk penelitian ini.
4. Laksamana Madya TNI (Purn) Dr. Moch. Yurianto S.E., M.M sebagai penguji 1 , Kolonel Laut (KH) Dr. Abdul Rivai Ras, M.M., M.Si sebagai penguji 2, dan Kolonel Laut (P) Purwanto, M.M., M.Si (Han) sebagai penguji 3.
5. Ketua Program Studi Keamanan Maritim Kolonel Laut (P) Purwanto, S.E., M.M., M.Si (Han), Staf Prodi Keamanan Maritim Neni Yanjiaurora M.Han, dan Hari Nugraha M.Han atas bantuannya dalam pengurusan administrasi dari awal perkuliahan hingga akhir.
6. Informan dari Direktorat Lalu Lintas dan Angkutan Laut Ayu Khariza S.Kom, informan dari Pusat Teknologi Informasi dan Komunikasi

Henry, dan informan dari Telkomsigma yaitu Agung Dwiyanto atas waktu luang dan ilmu baru yang diberikan.

7. Kedua orang tua yang selalu mendoakan kelancaran dan keberkahan seluruh rangkaian kegiatan perkuliahan dari awal hingga saat ini.
8. Keluarga “seventeen squad” keamanan maritim cohort 5 atas dukungan, keceriaan, dan kekeluargaannya selama awal perkuliahan hingga saat ini dan selamanya.
9. Teman-teman cohort 9 yang selalu aktif memberikan informasi-informasi terbaru mengenai dinamika yang ada.

Semoga Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas bantuannya.

Peneliti menyadari bahwa tesis ini masih kurang sempurna, oleh karena itu dengan kerendahan hati mengharapkan kritik dan saran yang konstruktif demi menunjang kesempurnaan penelitian ini.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi *stakeholder* terkait dalam upaya pencegahan dan penanganan secara cepat dan tepat untuk menghadapi ancaman *cyber* dalam domain maritim.

Bogor, Januari 2019

Asmaul Mufidasari

ABSTRAK

IMPLEMENTASI SISTEM PENGAMANAN INFORMASI DALAM APLIKASI INAPORTNET UNTUK *MARITIME CYBER SECURITY*

ASMAUL MUFIDASARI

Perkembangan teknologi informasi dan komunikasi telah mempengaruhi domain maritim. Perkembangan ini telah membawa ancaman baru dalam domain maritim yaitu ancaman *cyber*. Inaportnet merupakan salah satu pemanfaatan teknologi informasi dan komunikasi dalam domain maritim yang dilakukan oleh Kementerian Perhubungan. Inaportnet merupakan portal elektronik berbasis internet yang mampu mengintegrasikan seluruh sistem informasi pemangku kepentingan yang ada di pelabuhan. Ancaman *cyber* dalam aplikasi Inaportnet dapat dicegah apabila mempunyai sistem pengamanan informasi yang kuat. Tujuan dari penelitian ini yaitu menjelaskan mekanisme sistem pengamanan informasi dalam aplikasi Inaportnet dan memahami aspek pendukung dan penghambat dalam sistem pengamanan informasi di aplikasi Inapornet untuk melindungi informasi dari ancaman *cyber*. Metode penelitian yang digunakan adalah kualitatif eksploratif yaitu untuk mengungkapkan alasan tertentu mengapa informasi tersebut terjadi. Sedangkan pengolahan data untuk memeriksa keabsahan data menggunakan *software* NVivo, serta analisa data menggunakan teknik *Soft System Methodology* (SSM) untuk menghasilkan hasil analisa yang lebih mendalam, serta hasil pemikiran dan analisa yang lebih terstruktur. Hasil yang didapat adalah implementasi keamanan informasi dalam aplikasi Inaportnet belum berjalan dengan baik. Walaupun secara sistem teknologi sudah memenuhi namun aspek lain yaitu kesadaran untuk keamanan informasi masih kurang, hal ini berdasarkan temuan di lapangan. Inaportnet masih belum mempunyai *Information Security Handbook*, padahal buku ini diperlukan untuk banyak hal yang mendukung sistem keamanan informasi Inaportnet. Inaportnet juga belum mempunyai jadwal rutin untuk melakukan penetration test dan patch. Oleh karena itu, sebagai pemegang kebijakan aplikasi Inaportnet Direktorat Jenderal Perhubungan Laut perlu untuk membuat Inaportnet *information security handbook* agar sistem keamanan informasinya tidak hanya baik di teknologinya saja, namun juga baik secara manajemen antar *stakeholder* dan *cyber security awareness* di tingkat individunya.

Kata kunci: Inaportnet, Keamanan Informasi, *Maritime Cyber Security*.

ABSTRACT

INFORMATION SECURITY SYSTEM IMPLEMENTATION IN INAPORTNET APPLICATION FOR MARITIME CYBER SECURITY

ASMAUL MUFIDASARI

The development of information and communication technology has influenced the maritime domain. This development has brought cyber threats in the maritime domain. Inaportnet is one of the uses of information and communication technology in the maritime domain carried out by the Ministry of Transportation. Inaportnet is an internet-based electronic portal that is able to integrate all stakeholder information systems in the port. Cyber threats in Inaportnet applications can be prevented if they have a strong information security system. The purpose of this study is to explain the mechanism of information security systems in the Inaportnet application and understand the supporting and inhibiting aspects of the information security system in the Inapornet application to protect information from cyber threats. The research method used is qualitative explorative which is to reveal certain reasons why the information occurred. While processing data to check the validity of data using NVivo software, and data analysis using Soft System Methodology (SSM) techniques to produce more in-depth analysis results, as well as more structured results of thought and analysis. The results obtained are that the implementation of information security in the Inaportnet application is not running well. Although the technology system has fulfilled but other aspects, namely awareness for information security is still lacking, this is based on findings in the field. Inaportnet still does not have the Information Security Handbook, even though this book is needed for many things that support the Inaportnet information security system. Inaportnet also does not have a routine schedule for doing penetration tests and patches. Therefore, as the holder of the Inaportnet, Directorate General of Sea Transportation application policy, it is necessary to make Inaportnet information security handbook so that the information security system is not only good in the technology, but also in management between stakeholders and cyber security awareness at the individual level.

Keywords: Inaportnet, Information Security, Maritime Cyber Security.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era modern saat ini keamanan nasional tidak hanya tertuju pada segi militer saja, keamanan nasional pada era modern saat ini memiliki bentuk yang lebih global. Banyak negara yang menerapkan sistem keamanan nasional sesuai dengan perkembangan lingkungan strategis dan perkembangan ancaman yang terjadi di negaranya. Keamanan nasional dapat meliputi keselamatan dan keamanan suatu negara, melalui berbagai aspek seperti aspek militer, ekonomi, diplomasi, keamanan energi, lingkungan dan lain sebagainya. Begitupun dengan ancaman keamanan yang semula berorientasi pada ancaman tradisional, saat ini telah beralih menjadi ancaman yang lebih multidimensi.[1] Gagasan tentang keamanan nasional termasuk salah satu gagasan baru. Keamanan Nasional sering mengacu pada negara merdeka yang berusaha melindungi integritas dan wilayah teritorialnya. Definisi keamanan nasional dapat seringkali dikaitkan dengan kemampuan suatu negara dalam melindungi negaranya dari ancaman yang datang dari luar. Keamanan nasional sendiri merupakan keamanan suatu negara, keamanan nasional dan integritas keamanannya serta kedaulatannya.[2]

Dalam mempertahankan wilayah kedaulatan Indonesia, maka aspek pertahanan tidak akan terpisah dengan aspek keamanan nasional Indonesia. Keamanan nasional dipengaruhi oleh dinamika perubahan dalam lingkungan strategi atau faktor-faktor dari dalam negeri yaitu ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan.[3] Seiring

---

[1] Bambang Darmono, "Konsep dan Sistem Keamanan Nasional Indonesia", *Jurnal Ketahanan Nasional*, Volume 15 (1), 2010, hlm. 1.
[2] Natasha Grozdanoska, "National Defence and Security", *European Scientific Journal*, Volume.1, 2014, ISSN-1857-7431
[3] Kementerian Pertahanan Indonesia, "Buku Putih Pertahanan Indonesia", 2015, hlm 1.

dengan perkembangan teknologi informasi dan komunikasi yang saat ini telah dimanfaatkan dalam berbagai sektor lingkungan strategis menyebabkan perkembangan baru dalam dinamika lingkungan strategis tersebut. Akibat pengaruh dari teknologi informasi dan komunikasi seluruh dimensi lingkungan strategis telah terkonversi kedalam dunia *cyber space*.

Keberadaan *cyber space* yang lebih mudah dijangkau dan diakses harus diimbangi dengan kemampuan negara dalam menguasai, mengawasi, dan mengendalikan pergerakannya dalam dunia *cyber*. Perkembangan teknologi informasi dan komunikasi dapat menjadi sarana baru untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai lingkungan strategis yang ada di Indonesia. Globalisasi juga menyebabkan setiap negara dapat saling melintasi tanpa adanya kendali dan kontrol dari negara yang dominan (*borderless*). Pada akhirnya, ekspansi mulai dari sektor ekonomi, sosial, budaya, ideologi dan pemikiran dapat dilakukan dengan mudah karena adanya perdagangan bebas dan pasar bebas yang menjadi medianya. Lingkungan strategis seperti ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan telah dipengaruhi oleh digitalisasi dan lebih banyak menggunakan *cyber space* baik untuk penyebaran, pengoperasian, dan pemantauannya. Dengan wilayah Indonesia yang didominasi oleh laut, maka pengaruh dari lingkungan strategis juga dipengaruhi oleh kondisi Indonesia yang didominasi oleh wilayah laut.

Wilayah laut yang luas dan berbentuk pulau-pulau membuat Indonesia sangat rentan terhadap ancaman, baik ancaman militer maupun non-militer. Oleh karena itu, perkembangan Keamanan Nasional Indonesia juga dipengaruhi oleh posisi Indonesia sebagai negara kepulauan dan mempunyai wilayah laut yang luas. Oleh sebab itu, pembahasan tentang isu-isu dalam keamanan maritim sedang menjadi perhatian internasional. Menurut Bueger (2015) perbincangan tentang keamanan maritim sering merujuk pada ‘ancaman’ yang berlaku di domain maritim. Persoalan dalam keamanan maritim menyangkut banyak aspek seperti lingkungan laut,

pengembangan ekonomi, keamanan nasional, dan *human security*. Keamanan maritim merupakan sebuah kata kunci, oleh karena itu tidak ada definisi yang pasti mengenai keamanan maritim itu sendiri.[4] Keamanan maritim modern telah dipengaruhi oleh arus globalisasi dan perkembangan teknologi. Globalisasi membawa dunia modern pada perkembangan era informasi dan komunikasi yang menciptakan era serba digital (*digital world*).

Teknologi informasi dan komunikasi saat ini telah merambah domain maritim, banyak kementerian/lembaga yang berkepentingan di domain maritim menggunakan portal elektronik berbasis internet untuk memudahkan pelayanannya. Salah satunya adalah penerapan Inaportnet yang digunakan untuk mempermudah, mempersingkat waktu, serta transparansi pelayanan kegiatan pelabuhan yang standar. Penerapan aplikasi Inaportnet di pelabuhan telah membuat celah untuk masuknya ancaman baru, yaitu ancaman *cyber* dalam domain maritim.

Ancaman *maritime cyber* mengacu pada ukuran sejauh mana aset-aset teknologi dapat terancam oleh keadaan atau peristiwa potensial yang dapat mengakibatkan kegagalan operasional, keselamatan atau keamanan terkait dengan *shipping* yang merupakan konsekuensi dari informasi atau sistem yang rusak, hilang, atau dikompromikan.[5] Ancaman *cyber* yang terjadi di pelabuhan dapat berupa penghapusan data operasional yang berisi jadwal dan informasi untuk pengiriman kontainer. Ancaman dari *maritime cyber* dapat berubah menjadi sebuah bentuk serangan *cyber.* Ancaman dan serangan *cyber* sulit untuk dideteksi terkadang korban baru sadar ketika telah diserang. Namun, serangan ini dapat ditangkal apabila aplikasi Inaportnet mempunyai sistem pengamanan informasi yang tepat dan kuat. Untuk kondisi ini, sistem pengamanan informasi dalam aplikasi Inaportnet dinilai sangat penting, karena informasi-informasi penting para

[4] Christian Bueger, “What is Maritime Security?”, *Marine Policy*,Vol.53, 2014, hlm. 159.
[5] International Maritime Organization, “Guidelines on Maritime Cyber Risk Management”, IMO-MSC-FAL.1/CICC 3,2017.

pemangku kepentingan di pelabuhan akan melalui aplikasi ini setiap harinya.

Apabila sistem pengamanan informasi dalam aplikasi Inapornet tidak diperkuat, maka kondisi ini dapat menyebabkan dampak yang serius. Seperti halnya yang terjadi pada kasus-kasus dibawah ini:

Tabel 1.1 Kasus-kasus *cyber* yang terjadi dalam domain maritim

No.	Tahun	Kasus	Lembaga / perusahaan	Keterangan
1.	Antara tahun 2011-2013	Penyelun-dupan Narkoba	Pelabuhan Antwerp, Belgia	Para kriminal menggunakan jaringan *cyber* di pelabuhan untuk menyelundupkan narkoba, mereka menginstal sebuah alat kemudian mengirim malware yang di *attach* dalam email untuk menyusup ke dalam sistem komputer pelacak kargo dari berbagai perusahaan di pelabuhan. Dengan cara ini, mereka dapat mengidentifikasi *shipping containers* mana yang tempat narkoba disembunyikan. Ketika kontainer sudah datang mereka akan mengirim supir yang telah dipersiapkan untuk mengambil kontainer tersebut
2.	2014	Serangan *cyber*	Otoritas Maritim Denmark	Serangan *cyber* tersebut dilakukan melalui transmisi dokumen PDF dengan virus yang tertanam didalamnya. Akibatnya, virus ini menyebar di seluruh jaringan organisasi serta lembaga-lembaga pemerintah Denmark lainnya.
3.	2012	Pencurian data personel US Navy	Perusahaan Hewlett Packard	Terjadi di mana data sebanyak 134.000 personel US Navy dicuri oleh *hackers*. Mereka dapat melakukan peretasan melalui sebuah perusahaan bernama

No.	Tahun	Kasus	Lembaga / perusahaan	Keterangan
				Hewlett Packard yang memang bertanggung jawab untuk melakukan otomatisasi di lingkungan US Navy
4.	2015	*Cyber scam*	Nautilus Minerals dan Marine Assets Corportaion (MAC)	Kejadian ini menyebabkan kerugian bagi pihak Nautilus Minerals yang telah membayar sebesar $10 juta dari total kontrak $18 juta, sebagai pembayaran awal atas kontrak mereka untuk proyek *sea floor mining* di Papua Nugini. Pada bulan desember terdapat pihak ketiga yang melakukan *cyber scam*, dan menyebabkan Nautilus membayar uang tersebut kepada akun bank yang diyakini milik MAC, namun akun bank tersebut bukanlah milik MAC yang sebenarnya.
5.	2013	Percoba-an pembobo-lan *Automatic Identificati on System* (AIS)	Perusahaan keamanan Trend Micro	Perusahaan ini menemukan celah dalam percobaan untuk menguji sistem keamanan AIS. Pada kenyataannya sistem AIS dapat dibobol dan data yang sedang dikirim dapat dirubah. Perusahaan ini melakukan manipulasi dalam jaringan internet yang digunakan AIS ketika mentransmisikan data. Data-data yang dapat diubah adalah semuanya, mulai dari posisi kapal, jalur, muatan, nama kapal, mengirim sinyal bahaya palsu, informasi cuaca palsu hingga membuat posisi kapal palsu yang dapat muncul dilokasi

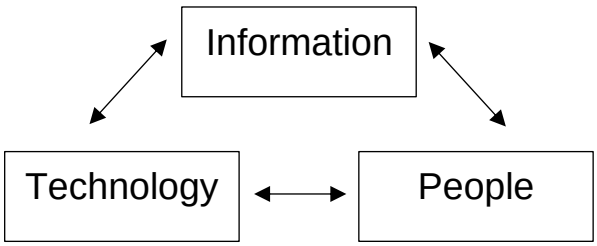
No.	Tahun	Kasus	Lembaga / perusahaan	Keterangan
				manapun dan mematikan AIS sepenuhnya di kapal.

Sumber: Hasil olahan peneliti dari berbagai sumber (2018)

Beralihnya sistem administrasi di pelabuhan dari sistem administrasi konvensional menuju digital telah menyebabkan resiko baru, berupa kerentanan pencurian data melalui jaringan *cyber*. Walaupun ranah *maritime cyber* masih terbilang baru, namun dampak yang dihasilkan apabila terjadi kejahatan *cyber* dalam domain maritim bisa sangat besar. Disinilah peran dari penguatan *Maritime Cyber Security* untuk pengamanan arus informasi digital yang berkaitan dengan domain maritim.

Terdapat 3 (tiga) elemen yang mendasari pengoperasian *cyber* dalam domain maritim, ketiga elemen tersebut adalah Informasi, Teknologi, dan Manusia. Informasi berkaitan dengan data mana yang mendukung di dalam operasi maritim, serta bagaimana informasi tersebut digunakan dan dengan cara apa informasi tersebut dapat dirusak di era modern ini. Teknologi mencakup sistem komputer, baik perangkat keras maupun perangkat lunaknya, serta platform yang lebih besar seperti kapal dan pelabuhan. Teknologi sangat penting karena merupakan fondasi yang mendasari perkembangan ekonomi global tetapi juga rentan secara fisik dan digital. Manusia merupakan bagian dari sistem yang kompleks dilingkungan maritim, mereka berinteraksi satu sama lain. Di setiap interaksi antara manusia dengan mesin selalu ada kemungkinan untuk terjadinya kesalahan, manipulasi, pemaksaan atau hasutan.[6]

[6] Oliver Fitton, *et al,* "The Future of Maritime Cyber Security", *Lancaster University*, 2015, Security Lancaster, hlm.2.



Gambar 1.1 Elemen dari pengoperasian *Maritime Cyber Security*

Sumber: Oliver Fitton, *et al*, "The Future of Maritime Cyber Security", Lancaster University, 2015, Security Lancaster, hlm.2

Setiap elemen ini mempunyai hubungan satu sama lain yang mungkin menjadi target dari gangguan dan ancaman, misalnya tingkat kepercayaan yang dimiliki seseorang dalam suatu teknologi akan mempengaruhi hubungan antara invidu tersebut dengan informasi yang akan dihasilkan teknologi. Penyebab kerentanan sistem komputerasi di pelabuhan terhadap gangguan dan ancaman, contohnya adalah terbatasnya pelatihan atau tenaga ahli dalam bidang *maritime cyber security*, kurangnya kesiapan untuk *maritime cyber security, software* yang mengalami gangguan, dan koneksi serta ketergantungan akan kondisi jaringan internet.[7] Agar tercipta kondisi tanpa gangguan pada sistem komputerisasi di pelabuhan, maka sistem pengamanan pada ketiga elemen tersebut harus dalam kondisi siap.

Diperlukan sinergitas antara ketiga elemen tersebut untuk mendukung *Maritime Cyber Security* dalam aplikasi Inaportnet. Tidak hanya elemen-elemen tersebut, namun pemusatan dalam sistem keamanan informasi dalam aplikasi Inaportnet juga perlu untuk dilakukan. Perlu adanya perhatian khusus dari Direktorat Jenderal Perhubungan Laut sebagai penanggung jawab aplikasi Inaportnet terkait dengan adanya kemungkinan ancaman *cyber* dalam aplikasi Inapornet yang semakin berkembang. Pencegahan serangan dan ancaman *cyber* dalam penerapan

[7] Jenna Ahokas dan Tuomas Kiiski, "Cyber security in Ports", *Publication of the Hazard Project*, Vol.3, 2017, hlm. 27.

aplikasi Inaportnet dapat dilakukan dengan cara pengamanan sistem informasi yang kompleks dan berlapis.

Keamanan fasilitas pelabuhan telah disebutkan dalam *International Ship and Port Facility Security Code* (ISPS Code), meskipun tidak menyebutkan tentang keamanan informasi secara terperinci. Namun, dalam bab 16 dalam ISPS Code tahun 2003 tentang mewajibkan adanya Rencana Keamanan Fasilitas Pelabuhan (*Port Facility Security Plan*) yaitu sebuah perencanaan pengembangan yang dibuat untuk melindungi fasilitas pelabuhan, kapal, pekerja, kargo, cargo transport unit, dari resiko insiden yang mengancam keamanan pelabuhan.[8] Serta ditambahnya dengan peraturan XI-2/1.3 yang menyatakan "Mewajibkan adanya kegiatan administrasi/pemerintah yang mengatur tingkat keamanan dan menjamin penyediaan informasi tingkat keamanan untuk kapal. Kegiatan ini dilakukan saat kapal sebelum memasuki pelabuhan atau saat sementara di pelabuhan".[9]

Ketentuan tentang administrasi untuk penyampaian informasi juga terdapat dalam Undang-undang Nomor 17 pasal 272 tahun 2008 tentang Pelayaran yaitu sebagai berikut:

(1) Setiap orang yang melakukan kegiatan di bidang pelayaran wajib menyampaikan data dan informasi kegiatannya kepada Pemerintah dan/atau pemerintah daerah.
(2) Pemerintah dan/atau pemerintah daerah melakukan pemuktahiran data dan informasi pelayaran secara periodic untuk menghasilkan data dan informasi yang periodik untuk menghasilkan data dan informasi yang sesuai dengan kebutuhan, akurat, terkini, dan dapat dipertanggungjawabkan.
(3) Data dan informasi pelayaran didokumentasikan dan dipublikasikan serta dapat diakses dan digunakan oleh masyarakat yang

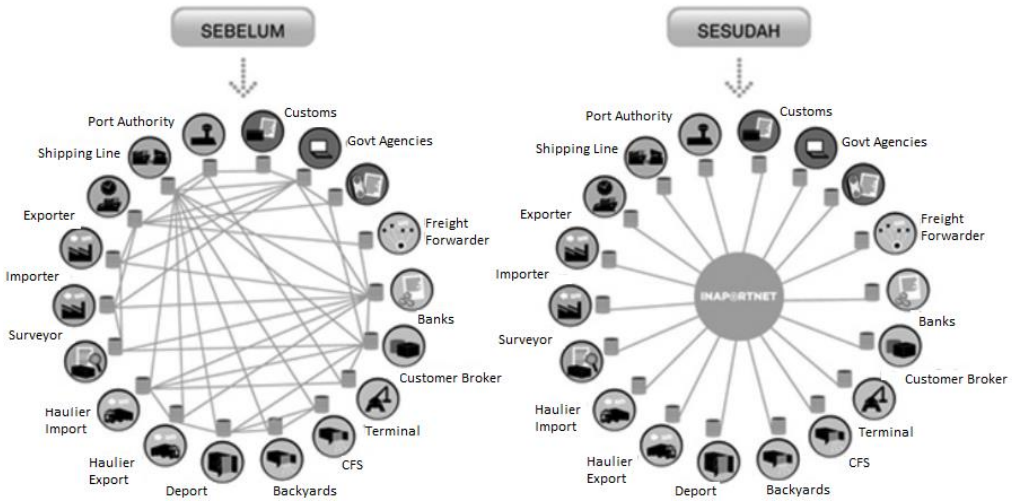
[8] ISPS Code Tahun 2003 tentang Port Facility Security Plan bagian 16
[9] ISPS Code Tahun 2003 tentang Functional Requirements bagian 1.3

membutuhkan dengan memanfaatkan teknologi informasi dan komunikasi.

(4) Pengelolaan sistem infomrasi pelayaran oleh Pemerintah dan pemerintah daerah dapat dilkaukan melalui kerja sama dengan pihak lain.

(5) Ketentuan lebih lanjut mengenai tata cara penyampaian dan pengelolaan informasi pelayaran diatur dengan Peraturan Menteri.

Komputerisasi di pelabuhan ini dilakukan agar pelabuhan di Indonesia dapat berjalan cepat, efektif, efisien serta berdaya saing. Teknologi informasi dan komukasi yang dilakukan berupa penerapan portal elektronik berbasis internet yang mampu mengintegrasikan seluruh sistem informasi pemaku kepentingan yang ada di pelabuhan. Sistem ini diberi nama aplikasi Inaportnet. Inaportnet merupakan sebuah program dari Kementerian Perhubungan yang dalam implementasinya perlu dukungan bersama dari para *stakeholder* di pelabuhan serta penyelenggaraannya dilakukan oleh Direktorat Jenderal Perhubungan Laut. Peran dari Inaportnet sebagai aplikasi yang mengintegrasikan sistem informasi yang ada di pelabuhan di ilustrasikan dalam gambar dibawah ini:



Gambar 1.2 Ilustrasi dari penggunaan aplikasi Inapornet

Sumber: Budi Sitorus, Tulus Irpan H. Sitorus, dan Prasadja Ricardianto, “Evaluasi Manajemen Sistem Informasi dan Teknologi Informasi Pelabuhan”, Jurnal Manajemen Transportasi & Logistik (JMTransLog), Volume 3 (3),2016.

Inaportnet merupakan sebuah sistem informasi layanan tunggal elektronik berbasis internet untuk mengintegrasikan sistem informasi kepelabuhanan yang standar dalam melayani kapal dan barang dari seluruh instansi terkait di pelabuhan.[10] Sesuai dengan Peraturan Menteri Perhubungan Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan, pada pasal 2 ayat (3) yang menyatakan penerapan Inaportnet pelayanan kapal dan barang dipelabuhan dilakukan sesuai tugas, fungsi, kewenangan, dan tanggung jawab dari setiap instansi Pemerintah dan pemangku kepentingan terkait di pelabuhan berdasarkan ketentuan peraturan perundang-undangan. Kemudian dilanjutkan dengan ayat (4) yang berisi instansi Pemerintah dan pemangku kepentingan terkait di pelabuhan sebagaimana dimaksud pada ayat (3), yaitu sebagai berikut:

Tabel 1.2 Instansi Pemerintah dan Pemangku Kepentingan di Pelabuhan

No.	Instansi Pemerintah dan Pemangku Kepentingan
1.	Kantor Otoritas Pelabuhan Utama
2.	Kantor Kesyahbandaran Utama
3.	Kantor Kesyahbandaran dan Otoritas Pelabuhan
4.	Kantor Unit Penyelenggara Pelabuhan/Kantor Pelabuhan
5.	Kantor Pabean
6.	Kantor Kesehatan Pelabuhan
7.	Balai Karantina Pertanian
8.	Kantor Karantina Ikan dan Pengawasan Mutu Ikan
9.	Kantor Imigrasi
10.	Badan Usaha Pelabuhan
11.	Perusahaan Angkutan Laut Nasional di pelabuhan
12.	Perusahaan Bongkar Muat di pelabuhan

Sumber: Peraturan Menteri Perhubungan RI Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan

Penanggung jawab atas pelaksanaan aplikasi Inaportnet dilakukan oleh Direktorat Jenderal Perhubungan Laut[11]. Berdasarkan Peraturan

[10] Peraturan Menteri Perhubungan RI Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan.
[11] Berdasarkan Peraturan Menteri Perhubungan RI Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan

Presiden Nomor 40 Tahun 2015 tentang Kementerian Perhubungan, pada Pasal 13 disebutkan penyelenggaraan tugas dan fungsi dari Direktorat Jenderal Perhubungan Laut adalah sebagai berikut:

1. Perumusan kebijakan di bidang penyelenggaraan angkutan di perairan, kepelabuhanan, sarana dan prasarana pelayaran, perlindungan lingkungan maritim, serta peningkatan keselamatan dan keamanan pelayaran;
2. Pelaksanaan kebijakan di bidang penyelenggaraan angkutan di perairan, kepelabuhanan, sarana dan prasarana pelayaran, perlindungan lingkungan maritim, serta peningkatan keselamatan dan keamanan pelayaran;
3. Penyusunan norma, standar, prosedur, dan kriteria di bidang penyelenggaraan angkutan di perairan, kepelabuhanan, sarana dan prasarana pelayaran, perlindungan lingkungan maritim, serta peningkatan keselamatan dan keamanan pelayaran;
4. Pelaksanaan pemberian bimbingan teknis dan supervise di bidang penyelenggaraan di perairan, kepelabuhanan, sarana dan prasarana pelayaran, perlindungan lingkungan maritim, serta peningkatan keselamatan dan keamanan pelayaran;
5. Pelaksanaan evaluasi dan pelaporan di bidang penyelenggaraan angkutan di perairan, kepelabuhanan, sarana dan prasarana pelayaran, perlindungan lingkungan maritim, serta peningkatan keselamatan dan keamanan pelayaran;
6. Pelaksanaan administrasi Direktorat Jenderal Perhubungan Laut; dan
7. Pelaksanaan fungsi lain yang diberikan oleh Menteri.

Untuk saat ini, terdapat 16 (enam belas) pelabuhan di Indonesia telah terintegrasi sistem aplikasi Inaportnet. Berikut adalah daftar nama pelabuhan yang telah terintegrasi Inaportnet:

Tabel 1.3 Pelabuhan yang terintegrasi aplikasi Inaportnet

No.	Nama Pelabuhan	Kelas	Alamat
1.	Pelabuhan Belawan	Pelabuhan Utama / I (satu)	Jl. Sumatera No.1, Kelurahan Belawan Bahagia, Medan, Sumatera Utara
2.	Pelabuhan Tanjung Priok	Pelabuhan Utama / I (satu)	Jl. Raya Pelabuhan No.8 Tanjung Priok, Jakarta Utara, DKI Jakarta
3.	Pelabuhan Makassar	Pelabuhan Utama / I (satu)	Jl. Soekarno No.1, Kel. Ujung Tanah, Kec. Wajon, Sulawesi Selatan
4.	Pelabuhan Tanjung Emas	Pelabuhan Kelas I	Jl. Coaster No.10, Semarang, Jawa Tengah
5.	Pelabuhan Bitung	Pelabuhan Kelas I	Jl. D.S Sumolang, Kel.Pateten, Kec. Bitung Timur, Kodya Bitung, Sulawesi Utara
6.	Pelabuhan Dumai	Pelabuhan Utama / I (satu)	Jl. Datuk Laksamana Dumai, Riau Daratan
7.	Pelabuhan Banten	Pelabuhan Kelas II	Jl. Raya Pelabuhan No.1 Ciwandan, Banten
8.	Pelabuhan Batam (Batu Ampar)	Pelabuhan Kelas I	Jl. Lumba-lumba No.5, Kel. Sei Jodoh, Kec. Batu Ampar, Batam, Kepulauan Riau
9.	Pelabuhan Panjang	Pelabuhan Kelas I	Jl. Yos Sudarso No.337, Panjang, Bandar Lampung
10.	Pelabuhan Banjarmasin	Pelabuhan Kelas II	Jl. Barito Hilir No.6, Banjarmasin, Kalimantan Selatan
11.	Pelabuhan Balikpapan	Pelabuhan Kelas I	Jl. Yos Sudarso No.30, Kel. Prapatan, Kec. Balipapan Selatan, Balikpapan, Kalimantan Timur
12.	Pelabuhan Sorong	Pelabuhan Kelas I	Jl. Jend. A. Yani No. 13, Sorong, Irian Jaya Barat
13.	Pelabuhan Manggar	Pelabuhan Kelas I	Jl. Jend. Sudirman, Manggar, Belitung Timur

No.	Nama Pelabuhan	Kelas	Alamat
14.	Pelabuhan Tanjung Uban	Pelabuhan Kelas II	Tj. Uban Kota, Bintan Utara, Kabupaten Bintan, Kepulauan Riau
15.	Pelabuhan Tanjung Perak	Pelabuhan Utama / I (satu)	Jl. Tanjung Perak Timur, No. 620, Kel. Perak Timur, Kec. Pabean Cantian, Surabaya, Jawa Timur
16.	Pelabuhan Ambon	Pelabuhan Kelas I	Jl. Yos Sudarso No.1, Maluku Utara

Sumber: Peraturan Menteri Perhubungan RI Nomor PM 192 Tahun 2015 tentang Perubahan atas Peraturan Menteri Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet

Pemanfaatan teknologi Inaportnet untuk memaksimalkan pelayanan kapal dan barang di pelabuhan mempunyai keunggulan dan juga kelemahan. Tabel berikut menunjukkan beberapa keunggulan dan kelemahan dalam penggunaan aplikasi Inaportnet:

Tabel 1.4 Keunggulan dan Kelemahan aplikasi Inaportnet

No.	Keunggulan	Kelemahan
1.	Lapor kapal tiba/berangkat dengan Inaportnet dapat dilakukan kapanpun dan dimanapun	Meskipun sudah mendaftar secara *online*, namun verifikasi dokumen masih menggunakan metode manual
2.	Semua prosedur *Delivery Order* (DO) dilakukan secara online melalui aplikasi	Lemahnya kemampuan Sumber Daya Manusia dalam sistem administrasi
3.	*Tracking dan Tracing* posisi kapal dan barang dengan mudah menggunakan Inaportnet V.2	Sistem masih sering mengalami *down*
4.	Kemudahan akses informasi bagi pemangku kepentingan di pelabuhan	Belum terjaminnya keamanan informasi dalam aplikasi ini

Sumber: Hasil olahan peneliti dari berbagai sumber (2018)

Oleh karena itu, sebagai aplikasi yang menjadi lalu lintas dari ribuan informasi setiap harinya, sistem keamanan informasi dari aplikasi Inaportnet harus menjadi prioritas. Hal ini dikarenakan ancaman *cyber* yang

semakin berkembang dalam dunia digital dan aplikasi Inaportnet merupakan sebuah aplikasi dalam bentuk digital yang mempunyai kemungkinan besar terhadap ancaman *cyber*. Jangan sampai kejadian penyelundupan narkoba dalam jumlah banyak yang terjadi di pelabuhan Antwerp Belgia[12] terjadi di Indonesia, karena aplikasi yang dibajak oleh *attacker* pada kasus tersebut merupakan aplikasi yang fungsinya mirip dengan Inaportnet.

1.2 Fokus dan Subfokus Penelitian

Fokus penelitian ini adalah implementasi sistem pengamanan informasi dalam aplikasi Inaportnet. Agar penelitian ini lebih terarah sesuai dengan fokus penelitian di atas, maka sub fokus penelitian yang digunakan meliputi:

1. Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet dari ancaman dan serangan *cyber.*
2. Aspek pendukung dan penghambat dalam sistem pengamanan informasi yang terdapat dalam aplikasi Inapornet.

1.3 Rumusan Masalah

Berdasarkan uraian permasalahan yang ada di latar belakang maka peneliti merumuskan masalah sebagai berikut **“Bagaimana penerapan sistem pengamanan informasi aplikasi Inaportnet dalam mendukung *Maritime Cyber Security?”*.** Dengan pertanyaan penelitian yang dapat diturunkan adalah sebagai berikut:

1. Bagaimana Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet dari ancaman dan serangan *cyber*?
2. Bagaimana aspek pendukung dan penghambat dalam sistem pengamanan informasi yang terdapat dalam aplikasi Inaportnet?

[12] Lihat Tabel 1.4 Kasus-kasus cyber yang terjadi dalam domain maritim

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui implementasi sistem pengamanan informasi dalam aplikasi Inaportnet untuk *Maritime Cyber Security*. Secara khusus tujuan penelitian ini ialah sebagai berikut:

1. Menganalisis mekanisme sistem pengamanan informasi dalam aplikasi Inaportnet untuk *Maritime Cyber Security*.
2. Menganalisis aspek pendukung dan penghambat dalam sistem pengamanan informasi untuk melindungi informasi dari ancaman *cyber* dalam aplikasi Inaportnet.

1.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dari penelitian ini dibagi menjadi dua yaitu manfaat teoritik dan manfaat praktis. Berikut adalah penjelasannya:

1.5.1 Manfaat Teoritik

Secara teoritik penelitian ini diharapkan dapat memberikan manfaat antara lain dapat berkontribusi dalam pengembangan ilmu studi keamanan maritim, terutama dalam domain *maritime cyber* yang ditinjau dari berbagai teori dan konsep yang juga dikembangkan sehingga dapat mendapatkan konsep baru mengenai keamanan maritim dalam domain *cyber*.

1.5.2 Manfaat Praktis

Secara praktis, penelitian ini diharapkan dapat memberikan manfaat praktis kepada kementerian/lembaga dan pihak terkait lainnya tentang pentingnya sistem pengamanan informasi dalam menjaga portal-portal elektronik yang digunakan dalam operasional dalam masing-masing kementerian/lembaga. Serta diharapkan hasil penelitian ini juga dapat memberikan rekomendasi tentang sistem pengamanan informasi yang dimulai dari Direktorat Jenderal Perhubungan Laut sebagai pengelola dari aplikasi Inaportnet yang kemudian akan meluas kepada seluruh kementerian/lembaga yang mempunyai portal-portal elektronik.

BAB II
KAJIAN TEORITIK

2.1 Deskripsi Konseptual

Pada penelitian ini digunakan beberapa teori dan konsep yang mendukung penelitian secara mendalam. Teori dan konsep yang digunakan adalah Teori Implementasi, Teori Keamanan Nasional, Konsep Keamanan Maritim, Teori *Cyber Security*, Teori Keamanan Informasi, Peraturan Menteri Perhubungan Nomor 192 Tahun 2015 pengganti PM Nomor 157 Tahun 2015 tentang penerapan Inaportnet untuk pelayanan kapal dan barang di pelabuhan. Berikut adalah penjelasannya:

2.1.1 Teori Implementasi

Implementasi mempunyai pengertian yaitu pelaksanaan atau penerapan.[13] Implementasi pengamanan *Internet of Things* (IoT) merupakan penerapan jaringan yang melibatkan sistem komunikasi dari berbagai jenis, mulai dari *people to people, people to things*, hingga *things to things*. Sistem dan perangkat dari IoT mudah diserang oleh musuh, oleh sebab itu implementasi pengamanan sistem dan jaringan komunikasi dari segala bentuk serangan merupakan bagian penting dari keamanan informasi saat ini. Implementasi keamanan untuk IoT dapat berupa desain algoritma kriptografi dan bentuk pengamanan terhadap serangan fisik. Aplikasi kriptografi digunakan untuk perlindungan jalur komunikasi. Namun, terkadang penyerang juga mempunyai akses fisik ke perangkat yang mengeksekusi algoritma kriptografi dan dapat mengukur *side channels* seperti waktu eksekusi, komsumsi daya, dan radiasi elektromagnetik. Pada IoT kriptografi diletakkan pada *side channels*, oleh karena itu perlindungan terhadap serangan pada *side channels* biasanya dilakukan dengan

[13] Menurut Kamus Besar Bahasa Indonesia, 2016

masking berdasarkan *Multi-Party Computation*.[14] Selain itu, implementasi perlindungan terhadap jaringan komunikasi juga dapat dilakukan dengan melakukan sertifikasi keamanan dengan evaluasi dan pengujian independen. Contohnya seperti standar dari *The Federal Information Processing Standar* (FIPS) yang merupakan standar keamanan komputer milik Pemerintah Amerika Serikat yang digunakan untuk persetujuan modul kriptorgrafi.[15]

Untuk mengamankan jaringan internet yang terkoneksi dengan jalur komunikasi, maka implementasi dari bentuk pengamanan dapat berupa *coding theory* dan kriptografi. [16] Ketika mengirim sebuah pesan, selalu ada gangguan kecil yang kemungkinan terjadi saat proses transmisi. Tujuan dari *coding theory* adalah untuk mengembangkan kode yang bagus untuk mendeteksi dan mengoreksi kejadian *error* saat transmisi data dilakukan. Sedangkan kriptografi digunakan untuk melindungi data rahasia ketika proses pembagian atau transmisi dilakukan. Dapat diilustrasikan seperti brankas yang membutuhkan beberapa kunci untuk membukanya.

Implementasi keamanan informasi membutuhkan beberapa komponen seperti Keamanan Fisik dan Lingkungan, Keamanan Sumber Daya Manusia, Kebijakan Keamanan, Kontrol Akses, Manajemen Aset, Manajemen Komunikasi dan Operasi, Pengaturan tentang Keamanan Informasi, Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi, dan Penilaian Resiko dan Perawatan. Komponen-komponen ini mempunyai kriteria masing-masing, yaitu (1) Keamanan Fisik dan Lingkungan kriteria yang termasuk dalam komponen ini adalah skema pengaturan apabila terjadi *force majure* seperti kebakaran, huru-hara, dan bencana alam, standar untuk redundant dan backup system termasuk disaster recovery

---

[14] Kwok T. Fung, Network Security Technologies: Second edition, (New York: Auerbach Publication, A CRC Press Company, 2005), hlm. 50.
[15] Begul Bilgin, Svetla Nikova, dan Vincent RIjmen, Theory of Implementation Security (TIs 2016)', *Proceedings of the 2016 ACM SIGCAC Conference on Computer and Communications Security*, 2016, hlm. 187.
[16] A.Klein dan L. Storme, *Application of finite geopmetry in coding theory and cryptography*, (Amsterdam: IOS Press, 2011), hlm.42.

system, *Network Operating System* (NOC), aturan tentang *cable managing*, server, router dan lain-lain, aturan akses kontrol ke ruang server, fasilitas penunjang seperti CCTV, alat pemadam kebakaran, alat pendeteksi gerakan, alat deteksi asap, pendeteksi audio video, serta aturan pembatasan penggunaan audio video termasuk kamera, handphone, dan perangkat elektronik portable lainnya. Yang ke (2) adalah Keamanan Sumber Daya Manusia kriteria yang termasuk didalamnya adalah aturan tentang batasan tanggung jawab, situasi dan kondisi setiap tingkatan pegawai, aturan baku tentang pengaturan hak akses untuk setiap tingkatan pegawai, kebijakan untuk pegawai yang membuat masalah, serta pengaturan *password* untuk *personal computer*. Komponen ke (3) Kebijakan Keamanan yang termasuk kriteria didalamnya adalah standar yang diterapkan khususnya untuk melindungi dokumen seperti kebijakan mobile computer, kebijakan *firewall*, kebijakan penggunaan internet, kebijakan penggunaan *password*, serta kebijakan mengenai keamanan untuk teknis. Komponen ke (4) Kontrol Akses kriteria yang termasuk didalamnya adalah aturan akses untuk masuk ke sistem, aturan tentang format penolakan, persetujuan, dan administrasi untuk permintaan data, *registrasi user*, aturan mengganti *password* secara berkala yang terdokumentasikan, hak akses untuk akun baru, *root security*, serta penggunaan algoritma yang benar. Komponen ke (5) Manajemen Aset yang termasuk kriteria didalamnya adalah dokumentasi tentang *data base*, kerjasama/kontrak, serta *user manual*, pendataan seluruh perangkat keras seperti komputer, peralatan komunikasi, media penyimpanan, sistem *back up*, serta perangkat lunak, *data base*, serta *tools* yang digunakan. Komponen ke (6) Manajemen Komunikasi dan Operasi yang termasuk kriteri didalamnya adalah prosedur operasional dan tanggung jawab, manajemen layanan untuk pihak ketiga, perlindungan terhadap kode berbahaya serta ponsel, manajemen keamanan jaringan, serta *monitoring*. Komponen ke (7) Pengaturan tentang Keamanan Informasi kriterianya adalah kebijakan tentang pendefinisian informasi yang masuk dan keluar,

aturan tentang analisa yang secara periodik dilakukan untuk sistem yang dibuat, aturan hak akses, serta penilaian resiko yang terjadi sebagai resiko akan koneksi yang dilakukan. Komponen ke (8) Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi, kriterinya adalah aturan untuk data input dan output, aturan tentang re-cek dan manual untuk verifikasi dan *cross checking*, aturan tentang tanggung jawab dan proses dalam merespon/mendeteksi adanya *error/trouble*, menggunakan metode enkripsi kriptografi untuk menjamin keamanan, serta membuat prosedur implementasi untuk mengontrol instalasi *software*. Komponen ke (9) Penilaian Resiko dan Perawatan, kriterianya adalah penilaian resiko keamanan, dan perawatan serta pengamanan resiko keamanan. [17]

Implementasi untuk keamanan informasi dapat dirangkum menjadi keamanan fisik, keamanan personal, keamanan operasional, keamanan komunikasi, dan keamanan jaringan. Implementasi untuk keamanan informasi ini dijadikan tolak ukur untuk sistem keamanan informasi yang diterapkan dalam aplikasi Inapornet. Implementasi sistem keamanan informasi ini digunakan sebagai pencegahan untuk masuknya ancaman yang kemungkinan dapat terjadi dalam aplikasi Inaportnet.

Inaportnet merupakan sistem pelayanan tunggal secara elektronik yang berbasis web/internet yang berfungsi untuk mengintegrasikan sistem informasi kepelabuhanan yang standar dalam melayani barang dan kapal secara fisik dari seluruh instansi serta pemangku kepentingan di pelabuhan.[18] Inapornet diselenggarakan oleh Kementerian Perhubungan dan pelaksanaanya dilakukan oleh Direktorat Jenderal Perhubungan Laut. Pelayanan dalam sistem Inaportnet meliputi kapal pindah, kapal masuk, kapal keluar, pembatalan pelayanan dan perpanjangan tambat.[19]

---

[17] Timothy P. Layton, *Informaton Security: Design, Implementation, Measurement, and Compliance*, (Florida: Auerbach Publications, Taylor & Francis Group, 2007), hlm.55.
[18] Peraturan Menteri Perhubungan Nomor 192 Tahun 2015 tentang perubahan atas PM Nomor 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan, Pasal 1, ayat (1)
[19] *Ibid*, Pasal 2, ayat (2), dan (3)

Pelayanan kapal dan barang dalam Inaportnet terintegrasi dengan sistem *Indonesia National Single Window* (INSW).[20] *Indonesia National Single Window* (INSW) merupakan istilah yang sudah dikenal dalam perdagangan internasional. INSW membantu proses perdagangan di Indonesia menjadi *National Single Window*. Hal ini dilakukan agar proses *trading* di Indonesia dapat dipantau dan dimonitor oleh pihak-pihak yang berkepentingan. Setiap percepatan proses administrasi dan fisik barang dipengaruhi oleh adanya faktor kebijakan pemerintah dan faktor operasional. Dalam kasus perijinan untuk impor, sekitar 18 kementerian/lembaga yang harus dilewati, dimana masing-masing kementerian/lembaga mengeluarkan perizinan sesuai dengan kewenangannya. Dari kasus inilah permasalahan tingginya angka *dwelling time* dalam tahap *pre-clearance*.[21]

2.1.2 Teori Keamanan Nasional

Isu-isu tentang pertahanan, keamanan dan keselamatan telah dijadikan subjek studi oleh banyak ilmuwan dari berbagai bidang. Hal ini berlaku juga terhadap pertahanan, di mana setiap anggaran dalam sebuah komunitas digunakan untuk meningkatkan keamanan personal dan anggota. Saat ini, manusia hidup ketika isu damai dan perang menjadi bagian yang tak terpisahkan dari permasalahan territorial, suku dan ras, agama serta kebangsaan. Salah satu bentuk sikap pertahanan adalah pengembangan dari pengalaman dan *trend* di negara lain, dan menghargai elemen-elemen yang berlaku secara universal dan general dalam perspektif internasional termasuk juga salah satu sikap dalam pertahanan.[22]

---

[20] *Ibid*, Pasal 4

[21] Johanes Ronaldy Polla, "INSW (Indonesia National Single Window)" ,2017,Binus University, dalam http://bbs.binus.ac.id/ibm/2017/06/insw-indonesia-national-single-window/, diakses pada 24 Juli 2018.

[22] Elinor C. Sloan, *Modern Military Strategy: An Introduction*, (London: Routledge,2012), hlm. 66.

Keamanan nasional modern tidak hanya tertuju pada segi militer saja, namun keamanan nasional pada era modern saat ini memiliki bentuk yang lebih global. Banyak negara yang menerapkan sistem keamanan nasional sesuai dengan perkembangan lingkungan strategis dan perkembangan ancaman yang terjadi di negaranya. Keamanan nasional dapat meliputi keselamatan dan keamanan suatu negara, melalui berbagai aspek seperti aspek militer, ekonomi, diplomasi, keamanan energi, lingkungan dan lain sebagainya. Begitupun dengan ancaman keamanan yang semula berorientasi pada ancaman tradisional, saat ini telah beralih menjadi ancaman yang lebih multidimensi.[23] Gagasan tentang keamanan nasional termasuk salah satu gagasan baru. Keamanan Nasional sering mengacu pada negara merdeka yang berusaha melindungi integritas dan wilayah teritorialnya. Definisi keamanan nasional dapat seringkali dikaitkan dengan kemampuan suatu negara dalam melindungi negaranya dari ancaman yang datang dari luar. Keamanan nasional sendiri merupakan keamanan suatu negara, keamanan nasional dan integritas keamanannya serta kedaulatannya.[24]

Keamanan nasional dapat diartikan sebagai kondisi ataupun sebagai fungsi. Sebagai kondisi, keamanan merupakan kebutuhan dasar manusia disamping dari kesejahteraan. Sebagai fungsi, keamanan nasional akan menciptakan rasa aman dalam pengertian luas yang didalamnya terdapat rasa nyaman, tenteram, damai dan tertib. Sedangkan negara lain yang telah mempunyai keamanan nasional di negaranya adalah Amerika Serikat, Rusia, Australia, Georgia, dan Azerbaijan.[25]

Keamanan nasional pada abad 21 ini telah berkembang. Semula inti persoalan dari keamanan nasional adalah cara menghadapi ancaman yang normalnya dibahas dari aspek kemiliteran. Akan tetapi, semakin berkembangnya dunia ini, maka karakter ancaman dari semi atau non-

[23] Bambang, *op cit*., Hlm.2
[24] Natasha Grozdanoska, “National Defence and Security”, *European Scientific Journal*, Volume.1, 2014, ISSN-1857-7431
[25] Bambang, op cit, hlm. 14-18.

militer juga semakin berkembang. Oleh karena itu, negara harus menghadapi dan bertahan dari ancaman yang semakin berkembang. Perkembangan ancaman pada dua abad terakhir juga memaksa penerapan persyaratan strategi yang semakin kompleks. Dibandingkan dengan era sebelumnya, di mana pengoperasian strategi diterapkan dalam 4 (empat) lingkungan yang berbeda yaitu laut, darat, udara dan luar angkasa. Saat ini, para ahli strategi memulai potensi pengoperasian lingkungan yang kelima yang disebut dengan *cyber space*. Di mana-mana data personal, komersial, pemerintah dan komputer militer seluruhnya terhubung dengan *World Wide Web* (WWW). WWW telah berhasil merevolusi komunikasi, sistem keuangan internasional, transaksi komersial, dan perdagangan internasional.[26]

Konsep Kebijakan Keamanan Nasional khusus untuk Teknologi Informasi (*National IT Security Policy*) bahkan telah dibuat dibeberapa negara seperti USA, Kanada, India, dan Australia. Kebijakan Nasional untuk TI digolongkan menjadi 6 bagian yaitu isu cyber security, isu pertahanan militer, isu interoperabilitas, isu sosial budaya, isu ekonomi dan isu struktural. Dalam masing-masing bagian terdapat beberapa isu yang dianggap kritis misalnya dalam isu *cyber security* terdapat 3 isu kritis yang dibahas terkait (1) Permasalahan utama bagi negara yang memutuskan kebijakan keamanan adalah untuk mengatasi masalah kerentanan, (2) Kebijakan mengenai informasi rahasia perlu diberlakukan di semua tingkatan, serta (3) Kemampuan untuk bertindak proaktif dalam mencegah dan percepatan pemulihan dari serangan *cyber* memang sangat penting. Isu pertahanan militer mempunyai 3 isu kritis yang terkait (1) Membangun kerangka kerja untuk berbagi informasi dalam masalah pertahanan, (2) Menciptakan jaringan yang aman untuk pertukaran informasi baik dalam kondisi damai dan perang, (3) Diperlukan niat baik untuk menghindari

[26] Dennis M. Drew, dan Donald M.Snow, Making Twenty First Century Strategy: An Introduction to Modern National Security Processes and Problems, (Alabama: Air University Press, 2006), hlm. 12-13.

tuduhan memata-matai antar negara dan memastikan keberhasilan pengaturan tersebut. Isu Interoperabilitas terdapat 2 isu kritis yang terkait dengan (1) Memastikan interoperabilitas infrastruktur TI dalam mempromosikan pertukaran informasi serta (2) Negara-negara maju harus memimpin dalam standarisasi infrastruktur informasi dasar yang memungkinkan negara lain untuk bekerja sama dengan lebih baik. Sedangkan untuk isu sosial budaya juga terdapat 2 isu kritis yang terkait dengan (1) Kebijakan TI harus didasarkan pada pemahaman yang luas tentang perbedaan budaya dan sosial antar negara, serta (2) Kebijakan TI harus fleksibel untuk mengakomodir struktur tata kelola yang berbeda dalam implementasi dalam mencerminkan prioritas budaya dari masing-masing negara.[27]

Keamanan Nasional setiap negara berbeda tergantung dari pada ancaman yang mengancam negara tersebut. Namun perkembangan keamanan nasional jelas membawa dunia kepada era pertahanan dan peperangan digital. Tidak dapat dihindari bahwa perkembangan teknologi membuat seluruh informasi yang ada didunia hanya ada dalam genggaman, aksesnya pun mudah baik melaui *surface web*, maupun untuk penikmat *deep web*. Potensi *cyberspace* untuk menjadi lingkungan pengoperasian kelima sangatlah mungkin, mengingat banyak kendali kontrol dari senjata pemusnah massal juga memanfaatkan teknologi yang rentan terhadap ancaman *cyber*. Oleh karena itu, sistem pengamanan perlu diperkuat agar sistem *cyber* tidak mudah dimasuki oleh penyerang.

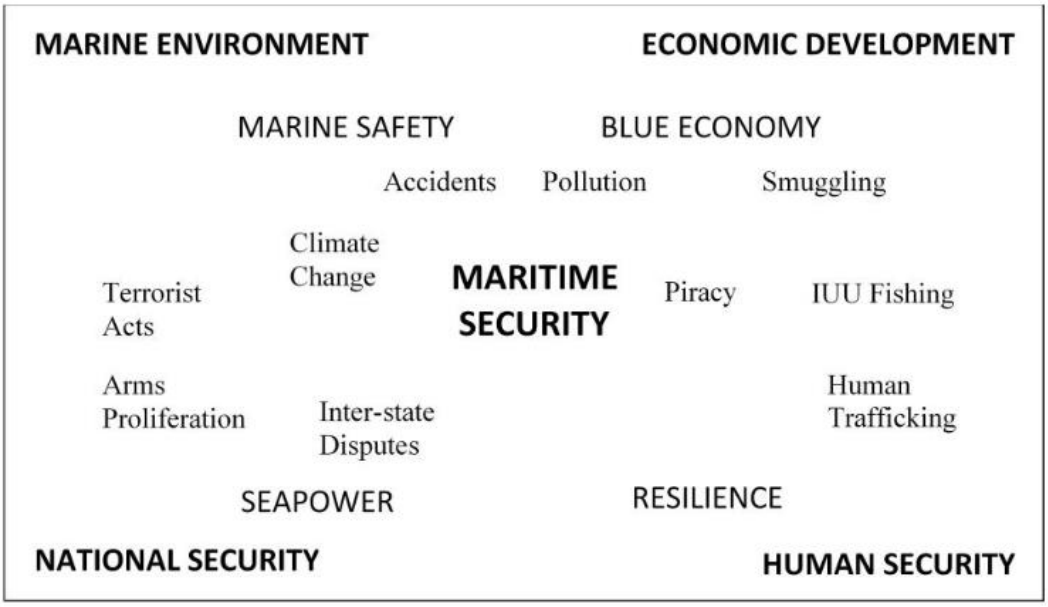
2.1.3 Konsep Keamanan Maritim

Keamanan maritim merupakan sebuah kata kunci yang akhir-akhir ini sering menjadi perhatian di dunia internasional. Aktor utama dalam keamanan maritim seperti kebijakan maritim, *ocean governance*, dan

[27] Karthik Venkataraman, H. Raghaw Rao, dan David Dewitt, National Information Technology (IT) Security Policies: An Overview of Issues, (Amsterdam: Elsevier,2007), hlm.41-45

keamanan internasional dalam dekade terakhir telah memasukkan keamanan maritim dalam mandat atau pekerjaan mereka. Konsep keamanan maritim lahir ketika ancaman perompakan di laut Somalia semakin marak terjadi pada tahun 2008 hingga 2011. Bahaya dari perompakan untuk perdagangan internasional membawa dimensi keamanan maritim kepada kesadaran global dan menempatkan keamanan maritim dalam agenda kebijakan yang diprioritaskan. Perbincangan mengenai keamanan maritim yang ada, secara berkala mengacu pada 'ancaman' yang terjadi pada domain maritim. Ancaman-ancaman tersebut diantaranya perbatasan maritim, *maritime terrorism*, perompakan, penyelundupan dan perdagangan narkoba, penyelundupan manusia dan barang, *illegal fishing*, kecelakaan laut dan bencana. Namun, masih banyak perdebatan hingga sekarang mengenai apakah climate change dan bencana termasuk dalam isu-isu keamanan maritim atau bukan, kemudian apakah masalah perbatasan laut dimasukan ke dalam keamanan nasional atau keamanan maritim. Matriks dibawah ini merupakan matriks dari keamanan maritim berdasarkan ancaman yang terjadi di domain maritim.[28]

[28] Christian, *op.cit.,* hlm. 160.



Gambar 2.1 *Maritime Security Matrix*

Sumber: Christian Bueger, “What is Maritime Security?”, 2015

Letak *maritime cyber security* dalam matrik diatas dapat terletak diseluruh aspek keamanan maritim. Mulai dari bidang *marine environtment, economic development, national security,* dan *human security*. Domain cyber dapat masuk di seluruh aspek keamanan maritim karena hampir seluruh aspek keamanan maritim diatas telah menggunakan sistem informasi dan komunikasi berbasis internet. Selain itu, beberapa kementerian/lembaga yang berperan dalam keamanan maritim telah menggunakan portal elektronik yang berbasis internet dalam pengoperasiannya.

Pembagian keamanan dapat dilihat dari tingkat dari analisisnya, dimensinya, serta konsep keamanannya. Pada tingkat analisisnya terdapat keamanan individu, keamanan nasional, dan keamanan internasional. Sedangkan menurut dimensinya terdapat keamanan sosial, keamanan ekonomi, dan keamanan lingkungan. Untuk konsep keamanan terdiri dari keamanan umum/publik, keamanan kolektif/grup, keamanan komprehensif, dan keamanan kooperatif. Kata-kata keamanan maritim dapat mempunyai

arti yang berbeda, tergantung dari orang dan organisasinya, tergantung jug dari kepentingan organisasi tersebut, atau terkadang bias secara politik dan secara ideologi[29]. Geoffrey Till[30], mengungkapkan analisisnya dengan sebuah konsep “good order at sea”, di mana laut merupakan sebuah sumber daya yang digunakan sebagai media untuk perdagangan dan pertukaran informasi, dan sebagai sebuah lingkungan. Laut menghadapi resiko dan ancaman terhadap sebuah tatanan di mana kontribusi yang berkelanjutan terhadap pembangunan manusia bergantung.

2.1.4 Teori *Cyber Security*

Cyber Security didefinisikan sebagai rentang proses teknologi informasi yang dimaksudkan untuk melindungi data yang dikirimkan melalui internet, dan untuk memerangi ancaman pemasangan program malware.[31] Cyber Security digunakan untuk melindungi dunia maya yang dipahami sebagai dunia elektronik dimana informasi, perangkat lunak dan orang-orang berbagi dan mentransferkannya ke dunia nyata. [32] Serangan terhadap infrastruktur penting telah menjadi kunci yang telah lama digunakan dalam suatu peperangan. Jaringan transportasi dan sistem komunikasi juga telah lama menjadi target serangan dan juga termasuk serangan secara fisik terhadap titik-titik penting, seperti jembatan dan persimpangan kereta api atau peperangan elektronik yang mencoba men-*jam* atau mengganggu sistem komunikasi. Saat ini, di negara maju jaringan listrik dan transportasi modern bergantung pada sistem komputer untuk pengoperasiannya. Inovasi ini membuat sebuah sistem listrik dan transportasi menjadi sebuah sistem yang lebih efisien selama jaringan ini berjalan sesuai dengan fungsinya. Namun kerusakan yang ditimbulkan

---

[29] Chris Rahman, Concepts of Maritime Security, (New Zealand: The Centre for Strategic Studies,2009), hlm.29.
[30] Geoffrey Till, *Sea Power*,(New York : Routledge,2015), hlm.5.
[31] IMO, ‘Interim Guidelines on Maritime Cyber Risk Management: IMO-MSC1/CICC 1526,2016.
[32] Jenna Ahokas, *Op cit.,* hlm. 9

ketika sistem ini mengalami *error* sangatlah fatal. Penggunaan sistem komputer pada operasional jaringan listrik dan transportasi juga berpotensi menyebabkan sebuah *cyber sabotage* yang akan membahayakan seluruh sistem.[33]

Dunia *cyber* mempengaruhi dan berinteraksi dengan semua domain, dan *cyber* dapat bermain sebagai pemeran utama dalam sebuah operasi militer. Komunikasi *cyber* merupakan satu-satunya cara untuk berkomunikasi dengan satelit di ruang angkasa. *Cyber* juga dapat mengontrol aset-aset yang berada di daerah terrestrial dan aset-aset angkatan laut yang ada dilapangan. *Cyber* juga dapat digunakan untuk mengubah rute pesawat udara baik yang diterbangkan manusia atau oleh mesin. Pertanyaan sebenarnya bukan kepada kegunaan dari kekuatan *cyber*, namun lebih kepada kemampuan domain untuk secara independen dapat mempengaruhi konflik antar negara. Apakah kekuatan *cyber* berkembang sangat pesat dapat memungkinkan untuk menimbulkan peperangan terjadi seluruhnya dalam dunia *cyber*? Di banyak negara, terdapat banyak perpindahan untuk membuat pasukan *cyber* terpisah dari domain tradisionalnya. Contohnya di Amerika Serikat yang membuat US *Cyber Command* yang menyatukan unit cyber dari masing-masing dinas militer menjadi satu kesatuan. US *Cyber Command* dibawah control dari Kementerian Pertahanan Amerika, US *Cyber Command* juga termasuk dalam *National Security Agency* (NSA). NSA telah mengembangkan reputasi sebagai lembaga *cyber* tekemuka di Amerika yang mampu menawarkan bantuan signifikan dalam mengamankan jaringan militer dan pemerintah, yang juga berpotensi untuk meluncurkan operasi serangan *cyber*.[34]

Persyaratan keamanan cyber dalam domain maritime telah diadopsi oleh *International Maritime Organization* (IMO). Komunitas maritim belum

---

[33] Paul J.Springer, *Cyber Warfare: a reference handbook*, (USA : ABC-CLIO, LLC 2013), hal. 33
[34] *Ibid*, hal. 60.

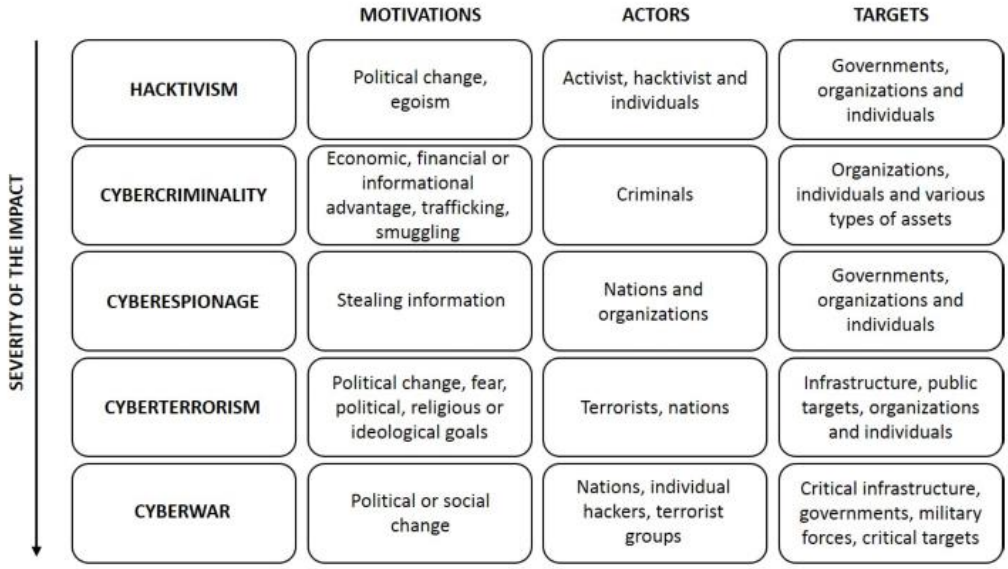
menetapkan definisi secara global untuk *Maritime Cyber Security*. Namun jika diturunkan dari pengertian *cyber security* maka *maritime cyber security* dapat diartikan sebagai suatu tindakan ukuran yang diambil untuk melindungi aset jaringan dan komputer baik di kapal, terminal, pelabuhan, dan semua peralatan yang terkomputerisasi guna mendukung operasi maritim.[35]

Maritime Cyber Security merupakan bagian dari *Cyber Security* yang membahas mengenai kemanan siber dalam domain maritim. *Cyber Security* merupakan teknologi, proses, dan praktek yang dibuat untuk melindungi komputer, jaringan, data dan program dari serangan, kerusakan, atau akses secara illegal. *Cyber Security* digunakan mengacu pada alat teknologi dan fungsi bisnis yang digunakan untuk melindungi aset informasi. Data milik perusahaan atau pemerintah yang saat ini telah beralih menjadi data digital merupakan data yang diincar oleh para *hacker* atau penyerang. Melindungi informasi dan data tersebut sudah bukan menjadi prioritas, namun sudah menjadi kebutuhan dari sebagian besar perusahaan dan instansi pemerintah di seluruh dunia. [36]

Beberapa ancaman dalam *cyber security* adalah *cyber crime, cyber espionage,* dan *cyberterrorism*. Ketiga aspek ancaman ini merupakan sebuah fenonema aspek modern yang terjadi di masyarakat. Tidak ada satupun aktivitas diatas yang termasuk dalam suatu tindakan perang yang nyata. Dalam domain *cyber* jauh lebih mudah untuk salah menafsirkan satu tindakan dengan tindakan lain. Namun, selama perang *cyber* aktivitas-aktivitas ini akan berguna menjadi layanan kepada negara dan merupakan sumber daya nasional utama dalam konflik yang terjadi dalam domain *cyber*.[37]

---

[35] Christopher R. Hayes, “Maritime Cyber Security: the future of national security”, *Tesis Magister*, (California: Homeland Security and Defense, Naval Postgraduate School 2016), hlm.6.
[36] Lawrence C. Miller, Cybersecurity for Dummies, Palo Alto Networks Edition, (New Jersey, 2014), hlm. 11.
[37] Paul, *op.cit.,* hlm. 80.



Gambar 2.2 Ancaman dalam *cyber security*

Sumber: Jenna Ahokas dan Tuomas Kiiski, ”Cyber security in Ports”, Publication of the Hazard Project, Vol.3, 2017, hlm. 14.

Cyber crime atau *cyber criminals* mempunyai motivasi yang sama dengan kriminal yang ada pada dunia nyata yaitu hal-hal yang bersifat finansial atau materi. Perbedaannya pelaku kriminal pada domain *cyber* menggunakan komputer dan jaringan dalam melakukan aksinya. Kerugian yang diakibatkan dari aksi ini bisa jauh lebih besar dibandingkan dengan perampokan bank di dunia nyata. Hal ini karena bank telah mempunyai banyak pengalaman tentang perampokan yang terjadi nyata dalam lingkungan mereka. Sedangkan dalam *cyber crime* selain domain yang lebih kompleks dan transfer uang secara digital lebih mudah jika dibanding dengan melakukannya secara tunai. Sangat beresiko jika melakukan transfer dalam jumlah besar ke dalam satu akun bank, lebih mudah jika hanya mengambil sejumlah uang dari jutaan korban dan inilah yang dilakukan oleh *cyber criminals*. Selain itu, pelaku dalam domain *cyber* sulit untuk terdeteksi. *Cyber crime* tidak terbatas pada perampokan pada dunia maya saja, pencurian data kartu kredit dan penipuan kartu kredit, pencurian

data, pembobolan sistem keamanan dan lain sebagainya juga termasuk *cyber crime*.[38]

Sama seperti pada *cyber crime, cyber espionage* merupakan praktek yang telah dari dulu dilakukan hanya saja diadopsi kedalam teknologi yang baru. Pada abad ke-20, kegiatan spionase membutuhkan waktu bulanan hingga tahunan untuk mendapatkan beberapa file kunci. Namun, pada abad ke-21 ini hanya dibutuhkan waktu beberapa menit untuk mendapatkan file kunci (jika file tersebut tidak diamankan dengan tepat). Negara-negara selalu terlibat dalam spionase terhadap negara lain, dan bahkan sekutu mereka telah menjadi target potensial. Kegiatan spionase telah memasukkan upaya untuk menentukan keputusan masa depan seorang pemimpin politik dan mendapatkan informasi yang memalukan tentang para pemimpin yang mungkin digunakan untuk mempengaruhi keputusan tersebut. Mereka juga telah memasukkan upaya untuk mencuri data teknis tentang sistem persenjataan, informasi tentang pertahanan nasional, dan lokasi aset militer, dan pada waktu kejadian untuk mendapatkan contoh perangkat keras militer yang mungkin dibawa keluar dari negara dan disalin.[39]

Cyberterrorism telah menjadi salah satu dari ancaman yang paling banyak dibahas pada abad ke 21 ini. Hal ini karena sekelompok orang yang menggunakan aset *cyber* untuk melakukan serangan terror dengan cara yang sangat lihai dalam memanipulasi outlet media, dan sasarannya yang tidak mengerti tentang *cyber domain* sehingga mudah terjerumus dalam ajaran-ajaran yang tidak benar. Kemampuan cyber tentu menawarkan prospek dalam penyebaran ketakutan pada populasi target yang sangat besar, dan komputer menjadi alat komunikasi yang digunakan untuk menimbulkan kekerasan. Teroris memanfaatkan media sosial untuk menyebarkan pesan-pesan, menghimpun anggota, dan mempengaruhi

[38] Paul, *loc.cit*.
[39] Paul, op.cit., hlm.84.

target dengan ajaran-ajaran mereka.[40] Hal ini seperti yang disampaikan oleh juru bicara dari Badan Siber dan Sandi Negara, Anton Setiawan ketika menjadi pembicara pada seminar IIDSS 2018, bahwa ketika teroris sudah memahami lebih jauh tentang domain cyber, maka mereka tidak butuh senjata untuk menghancurkan dunia. Hanya membutuhkan sebuah laptop, dan para ahli dibidang *cyber* (*hacker*). Bahkan saat ini teroris sudah merambah dunia *game online* sebagai sarana berkomunikasi, padahal game online biasanya digunakan oleh anak-anak dari seluruh dunia. Beberapa *game online* yang diduga menjadi sarana komunikasi oleh kelompok terror diantaranya adalah *Clash of Clan, War of World Craft, Brutal Age, Clash of the Titans,* dan lain-lain.[41]

Cyberwar selalu merujuk pada macam-macam serangan terhadap jaringan komputer lawan. *Cyberwar* dapat mempengaruhi masyarakat, organisasi dan individu. *Cyberwar* dapat didefinisikan dalam berbagai makna, beberapa ahli membandingkan *cyberwar* dengan konsep *drug war* dan *war against poverty*. Ada yang mengatakan bahwa bukan *cyberwar* jika tidak menyebabkan kerusakan fisik, atau merupakan *cyberwar* ketika dapat menyebabkan konfrontasi fisik antar negara. Namun, pada dasarnya *cyberwar* digunakan untuk mengganggu, contohnya mengganggu sistem transport sehingga pelabuhan tidak dapat beroperasi secara maksimal.[42] *Cyberwar* itu nyata, *cyberwa*r dapat menyebabkan sebuah negara yang mempunyai kekuatan *cyber* untuk melakukan *cyber war* dan menhancurkan sebuah negara modern. *Cyberwar* terjadi seperti kecepatan cahaya, ini artinya serangan ketika diluncurkan dan efeknya hampir tidak bisa diukur, hal ini sangat beresiko terhadap pengambilan keputusan. *Cyberwar* bersifat global, dalam banyak konflik serangan *cyber* dengan cepat menyebar secara global karena hanya membutuhkan komputer dan server untuk

---

[40] Paul, *op.cit*., hlm. 88.
[41] Anton Setiawan, "Technology Utilization to Uncover Terrorist Networks in Indonesia and Regionally", pada seminar IIDSS 2018 di Hotel Grand Mercure Kemayoran, tanggal 13 Juli 2018.
[42] Jenna, *op.cit*, hlm. 18.

menyebarkannya. *Cyberwar* juga tidak membutuhkan medan perang, sistem mulai dari bank hingga radar pertahanan udara, merupakan media-media yang termasuk dalam *cyberspace* dan dapat menyingkirkan negara tanpa harus mengalahakan kekuatan tradisional negara tersebut. *Cyberwar* baru dimulai, untuk antisipasi serangan *cyber* beberapa negara telah mempersiapkan mulai dari sumber daya manusia hingga peralatannya untuk bertahan dan menyerang dalam domain *cyber.*[43]

Ancaman dalam *maritime cyber* dapat masuk dari ketiga aktivitas yaitu *cyber crime, cyber espionage*, dan *cyber terrorism*. Hanya saja konteks dari tempat, lokasi, media yang digunakan berhubungan dengan domain maritim. Misalnya, pembajakan hingga pencurian data jaringan komunikasi di kapal, dan pelabuhan, pencurian data penelitian laut, pencurian data survei pemetaan batimetri dan lain sebagainya. Serangan *cyber* pada domain maritim terjadi secara berkala. Jauh dari yang komunitas maritim percayai karena jumlah serangannya tidak dilaporkan dan tidak terdeteksi.[44] Serangan *cyber* dalam domain maritim dapat diartikan sebagai upaya untuk merusak, mengganggu, atau mendapatkan akses secara tidak sah ke sistem komputer atau elektronik jaringan komunikasi. Serangan *cyber* yang terjadi berhubungan dengan aset komputer di kapal, terminal, pelabuhan dan semua peralatan terkomputerisasi yang mendukung operasi maritim.[45]

Ancaman *cyber* dapat diminimalisir atau dapat dicegah dengan *cyber security* yang maksimal. *Cyber security* terbagi atas *cyber security* secara sistem baik *software* maupun *hardware*, dan *cyber security awareness* yaitu *cyber security* yang lebih menitik beratkan kepada operator atau orang yang menjalankan *cyber security* secara sistem. Orang-orang yang berada dalam organisasi dapat memiliki peran kunci untuk menciptakan suasana strategi *cyber security* yang efektif dengan

---

[43] Richard A. Clarke dan Robert K. Knake*, Cyber war: the next threat to national security and what to do about it*, (USA: ECCO Harper Collin Publishers 2012, hlm 30-31.
[44] Christopher, *op.cit*., hlm 2.
[45] Christopher, *loc.cit*

menggunakan kebijakan dan prosedur untuk menghindari serangan yang paling mendasar.

Mengurangi resiko yang dibuat oleh manusia bukan hanya tentang meningkatkan peraturan dan pembatasan. Namun sebaliknya, pengembangan budaya keamanan yang efektif akan tergantung pada tingkat kesadaran dan pemahaman akan resiko dunia maya. Serta penanaman nilai-nilai dan perilaku "sadar keamanan" penting untuk dibina dalam organisasi tersebut. Menunjukkan hubungan antara langkah-langkah teknis, perilaku karyawan dan tindakan organisasi baik selama maupun diluar jam kerja dapat meningkatkan lingkungan kerja yang aman. Beberapa pendekatan yang dapat untuk meningkatkan kesadaran cyber security adalah eksplorasi yaitu dengan memutar ulang suatu kejadian, sehingga orang-orang dapat mencapai solusi konstruktif yang disepakati bersama. Kedua yaitu Kesadaran yaitu dengan mengalami sendiri bagaimana suatu situasi dapat berubah, dan para pemangku kepentingan dapat melihat dampak dari kebijakan dan peraturan mereka. Ketiga, Perubahan Perilaku dengan cara mengalami dan merefleksikan suatu situasi, sehingga orang akan sadar terkait perilakunya dan memiliki kesempatan untuk menghadapinya dengan perilaku yang berbeda dan lebih tepat sasaran. Keempat adalah pelatihan dengan mengadakan pelatihan maka orang-orang dapat dengan aman bereksperimen, melakukan kesalahan, dan belajar sekaligus melakukan.[46]

Semakin berkembangnya era *cyber* maka *Cyber security* semakin dibutuhkan. Proses pengalihan data dari data fisik menuju data digital yang lebih praktis, mudah dijangkau dan memiliki kapasitas besar untuk melindungi informasi dari ancaman *cyber* semakin meluas ke banyak lingkungan, hal ini dikarenakan perkembangan teknologi informasi dan komunikasi. Termasuk kedalam lingkungan maritim, banyak kapal telah dilengkapi peralatan canggih dengan menggunakan jaringan internet untuk

---

[46] Anita Chandraker,"*How can you improve cyber security awareness in your organization*?", 2012, dalam https://www.paconsulting.com/insights.

memudahkan pengoperasian dan untuk mengurangi kecelakaan di laut. Di banyak pelabuhan di dunia menggunakan jaringan untuk menampilkan performa pelabuhan yang cepat, efisien, efektif, serta berdaya saing internasional. Dalam penelitian ini, pembahasan mengenai peran *maritime cyber security* diwakili oleh aplikasi Inaportnet, terutama untuk sistem pengamanan informasinya.

2.1.5 Teori Keamanan Informasi

Keamanan informasi merupakan strategi untuk mengelola proses, alat, dan kebijakan yang diperlukan untuk mencegah, mendokumentasikan, mendeteksi, dan melawan ancaman terhadap informasi baik digital maupun non-digital. Keamanan informasi membangun serangkaian jaringan yang akan melindungi aset informasi dimanapun informasi itu berada, baik dalam format, proses, saat transmisi atau sedang berada di penyimpanan. Keamanan informasi bertujuan untuk memastikan bahwa informasi yang sensitive hanya dapat diinformasikan kepada pihak yang berwenang (*confidentiality*), mencegah modifikasi data yang tidak sah (*integrity*), dan menjamin data dapat diakses oleh pihak yang berwenang ketika diminta (*availability*). Keamanan informasi dirancang untuk melindungi *confidentiality, integrity, dan availability* data dalam sistem komputer dari serangan cyber. Ketiga hal ini terkadang disebut sebagai CIA *Triad Information Security*. Sekarang Triad ini telah berevolusi menjadi Parkerian Hexad yang mencakup kerahasiaan, kepemilikan (kontrol), integritas, keaslian, ketersediaan dan utilitas.[47] Ilustrasi tentang aspek keamanan informasi dapat dilihat dalam gambar dibawah ini:

---

[47] Margaret Rouse, “Information Security”, dalam https://searchsecurity.techtarget.com/definition/information-security-infosec, 2018, diakses pada 17 Agustus 2018.

Gambar 2.3 Prinsip dasar Keamanan Informasi

Sumber: Haikal Azaim, "Mengenal Confidentiality, Integrity, dan Availability pada Keamanan Informasi" dalam www.netsec.id.

Dalam *Cyber Security*, keamanan informasi merupakan hal yang sangat penting. Hal ini dikarenakan pada umumnya penyerang mempunyai tujuan yang sama yaitu dapat mengakses informasi, bahkan mengendalikan informasi yang bersifat terbatas dan strategis. Oleh karena itu keamanan informasi mempunyai prinsip dasar yaitu *Confidentiality* (kerahasiaan) di mana informasi yang ada pada sistem/*data base* merupakan hal yang rahasia dan pengguna yang tidak berkepentingan tidak berhak mengaksesnya. Prinsip dasar kedua adalah *Integrity* (integritas) yang mempunyai arti data tidak dapat dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, validitas, dan akurasi data tersebut masih terjaga. Kemudian prinsip dasar keamanan informasi yang terakhir adalah *Availability* (ketersediaan) yang berarti memastikan sumber daya akan selalu siap (*stand by*) dan siap diakses kapanpun dan dimanapun oleh user yang berhak. Faktor-faktor yang mempengaruhi *availability* dapat disebabkan oleh ketersengajaan seseorang/kelompok atau memang karena kecelakaan atau kejadian-kejadian alam seperti gempa bumi, kebakaran, dan lainnya.

Keamanan informasi dulunya murni teknis, namun berkembang seiring waktu untuk mengimbangi perubahan pada komputer dan jaringan. Tujuan keamanan informasi melibatkan penjagaan kerahasiaan, integritas

dan ketersediaan informasi.[48] Beberapa dekade terakhir telah terjadi perubahan persyaratan dalam keamanan informasi. Sebelum penggunaan peralatan pemrosesan data berkembang seperti saat ini, keamanan informasi masih menggunakan sarana fisik dan administratif. Seperti penggunaan lemari arsip dengan kunci kombinasi yang digunakan untuk menyimpan dokumen rahasia/sensitif. Perubahan pertama yaitu sejak diperkenalkannya teknologi komputer membuat kebutuhan akan sebuah alat otomatis untuk melindungi file dan informasi lain yang tersimpan dalam komputer menjadi jelas. Perubahan kedua yang mempengaruhi keamanan informasi adalah penggunaan jaringan dan fasilitas komunikasi untuk transmisi data antar pengguna terminal dan komputer atau antara komputer dengan komputer.[49] Tindakan keamanan jaringan diperlukan untuk melindungi data selama proses transmisi. Jaringan ini saling terhubung satu sama lain mulai dari organisasi bisnis, pemerintah, akademik, kementerian dan lain sebagainya dalam sebuah jaringan yang dinamakan internet.[50]

Dahulu keamanan informasi masih berada dalam fase perlindungan fisik yaitu berupa perlindungan dokumen-dokumen penting yang metode pengamanannya masih menggunakan cara manual seperti lemari besi, brankas, *cryptex*, dan lain-lain. Barulah sejak dikenalkan komputer data-data beralih dari dokumen fisik menuju dokumen digital. Sistem pengamanan informasinya berubah menjadi fokus terhadap pengamanan terhadap komputer itu sendiri. Kemudian dalam perkembangannya teknologi komputer diperbaharui dengan jaringan internet agar proses transmisi data antar organisasi bisa berjalan lebih cepat dan tidak terbatas pada jarak dan waktu. Oleh karenanya sistem pengamanan jaringan juga digunakan agar ketika proses transmisi, gangguan-gangguan dari ancaman *cyber* dapat ditangkal. Pada abad ke-21 ini, keamanan informasi tidak

---

[48] Craig A. Horne, Atif Ahmad, and Sean B. Maynard, *A Theory on Information Security*, (Australia: Australasian Conference on Information Systems, 2016), hlm. 3
[49] William Stallings, *Crytography and Network Security Principles and Practices: Fourth Edition*, (New Jersey: Prentice Hall, 2005), hlm.8.
[50] Ali Ismail Awad, *Introduction to Information Security Foundations and Applications*, (London:The Institution of Engineering and Technology), hlm.3.

hanya informasinya yang diamankan namun didalamnya termasuk juga pengamanan komputer dan jaringan internetnya. Aplikasi ini merupakan aplikasi tempat dimana informasi-informasi antar pemangku kepentingan di pelabuhan terkoneksi satu sama lain. Maka sangat penting untuk memahami sistem pengamanan informasi dalam aplikasi Inaportnet agar ancaman-ancaman *cybe*r dapat ditangkal dan terdeteksi dini.

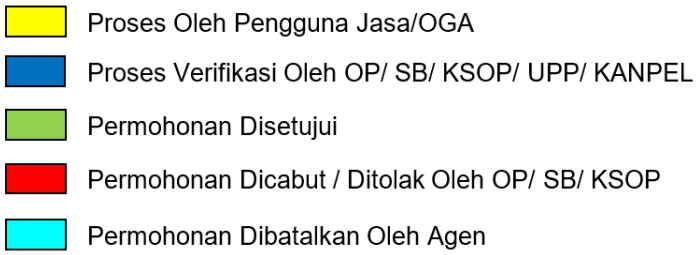
Keamanan informasi saat ini juga termasuk kedalam keamanan nasional modern. Hal ini dikarenakan perkembangan jaman untuk penggunaan teknologi informasi dan komunikasi dalam segala sisi kehidupan. Begitu pula aplikasi Inaportnet yang perlu dijaga keamanannya demi mendukung *maritime cyber security* dan secara tidak langsung juga akan mendukung terwujudnya keamanan nasional dalam ranah modern. Perkembangan era informasi digital telah membawa segala kemudahan baik dalam menjalankan sistem pemerintahan, sistem organisasi, pelayanan hingga kehidupan sehari-hari. Informasi dalam bentuk digital ini telah membantu banyak sektor lini kehidupan berorganisasi maupun personal, namun selain berbuah positif informasi dalam bentuk digital ini juga terbukti sangat rentan keamanannya. Tidak hanya lebih mudah untuk diakses, namun juga menjadi lebih mudah untuk dicuri. Hal ini akan sangat berbahaya terutama untuk informasi-informasi yang bersifat strategis seperti informasi-informasi yang ada didalam aplikasi Inaportnet. Oleh karena itu, keamanan informasi juga menjadi perhatian karena apapun yang berlalu-lalang dalam dunia *cyber* itu adalah informasi dan data.

Seperti yang telah dijelaskan dalam teori Keamanan Nasional Modern oleh Elinor C. Sloan, bahwa keamanan nasional modern mempunyai domain baru selain dari domain laut, udara, darat, dan luar angkasa. Domain tersebut adalah domain *cyber*, di mana perkembangan informasi dan teknologi yang telah mengembangkan domain ini. Begitu juga dengan ancaman dalam keamanan yang pada awalnya hanya bersifat tradisional. Sekarang ancaman lebih bersifat multidimensi akibat dari perkembangan informasi dan teknologi. Hal ini mengartikan bahwa sistem

keamanan informasi akan mendukung keamanan nasional modern dengan cara mengamankan informasi-informasi penting yang berlalu-lalang di dalam *cyber space*.

Inaportnet sebagai aplikasi sistem untuk mengintegrasikan seluruh aplikasi milik para *stakeholder* di pelabuhan merupakan suatu bentuk kemajuan era digital yang telah memasuki domain maritim. Layanan dalam bentuk digital saat ini selain sangat populer, juga sangat membantu proses pelayanan di pelabuhan menjadi lebih cepat, efisien, efektif dan transparan. Dahulu proses pelayanan masih manual dan berjalan sendiri-sendiri, sehingga waktu yang dibutuhkan untuk mengurus administrasi bisa sangat lama. Selain itu, praktek pada jaman dahulu sangat rentan untuk terjadi pungli. Saat ini, dengan bantuan teknologi digital pelayanan dapat dijalankan dengan mudah dan cepat. *User* tidak perlu mengantre lagi di satu persatu loket, cukup mengakses pelayanan administrasi melalui portal Inaportnet dan menginput data-data yang dibutuhkan.

Aplikasi Inaportnet memuat seluruh informasi tentang kapal dan kontainer yang ada di pelabuhan. Mulai dari manifest kapal dan barang hingga pergerakan kapal di dalam pelabuhan, pelacakan pergerakan posisi kontainer, mulai dari proses bongkar muat hingga proses pengiriman. *User* juga dapat mengetahui sejauh mana perkembangan dokumen yang sudah di *submit* ke dalam aplikasi Inaportnet. Apakah permohonannya telah disetujui atau dicabut, atau telah dibatalkan oleh agen. Berikut adalah arti simbol yang digambarkan dengan warna beserta dengan keterangannya:



Gambar 2.4 Status Permohonan Dokumen dari Pengguna Jasa dalam Aplikasi Inaportnet

Sumber: Aplikasi Inaportnet

Informasi yang berlalu-lalang melalui aplikasi Inaportnet begitu banyak dan semuanya penting karena menyangkut data-data administrasi kapal. Seperti data-data muatan kapal, jenis kapal, identitas awak dan nahkoda kapal, surat-surat administrasi untuk kapal, invoice pembayaran, pergerakan kontainer dan lain sebagainya. Apabila data-data tersebut jatuh ke tangan yang tidak bertanggung jawab, maka hal ini dapat menyebabkan kerugian bagi perusahaan pelayaran tersebut, serta membuat kepercayaan *customer* terhadap Inaportnet akan menurun.

2.2 Hasil Penelitian terdahulu

Peneliti menggunakan 3 (tiga) terdahulu yang berkaitan dengan tema besar yang digunakan yaitu *Maritime Cyber Security*. Pertama menggunakan penelitian tesis *Naval Postgraduate School* dari Christopher R.Hayes pada tahun 2016. Hayes membahas mengenai *Maritime Cyber Security* dari segi kebijakan cyber security dengan membandingkan antara lembaga *cyber security* di Amerika Serikat dan Uni Eropa. Kedua, menggunakan jurnal penelitian dari S. de Vleeschhouwer yang merupakan peneliti dari *Netherlands Maritime Technology*. Vleeschhouwer membandingkan beberapa guideline tentang cyber security dan merangkum poin-poin penting untuk *maritime cyber risk management*. Ketiga jurnal penelitian dari Jenna Ahokas dan Tuomas Kiiski pada tahun 2017, yang merupakna peneliti dari University of Turku di Finlandia. Pada penelitian ini, mereka membahas mengenai fenomena-fenomena ancaman *cyber* yang terjadi di pelabuhan. Berdasarkan fenomena-fenomena tersebut maka mereka merumuskan ancaman-ancaman dalam *maritime cyber* yang akan kemungkinan terjadi pada pelabuhan di masa depan. Berikut adalah penjelasan lebih lanjut mengenai ketiga penelitian terdahulu:

Tabel 2.1 Penelitian Terdahulu

No.	Penulis	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi
1.	Christopher R. Hayes (2016) Tesis California: Naval Postgraduate School	*Maritime Cyber Security: the future of national security*	Kualitatif	a. Artikel ini membahas mengenai perbandingan *Maritime Cyber Security* antara Amerika Serikat dengan Uni Eropa; b. Pembahasan meliputi serangan dan kejadian *maritime cyber* terbaru, keamanan nasional *dan maritime cyber warfare*, institusi-institusi yang bertanggung jawab atas *cyber security* di UE maupun AS, dan dalam domain maritimnya; c. Menyarankan di dalam komunitas maritim adanya pelatihan sumber daya manusia untuk menghadapi ancaman *cyber*, pengembangan peralatan teknologi dan prosedur dalam *back up* data, menyarankan pengaturan kebijakan yang standar untuk *maritime cyber security*; d. Menyarankan pendekatan lain dalam meneliti maritime cyber security	Relevansi penelitian ini adalah domain yang dibahas sangat menekankan pada *Maritime Cyber Security*, serta penjelasan *Maritime Cyber Security* yang secara menyeluruh, mulai dari kapal, pelabuhan, sumber daya manusia, teknologi, insiden *maritime cyber.*

No.	Penulis	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi
				misalnya evaluasi cyber security dari negara maritim lain selain Amerika Serikat dan Uni Eropa, terhadap penlilaian standar terhadap Maritime cyber security yang dilakukan oleh IMO.	
2.	S. de Vleeschhouwer (2017) Jurnal Netherlands Maritime Technology	*Safety of data: The risk of Cyber Security in the maritime sector*	Kualitatif Ekploratif	a. Penelitian ini berfokus kepada pengamanan data dalam *cyber security* di sektor pelayaran berdasar kepada *guideline* yang ada sebelumnya; b. Keamanan *cyber* adalah masalah nyata dan menjadi perhatian penting bagi perusahaan yang beroperasi di domain maritim. Ancaman *cyber* adalah nyata untuk kapal saat ini, apakah mereka terhubung ke internet atau tidak. Perangkat lunak perusak dapat disuntikkan melalui berbagai jalur, ini termasuk: USB drive, melalui komponen yang terinfeksi	Relevansi penelitian ini adalah mengulas tentang komponen yang dibutuhkan dalam pengamanan data dalam *cyber security* terutama di bidang maritim sesuai dengan *guideline maritime cyber risk management* yang sudah ada

No.	Penulis	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi
				(membangun dan retrofit baru), atau melalui koneksi jaringan (nirkabel); c. Persamaan dari pedoman-pedoman tersebut adalah sebagai berikut: (1) mengidentifikasi resiko dan mengumpulkan informasi mengenai ancaman yang mungkin terjadi; (2) Mencegah dan melindungi organisasi dari *cyber incidents*; (3) Selalu memonitor dan mendeteksi anomali dan insiden didalam sistem; (4) Merespon dan *recover* untuk mengurangi dampak dan mencegah lebih banyak kerusakan; (5) Memastikan karyawan terlatih untuk selalu waspada dan mempunyai skill dalam bidang *cyber.*	
3.	Jenna Ahokas dan Tuomas Kiiski (2017) Jurnal	*Cybersecurity in Ports*	Kualitatif	a. Laporan ini berfokus pada konsep *cyber security* dan pelabuhan, dan bagaimana pelabuhan dipengaruhi oleh *cyber security*. Konsep *cyber security* dan pelabuhan juga	Relevansi penelitian ini adalah mengulas tentang *cyber security* yang diterapkan di pelabuhan

No.	Penulis	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi
	Finlandia: Publication of the Hazard Project			membantu untuk memahami dan mengklarifikasi aspek-aspek *cyber security* yang akan dihadapi pelabuhan di masa depan. b. Perhatian utama *cyber security* adalah bahwa saat ini, individu dengan peralatan dan pengetahuan minimal tentang *cyberspace* atau tekniknya dapat meluncurkan serangan *cyber*. Biasanya, *cyber attackers* yang lebih kecil bertujuan untuk menarik perhatian tentang betapa mudahnya sistem ICT dari organisasi dan pelabuhan dapat diserang, tetapi serangan *cyber* juga terjadi dalam skala besar dengan konsekuensi yang berat. Meskipun lima c*yberthreats* telah diidentifikasi sejauh ini (*hacktivism, cybercriminality, cyberespionage, cyberterrorism dan cyberwar*), ancaman baru terus bermunculan.	serta ancaman *cyber* yang mungkin terjadi di pelabuhan.

No.	Penulis	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi
				c. Khusus untuk port, ancaman berfokus pada *cyberespionage dan cybercriminality*, karena sistem data mereka mengandung sejumlah besar informasi yang berkaitan dengan jadwal transportasi dan pelanggan. Kerentanan biasanya merupakan malfungsi atau celah dalam sistem ICT.	

Sumber: Hasil olahan peneliti dari berbagai sumber (2018)

BAB III
METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

Berdasarkan permasalahan penelitian yang telah ditetapkan, maka peneliti membuat perencanaan untuk melakukan penelitian pada lingkungan Kementerian Perhubungan, Direktorat Jenderal Perhubungan Laut, dan Telkomsigma (PT. Sigma Cipta Caraka).

3.1.1 Tempat Penelitian

Tempat penelitian merupakan lokasi dimana peneliti melakukan penelitian. Pemilihan lokasi tersebut disesuaikan dengan mempertimbangkan data yang diperoleh untuk menjawab permasalahan yang diteliti. Tempat-tempat penelitian tersebut adalah sebagai berikut:

Tabel 3.1 Tempat penelitian

No.	Instansi	Lokasi	Alamat
1.	Kementerian Perhubungan	Jakarta	Jl. Medan Merdeka Barat No.8 RT.02/RW.03, Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10110
2.	Direktorat Jenderal Perhubungan Laut	Jakarta	Jl. Medan Merdeka Barat No.8 RT.02/RW.03, Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10110
3.	Telkomsigma	Tangerang	Jl. Kapt. Subijanto Dj. Bumi Serpong Damai,Tangerang 15321, Indonesia

3.1.2 Waktu Penelitian

Tahapan yang dilaksanakan pada penelitian mengacu kepada kalender Akademik Universitas Pertahanan Program Studi Keamanan Maritim Tahun Ajaran 2017/2018, yang dimulai dari tahap studi pendahuluan, identifikasi masalah, pengumpulan data, penyusunan proposal, penyelesaian penelitian dan pembuatan laporan penelitian. Pengambilan dan pengolahan data untuk penelitian ini dimulai dari bulan Oktober hingga November 2018. Sedangkan penyusunan hasil penelitian dan pembahasan dimulai dari bulan Desember 2018 hingga Januari 2019. Tahan revisi dan penyelesaian administrasi dilakukan dari bulan Januari hingga Februari 2019.

3.2 Subjek dan Sampel Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif. Metode kualitatif mempunyai tujuan utama yaitu untuk eksplorasi dan pemahaman data secara lebih mendalam. Data dalam konteks kualitatif berkaitan dengan makna dari ungkapan mengenai masalah penelitian yang disampaikan langsung oleh informan, terutama untuk informan-informan utama.[51] Sedangkan pendekatan yang digunakan adalah eksplanatori. Dalam penelitian eksplanatori peneliti mengungkapkan alasan mengapa dan bagaimana fenomena tersebut terjadi.[52] Informasi deskriptif yang di dapat mengungkapkan alasan-alasan tertentu mengapa informasi tersebut terjadi.

Pada penelitian ini, penulis telah menentukan instansi/lembaga pemerintah yang dijadikan sebagai subjek penelitian. Penentuan subjek didasarkan pada permasalahan dalam penelitian ini. Instansi/lembaga pemerintah ini diharapkan dapat memberikan masukan berupa data, baik

[51] Agustinus Bandur, *Penelitian Kualitatif: Metodologi, Desain, dan Teknik Analisis Data dengan NVIVO 11 plus*, (Jakarta: Mitra Wacana Media 2016), hal. 18.
[52] *Ibid*, hlm.49.

primer maupun sekunder sehingga dapat menjawab permasalahan yang akan diteliti.

3.2.1 Subjek Penelitian

Subjek penelitian merupakan tempat dimana data untuk variabel penelitian diperoleh. Subjek penelitian dapat berupa orang, tempat, atau benda yang diamati dalam rangka penelitian sebagai tujuan atau sasaran dari penelitian.[53] Subjek dipilih berdasarkan kompetensinya dan kesesuaian dengan kebutuhan data. Hal ini dilakukan agar data yang didapatkan tepat dan sesuai dengan tujuan atau sasaran. Berikut adalah subjek penelitan yang digunakan yaitu:

Tabel 3.2 Subjek penelitian

No.	Bagian	Instansi	Lokasi
1.	Pusat Teknologi Informasi dan Komunikasi	Kementerian Perhubungan	Gedung Rabobank, Lantai 5 Jl. Abdul Muis No.28, RT.2/RW.8, Petojo Sel., Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10160
2.	Direktorat Lalu Lintas dan Angkutan Laut	Direktorat Jenderal Perhubungan Laut	Wisma Antara, Lantai 10 Jl. Merdeka Selatan, Gambir, Kota Jakarta Pusat, DKI Jakarta, 10110
3.	Direktur Operasional	Telkomsigma	Graha Telkomsigma Jl. Kapt. Subijanto Dj. Bumi Serpong Damai, Tangerang 15321, Indonesia

[53] Arikunto, S. (2005). *Manajemen Penelitian*. (Cetakan Ketujuh).Jakarta: Rineka Cipta.

Tempat penelitian utama bertempat di Kementerian Perhubungan dan Direktorat Jenderal Perhubungan Laut sebagai penanggung jawab serta pengelola aplikasi Inaportnet. Kemudian Telkomsigma yang berinduk kepada PT. Telkom Indonesia dan PT. Media Nusantara Data Global. Telkomsigma merupakan pihak ketiga yang mengelola sistem keamanan informasi pada seluruh *data base* milik Kementerian Perhubungan.

3.2.2 Sampel Penelitian

Sampel penelitian dalam penelitian kualitatif bukan disebut sebagai responden, akan tetapi dikenal sebagai narasumber, partisipan, informan, guru dan teman dalam penelitian. Sampel disini juga bukan sampel statistik, tapi merupakan sampel teoritis. Sampel dalam penelitian kualitatif juga disebut sebagai sampel konstruktif. Alasannya adalah karena dengan sumber data pada sampel tersebut dapat dikonstruksikan sebuah fenomena yang semula masih belum jelas. Sampel (narasumber) dipilih secara *purposive*, yaitu dipilih berdasarkan pertimbangan dan tujuan tertentu. Berikut adalah sampel dari penelitian ini:

Tabel 3.3 Sampel Penelitian

No.	Informan	Instansi	Teknik Pengumpulan Data
1.	Pranata Komputer Pustikom Perhubungan	Pusat Teknologi Informasi dan Komunikasi Perhubungan	Wawancara
2.	Kepala Seksi Sistem Informasi Angkutan Laut	Direktorat Jenderal Perhubungan Laut, Direktorat Lalu Lintas dan Angkutan Laut	Wawancara
3.	Kepala Bagian Manajemen IT dan *Data Center*	Telkomsigma	Wawancara

3.3 Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan oleh peneliti untuk menjaring atau mengungkap informasi dan data dari informan sesuai dengan lingkup penelitian. Teknik pengumpulan data yang tepat akan menghasilkan data yang sesuai dengan permasalahan penelitian yang akan diteliti. Oleh karena itu, langkah-langkah dalam pengumpulan data harus dilakukan secara teliti dan cermat sesuai dengan prosedur dan kaidah penelitian kualitatif.[54] Teknik pengumpulan data yang akan digunakan dalam penelitian ini adalah teknik studi literatur dan wawancara.

3.3.1 Studi Literatur

Studi Literatur atau *Record Review* atau analisis dokumen merupakan segala usaha yang dilakukan untuk menghimpun informasi – informasi yang relevan dengan topik permasalahan dari penelitian ini. Informasi tersebut dikumpulkan dari berbagai media seperti buku, laporan penelitian, jurnal ilmiah, disertasi, peraturan-peraturan, ketetapan-ketetapan, buku tahunan, ensiklopedia, koran dan sumber-sumber elektronik dengan sumber terpercaya.[55] Dokumen-dokumen yang dibutuhkan dalam penelitian ini berasal baik dari sumber buku, peraturan-peraturan, internet, majalah, jurnal maupun hasil seminar. Sumber buku dan peraturan sudah jelas, untuk sumber internet terdiri dari website resmi instansi, media berita elektronik, *e-journal,* dan *e-book.* Sedangkan majalah juga digunakan baik yang bersifat *online* maupun *text book.* Serta hasil seminar, merupakan hasil dari seminar yang diselenggarakan oleh universitas yang berkaitan dengan tema penelitian.

---

[54] Sujarweni Wiratna, Metodologi Penelitian, (Yogyakarta: PT. Pustaka Baru 2014), hal.31.
[55] Bandur, *op.cit*., Hal. 109.

3.3.2 Wawancara

Teknik Wawancara merupakan proses penggalian informasi dan keterangan kepada narasumber. Teknik wawancara dilakukan untuk mendapatkan sebuah informasi secara lebih detail dan utuh. Teknik wawancara merupakan proses tanya jawab yang dilakukan oleh tim peneliti kepada narasumber *face to face* (secara langsung) disertai dengan daftar pertanyaan yang telah dipersiapkan oleh peneliti. Teknik wawancara dilakukan karena menjadi teknik yang efektif terutama dalam mengumpulkan infomasi dan data yang berasal dari narasumber kunci. Sehingga teknik ini dapat membuat narasumber memberikan gambaran yang jelas serta terstruktur mengenai permasalahan yang berkaitan dengan permasalahan dalam penelitian.[56] Wawancara dilakukan sesuai dengan instrumen penelitian yang telah dibuat. Wawancara dilakukan dengan narasumber dari masing-masing instansi yang telah dijelaskan pada sampel penelitian. Waktu wawancara dilakukan menyesuaikan dengan kegiatan dari narasumber. Wawancara dilakukan di ketiga subjek penelitian yaitu Pusat Teknologi Informasi dan Komunikasi Kementerian Perhubungan, Direktorat Jenderal Perhubungan Laut, dan Telkomsigma.

3.4 Pemeriksaan Keabsahan Data

Pemeriksaan Keabsahan Data pada penelitian ini menggunakan bantuan dari *software* NVivo. *Software* NVivo ini juga akan membantu peneliti dalam memeriksa keabsahan data penelitian dengan membandingkan hasil wawancara antar informan sehingga mempermudah dalam menarik kesimpulan. Selain untuk triangulasi data, *software* ini juga berguna untuk membantu peneliti dalam proses koding data. Tujuannya adalah untuk proses pembentukan kategori-kategori utama dari sumber data yang didapat. Kategori-kategori ini dapat dihubungkan dengan

[56] John W. Creswell, “Research Design: Pendekatan Metode Kualitiatif, Kuantitatif dan Campuran”, Edisi 4, (Yogyakarta: Pustaka Pelajar 2016), hal. 254

membentuk koding-koding. Koding berguna untuk mengumpulkan informasi yang relevan dari semua data yang masuk dan dikelompokkan sesuai dengan kategori yang diperoleh dari rumusan masalah, pertanyaan penelitian, dan pedoman wawancara (instrumen penelitian). Setelah koding dilakukan, maka dibentuklah model yang sesuai dengan kebutuhan penelitian, misalnya model triangulasi, model pemetaan faktor, atau model pohon untuk mengetahui variabel yang sering disebutkan dalam penelitian. Hasil olahan dari sini akan selanjutnya diproses dalam analisis penelitian.

Software ini dikembangkan sejak tahun 1981 oleh seorang programmer Tom Richards. Dulu NVivo bernama *Non-Numerical Unstructured Data Indexing Searching and Theorizing* (NUD*IST). Barulah pada tahun 2002 NUD*IST berganti nama menjadi NVivo. 'N' merupakan singkatan dari NUD*IST dan 'Vivo' diambil dari istilah dalam *grounded theory* yaitu 'in-vivo' yang bermakna melakukan koding berdasarkan data yang nyata (hidup) dan dialami oleh partisipan di lapangan. Fungsi utama dari *software* ini adalah untuk melakukan koding data dengan efektif dan efisien. Melakukan presentasi data dalam bentuk, grafik, tabel, diagram dan model untuk penelitian kualitiatif dengan menggunakan NVivo adalah bagaimana melakukan koding terhadap sumber data penelitian. Selain itu, *software* ini juga dapat membuat analisis hubungan berdasar pada hasil koding. Versi NVivo 11 *Plus* merupakan versi terakhir yang terlengkap dari dua seri sebelumnya yaitu NVivo 11 *starter* dan NVivo 11 *Pro*. Pada seri NVivo starter hal yang dapat dilakukan diantaranya adalah mengatur dan menganalisis data berupa teks, koding data teks, *word frequency queries* mengetahui dengan cepat kata-kata utama yang sering muncul dalam data, juga mempresentasikan data ke dalam bentuk diagram dan grafik. Sedangkan pada versi NVivo 11 *Pro* berada di atas dari versi sebelumnya yaitu NVivo 11 *Starter*. Seluruh pengolahan data yang dapat dilakukan di versi NVivo 11 *Starter* dapat dilakukan dalam versi Nvivo 11 *Pro* dengan beberapa tambahan *tools* seperti dapat menganalisis hubugan berdasarkan hasil koding data teks, melakukan koding otomatis, *matrix coding* yang

digunakan untuk melakukan analisis perbandingan.[57] Versi NVivo 11 *Plus* berada diatas versi NVivo 11 *Pro,* tools tambahannya adalah *social network analysis, network sociograms, network matrics, automated insights,* dan *pattern-based autocoding*. Seluruh versi dari NVivo sudah *compatible* dengan OS windows.

3.5 Teknik Analisis Data

Data yang telah diperoleh dan diolah menggunakan *software* NVivo 11 *plus*, selanjutnya akan memasuki proses analisis data. Proses analisis data dalam penelitian ini menggunakan teknik analisis data yaitu *Soft System Methodology* (SSM). SSM merupakan sebuah proses pendekatan untuk memecahkan situasi dari permasalahan yang kompleks, tidak terstruktur berdasarkan analisis holistik dan berpikir sistem. Menurut Chekland dan Poutler (2006)[58], pengertian SSM secara ringkas adalah sebagai berikut:

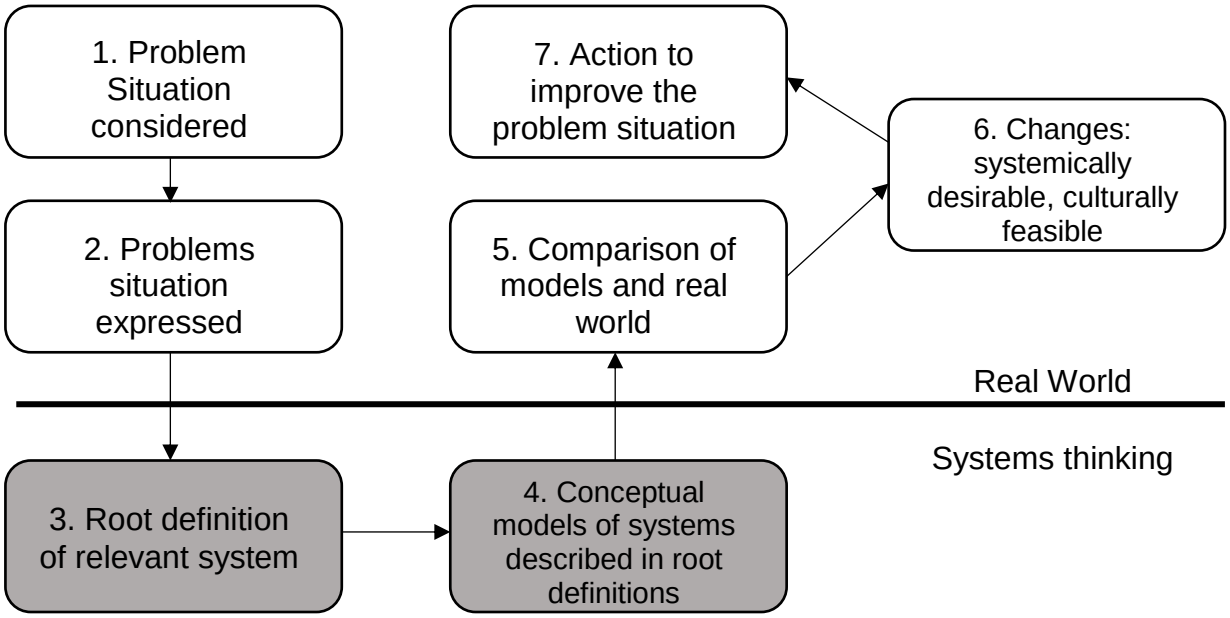
> "SSM adalah proses mencari tahu yang berorientasi aksi atas situasi problematis dari kehidupan nyata sehari-hari; para pengguna SSM melakukan pembelajaran yang dimulai dari menemu-kenali situasi sampai merumuskan dan atau mengambil tindakan guna memperbaiki situasi problematis tersebut. Proses pembelajaran terjadi melalui proses yang terorganisir di mana situasi nyata dieksplorasi dengan menggunakan alat intelektual – yang memungkinkan terjadinya diskusi yang terarah - yang disebut sejumlah model aktivitas yang punya maksud yang dibangun berdasarkan sejumlah sudut pandang (*worldviews*) yang murni"

SSM melihat kejadian yang terjadi sebagai *Human Activity System* karena aktivitas manusia dapat dijadikan sebagai sebuah serangkaian

---

[57] Bandur, *Op Cit* ., hlm 2
[58] Peter Checkland, *Soft System Methodology in Action*, (Denmark: University of Aalborg,1991).

sistem di mana setiap aktivitas yang dilakukan saling berhubungan dan membentuk sebuah ikatan. SSM dapat digunakan ketika pendekatan mekanikal tidak dapat menjelaskan secara utuh realitas dunia nyata. SSM merupakan metode yang unik karena dapat digunakan untuk menganalisa berbagai situasi kompleks, riil, serta konseptual paradigmatik di lingkungan sosial, ekonomi, politik, atau pada tataran kebijakan sekalipun.[59] Terdapat 7 (tujuh) langkah dalam analisis data SSM yang dibagi kedalam 2 (dua) ranah yaitu ranah dunia nyata dan ranah berpikir dalam sistem tentang dunia nyata. Digambarkan pada diagram dibawah ini:



Gambar 3.1 Tujuh tahap siklus baku SSM

Sumber: Suharsono Hardjosoekarto, "Soft System Methodology: Metode serba sistem lunak", (Jakarta: UI Press,2012), hlm.66.

[59] A. Octavian, "Teknik Analisa Data Kualitatif", pada kuliah FIMP di Universitas Pertahanan Indonesia, tanggal 13 Oktober 2017.

Tabel 3.4 Penjelasan tujuh tahap SSM

No.	Tahapan SSM	Keterangan
1.	*Problem situation considered problematic* (Penentuan Masalah)	Dalam tahap ini peneliti melakukan proses penetapan situasi dunia nyata yang dianggap problematis. Situasi problematis yang menarik untuk dilakukan sebuah tindakan perubahan, perbaikan, atau penyempurtaan atas situasi problematis tersebut.
2.	*Problem situation expressed* (Penggambaran masalah)	Tahap kedua peneliti melakukan penjabaran situasi masalah ke dalam bentuk metode yang disebut *rich picture*. Penyusunan rich picture dimaksudkan untuk menggambarkan seluruh latar belakang penelitian
3.	*Root definition of relevant system* (*Root Definition*)	Dalam tahap ini peneliti melakukan *system thinking*, yaitu sebuah pendekatan secara menyeluruh dalam proses analisa. Proses ini dilakukan dengan memahami suatu fenomena yang memandang dari beragam sudut dan memahami bahwa sebuah fenomena dipicu oleh banyak fenomena lainnya. Permasalahan penelitian dijabarkan dengan CATWOE (sebuah definisi tujuan dan pada awalnya didefinisikan oleh Peter Checkland untuk menggambarkan aktivitas manusia dan situasinya sebagai bagian dari SSM). Pada akhirnya, root definition mampu menggambarkan permasalahan menjadi bagian-bagian *How, What,* dan *Why.*
4.	*Conceptual models of systems described in root definitions* (Pemodelan untuk melihat pola dari permasalahan penelitian)	Dalam tahap ini peneliti melakukan permodelan untuk melihat pola dari permasalahan penelitian. Pada tahap keempat ini merupakan penggabungan tahap 1, 2 dan 3 dalam sebuah CATWOE.

No.	Tahapan SSM	Keterangan
5.	*Comparison of models and real world* (Perbandingan hasil analisa dengan kenyataan di lapangan)	Tahap kelima merupakan berbandingan antara hasil analisa (model konseptual) dengan fakta di lapangan.
6.	*Changes: systemically desirable, culturally feasible* (Tahap analisis Bab 4)	Tahap keenam merupakan tahapan analisis untuk menjawab rumusan masalah atau pertanyaan penelitian. Terdapat 2 (dua) pertimbangan yaitu argumen dapat diterima atau dapat dimungkinkan secara kultural (*cultural feasible*)
7.	*Action to improve the problem situation* (Rekomendasi Bab 5)	Dalam tahap terakhir, peneliti mengemukakan rekomendasinya sesuai dengan manfaat yang ingin diperoleh

Sumber: Suharsono Hardjosoekarto, "Soft System Methodology: Metode serba sistem lunak", (Jakarta: UI Press,2012), hlm.63-65.

Analisis CATWOE yang digunakan dalam SSM merupakan sebuah alat bantu untuk mengingat supaya *root definition* yang dibuat benar-benar menggambarkan sebuah sistem aktivitas manusia yang relevan dengan penelitian. Berikut adalah penjelasan mengenai singkatan dari CATWOE[60]:

- **C** : *Customers*, orang atau sekelompok orang yang diuntungkan dari proses Transformasi;
- **A** : *Actors*, orang atau sekelompok orang yang melakukan kegiatan proses Transformasi;
- **T** : *Transformation*, proses pengubahan input menjadi output, baik konkret maupun abstrak;
- **W** : *Worldview (Weltanschauung),* sudut pandang, atau kerangka pikir yang menjadikan root definition atau Transformasi menjadi bermakna;

[60] Suharsono Hardjosoekarto, *Soft System Methodology: Metode serba sistem lunak*, (Jakarta: UI Press,2012), hlm.97.

- **O** : *Owners*, orang atau sekelompok orang yang berkuasa atas sistem, dan punya kewenangan untuk menghentikan proses Transformasi;
- **E** : *Environtmental constraints*, Lingkungan yang menjadi kendala berlangsungnya proses Transformasi.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

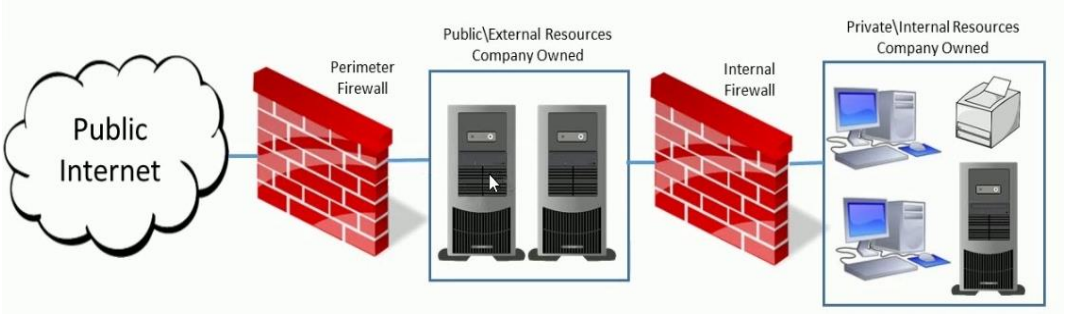
Dalam penelitian ini, data yang diperoleh berupa data primer dan data sekunder. Data primer diperoleh dari hasil wawancara dan data internal berupa *softfile* dari instansi tersebut yang diberikan kepada peneliti. Sedangkan data sekunder diperoleh dengan teknik studi literatur dari berbagai sumber mulai dari media online, cetak, majalah, jurnal, koran serta seminar-seminar yang berkaitan dengan tema penelitian. Temuan yang diperoleh dalam proses pengumpulan data primer dari masing-masing instansi dan perusahaan dijadikan landasan utama dalam penelitian ini.

Data sekunder yang digunakan sebagai pendukung penelitian ini adalah Peraturan Menteri Perhubungan Nomor 192 Tahun 2015 tentang perubahan atas PM Nomor 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan, IMO Guideline tentang *Maritime Cyber Risk Management* MSC-FAL.1/Circ.3 tahun 2017, dan ISO/IEC 27001 tentang *Information Security Management Systems*.

4.1.1 Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet dari ancaman dan serangan cyber

Sistem keamanan informasi aplikasi Inaportnet ditangani oleh Telkomsigma. Kerjasama dengan Telkomsigma meliputi server Inaportnet baik untuk *data base* dan aplikasi berserta dengan sistem pengamanannya menjadi satu paket. Implementasi sistem keamanan informasi dalam aplikasi Inaportnet dilakukan setiap hari selama 24 jam penuh (24x7) oleh Telkomsigma. Selain dengan penjagaan secara fisik, sistem pengamanan yang sama juga berlaku untuk sistem virtual termasuk sistem *network*nya.

Penjagaan dengan fisik berupa komputer itu sendiri, kamera cctv, petugas kontrol dan lain-lain. Sedangkan untuk penjagaan virtualnya dilakukan dengan memasang *firewall*[61] dalam *Demilitarized Zone* (DMZ)[62], *user password*, *biometric access control*, PIN, serta *proximity card*. Gambaran dari sistem pengamanan jaringan dalam DMZ adalah sebagai berikut:



Gambar 4.1 Sistem pengamanan *Firewall* dalam DMZ

Sumber: www.onlinecomputertips.com

Pengawasan dan regulasi sistem pengamanan dalam aplikasi Inaportnet dilakukan oleh Pusat Teknologi Informasi dan Komunikasi serta Direktorat Lalu Lintas dan Angkutan Laut. Mereka belum mempunyai jadwal secara berkala dalam melakukan *Penetration Test* (Pentest), pentest merupakan kegiatan untuk mensimulasikan serangan terhadap sistem keamanan dalam jaringan dalam suatu perusahaan/instansi. Pentest secara aktif dapat menilai kontrol keamanan yang ditempatkan dalam sistem atau jaringan, sehingga kelemahan yang terdeteksi dapat segera diperbaiki dan dievaluasi. Pentest ini digunakan untuk menutup celah bagi

[61] Firewall digunakan untuk menyaring lalu lintas antar jaringan, baik lalu lintas jaringan yang masuk dan keluar dari server. Firewall juga akan melindungi jaringan dari lalu lintas yang tidak wajar, di mana lalu lintas yang tidak wajar ini kemungkinan besar dilakukan oleh penyerang. Firewall akan memblokir pengguna dari situs-situs dan unduhan yang mempunyai potensi berbahaya. Dalam firewall terdapat fitur-fitur seperti Virtual Private Network (VPN), Network Address Translation (NAT), dan Port Address Translation (PAT) yang merupakan fitur-fitur untuk tingkat keamanan yang tinggi.

[62] Demilitarized Zone (DMZ) merupakan zona buffer antara internet dan *internal network*. DMZ menyediakan lapisan perlindungan untuk *internal network*.

penyerang dalam melakukan serangan terhadap jaringan IT perusahaan/instansi. [63]

Sistem pengamanan untuk *database* untuk aplikasi Inaportnet dilakukan oleh Telkomsigma. Sejak tahun 2015, Telkomsigma telah bekerjasama dengan Kementerian Perhubungan untuk *Data Center Services*. Kerjasama yang pertama dilakukan dengan transportasi sektor udara yaitu aplikasi Aviationet dan transportasi darat seperti kereta api dan KRL. Kemudian pada tahun 2016, Sistem Inaportnet dikembangkan dan *Data Center*-nya juga menggunakan jasa dari Telkomsigma. Sehingga sistem pengamanan untuk *Data Center* dilakukan oleh Telkomsigma. Telkomsigma dipilih karena selain perusahaan ini termasuk dalam BUMN, tetapi juga karena perusahaan ini memang terbukti andal di bidangnya. Dalam bidang *Data Center* Telkomsigma telah mengantongi beberapa sertifikasi standar internasional, diantaranya adalah ISO 27001 : 2005 untuk *Information Security Management System*, TIER III dan IV Design, ISO 9001 : 2008 untuk *Quality Management System*, dan BS OHSAS 18001 : 2007 untuk *Occupational Health and Safety Management System*.

Sistem pengamanan untuk *Data Center* dilakukan baik dalam jaringan virtual maupun bangunan fisiknya. Sistem pengamanan secara fisik meliputi *Cable Management, Fire Safety,* konstruksi bangunan, lokasi bangunan, sistem pengamanan seperti CCTV, penguncian dan akses bangunan, sistem cadangan daya, sistem tata udara. Untuk sistem pengamanan secara virtual, hal-hal yang termasuk didalamnya adalah sistem *Firewall* dan *Zero Trust Network* (ZTN)[64]. Untuk sistem keamanan jaringan virtual meliputi keamanan jaringan intranet maupun internet,

---

[63] Darril Gibson, *CompTIA Security+ Get Certified Get Ahead: SY0-301 Study Guide*, (North Charleston: CreateSpace, 2011), hlm. 342.

[64] ZTN merupakan pendekatan untuk sistem keamanan jaringan dan perangkat dengan menempatkan sistem keamanan pada inti jaringan secara terpusat untuk seluruh aktifitas dalam jaringan. Sistem keamanan terpusat ini memberikan keuntungan yaitu para karyawan/staff perusahaan/instansi dapat mengakses aplikasi tersebut menggunakan perangkat apa saja seperti laptop pribadi, tablet, smartphone dari berbagai lokasi.

firewall, hak akses jaringan, *Intrusion detection*, kontrol akses logical yang menyangkut siapa, apa dan bagaimana data dapat diakses misalnya penggunaan *password*, sistem penyimpanan data, back up data dan enkripsi data, termasuk juga kebijakan terkait dengan kontrol akses fisik terhadap *Data Center*.

Untuk mendukung sistem pengamanan infomasi dari aplikasi dan *data base* Inaportnet dilakukan oleh Telkomsigma. Kerjasama antara Telkomsigma dengan Direktorat Jenderal Perhubungan Laut telah dilaksanakan sejak tahun 2016, yakni semenjak pengembangan aplikasi Inapornet. Kementerian Perhubungan sebelumnya telah menjalin kerjasama dengan Telkomsigma sejak tahun 2015. Dimulai dari aviationet yang merupakan aplikasi pelayanan administrasi untuk kegiatan penerbangan dibawah Direktorat Jenderal Perhubungan Udara. Bahkan kerjasama sebelumnya dimulai dari penggarapan sistem e-ticketing dari PT. KAI dan KRL *Commuterline*.

Sebagai perusahaan yang bergerak dalam bidang IT, pengamanan disini memang luar biasa ketat. Pemeriksaan dilakukan 3 lapis (gate, gedung, data center), dan tidak diperkenankan membawa alat *electronic portable device* dalam bentuk apapun (handphone, recorder, kamera, USB, Harddisk portable, Laptop, kabel-kabel, dan lain-lain) masuk kedalam gedung. Ketika masuk ke dalam data center juga tidak diperkenankan memotret dan membawa tas.

Telkomsigma merupakan sebuah perusahaan yang bergerak dalam bidang bisnis *Information Computer Technology* (ICT). Perusahaan ini didirikan pada tahun 1987 dengan nama PT. Sigma Cipta Caraka, setelah diakuisisi pada tahun 2008 oleh salah satu anak perusahaan dari Telkom Indonesia yaitu PT. Multimedia Nusantara (Telkommetra) nama PT. Sigma Cipta Caraka berubah menjadi Telkomsigma dan sejak tahun 2010 Telkomsigma resmi 100% menjadi anak perusahaan PT. Telekomunikasi Indonesia (TELKOM). Pada awalnya PT. Sigma Cipta Caraka merupakan

partner dari IBM untuk menjual produk *hardware* kepada perusahaan perbankan. Kemudian pada tahun 1997 PT. Sigma Cipta Caraka menjadi *pioneer* dalam pengembangan bisnis *Data Center* di Indonesia. Kantor pusat dari Telkomsigma terletak di Desa Sigma, German Centre, Serpong, Tangerang Indonesia. Sebagai *market leader* untuk perusahaan di bidang ICT, saat ini Telkomsigma telah mengimplementasikan solusi dan layanan yang mendominasi dalam bidang ICT. Terutama untuk Industri Perbankan, Media dan Komunikasi, Properti dan Konstruksi, Pariwisata dan Perhotelan, Pendidikan, Asuransi dan Keuangan, Manufaktur dan Agribisnis, Transportasi, Kesehatan, Energi dan Sumberdaya, Maritim dan Logistik, Informasi dan Bisnis, Pemerintah, Perusahaan Kecil dan Menengah, Perdagangan dan Distribusi, Grosir dan Eceran.

Telkomsigma tengah berfokus mengembangkan aplikasi Transportasi di Indonesia untuk mengimbangi pembangunan infrastruktur fisik yang dilakukan oleh Pemerintah. Misalnya dalam program pembangunan Tol laut[65], saat Tol laut dibangun maka infrastruktur IT dari Tol Laut juga harus dibangun untuk menunjang performa dari Tol Laut itu sendiri. Oleh karena itu kerjasama Telkomsigma dengan Direktorat Jenderal Perhubungan Laut dilakukan untuk saling mendukung. Dalam era digital seperti saat ini, pengaruh dari Teknologi Informasi saling mengimbangi infrastruktur fisik. Dalam penelitian ini berarti aplikasi Inaportnet dibuat untuk mendukung infrastruktur fisik yang telah ada dilapangan dan membuatnya lebih mudah, cepat dan transparan dalam

[65] Berdasarkan Lampiran II Peraturan Presiden Republik Indonesia Nomor 16 Tahun 2017 Tentang Kebijakan Kelautan Indonesia. Di mana pembangunan Poros Maritim Meliputi (1) Membangun budaya maritim Indonesia, (2) Menjaga laut dan sumber daya laut dengan fokus membangun kedaulatan pangan laut melalui pengembangan industry perikanan dengan menempatkan nelayan sebagai pilar utama, (3) Memberi Prioritas pada pengembangan infrastruktur dan konektivitas maritim dengan membangun Tol Laut, deep seaport, logistic, dan industri perkapalan dan pariwisata maritim, (4) Memperkuat diplomasi maritim, kerja sama di bidang kelautan, menghilangkan sumber konflik di laut seperti pencurian ikan, pelanggaran kedaulatan, sengketa wilayah, perompakan, dan pencemaran laut, serta (5) Membangun kekuatan pertahanan maritim untuk menjaga kedaulautan dan kekayaan maritim serta bentuk tanggung jawab dalam menjaga keselamatan pelayaran dan keamanan maritim.

operasionalnya. Hal ini disebut sebagai *Infostructure* yang didalamnya terdapat konektivitas dan aplikasi sehingga bisnis berjalan menjali lebih murah dan *controlable*.[66]

Data Center Telkomsigma telah menerima berbagai penghargaan diantaranya adalah pada tahun 2014 penghargaan sebagai "*Data Center* of The Year" dari Frost and Sullivan, "*The Indonesia's Most Admired Companies* untuk kategori *Data Center Provider*" dari Frontier Consulting Group dan Tempo Media Group. Pada tahun 2015 mendapatkan penghargaan untuk "*Data Center Service Provider* dan *Telco Cloud Service Provider* of the Year 2015" dari *Frost and Sullivan*. Pada tahun 2016, Telkomsigma tercatat dalam rekor MURI sebgai Perusahaan Penyedia *Data Center* Indonesia Pertama yang menerima Sertifikat Uptime TIER III *Construction Facility* dan sebagai Perusahaan penyedia *Data Center* Indonesia yang menerima sertifikat Uptime TIER III for Design Document terbanyak.[67] Pada tahun 2017, *Data Center* Telkomsigma meraih peringkat ke-16 dalam World-rangking Cloudscene "The Fast 50 Most Resilient *Data Center* Operators in 2017" untuk wilayah Amerika Utara, Eropa, The Middle East, and Afrika (EMEA), Oceania dan Asia. Bahkan peringkat Telkomsigma mengungguli beberapa *Data Center* kenamaan Amerika seperti T5 *Data Center* dan Green Mountain.

Terdapat 3 (tiga) layanan di bidang ICT yang disediakan oleh Telkomsigma yaitu *System Integration* (SI), *Data Center Services*, dan *Managed Services (Cloud Computing)*. Jenis layanan Telkomsigma yang digunakan oleh Kementerian Perhubungan adalah *Data Center Services*. *Data Center* Telkomsigma terdapat di tiga area yang berbeda yaitu di Sentul seluas 8.000 m^2, Serpong dengan luas 22.000 m^2, dan Surabaya seluas 6.500 m^2. Untuk *Data Center* di Surabaya digunakan sebagai *Data*

[66] Kusnan Djawahir dan Yosa Maulana. "Telkomsigma Fokus Kembangkan Aplikasi untuk Transportasi" 2017, dalam http://www.telkomsigma.co.id/
[67] Press Release News. "Telkomsigma Dinobatkan sebagai The Best Disruptor Company" 2017, dalam http://www.telkomsigma.co.id/

Recovery Site untuk mendukung *Data Center* di Serpong dan Sentul, selain itu juga digunakan untuk memenuhi kebutuhan perusahaan di wilayah Indonesia Timur.

Operator dalam pelaksanaan implementasi sistem keamanan informasi aplikasi Inaportnet adalah Telkomsigma. Hal ini dikarenakan seluruh server baik aplikasi dan *data base* Inaportnet yang mengelola adalah pihak Telkomsigma. Hal ini dilakukan untuk menjaga sistem aplikasi Inaportnet agar selalu ON, tidak terganggu oleh ancaman *cyber* ataupun kesalahan teknis seperti sistem *down*, atau bahkan kejadian-kejadian *force majure* seperti kebakaran dan bencana alam.

Dalam keamanan informasi, sistem pencengahan lebih banyak dilakukan untuk mencegah ancaman-ancaman seperti virus, malware, DDoS, dan lain sebagainya untuk masuk dan menyerang sistem. Hal ini dilakukan karena tindakan pencegahan yang di pasang secara berlapis lebih baik dibanding jika ancaman tersebut sudah masuk dan merusak sistem, karena ketika ancaman tersebut sudah masuk maka penanganannya akan lebih susah (tentunya hal ini tergantung dari jenis ancamannya). Untuk menghindari dampak kerugian yang besar maka tindakan pencegahan ini sangat perlu untuk dilakukan. Hal ini seperti yang diimplementasikan dalam aplikasi Inaportnet, di mana sistem pengamanan berlapis dipasang sedemikian rupa untuk mencegah serangan *cyber* masuk. Namun ketika terjadi serangan cyber yang berhasil menembus sistem keamanan informasi dalam aplikasi Inaportnet maka hal yang dilakukan adalah penanganan langsung terhadap sistem yang terinfeksi. Dalam aplikasi Inaportnet, server dan data base dijaga selama 24 jam non stop dan disana juga terdapat sistem yang dapat mendeteksi jika terjadi serangan cyber terletak dimana. Ada juga untuk gangguan-gangguan kecil yang dapat ditangani secara otomatis. Contohnya adalah ketika terjadi down, maka sistem secara otomatis akan mengaktifkan sistem replika dari sistem utama dan memindahkan seluruh sistem kedalam sistem replika.

Menurut Teori Implementasi Keamanan Informasi yang dikemukakan oleh Timothy P. Layton dalam bukunya yaitu *Informaton Security: Design, Implementation, Measurement, and Compliance.* Terdapat 9 (Sembilan) komponen dalam keamanan informasi yaitu (1) Keamanan Fisik dan Lingkungan, (2) Keamanan Sumber Daya Manusia, (3) Kebijakan Keamanan, (4) Kontrol Akses, (5) Manajemen Aset, (6) Manajemen Komunikasi dan Operasi, (7) Pengaturan tentang Keamanan Informasi, (8) Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi, dan (9) Penilaian Resiko dan Perawatan. Berikut adalah implementasi sistem keamanan informasi dalam aplikasi Inaportnet berdasarkan komponen-komponen yang dikemukakan oleh Timothy P. Layton:

1. Keamanan Fisik dan Lingkungan

   Kriteria dalam komponen ini telah dipenuhi oleh Telkomsigma sebagai penyedia *data center*. Seperti skema yang mengatur ketika terjadi *force majure* seperti kebakaran telah tersedia, serta peralatan yang mendukungnya juga seperti alat pendeteksi asap dan alarm, alat pendeteksi kebocoran air, *Automatic Gas Fire Suppression System*, pemadam api portable disetiap sudut ruangan. Selain itu, Telkomsigma juga telah mengantongi standar SNI untuk standar perencanaan ketahaan gempa untuk struktur bangunan gedung.

   Untuk standar power system Telkomsigma dipasok listrik dari PLN, serta untuk redundant power system didukung oleh genset dengan redundancy N+1 yang akan aktif dalam waktu 10 detik setelah pemadaman listrik. Genset ini juga dilengkapi dengan tanki bahan bakar solar yang dapat menyediakan sumber listrik selama 2 hari dan dapat diisi kembali. Selain itu, *cable management* untuk jaringan diletakkan diatas, sedangkan untuk kelistrikan diletakkan dibawah lantai panggung. Sistem monitoring lingkungan dengan CCTV berbasis IP, penggunaan PIN, *Proximity Card* dan *Biometric Access Control* untuk memasuki ruangan-ruangan, mekanisme *cooling system*. Serta aturan pelarangan

penggunaan kamera, ponsel, *smartphone*, dan *electronic portable device* lainnya.

2. Keamanan Sumber Daya Manusia

   Dalam kriteria ini, sebagai pihak ketiga dalam penyedia layanan server dan *data base* beserta keamanannya Telkomsigma telah mengatur skema tentang hak akses kontrol untuk kelancaran pelayanan Inaportnet. Untuk skema yang dibuat menyangkut *manage service* antara kedua belah pihak. Aturan-aturan tentang pembatasan hak akses pegawai sesuai dengan tingkatan jabatan serta departemennya juga telah dilaksanakan.

3. Kebijakan Keamanan

   Kebijakan keamanan disini terkait dengan permasalahan tentang bagaimana perusahaan dapat memenuhi berbagai aturan keamanan serta *privacy regulation*. Kebijakan keamanan yang telah dilaksanakan menyangkut kebijakan penggunaan *e-mail* bagi para pegawai di Telkomsigma, kebijakan untuk penggunaan *firewall*, kebijakan untuk penggunaan laptop/komputer tablet, hingga kebijakan penggunaan *password*.

4. Kontrol Akses

   Dalam kriteria ini, aktor yang paling berperan adalah Direktorat Jenderal Perhubungan Laut, selaku penanggung jawab dari Inaportnet. Hal ini dikarenakan akses kontrol penuh Inaportnet tetap berada di Direktorat Jenderal Perhubungan Laut. Termasuk juga untuk registrasi *user* serta pembatasan akses untuk *user* diatur dalam kriteria ini.

5. Manajemen Aset

   Kriteria ini telah dilaksanakan oleh Telkomsigma salah satunya adalah dengan mendata seluruh peralatan komputer, komunikasi,

media penyimpanan, *back up data*, perangkat lunak, dan membuat labeling informasi. Tidak hanya perangkat lunak dan keras saja yang perlu didata. Akan tetapi juga dokumen-dokumen penting seperti kontrak/kerjasama, SOP, *training material* dan lain-lain juga diklasifikasikan sebagai aset.

6. Manajemen Komunikasi dan Operasi

   Hal-hal yang telah dilaksanakan diantaranya adalah SOP untuk penanganan teknis ketika terjadi serangan *cyber* atau sistem mengalami *down*, pengaturan kerja shift dalam server, peraturan kerjasama antara Kementerian Perhubungan dengan Telkomsigma serta mengatur level instalasi untuk setiap user dalam mengakses data dalam *data center*.

   Selain itu hal-hal mengenai aturan tentang pencegahan, deteksi serta respon terhadap kode berbahaya adalah dengan mengatur *upgrade* sistem secara terpusat, menggunakan VPN dalam transmisi data, serta audit yang dilakukan tiap 6 bulan sekali. Aturan tentang manajemen keamanan jaringan juga diatur dalam kriteria ini hal ini dilakukan untuk melindungi informasi pada jaringan dan *supporting network infrastructure*. Hal-hal yang telah dilakukan diantaranya adalah menggunakan layanan network dengan *authentication*, enkripsi dan kontrol koneksi, aturan tentang penggunaan e-mail.

7. Pengaturan tentang Keamanan Informasi

   Kriteria internal yang telah diterapkan oleh Telkomsigma diantaranya termasuk kebijakan tentang pendefinisian informasi *input* maupun *output* serta infomasi tersebut harus diklasifikasikan. Termasuk aturan hak akses antara Telkomsigma dan Kementerian Perhubungan. Selain itu, sertifikasi ISO 27001 untuk manajemen Keamanan Informasi telah dikantongi oleh Telkomsigma sebagai penyedia data center untuk Inaportnet. Namun dari segi kebijakan keamanan informasi Direktorat Lalu Lintas dan Angkutan Laut belum membuat *handbook* untuk

keamanan informasi sebagai representatif dari kebijakaan keamanan informasi yang diterapkan dalam aplikasi Inaportnet.

8. Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi

   Hal yang telah dilakukan oleh Telkomsigma adalah pemeliharaan sistem dengan melakukan audit internal dua kali dalam satu tahun, menggunakan metode enkripsi kriptografi untuk menjamin keamanan, integrasi dan keaslian informasi. Serta membuat prosedur implementasi untuk mengontrol instalasi perangkat lunak. Kemudian Inaportnet juga menggunakan data center ganda yang beroperasi dalam sistem pola replikasi *real time* sehingga memberikan ketersediaan koneksi secara terus menerus.

9. Penilaian Resiko dan Perawatan

   Hal yang telah dilakukan adalah dengan melakukan *penetration test*, yaitu menyerang sendiri sistem Inaportnet untuk mengetahui kelemahan sistem pengamanannya. Hal itu kemudian dilanjutkan dengan patching, yaitu kegiatan yang dilakukan untuk memperbaiki kelemahan-kelemahan tersebut. Namun kegiatan ini belum terjadwal secara berkala di tingkat regulator yaitu Direktorat Lalu Lintas dan Angkutan Laut. Selain itu, kemampuan sistem untuk pulih setelah layanan terhenti telah dibuktikan Telkomsigma dengan mendapatkan sertifikasi dari TIER III dan IV dimana toleransi untuk *downtime data center* hanya 30 menit per tahunnya.

4.1.2 Aspek pendukung dan penghambat dalam sistem pengamanan informasi dalam aplikasi Inapornet

Cikal bakal dari aplikasi Inaportnet sudah ada sejak tahun 2005, namun pada saat itu sistem masih berjalan secara tunggal dari masing-masing instansi pemerintahan yang terkait dengan kegiatan kepelabuhanan. Misalnya SIMLALA milik Direktorat Lalu Lintas dan

Angkutan Laut, SIMPONI milik Direktorat Jenderal Anggaran, *Indonesia National Single Window* (INSW), Master Terminal milik Pelindo, serta aplikasi kenavigasian milik Direktorat Kenavigasian berjalan sendiri-sendiri. Untuk menyatukan seluruh sistem administrasi pelabuhan tersebut maka dikembangkan aplikasi Inaportnet yang berguna dalam me ngintegrasikan seluruh sistem kepelabuhanan milik instansi terkait kegiatan kepelabuhanan.

Pada tahun 2016, aplikasi Inaportnet resmi diluncurkan, namun saat itu baru diterapkan pada 6 pelabuhan utama saja. Sejak tahun 2017, Inaportnet telah berkembang dan dioperasikan di-16 (enam belas) pelabuhan di Indonesia. Pada tahun 2018, Inaportnet generasi kedua diluncurkan yaitu Inaportnet 2.0. Pada Inaportnet 2.0 terdapat pembaharuan dari seri aplikasi Inaportnet sebelumnya, di mana dalam versi terbaru Inaportnet dilengkapi dengan sistem *tracking* untuk kontainer. Untuk saat ini, Inapornet 2.0 masih dioperasikan di 5 (lima) pelabuhan utama di Indonesia, yaitu di Tanjung Priok, Tanjung Perak, Belawan, Makassar, dan Tanjung Emas.

Dalam pelaksanaannya, aplikasi Inaportnet mempunyai beberapa kekurangan seperti disampaikan oleh Ibu Ayu Kharisza, S.Kom yang menjabat sebagai Kasi Sistem Informasi Angkutan Laut yaitu keberadaan *service center* yang dibawah pustikom dinilai terlalu kecil. Kemudian menurut Bapak Henry yang menjabat sebagai Pranata Komputer di Pusat Teknologi Informasi dan Komunikasi Perhubungan juga menyatakan beberapa kekurangan dari Inapornet yaitu karena Inaportnet ini bersifat sebagai sistem yang mengingtegrasikan dari seluruh sistem aplikasi milik instansi /lembaga yang menjalankan kegiatan kepelabuhanan, ketika terdapat *trouble* pada salah satu sistem milik instansi /lembaga tersebut maka sistem dari Inaportnet juga akan mengalami gangguan.

Direktorat Lalu Lintas dan Angkutan Laut (Ditlala) merupakan direktorat dibawah Direktorat Jenderal Perhubungan Laut. Kantor pusatnya terletak di Kompleks Kementerian Perhubungan yang terletak di Jl. Medan

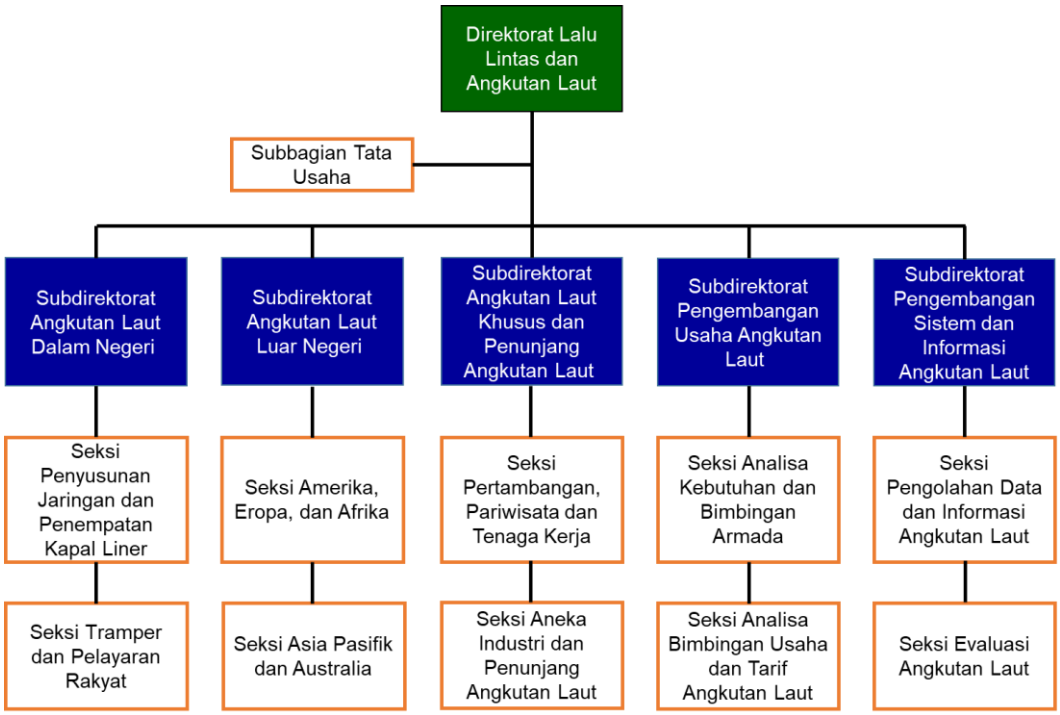
Merdeka Barat, namun kebakaran pada Minggu, 8 Juli 2018 di gedung karya mengakibatkan tersebarnya kantor pelayanan direktorat Kementerian Perhubungan. Di dalam gedung karya terdapat beberapa subsektor dari Kementerian Perhubungan seperti Sekretariat Jenderal Kementerian Perhubungan, Inspektorat Jenderal Kementerian Perhubungan, serta Direktorat Jenderal Perhubungan Darat, Laut, Udara serta Perkeretaapian. Direktorat Jenderal Perhubungan Laut dipindahkan ke Wisma Antara Jl. Medan Merdeka Selatan lantai 9-10 dan Wisma BSG Jl. Abdul Muis lantai 11, kemudian untuk Pustikom dievakuasi di gedung Rabobank Jl. Abdul Muis lantai 5.

Akibat dari kebakaran ini, peneliti sempat mengalami kendala lamanya proses disposisi surat hingga lebih dari 3 minggu. Hal ini dikarenakan kantor subbagian yang sekarang terpisah-pisah dari gedung utama Kementerian Perhubungan yang ada di Merdeka Barat. Namun peneliti mempunyai inisiatif untuk memberi surat langsung kepada bagian-bagian yang termasuk dalam obyek penelitian. Pertama peneliti meletakkan surat di bagian umum Direktorat Jenderal Perhubungan Laut yang terletak di Wisma BSG lantai 11, kemudian atas izin bagian umum dari Direktorat Jenderal Perhubungan laut, peneliti juga memberikan surat secara langsung kepada Direktorat Lalu Lintas dan Angkutan Laut yang terletak di Wisma Antara Lantai 9.

Direktorat Jenderal Perhubungan Laut terdiri dari 5 (lima) direktorat yaitu Direktorat Lalu Lintas dan Angkutan Laut, Direktorat Pelabuhan dan Pengerukan, Direktorat Perkapalan dan Kepelautan, Direktorat Kenavigasian, dan Direktorat Kesatuan Penjaga Laut dan Pantai. Pemeliharaan dan pengawasan aplikasi Inaportnet dilakukan oleh Direktorat Lalu Lintas dan Angkutan Laut, dan Pusat Teknologi Informasi dan Komunikasi Perhubungan.

Tugas dan fungsi dari Direktorat Lalu Lintas dan Angkutan Laut adalah untuk melaksanakan dan mempersiapkan perumusan dan pelaksanaan kebijakan, penyusunan norma, standar, prosedur dan kriteria,

pemberian bimbingan teknis dan supervisi serta evaluasi dan pelaporan di bidang lalu lintas dan angkutan laut dalam negeri, angkutan laut luar negeri, angkutan laut khusus, usaha jasa terkait angkutan laut, pengembangan usaha angkutan laut, sistem informasi angkutan laut dan sarana prasarana angkutan laut. Serta pelaksanaan urusan tata usaha, kepegawaian, tata usaha dan rumah tangga Direktorat.[68] Berikut adalah struktur organisasi dari Direktorat Lalu Lintas dan Angkutan Laut:



Gambar 4.2 Struktur Organisasi Direktorat Lalu Lintas dan Angkutan Laut

Sumber: www.hubla.dephub.go.id

Selain Direktorat Lalu Lintas dan Angkutan Laut (Ditlala), pemeliharaan dan pengawasan aplikasi Inaportnet juga dilakukan secara bersama antara Direktorat Lalu Lintas dan Angkutan Laut (Ditlala) dengan Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom). Pada saat penyerahan surat ijin penelitian, peneliti sempat mengalami kendala

[68] Direktorat Jenderal Perhubungan Laut, "Tugas dan Fungsi Direktorat Lalu Lintas Angkutan Laut", 2014 dalam www.hubla.dephub.go.id

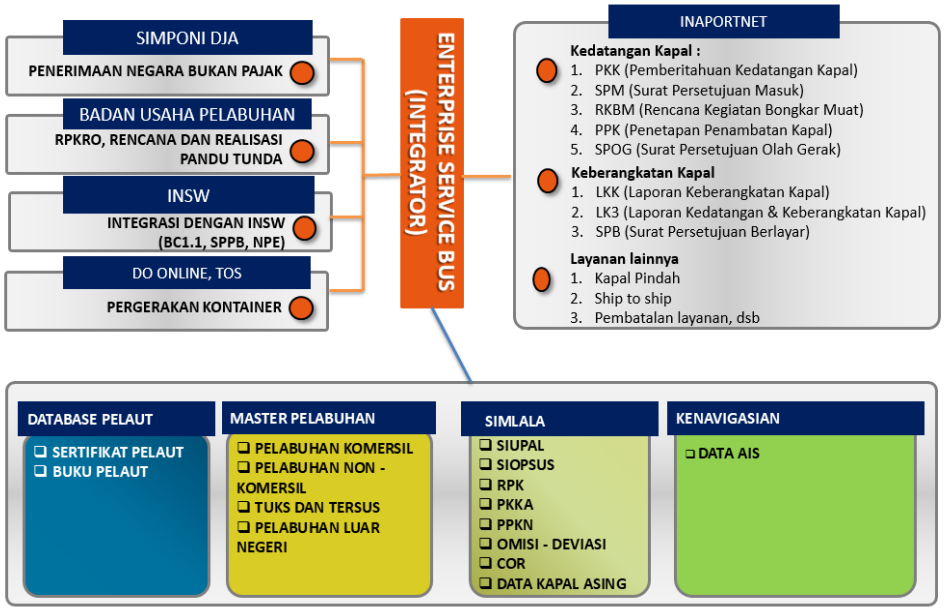
yang hampir sama saat di Direktorat Jenderal Perhubungan Laut. Namun atas bantuan dari narasumber di Direktorat Lalu Lintas dan Angkutan Laut, peneliti dapat memberikan secara langsung surat untuk Kepala Pusat Teknologi Informasi dan Komunikasi Perhubungan yang langsung didisposisikan kepada salah satu stafnya yang menjabat sebagai pranata komputer di Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom).

Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom) merupakan salah satu dari 3 (tiga) unsur penunjang dari tugas dan fungsi Sekretariat Jenderal Perhubungan. Di mana ketiga unsur tersebut adalah Pusat Teknologi Informasi dan Komunikasi Perhubungan, Pusat Pengelolaan Transportasi Berkelanjutan, dan Pusat Fasilitasi Kemitraan dan Kelembagaan Internasional. Adapun tugas dan fungsi dari Pustikom dalam Surat Keputusan Menteri Perhubungan RI Nomor KP. 336 Tahun 2018 disebutkan:

1) Penyiapan penyusunan rencana strategis, pengelolaan program, perumusan dan pembinaan pelaksanaan standar kebijakan dan tata kelola, serta manajemen resiko sistem teknologi informasi dan komunikasi;
2) Penyiapan perancangan, pembangunan, pengembangan dan pengujian sistem aplikasi, basis data, dan infrastruktur;
3) Penyiapan pengelolaan data dan layanan operasional sistem teknologi informasi dan komunikasi; dan
4) Penyusunan rencana, program, anggaran, urusan keuangan, kepegawaian, persuratan, kearsipan, perlengkapan, rumah tangga, pengelolaan administrasi barang milik negara serta evaluasi dan pelaporan.[69]

[69] Surat Keputusan Menteri Perhubungan RI Nomor KP. 336 Tahun 2018 tanggal 20 Februari 2018 Tentang Reviu Rencana Strategis Sekretariat Jenderal Kementerian Perhubungan Tahun 2015-2019 Subbab 1.1.1 Ketugasan Sekretariat Jenderal point H. Tugas dan Fungsi Pusat Teknologi Informasi dan Komunikasi Perhubungan.

Inaportnet merupakan sebuah aplikasi portal elektronis yang terbuka dan netral. Layanan aplikasi Inaportnet tergabung dengan beberapa instansi dan stakeholder yang berkaitan dengan kegiatan kepelabuhanan seperti, SIMLALA milik Direktorat Lalu Lintas dan Angkutan Laut, SIMPONI milik Direktorat Jenderal Anggaran, *Indonesia National Single Window* (INSW), Master Terminal milik Pelindo, serta aplikasi kenavigasian milik Direktorat Kenavigasian, dan Bea Cukai. Seperti yang disajikan dalam diagram berikut ini:



Gambar 4.3 Kolaborasi Digital Aplikasi Inaportnet

Sumber: Data Internal Direktorat Lalu Lintas dan Angkutan Laut, DIrektorat Jenderal Perhubungan Laut

Aplikasi Inapornet digunakan untuk menunjang kegiatan kepelabuhanan agar lebih efektif, efisien, cepat, dan transparan. Aplikasi ini telah digunakan di 16 pelabuhan di Indonesia. Selain itu, seluruh data dan informasi dalam Inapornet ini saling terhubung ke kantor pusat melalui *cloud computing*. Pemanfaatan teknologi Inaportnet untuk memaksimalkan pelayanan kapal dan barang di pelabuhan mempunyai aspek pendukung

dan penghambat terutama dalam sistem pengamanan informasinya. Tabel berikut menunjukkan beberapa aspek pendukung dan penghambat dalam penggunaan aplikasi Inaportnet:

Tabel 4.1 Aspek Pendukung dan Penghambat aplikasi Inaportnet

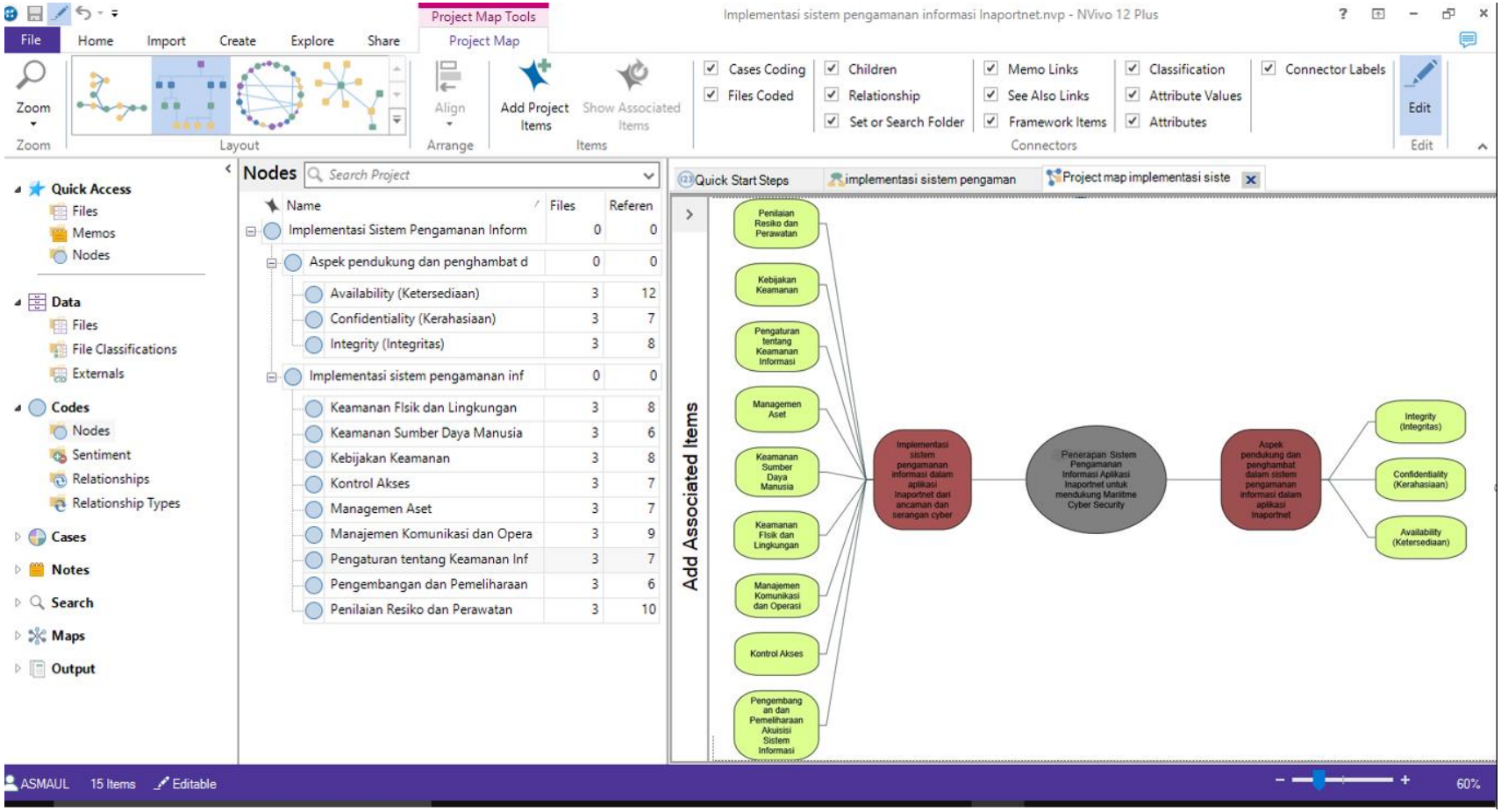
No.	Pendukung	Penghambat
1.	Sistem keamanan informasi aplikasi Inapornet didukung oleh kerjasama dengan Telkomsigma sebagai penyedia Data Center dan aplikasi	Tidak adanya jadwal yang pasti dari Ditlala untuk melakukan uji berkala sistem keamanan informasi dalam aplikasi Inapornet
2.	Sistem keamanan informasi sudah menggunakan standar ISO 27001 untuk Sistem Manajemen Keamanan Informasi (SMKI)	Kesadaran secara personal akan pentingnya informasi di dalam aplikasi Inapornet dapat dinilai masih kurang
3.	Sistem keamanan berlaku 24x7	Service center yang kecil
4.	Sistem keamanan tidak hanya dilakukan secara virtual, namun juga sistem keamanan yang menyangkut bangunan data center dan perangkat itu sendiri	Ketika salah satu sistem milik instansi lain yang tergabung dalam Inaportnet mengalami gangguan maka seluruh sistem Inaportnet akan mengalami gangguan
5.	Semua aplikasi milik stakeholder terkait kegiatan kepelabuhanan telah terintegrasi dengan Inaportnet	Belum adanya *handbook* khusus keamanan informasi Inaportnet untuk para stakeholder tersebut

Sumber: Hasil olahan peneliti dari berbagai sumber (2018)

4.1.3 Hasil Pengolahan Data dengan NVivo

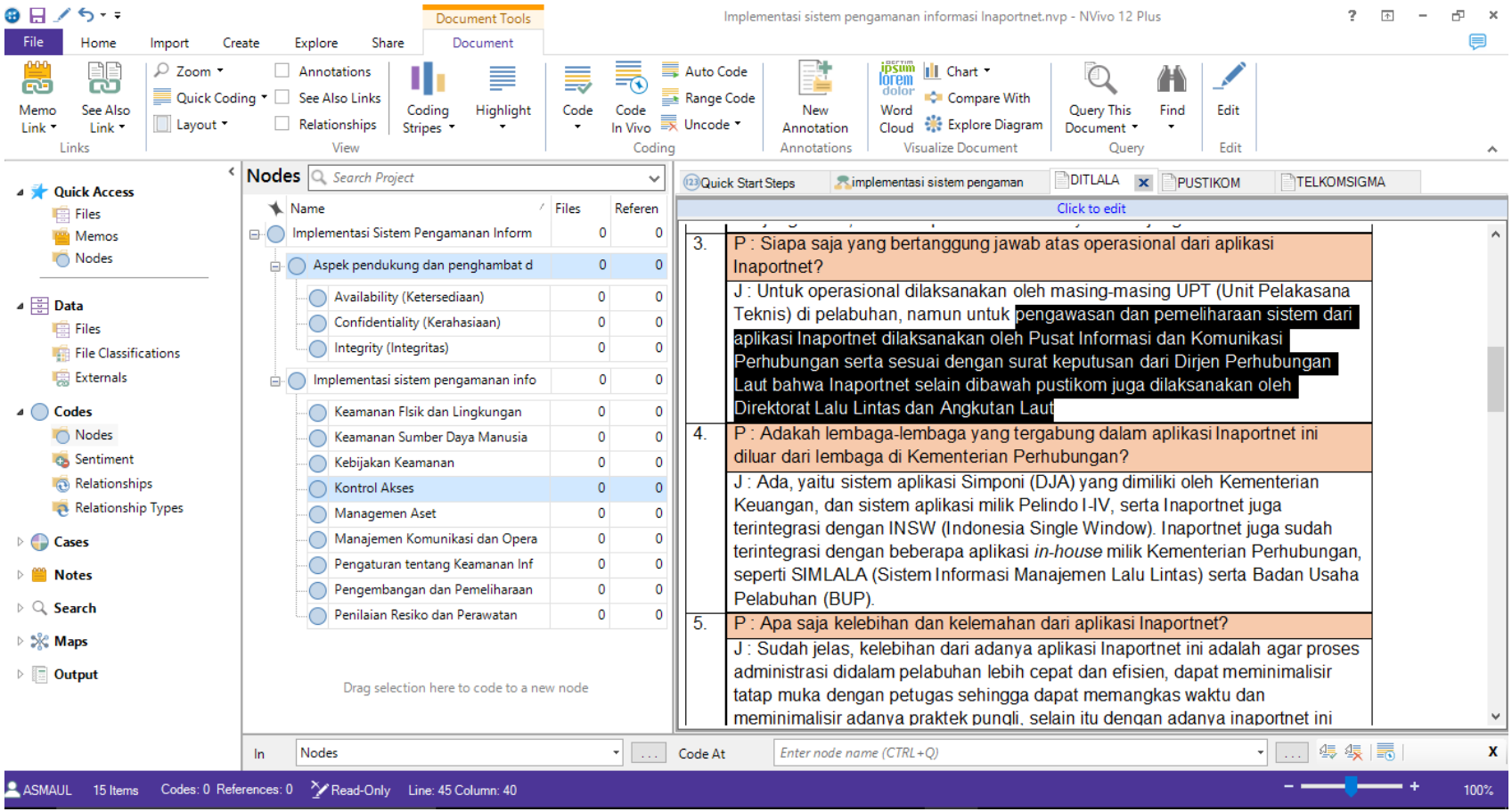
Pengolahan data dalam penelitian ini mengunakan *software* NVivo. *Software* ini digunakan untuk membantu menyusun tema dan mengeksplorasi tentang bagaimana hubungan antar atribut atau hal-hal tematik yang ditemukan dilapangan. *Nodes* untuk penelitian Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk Mendukung *Maritime Cyber Security* merupakan koding yang diturunkan dari rumusan masalah. Rumusan masalah diturunkan menjadi pertanyaan penelitian 1 dan 2, dimana terdapat tema besar di dalam masing-masing pertanyaan penelitian. Kemudian masing-masing pertanyaan penelitian diturunkan

kembali menjadi koding yang berdasarkan kepada teori implementasi keamanan informasi dan teori keamanan informasi. Agar lebih mudah, peneliti membuat *mind map* penelitian terlebih dahulu, seperti yang disajikan dalam gambar dibawah ini:



Gambar 4.4 Mind map penelitian hasil dari NVivo

Sumber: Hasil olahan peneliti menggunakan Nvivo



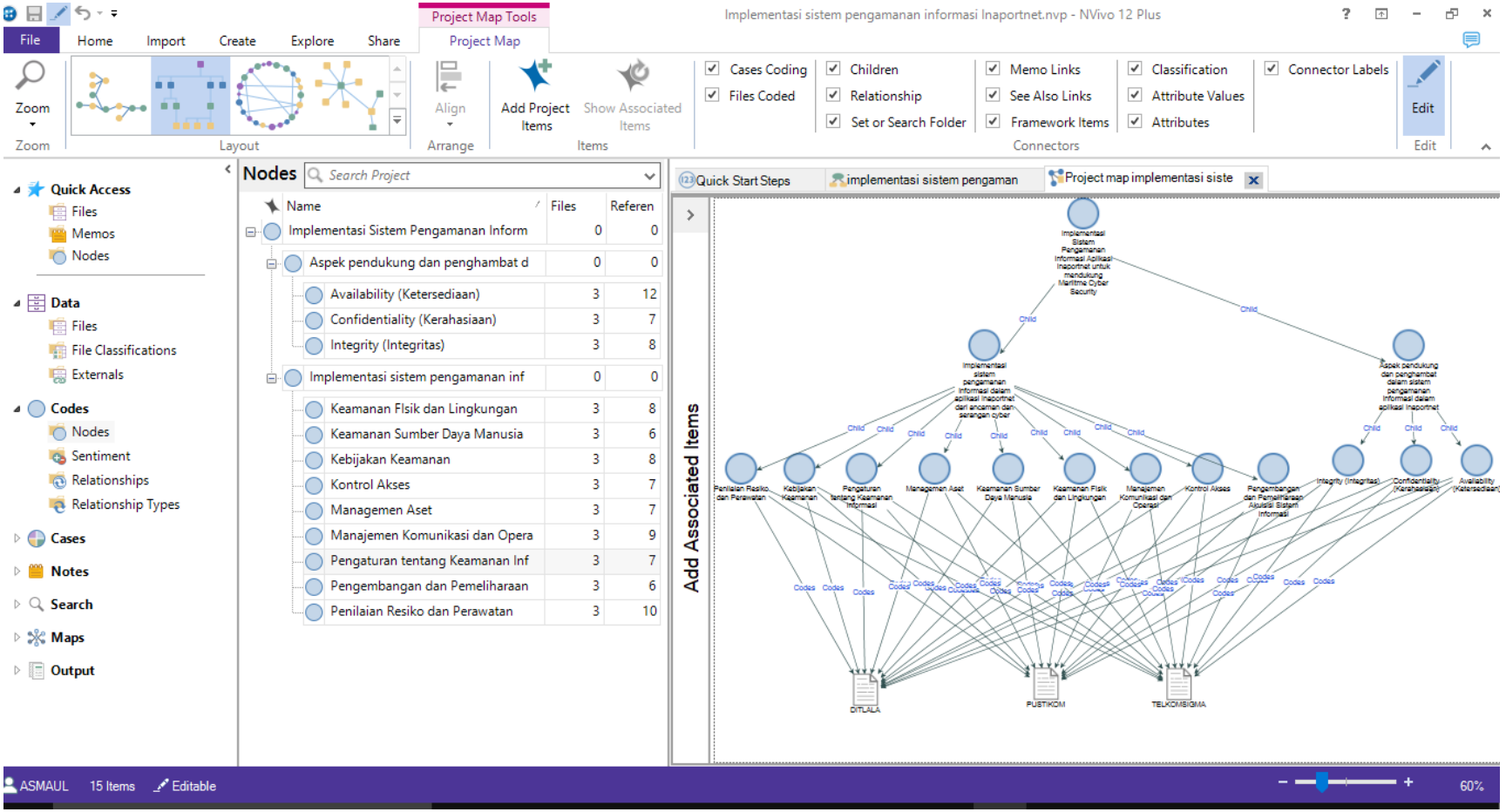
Gambar 4.5 Proses Koding dalam *Software* NVivo

Sumber: Hasil olahan peneliti menggunakan Nvivo

Pertanyaan penelitian 1 dibuat kedalam bentuk pernyataan menjadi "*Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet dari ancaman dan serangan cyber"* diturunkan menjadi *Nodes* berdasarkan teori implementasi keamanan informasi. *Nodes* yang dibuat berdasarkan komponen dalam teori implementasi keamanan informasi yang terdiri dari 9 komponen yaitu (1) Keamanan Fisik dan Lingkungan, (2) Keamanan Sumber Daya Manusia, (3) Kebijakan Keamanan, (4) Kontrol Akses, (5) Manajemen Aset, (6) Manajemen Komunikasi dan Operasi, (7) Pengaturan tentang Keamanan Informasi, (8) Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi, dan (9) Penilaian Resiko dan Perawatan.

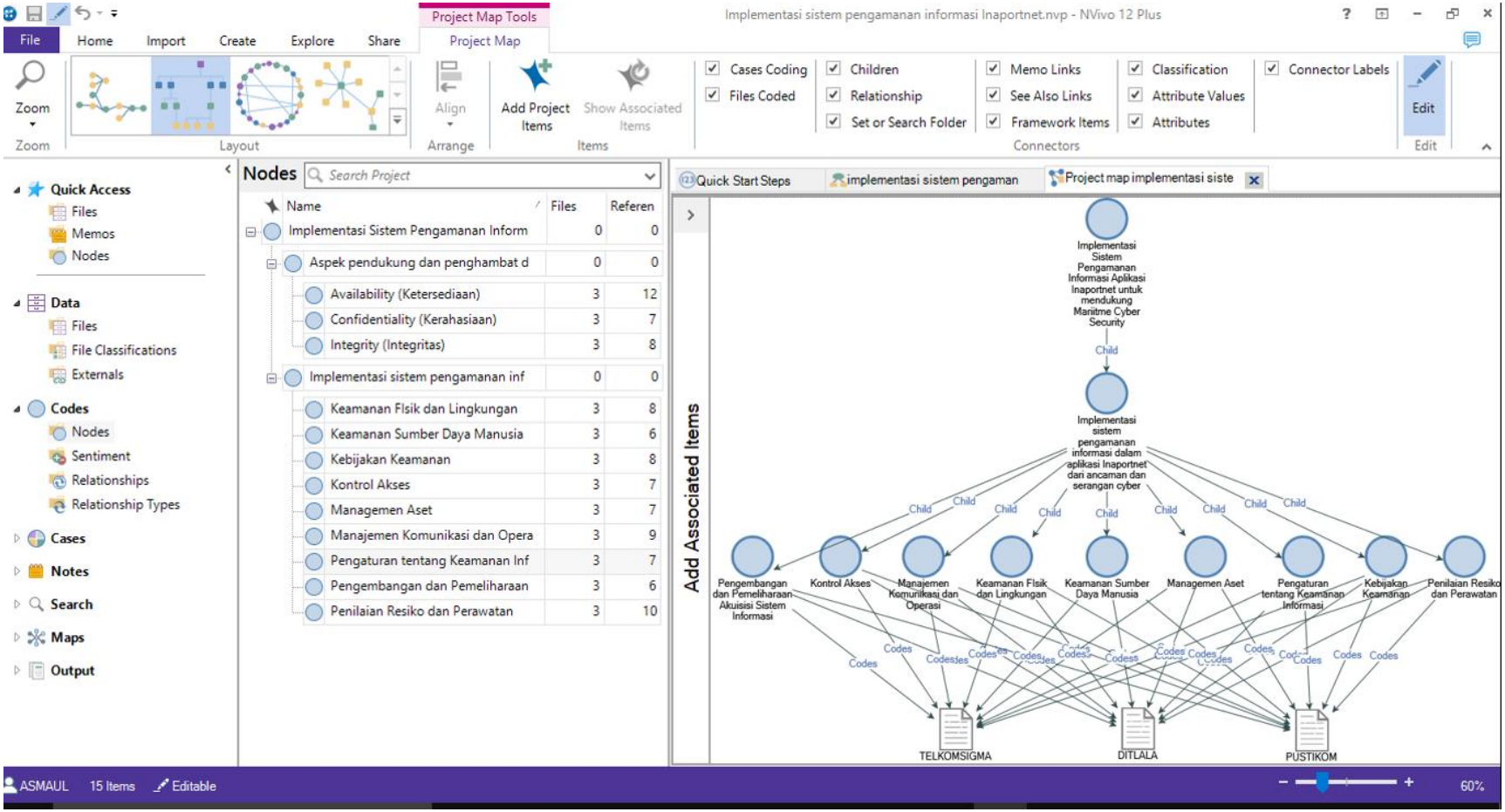
Pertanyaan penelitian ke 2 juga dibuat kedalam bentuk pernyataan menjadi "*Aspek pendukung dan penghambat dalam sistem pengamanan informasi yang terdapat dalam aplikasi Inapornet*". Pernyataan penelitian ke dua diturunkan menjadi bentuk *nodes* dengan berdasar kepada teori keamanan informasi. Di mana teori keamanan informasi terdiri dari 3 aspek utama yaitu integritas (*integrity*) yaitu data/informasi yang tidak bisa dirubah, ketersediaan (*availability*) yaitu sumber daya selalu tersedia, dan kerahasiaan (*confidentiality*) berhubungan dengan kerahasiaan data dan hak akses.

Tahap selanjutnya adalah melakukan pengkodingan terhadap transkrip hasil wawancara. Seluruh transkrip disisir satu per satu untuk dilakukan koding. Hasilnya berupa diagram yang menunjukkan hubungan antara *nodes* dengan transkrip wawancara. Hasilnya adalah sebagai berikut:



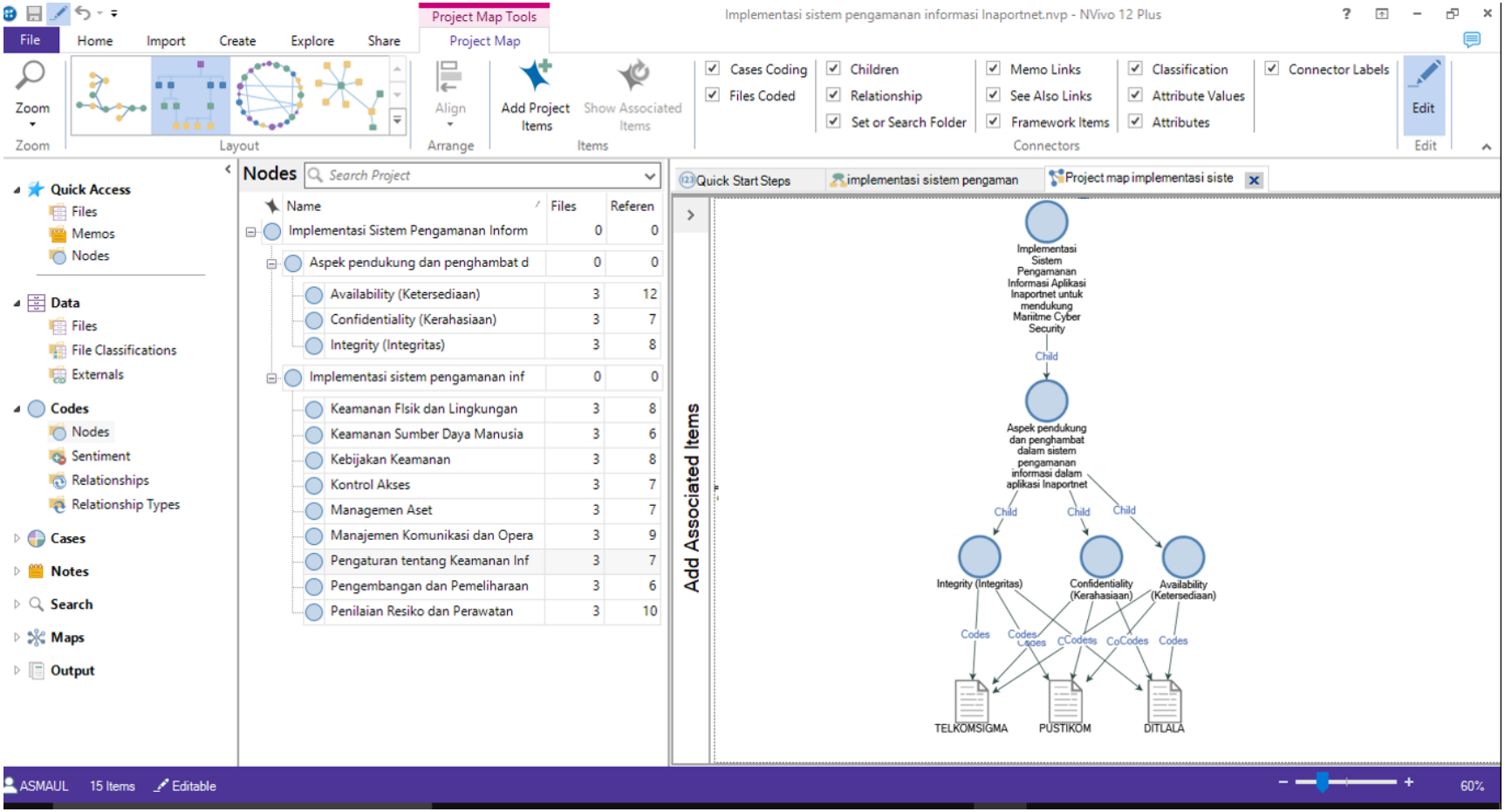
Gambar 4.6 Bagan Triangulasi atas Rumusan Masalah

Sumber: Hasil olahan peneliti menggunakan Nvivo



Gambar 4.7 Bagan Triangulasi terhadap Pertanyaan Penelitian 1

Sumber: Hasil olahan peneliti menggunakan Nvivo



Gambar 4.8 Bagan Triangulasi terhadap Pertanyaan Penelitian 2

Sumber: Hasil olahan peneliti menggunakan Nvivo

4.1.4 Analisa Data dan Interpretasi Hasil

Proses analisa data dalam penelitian ini menggunakan *Soft System Methodolgy* (SSM). Proses dalam SSM terdiri dari 7 langkah. Langkah 1 (pertama) tentang penentuan permasalahan penelitian telah dilakukan pada bab pendahuluan. Pada subbab ini, akan membahas langkah dari analisis SSM untuk langkah ke 2 (Penggambaran masalah / *rich picture*) hingga langkah ke 5 (perbandingan antara model konseptual dengan kenyataan).

4.1.4.1 Analisis Satu (Intervensi)

Tahap pertama dalam analisis satu yaitu memahami situasi permasalahan yang dikemukakan dalam penelitian. Dalam tahap ini instrumen atau pihak - pihak yang terkait pada permasalahan ditentukan. Menurut Checkland (2006) terdapat tiga kategori pihak yang termasuk atau terkait dengan penelitian yaitu Klien, Praktisi dan Pemilik Isu.

a. Klien (*Clients*)

   Klien (*Clients*) merupakan individu atau kumpulan individu yang menyebabkan terjadinya sebuah intervensi terkait situasi problematis yang sedang dikaji. Dalam penelitian ini yang bertindak sebagai klien (*Clients*) adalah pembimbing 1 yaitu Laksamana Muda TNI Dr. Amarulla Octavian, S.T., M.Sc., D.E.S.D., dan pembimbing 2 yaitu Dr. Herlina Juni Saragih, serta peneliti yaitu Asmaul Mufidasari.

b. Praktisi (*Practitioners*)

   Praktisi (*Practititoners*) merupakan individu atau kumpulan individu yang melakukan kajian penelitian dengan menggunakan metode *Soft System Methodology* (SSM). Dalam penelitian ini yang bertindak sebagai praktisi (*Practititoners*) adalah Asmaul Mufidasari.

c. Pemilik Isu (*Owners*)

   Pemilik Isu (*Owners*) merupakan individu atau kumpulan individu yang terkena dampak atau berkepentingan dari hasil atas upaya perbaikan situasi problematik. Dalam penelitian ini yang bertindak

sebagai *owners* adalah Kementerian Perhubungan (Direktorat Lalu Lintas dan Angkutan Laut serta Pusat Teknologi Informasi dan Komunikasi Perhubungan), dan Telkomsigma.

4.1.4.2 Analisis Dua (Sosial)

Analisis sosial yang termasuk kedalam tahap analisis dua akan menggambarkan obyek penelitian secara lebih mendetail. Analisis sosial terdiri dari tiga elemen yaitu elemen peran, norma, dan nilai. Berikut adalah penjabaran dari masing-masing analisis sosial:

a. Elemen peran (role)

Sebelum menentukan elemen peran, hal yang perlu dilakukan adalah mengidentifikasi siapa saja aktor-aktor yang terlibat dalam penelitian ini. Dalam analisis intervensi (analisis satu) telah disebutkan bahwa pemilik isu (*owners*) dari penelitian ini terdiri dari tiga aktor yaitu Direktorat Lalu Lintas dan Angkutan Laut (Ditlala) dan Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom) yang bertugas untuk pemeliharaan dan pengawasan aplikasi Inaportnet. Kemudian aktor ketiga yaitu Telkomsigma, perusahaan di bidang ICT yang mendukung kinerja dari aplikasi Inaportnet baik itu dalam aplikasi maupun *data base*.

Dalam penelitian ini peran dari Direktorat Lalu Lintas dan Angkutan Laut (Ditlala) dan Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom) adalah sebagai pengawas dari sistem aplikasi Inaportnet. Sedangkan peran dari Telkomsigma adalah sebagai pelaksana (pendukung) pengamanan dan penyedia baik untuk aplikasi maupun *data base*nya. Sehingga keamanan informasi dari sistem aplikasi Inaportnet bergabung dengan layanan yang diberikan oleh Telkomsigma. Sebagai penyedia (pendukung) dalam sistem keamanan informasi aplikasi Inaportnet tentu performa dari layanan yang diberikan oleh Telkomsigma sangat diperhitungkan. Peran dari masing-masing aktor akan disajikan dalam tabel berikut ini:

Tabel 4.2 Pembagian pada Elemen Peran

Pengawas dan regulator	**Direktorat Lalu Lintas dan Angkutan Laut** Direktorat Lalu Lintas dan Angkutan Laut (Ditlala) berperan sebagai regulator dan pengawas terhadap aplikasi Inapornet. Sesuai dengan salah satu fungsinya yaitu untuk penyiapan pelaksanaan kebijakan di bidang lalu lintas dan angkutan laut dalam dan luar negeri, angkutan laut khusus, usaha jasa angkutan laut, sistem informasi angkutan laut dan sarana prasarana angkutan laut. Namun pengawasan yang dilakukan Ditlala lebih kepada pengawasan untuk kelancaran operasional dan pelayanan Inaportnet.
	Pusat Teknologi Informasi dan Komunikasi Perhubungan Bersama-sama dengan Ditlala, Pusat Teknologi Informasi dan Komunikasi Perhubungan (Pustikom) bertugas sebagai pemelihara dan pengawas terhadap aplikasi Inaportnet. Sesuai dengan salah satu fungsi dari Pustikom yaitu penyiapan pengelolaan data dan layanan operasional sistem teknologi informasi dan komunikasi. Peran pengawasan dari pustikom adalah untuk mengawasi kelancaran jaringan dalam operasional Inaportnet.
Penyedia dan Pelaksana	**Telkomsigma** Peran dari Telkomsigma untuk sistem pengamanan informasi yang terjadi dalam aplikasi Inaportnet sangat signifikan. Hal ini dikarenakan Telkomsigma-lah penyedia jasa keamanan serta pemeliharaan reguler untuk aplikasi dan data center untuk Inapornet. Sehingga sistem keamanan informasi yang digunakan untuk aplikasi Inaportnet mengikuti standar yang digunakan oleh Telkomsigma.

b. Elemen norma (*norms*)

Elemen norma merupakan elemen yang menjelaskan tentang kriteria, standar atau ketentuan yang berlaku sesuai dengan penelitian. Norma yang digunakan dalam penelitian ini adalah segala peraturan atau pedoman baik tertulis yang terkait dengan bagaimana Direktorat

Lalu Lintas dan Angkutan Laut, Pusat Teknologi Informasi dan Komunikasi Perhubungan serta Telkomsigma berkolaborasi menciptakan sistem keamanan informasi yang ada di dalam aplikasi Inaportnet guna mendukung *Maritime Cyber Security*.

Norma yang digunakan dalam penelitian ini berdasar kepada beberapa dokumen yang dijadikan sebagai pedoman, seperti Peraturan Menteri Perhubungan Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan sebagaimana telah diubah kedalam Peraturan Menteri Perhubungan Nomor PM 192 Tahun 2015, Peraturan Direktur Jenderal Perhubungan Laut Nomor HK.103/3/11/DJPL-15 tentang Tata Cara Pelayanan Kapal dan Barang Menggunakan Inaportnet di Pelabuhan, Standar ISO 27001 untuk Sistem Manajemen Keamanan Informasi.

c. Elemen nilai (*value*)

Dalam penelitian ini yang dimaksud dengan elemen nilai adalah aspek kebenaran dari seluruh informan yang terlibat serta bagaimana penerjemahannya di lapangan. Nilai tersebut mengacu pada aspek sistem keamanan informasi dalam aplikasi Inaportnet untuk mendukung *Maritime Cyber Security*. Dalam penelitian ini melihat pandangan dari informan terkait (i) Implementasi dari sistem pengamanan informasi untuk aplikasi Inaportnet dan isu dari serangan *cyber* dan (ii) Aspek pendukung dan penghambat aplikasi Inaportnet dari sisi sistem pengamanan informasinya baik secara *software*, *hardware,* maupun lingkungannya. Nilai yang didapat adalah sebagai berikut:

(i) Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet:

1. Sebagian besar informan menyadari akan ancaman *cyber* namun kegiatan pendukung seperti *penetration test* tidak terjadwal hanya dianggarkan pertahun dan tidak terjadwal secara rutin.

2. Kerjasama dengan pihak ketiga membuat sistem pengamanan informasi dalam Inapornet baik aplikasi dan *data base*-nya diserahkan ke pihak ke tiga (Telkomsigma).

(ii) Aspek Pendukung dan Penghambat Sistem Pengamanan Informasi dalam aplikasi Inaportnet:

1. Sistem Pengamanan Informasi yang digunakan akan menjamin seberapa aman infomasi dan data-data yang terdapat / melalui aplikasi Inaportnet.
2. Kerjasama dengan pihak ketiga (Telkomsigma) dalam penanganan Sistem Pengamanan Informasi dalam aplikasi Inaportnet membuat performa layanan Inaportnet semakin prima.

4.1.4.3 Analisis Tiga (Politik)

Analisis politik merupakan analisis yang menentukan sesuatu boleh dilakukan atau tidak. Analisis politik akan menguraikan struktur kekuasaan dalam sebuah situasi dan menentukan bagaimana mengatasinya. Analisis politik terdiri dari pembahasan tentang Disposition of Power dan Nature of Power yang dikaji dari setiap institusi terkait dengan penelitian ini.

a. Disposition of Power

Direktorat Lalu Lintas dan Angkutan Laut merupakan direktorat dibawah Direktorat Jenderal Perhubungan Laut. Direktorat Lalu Lintas dan Angkutan Laut merupakan pengawasan dan regulator dari aplikasi Inaportnet. Untuk pengawasan ini Direktorat Lalu Lintas dan Angkutan Laut dibantu oleh Pusat Teknologi Informasi dan Komunikasi Perhubungan. Pusat Teknologi Informasi dan Komunikasi Perhubungan merupakan unsur penunjang di dalam Sekretariat Perhubungan. Segala kebijakan yang terdapat dari Inaportnet dikeluarkan oleh Direktorat Jenderal Perhubungan Laut berdasar kepada Undang-undang Nomor 17 Tahun 2008 tentang Pelayaran, Peraturan Menteri Perhubungan Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan sebagaimana telah diubah

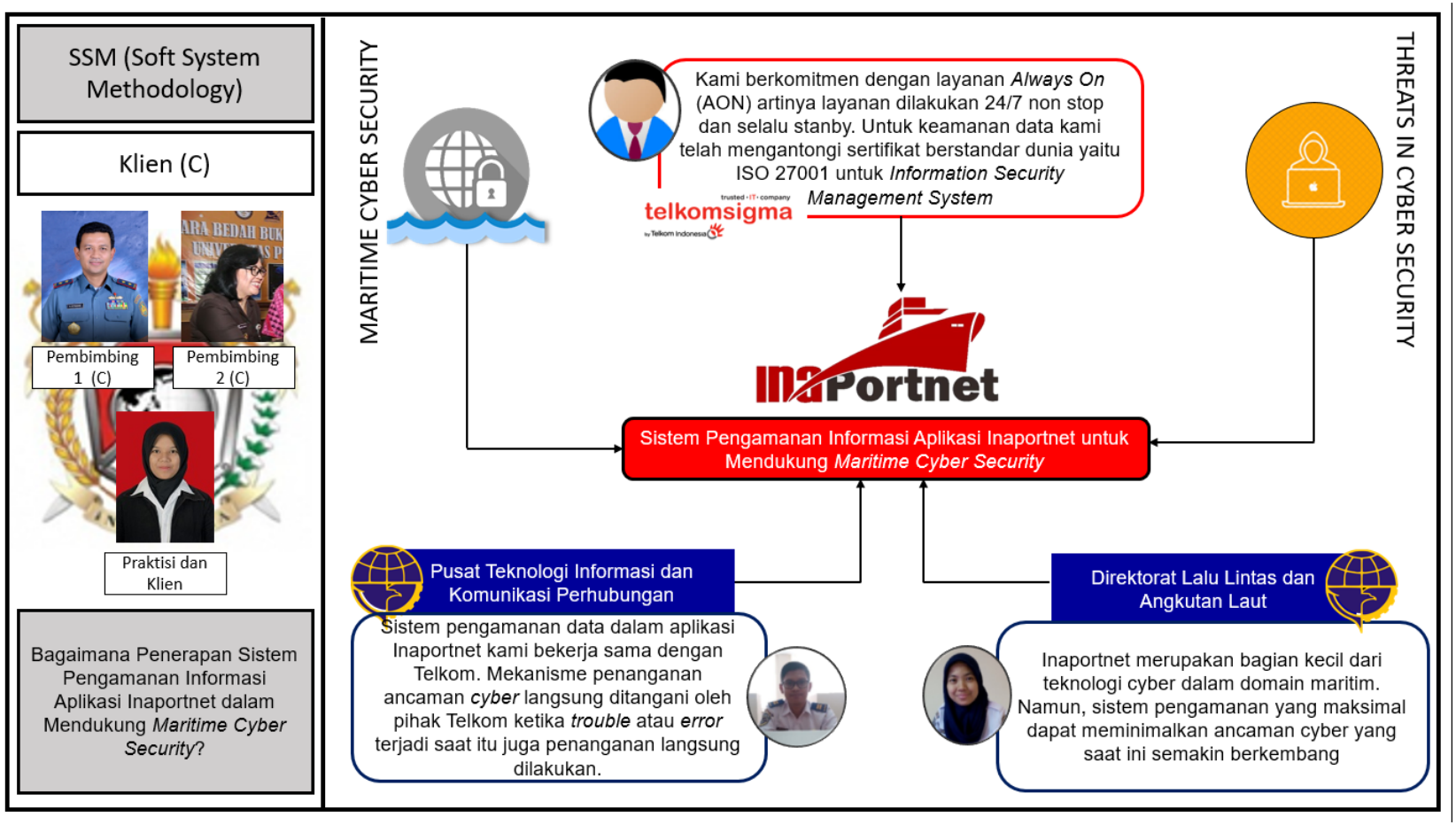
kedalam Peraturan Menteri Perhubungan Nomor PM 192 Tahun 2015, serta ISO 27001 yang merupakan standar internasional untuk manajemen sistem keamanan informasi. Telkomsigma sebagai pihak ketiga dalam pelaksanaan sistem pengamanan dalam aplikasi Inaportnet merupakan ujung tombak dari keamanan aplikasi ini. Hal ini dikarenakan baik aplikasi dan *data base* dari Inaportnet menggunakan layanan dari Telkomsigma.

b. *Nature of Power*

Era digital telah memasuki ranah domain maritim Indonesia. Hal ini dilakukan agar pelayanan terutama untuk di pelabuhan selain menjadi lebih cepat, transparan, murah juga berdaya saing dengan pelabuhan-pelabuhan internasional di negara lain. Indonesia saat ini dengan visi sebagai Poros Maritim Dunia perlahan-lahan mulai membangun infrastruktur di bidang kemaritiman. Pembangunan infrastruktur yang ada diimbangi dengan pembangunan dalam bidang infostrukturnya (teknologi informasi). Salah satunya adalah Inaportnet ini yang membantu pemerintah dalam hal pembangunan teknologi informasi di bidang kepelabuhanan.

4.1.4.4 *Rich Picture*

Untuk memperoleh gambaran keseluruhan atas permasalahan dan temuan dari penelitian maka dilakukan *Rich Picture*. *Rich Picture* merupakan gambaran dari langkah SSM sebelumnya, di mana hasil dari pengambilan data ditampilkan dalam bentuk rancang gambar. Di dalam rancang gambar ini terdapat pandangan dari masing-masing informan terkait dengan isu penelitian yang dibahas, yaitu bagaimana kelemahan dan keunggulan dari sistem pengamanan informasi dalam aplikasi Inapornet dan bagaimana implementasinya untuk mendukung *Maritime Cyber Security*. Berikut adalah gambar dari rich picture yang dihasilkan:



Gambar 4.9 *Rich Picture*

Sumber : Hasil olahan peneliti

4.1.4.5 *System Thinking*

Proses ketiga dari analisis SSM setelah membuat rich picture adalah pembuatan root definition. Root definition berfungsi untuk mengetahui apakah penyelesaian masalah sudah cukup relevan dengan situasi problematis dari penelitian ini. Hasil dari analisa tahap ini berupa Conseptual Model.

a. Root Definition

Root definition akan dirumuskan ke dalam dua pertanyaan yang mewakili pertanyaan penelitian. Pembahasan Root definition menggunakan rumus PQR yang digunakan untuk menjawab pertanyaan Apa, Mengapa, dan Bagaimana, rumus PQR adalah sebagai berikut:

"Melakukan P dengan Q untuk mencapai R"

Root definition yang telah dirumuskan akan diuji dan disempurnakan dengan penggunaan analisa CATWOE (*Customers, Actors, Transformation, Worldview, Owners, Environtment*). Identifikasi dengan menggunakan CATWOE sesuai dengan langkah-langkah dalam pengolahan data SSM. Model Konseptual yang nantinya akan dibuat berdasarkan hasil identifikasi dari CATWOE.

Selanjutnya hasil dari CATWOE akan dianalisa lebih lanjut dengan kriteria '3E'. '3E' digunakan untuk mengukur kinerja dari sistem aktivitas tersebut. '3E' terdiri dari 'E' pertama adalah *Efficacy* yang menunjukkan apakah proses transformasi tersebut dapat benar-benar diwujudkan dalam hasil yang diinginkan, 'E' kedua yaitu *Efficiency* yang menunjukkan apakah proses tersebut dapat berlangsung secara efisien dengan penggunaan sumber daya yang minimal. 'E' ketiga adalah *Effectiveness* yang menunjukkan apakah proses tersebut dapat membantu tercapainya tujuan jangka panjang dari rumus PQR. Penilaian kriteria '3E' ini diharapkan akan menjawab obyek penelitian.

Tabel 4.3 Root Definition Penelitian

Root Definition	**Pertanyaan Penelitian (dalam bentuk pernyataan)**	***Relevant System***
RD-1	Implementasi sistem pengamanan informasi dalam aplikasi Inaportnet dari ancaman dan serangan cyber	Menerapkan standar keamanan informasi (P) dengan mengimplementasikannya dalam aplikasi Inaportnet (Q) untuk menangani ancaman dan serangan cyber (R).
RD-2	Aspek pendukung dan penghambat dalam sistem pengamanan informasi yang terdapat dalam aplikasi Inapornet	Menjadikan aspek pendukung dan penghambat aplikasi Inaportnet (P) dengan memaksimalkan kondisi sistem keamanan informasi (Q) untuk mencapai sistem integrasi yang aman (R)

Tabel 4.4 RD-1 Analisa CATWOE dan Kriteria 3E

RD-1	Menerapkan standar keamanan informasi (P) dengan mengimplementasikannya dalam aplikasi Inaportnet (Q) untuk menangani ancaman dan serangan cyber (R).
ANALISA CATWOE	
C (*Customer*)	Sistem Keamanan Informasi dalam aplikasi dan *data base* Inaportnet
A (*Actor*)	Telkomsigma
T (*Transfomation*)	Penerapan standar keamanan informasi baik secara virtual maupun fisik untuk aplikasi Inaportnet
W (*Worldview*)	Standar keamanan informasi yang digunakan dapat menjadi pendukung untuk meminimalisir adanya ancaman dan serangan cyber
O (*Owners*)	Direktorat Jenderal Perhubungan Laut
E (*Environment*)	Tidak ada jadwal yang tetap untuk melakukan *penetration test* dari Direktorat Lalu Lintas dan Angkutan Laut sendiri

KRITERIA 3E	
Efficacy	Sebagai partner dari Kementerian Perhubungan, Telkomsigma keamanan informasi yang ditawarkan untuk keamanan *data base* dan aplikasi dapat dilihat dari sertifikat ISO 27001 yaitu yang merupakan standar Internasional untuk manajemen keamanan informasi. Untuk elemen *information security awareness* dapat diwujudkan dalam bentuk *information security handbook* sebagai bentuk representatif dari kebijakan keamanan informasi dalam aplikasi Inaportnet.
Efficiency	Kerjasama antara Telkomsigma dan Kementerian Perhubungan sangat menguntungkan, salah satunya adalah jaminan kerahasian, kelangsungan, keamanan, serta kemudahan akses untuk aplikasi Inaportnet. Selain itu, untuk perawatan reguler dilakukan secara terpusat, sehingga memudahkan dalam melakukan *monitoring*.
Effectiveness	Standar yang digunakan oleh Telkomsigma untuk manajemen keamanan informasi adalah ISO 27001. Standar ini merupakan standar internasional yang diberlakukan terutama untuk industri/bisnis/organisasi yang bergerak dalam bidang IT. Mempertahankan standar ini dapat terbilang sulit, karena evaluasi dilakukan setiap 6 bulan sekali, banyaknya aspek-aspek yang diuji/diaudit sehingga standar ini merupakan penjamin keamanan informasi dalam data center Telkomsigma

Tabel 4.5 RD-2 Analisa CATWOE dan Kriteria 3E

RD-2	Menjadikan aspek pendukung dan penghambat aplikasi Inaportnet (P) dengan memaksimalkan kondisi sistem keamanan informasi (Q) untuk mencapai sistem integrasi yang aman (R)
ANALISA CATWOE	
C (*Customer*)	Aplikasi Inaportnet beserta aplikasi-aplikasi yang terintegrasi dengannya
A (*Actor*)	Direktorat Lalu Lintas dan Angkutan Laut serta Pusat Teknologi Informasi dan Komunikasi Perhubungan

T (*Transfomation*)	Menggunakan prinsip dasar keamanan informasi dalam aplikasi Inaportnet untuk mengetahui penghambatnya
W (*Worldview*)	Sebagai aplikasi sistem yang mengintegrasikan seluruh aplikasi lainnya yang terkait dengan kegiatan kepelabuhanan, arus informasi dan data dalam Aplikasi Inaportnet terjadi begitu cepat dan transparan. Hal ini memiliki arti bahwa sistem keamanan informasi dalam aplikasi Inapornet sangat penting adanya untuk melindungi dari ancaman-ancaman yang ada
O (*Owners*)	Direktorat Jenderal Perhubungan Laut
E (*Environment*)	Belum adanya *handbook* tentang keamanan informasi khusus untuk aplikasi Inaportnet.
KRITERIA 3E	
Efficacy	Prinsip keamanan informasi pada aplikasi Inapornet dikaji agar mengetahui celah atau kelemahan sistem pengamanan informasi dari aplikasi Inaportnet
Efficiency	Prinsip keamanan informasi sebenarnya digunakan sebagai parameter untuk menguji sejauh mana aplikasi Inaportnet menerapkan parameter-parameter tersebut untuk sistem keamanan informasinya
Effectiveness	Dengan mengetahui penghambat yang ada pada sistem pengamanan aplikasi inapornet. Maka penghambat tersebut dapat segera ditangani. Sehingga keamanan informasi dalam aplikasi Inapornet dapat terjalin secara terus menerus.

b. Model Konseptual

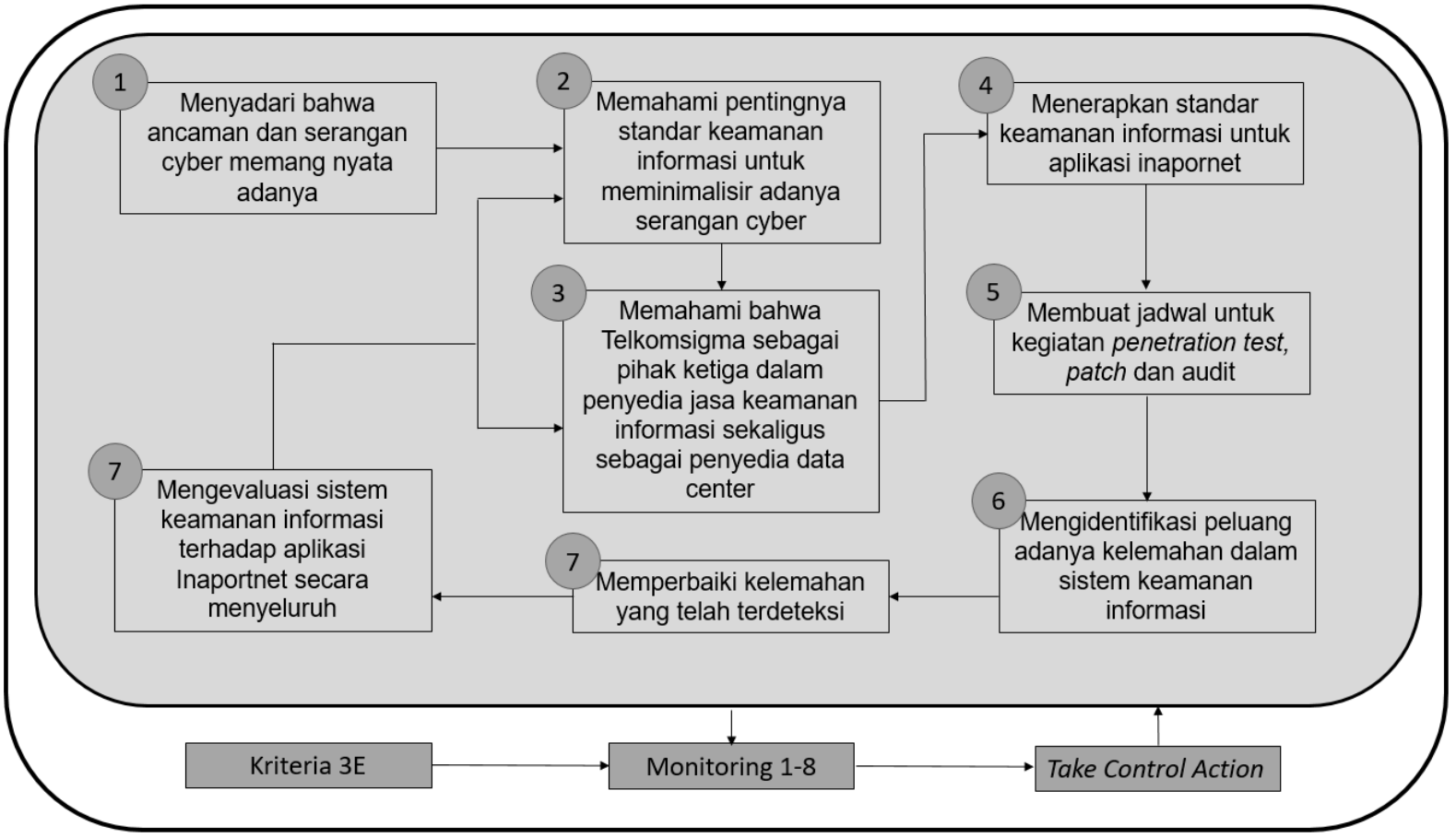
Tahapan dalam analisis SSM selanjutnya adalah pembentukan model konseptual yang merupakan tahap ke empat dari tujuh tahap yang ada. Pembentukan model konseptual menghubungkan seluruh kegiatan yang dilakukan dalam proses T pada analisa CATWOE sehingga menjadi suatu sistem yang utuh. Langkah ini merupakan langkah yang menggabungkan seluruh langkah yang terdapat pada tahap ke 3 (root definition) untuk menentukan sistem yang relevan dan dapat digunakan dalam menyelesaikan permasalahan penelitian.

Tabel 4.6. Model Konseptual dalam RD-1

RD-1	Aktivitas	Deksripsi Aktivitas
Menerapkan standar keamanan informasi (P) dengan mengimplementasikannya dalam aplikasi Inaportnet (Q) untuk menangani ancaman dan serangan cyber (R).	Aktivitas 1	Menyadari bahwa ancaman dan serangan cyber memang nyata adanya
	Aktivitas 2	Memahami pentingnya standar keamanan informasi untuk meminimalisir adanya serangan cyber
	Aktivitas 3	Memahami bahwa Telkomsigma sebagai pihak ketiga dalam penyedia jasa keamanan informasi
	Aktivitas 4	Menerapkan standar keamanan informasi untuk aplikasi inapornet
	Aktivitas 5	Membuat jadwal untuk kegiatan *penetration test, patch* dan audit secara berkala
	Aktivitas 6	Mengidentifikasi peluang adanya kelemahan dalam sistem keamanan informasi
	Aktivitas 7	Memperbaiki kelemahan yang telah terdeteksi
	Aktivitas 8	Mengevaluasi sistem keamanan informasi terhadap aplikasi Inaportnet secara menyeluruh

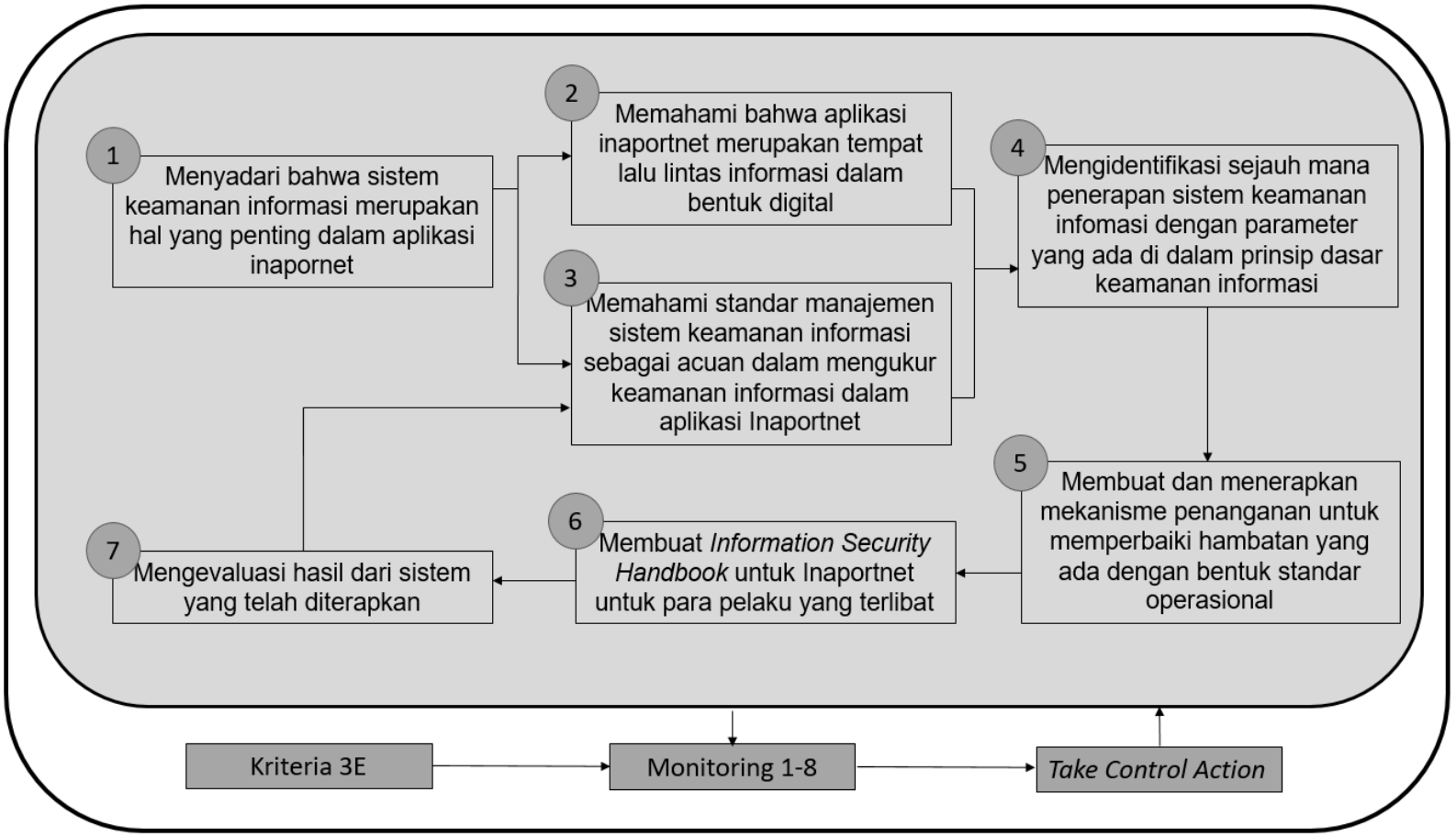
Tabel 4.7 Model Konseptual dalam RD-2

RD-2	Aktivitas	Deksripsi Aktivitas
Menjadikan aspek pendukung dan penghambat aplikasi Inaportnet (P) dengan memaksimalkan kondisi sistem keamanan informasi (Q) untuk mencapai sistem integrasi yang aman (R)	Aktivitas 1	Menyadari bahwa sistem keamanan informasi merupakan hal yang penting dalam aplikasi inapornet
	Aktivitas 2	Memahami bahwa aplikasi inaportnet merupakan tempat lalu lintas informasi dalam bentuk digital
	Aktivitas 3	Memahami standar manajemen sistem keamanan informasi sebagai acuan dalam mengukur keamanan informasi dalam aplikasi Inaportnet
	Aktivitas 4	Mengidentifikasi sejauh mana penerapan sistem keamanan infomasi dengan parameter yang ada di dalam prinsip dasar keamanan informasi
	Aktivitas 5	Membuat dan menerapkan mekanisme penanganan untuk memperbaiki hambatan yang ada
	Aktivitas 6	Membuat *Information Security Handbook* untuk Inaportnet untuk para pelaku yang terlibat
	Aktivitas 7	Mengevaluasi hasil dari sistem yang telah diterapkan



Gambar 4.10 Model Konseptual dan Aktifitas dari RD-1

Sumber : Hasil Olahan Peneliti



Gambar 4.11 Model Konseptual dan Aktifitas dari RD-2

Sumber : Hasil Olahan Peneliti

4.1.4.6 Perbandingan Model Konseptual dengan Realitas

Tahap kelima dari analisis SSM adalah perbandingan dari model konseptual dengan realitas yang terjadi nyata di lapangan. Dari berbagai temuan yang didapatkan, temuan tersebut akan dijadikan sebagai rumusan untuk tindakan perbaikan yang dapat direkomendasikan sebagai penyelesaian permasalahan di lapangan. Perbandingan ini dibuat berdasarkan model konseptual yang telah dibuat sebelumnya. Peneliti selanjutnya menentukan pertanyaan untuk meriview situasi problematis di dunia nyata berdasarkan sistem aktivitas dalam model konseptual. Pertanyaan dibuat berdasarkan pemikiran logis dari peneliti sebagai praktisi SSM.

Tabel 4.8 Perbandingan Model Konseptual RD-1

No.	Aktivitas RD-1	Apakah kegiatan dalam model konseptual terjadi nyata di lapangan dan apakah memberikan solusi terhadap permasalahan yang terjadi?	Aktor yang berperan	Homogenisasi
1.	Menyadari bahwa ancaman dan serangan cyber memang nyata adanya	Belum terlalu terlaksana, secara sistem memang sudah dilakukan namun untuk kesadaran secara personal masih belum menganggap ancaman *cyber* sebagai hal yang prioritas.	Ditlala dan Pustikom	Ancaman cyber belum dianggap prioritas dalam operasional aplikasi Inapornet. Namun tindakan pencegahan telah dilakukan untuk mendukung sistem pengamanan informasinya.
2.	Memahami pentingnya standar keamanan informasi untuk meminimalisir adanya serangan cyber	Telah terlaksana, standar ISO 27001 menyediakan kerangka kerja untuk mencegah serangan cyber.	Telkomsigma	Standar ISO 27001 yang digunakan merupakan paket lengkap untuk mengamankan informasi dari segala bentuk ancaman *cyber*.
3.	Memahami bahwa Telkomsigma sebagai pihak ketiga dalam penyedia jasa keamanan informasi	Telah terlaksana, kerjasama telah dilakukan sejak tahun 2016 untuk aplikasi Inapornet.	Ditlala, Pustikom, dan Telkomsigma	Telkomsigma dipercaya sebagai perusahaan untuk mengurus data center beserta keamanan informasi dalam aplikasi Inapornet.
4.	Menerapkan standar keamanan informasi untuk aplikasi inapornet	Telah terlaksana, untuk manajemen sistem keamanan informasi menggunakan ISO 27001	Telkomsigma	Standar untuk keamanan informasi yaitu ISO 27001 menjamin terlindungnya aplikasi Inapornet dari penyalahgunaan akses

5.	Membuat jadwal untuk kegiatan *penetration test, patch* dan audit secara berkala	Aktivitas ini belum terlaksana	Ditlala	*Penetration test* dan *patching* dilaksanakan tidak terjadwal secara tetap, namun selalu dianggarkan setiap tahunnya.
6.	Mengidentifikasi peluang adanya kelemahan dalam sistem keamanan informasi	Telah terlaksana, kegiatan ini termasuk dalam audit untuk ISO 27001	Telkomsigma	Audit ISO 27001 dilakukan satu tahun sekali, berfungsi untuk mengupgrade sistem keamanan informasi yang digunakan di aplikasi inapornet
7.	Memperbaiki kelemahan yang telah terdeteksi	Telah terlaksana, kegiatan ini termasuk dalam audit untuk ISO 27001	Telkomsigma	
8.	Mengevaluasi sistem keamanan informasi terhadap aplikasi Inaportnet secara menyeluruh	Telah terlaksana, dengan audit untuk upgrade ISO 27001 yang diselenggarakan 1 tahun sekali	Telkomsigma	

Tabel 4.9 Perbandingan Model Konseptual RD-2

No.	Aktivitas RD-2	Apakah kegiatan dalam model konseptual terjadi nyata di lapangan dan apakah memberikan solusi terhadap permasalahan yang terjadi?	Aktor yang berperan	Homogenisasi
1.	Menyadari bahwa sistem keamanan informasi merupakan hal yang juga penting dalam aplikasi inapornet	Belum terlalu terlaksana, secara sistem memang sudah dilakukan namun untuk kesadaran secara personal masih belum menganggap keamanan informasi sebagai hal yang prioritas	Ditlala	Hal ini merupakan dasar untuk penggunaan informasi digital sebagai media informasi. Tidak hanya by system namun juga kesadaran personal harus ditumbuhkan
2.	Memahami bahwa aplikasi inaportnet merupakan tempat lalu lintas informasi dalam bentuk digital	Telah terlaksana, kegiatan ini telah mempermudah *user* dan *operator* inapornet dalam operasionalnya	Ditlala dan Pustikom	Kegiatan *upload* dokumen serta pengisian data-data dan manifest kapal dilakukan dalam aplikasi inaportnet
3.	Memahami standar manajemen sistem keamanan informasi sebagai acuan dalam mengukur keamanan informasi dalam aplikasi Inaportnet	Telah terlaksana, standar ini telah diterapkan dalam aplikasi Inapornet	Telkomsigma	Standar yang digunakan untuk sistem manajemen keamanan informasi adalah ISO 27001

4.	Mengidentifikasi sejauh mana penerapan sistem keamanan infomasi dengan parameter yang ada di dalam prinsip dasar keamanan informasi	Aktivitas ini belum terlaksana	Ditlala dan Pustikom	Prinsip keamanan informasi adalah *availability, confidentiality, dan integrity*. Kegiatan ini menyesuaikan prinsip ini dengan hal-hal yang telah diterapkan dalam aplikasi inapornet
5.	Membuat dan menerapkan mekanisme penanganan untuk memperbaiki hambatan yang ada dengan bentuk standar operasional	Telah terlaksana, penanganan *trouble/error* akan langsung ditangani ketika terjadi	Telkomsigma	Standar operasional untuk mengatasi trouble/error adalah dengan metode penanganan secara langsung
6.	Membuat *Information Security Handbook* untuk Inaportnet untuk para pelaku yang terlibat	Aktivitas ini belum terlaksana	Ditlala	Membuat *handbook* keamanan informasi untuk aplikasi Inaportnet yang akan menjadi acuan untuk stakeholder lainnya.
7.	Mengevaluasi hasil dari sistem yang telah diterapkan	Telah terlaksana, sistem keamanan informasi diaudit satu tahun sekali	Telkomsigma	Evaluasi keamanan informasi dilakukan setiap satu tahun sekali, hal ini dilakukan untuk mengupgrade sistem pengamanan

4.2 Pembahasan

Setelah tahapan perbandingan model konseptual dengan realitas dilakukan, maka tahap selanjutnya adalah melakukan peninjauan lebih lanjut antara penelitian dengan teori, konsep, dan hasil penelitian terdahulu yang relevan serta membentuk pola pikir dari penelitian ini. Proses analisis ini disebut juga dengan refleksi teoritis, proses ini mengacu pada tabel perbandingan model konseptual yang telah dibuat. Tahap ini merupakan tahap ke enam dari analisa SSM.

4.2.1. Implementasi Sistem Keamanan Informasi Aplikasi Inaportnet

Inaportnet sebagai sistem aplikasi untuk layanan tunggal berbasis internet/web berperan untuk mengintegrasikan sistem informasi kepelabuhanan yang melayani kapal dan barang dari seluruh intansi atau pemangku kepentingan di pelabuhan. Inapornet bersifat terbuka dan netral oleh karena itu Inaportnet merupakan jalur lalu lintas informasi yang padat selain karena pelayanan di dalamnya banyak, juga karena aplikasi ini terhubung satu Indonesia. Tantangan dari penerapan Inaportnet di Indonesia adalah dukungan infrastruktur jaringan internet yang harus dibangun di setiap pelabuhan untuk mendukung kelancaran operasional Inaportnet.

Pembagian peran aplikasi Inapornet adalah sebagai berikut, Inaportnet berada dibawah tanggung jawab Direktorat Jenderal Perhubungan Laut. Untuk pengontrolan dan pengawasan dari aplikasi ini dilakukan oleh Direktorat Lalu Lintas dan Angkutan Laut, dan dibantu oleh Pusat Teknologi Informasi dan Komunikasi Perhubungan. Sedangkan untuk operasional pelayanan dari aplikasi Inaportnet diserahkan kepada masing-masing Unit Pelaksana Teknis di pelabuhan. Kemudian sistem pengamanan dari Aplikasi Inapornet ini dilakukan secara terpusat, termasuk penggunaan dan transmisi data/informasi didalamnya semuanya disimpan dalam *data base* terpusat yang dikelola oleh Telkomsigma.

Menurut Timothy P. Layton (2007) dalam bukunya *Informaton Security: Design, Implementation, Measurement, and Compliance*. Terdapat Sembilan komponen dalam implementasi keamanan informasi. Di mana ke-sembilan komponen tersebut terdiri atas kriteria-kriteria yang relevan dengan setiap komponennya. Dari Sembilan komponen tersebut terdapat satu komponen yang belum terakomodir dengan baik yaitu komponen pengaturan tentang keamanan informasi.

4.2.1.1 Potensi ancaman *cyber* dalam aplikasi Inaportnet

Dalam dunia *cyber* yang segala sesuatunya terhubung satu sama lain, ancaman menjadi sangat nyata, namun sulit untuk terdeteksi karena bersifat maya. Segala sesuatu yang berhubungan dengan domain *cyber*, apabila terjadi serangan yang tidak terdeteksi dapat menyebabkan dampak yang luar biasa besar. Namun, karena sulitnya untuk mendeteksi ancaman *cyber*, maka tindakan pencegahan lebih banyak dilakukan untuk mencegah dan meminimalisir serangan *cyber*. Hal inilah yang sering disebut sebagai *cyber security.*

Perkembangan teknologi informasi dan komunikasi juga mempunyai andil yang besar terhadap perkembangan dunia *cyber*. Ditambah lagi dengan kombinasi perkembangan jaringan internet yang semakin meluas, membuat akses menuju informasi jauh lebih mudah dan cepat. Apalagi format informasi digital sekarang ini sudah menjadi suatu kebiasaan, karena dianggap lebih efisien, efektif dan murah. Perlindungan informasi bukan menjadi prioritas lagi, namun menjadi sebuah kebutuhan. Perlindungan juga tidak hanya dilakukan dalam lingkup informasinya, namun juga meliputi hardware, *software* maupun lingkungan fisiknya.

Teknologi informasi dan komunikasi telah mencapai domain maritim di Indonesia, salah satunya adalah Inaportnet yang dalam pengoperasiannya berbasiskan kepada jaringan internet. Walaupun dapat dikatakan Inaportnet merupakan sebagian kecil bagian dari *maritime cyber* namun informasi yang berlalu lalang di dalam aplikasi ini sangat banyak.

Kemudian data/informasi yang dimuat didalamnya juga bersifat penting. Oleh karena itu, menjadi sebuah kebutuhan aplikasi Inaportnet untuk melakukan tindakan pencegahan dalam menghadapi ancaman *cyber*. Teknologi yang termasuk *maritime cyber* lainnya adalah sistem IT milik perusahaan kontainer dan perusahaan pelayaran (misalnya Maersk-Petya/Goldeneye), jaringan komputer perusahaan pelayaran yang mengatur rute perjalanan kapal secara otomatis, sistem IT di kilang minyak lepas pantai, serta AIS (*Automatic Identification System*) dan lain-lain.

Berdasarkan keterangan hasil wawancara dengan pihak Direktorat Lalu Lintas dan Angkutan Laut serta Pusat Teknologi Informasi dan Komunikasi Perhubungan tidak ada serangan *cyber* yang menyerang sistem Inaportnet hingga menyebabkan hal yang serius terhadap aplikasi Inaportnet. Namun diakui adanya serangan yang dihadapi hanya serangan dengan level ringan, yakni serangan yang hanya menyerang sistem pengamanan luar dari Inaportnet itupun jarang frekuensinya. Menurut penelitian terdahulu yang dilakukan oleh Jenna Ahokas dan Tuomas Kiiski (2017) dalam tulisannya yang berjudul "*Cyber Security in Ports*" hal ini dikarenakan ancaman dalam *cyber security* dapat dicegah dan diminimalisir apabila sistem pengamanannya telah dipersiapkan secara maksimal, mulai dari jaringan, *hardware*, *software*, *virtual*, lingkungan, *data base*nya serta individunya. Juga berdasarkan teori *cyber security*, pertahanan terbaik dalam menjaga keamanan *cyber* adalah dengan melakukan pencegahan-pencegahan agar informasi di dalam sistem tetap aman.

Namun tidak adanya serangan *cyber* dalam aplikasi Inaportnet yang bersifat serius, bukan berarti membuat aplikasi Inaportnet bebas dari ancaman *cyber*. Potensi ancaman *cyber* akan selalu ada, setiap aplikasi yang berhubungan dengan *Electronical Communication Networks* (ECN), dan internet akan tetap mempunyai potensi ancaman *cyber*. Oleh karena itu tindakan-tindakan pencegahan dilakukan demi pencegahan terhadap potensi ancaman yang ada.

Sistem pencegahan ini berguna untuk keamanan informasi dalam aplikasi Inaportnet. Meski prosedur pencegahan ini telah dilakukan oleh Telkomsigma sebagai pihak ketiga dalam penyedia dan pelaksana sistem pengamanan informasi Inaportnet. Namun, perlu juga untuk menumbuhkan *cyber security awareness* dalam tingkat individu karena pada dasarnya individu-individu ini merupakan pencegahan dari ancaman *cyber* yang efektif.

Apabila dilihat dari chart ancaman cyber (Gambar 2.2 Ancaman dalam cyber security), untuk aplikasi Inaportnet mempunyai potensi untuk ancaman cyber jenis *hacktivism, cyber criminality, cyber espionage,* dan *cyber terrorism.* Namun berdasarkan hasil wawancara dengan pihak Pusat Teknologi Informasi dan Komunikasi Perhubungan, potensi ancaman *cyber* dalam aplikasi Inaportnet masih lebih cenderung kepada *hacktivism, cyber criminality, cyber espionage.* Hal tersebut dikarenakan serangan jenis-jenis ini mempunyai motif keuntungan dan kepuasan untuk diri sendiri dan kelompok kecil. Hal ini berdasarkan penelitian terdahulu dari Jenna Ahokas dan Tuomas Kiiski (2017) yang mengkaji tentang *cyber security in Ports*.

4.2.1.2 *Cyber Security Awarenesss* dalam aplikasi Inaportnet

Pelabuhan telah lama dipertimbangkan sebagai industri yang tidak terlihat dan selalu beroperasi sendiri dengan sedikit perhatian dan kesadaran dari lingkungan sosial. Resiko yang ada di pelabuhan telah berkembang seiring dengan berkembangnya waktu dan teknologi. Hal ini juga berlaku untuk tindakan pengamanan di Pelabuhan yang juga mengalami perkembangan. Biasanya resiko di pelabuhan meliputi kecelakaan kapal di pelabuhan, bencana alam, gangguan sistem transport, atau kerusakan-kerusakan akibat kelalaian pegawainya. Kejadian-kejadian seperti hal diatas dapat diminimalisir dengan hadirnya teknologi yang serba komputerisasi. Disinilah timbul resiko baru di pelabuhan, yakni ancaman yang mengancam sistem komputerisasi tersebut.

Menurut John R.Vacca (2009) dalam bukunya “Computer and Information Security *Handbook*”, salah satu kekuatan dari keamanan informasi dalam suatu organisasi/instansi, selain dari sistemnya juga datang dari orang-orang yang terlibat didalamnya. Begitu pula dalam keamanan informasi Inaportnet orang-orang yang terlibat didalamnya harus menyadari betapa pentingnya informasi yang ada di dalam aplikasi Inaportnet. Peningkatan *awareness* dan pemahaman bahwa manajemen serta disiplin operasional sama pentingnya dengan menjaga keterbaharuan teknologi dalam keamanan informasi.

Berdasarkan hasil temuan dilapangan *cyber security awareness* dalam aplikasi Inaportnet dapat dinilai kurang. Hal ini terbukti dengan tidak terjadwal secara berkala pelaksanaan *penetration test* dan *patching* untuk mengidentifikasi kelemahan-kelemahan dalam sistem keamanan informasi Inaportnet. Memang dianggarkan namun tidak ada jadwal tetap seperti 6 bulan sekali atau satu tahun sekali pelaksanaan kegiatan tersebut. Selain itu, ketika peneliti menceritakan kejadian *cyber crime* di pelabuhan Antwerp Belgia, informan dari Direktorat Lalu Lintas dan Angkutan Laut seperti belum mengetahui tentang kejadian tersebut dan kemungkinan terjadi hal yang sama dalam aplikasi Inaportnet.

Kejadian tersebut merupakan kejadian *hacking* untuk *cyber crime* yang dapat dikatakan terbesar yang terjadi di pelabuhan. Para gembong narkoba membeli jasa kelompok hacker untuk menyelundupkan narkoba dengan jumlah yang sangat besar tanpa diketahui. Akhirnya para hacker dapat menginjeksikan virus ke dalam data sistem pelabuhan yang memberi mereka kontrol atas pergerakan dan jadwal kontainer. Mereka dapat melakukannya tanpa sepengetahuan pekerja di pelabuhan. Para *hacker* ini bisa saja mentargetkan hal yang lain seperti pelabuhan itu sendiri, operator pelabuhan, atau pihak ketiga seperti pemasok atau penerima kargo.

Berdasarkan teori *cyber security awareness* dapat diaplikasikan melalui beberapa pendekatan, salah satunya adalah melalui training atau pelatihan. Pelatihan-pelatihan untuk kesadaran *cyber security* cukup sering

dilakukan oleh Kementerian Perhubungan untuk membekali pegawainya dengan kesadaran akan pentingnya informasi dalam aplikasi Inaportnet. Namun sepertinya kesadaran pegawai akan cyber security masih belum menjadi prioritas. Prioritas dari Direktorat Jenderal Perhubungan Laut sampai saat ini adalah kelancaran dari tingkat regulasi hingga operasional Inaportnet dilapangan.

Seperti yang telah dijelaskan oleh John R.Vacca (2009) orang merupakan elemen terlemah dalam sebuah formula keamanan yang digunakan untuk pengamanan sistem dan jaringan. Faktor orang (bukan faktor teknologi) merupakan faktor kritis yang paling sering diabaikan dalam keamanan. Oleh karena itu pelatihan-pelatihan yang dilakukan dalam keamanan informasi sebaiknya difokuskan untuk kegiatan kesadaran dan pelatihan berbasis kepada peran. Hal ini dikarenakan orang-orang ini adalah satu-satunya kontrol keamanan yang dapat meminimalkan risiko inheren yang dihasilkan dari orang-orang yang menggunakan, mengelola, mengoperasikan serta memelihara sistem dan jaringan informasi.

Untuk mencapai solusi keamanan informasi yang total, aspek tenaga kerja dalam mencapai tujuan keamanan informasi dan pentingnya pelatihan sebagai tindakan pencegahan dan persiapkan haruslah berjalan dengan baik. Memelihara dan membangun program pelatihan dan kesadaran akan keamanan informasi yang kuat dan relevan merupakan jalan utama untuk memberi karyawan sebuah informasi dan alat yang diperlukan dalam melindungi sumber daya informasi vital dalam aplikasi Inaportnet. Program pelatihan dan kesadaran keamanan informasi akan memastikan setiap personel di semua tingkatan organisasi memahami tanggung jawab keamanan informasi dalam bagiannya, serta menggunakan dan melindungi informasi beserta sumber daya yang dipercayakan kepadanya dengan benar.

4.2.2 Aspek Keamanan Informasi Aplikasi Inaportnet

Berdasarkan teori keamanan informasi terdapat aspek dasar keamanan informasi harus memenuhi 3 kriteria yaitu Keamanan informasi bertujuan untuk memastikan bahwa informasi yang sensitive hanya dapat diinformasikan kepada pihak yang berwenang (*confidentiality*), mencegah modifikasi data yang tidak sah (*integrity*), dan menjamin data dapat diakses oleh pihak yang berwenang ketika dibutuhkan (*availability*). Aspek ini dapat dicapai ketika implementasi sistem keamanan informasi diterapkan secara maksimal.

Dalam implementasi keamanan informasi juga terdapat sembilan komponen yang akan mendukung tercapainya ketiga aspek dasar keamanan informasi tersebut. Pelaksanaan sembilan komponen tersebut telah terpenuhi dengan baik dalam aplikasi Inaportnet. Sehingga ketiga aspek tersebut juga telah terpenuhi. Ke-sembilan komponen ini mencakup seluruh implementasi keamanan informasi dalam aplikasi Inaportnet. Mulai dari keamanan dari segi informasi itu sendiri, lingkungan baik fisik maupun virtual, keamanan *hardware* dan *software*, pembagian hak akses, perlindungan terhadap informasi jaringan serta pembagian level informasi.

Menurut John R.Vacca (2009) ketiga aspek dasar keamanan informasi yang pertama integritas yaitu dengan mengaplikasikan beberapa teknologi seperti enkripsi, authentikasi dan validasi yang kuat, pembatasan dan pembagian akses kontrol yang jelas. Kedua adalah ketersediaan yaitu dengan memastikan beberapa hal seperti *Disaster Recovery Plan*, Tenaga Cadangan untuk sumber listrik, RAID (*Redundant Array of Independent Disks*), serta data *backup*. Ketiga adalah kerahasiaan hal yang dapat dipastikan adalah enkripsi saat transmisi data dan kekuatan *password*. Berdasarkan ketentuan tersebut dapat disimpulkan bahwa aspek keamanan informasi dalam aplikasi Inaportnet telah terpenuhi.

Walaupun aspek dasar keamanan informasi telah terpenuhi, terdapat satu hal yang dapat menyempurnakan keamanan informasi dalam aplikasi Inaportnet, yaitu apabila aplikasi ini mempunyai *Information*

Security Handbook for Inaportnet. Handbook ini juga sering disebut sebagai *standard*, *guideline* atau *guidance*. Hal ini dilakukan untuk mengatur hal-hal penting yang berkaitan dengan segala kegiatan dan kebijakan untuk mendukung terwujudnya keamanan informasi dalam aplikasi Inaportnet yang maksimal.

Menurut Armour (2015)[70], Keamanan dunia maya dalam industri maritim adalah masalah utama, karena kurangnya kesadaran keamanan atau akuntabilitas sementara meningkatnya penggunaan teknologi komunikasi baru yang canggih meningkatkan tingkat ancaman menjadi tinggi. Dengan potensi kebocoran data pelanggan yang sensitif melalui ECDIS, AIS, RFID dan GPS, penting agar prosedur dan proses keamanan tersedia sehingga operator tahu bagaimana mengidentifikasi ancaman keamanan potensial atau telah dilatih untuk merespons ketika serangan *cyber* terjadi.

Para pelaku aktif dalam industri maritim sebagian besar karena tertarik pada keuntungan finansial, mencari cara untuk mendapatkan akses dengan tetap tersembunyi dan mengambil keuntungan finansial dari targetnya. Namun, mengakses dan mengekstraksi informasi sensitif atau kekayaan intelektual juga dapat membantu organisasi kriminal atau teroris yang memiliki motif untuk menggunakan media aplikasi Inaportnet untuk mengangkut bahan berbahaya atau senjata atau bahkan menggunakan kapal itu sendiri sebagai senjata di daerah konflik atau dekat dengan pelabuhan. Dalam ancaman lanjutan, penyerang (*attacker*) akan menghabiskan banyak waktu untuk meneliti daftar target potensial, mengumpulkan informasi tentang struktur organisasi, klien, dan lain-lain. Aktivitas media sosial dari orang-orang di perusahaan target akan dipantau untuk mengekstrak informasi tentang sistem dan forum yang disukai oleh pengguna dan setiap kerentanan teknologi yang dinilai. Begitu kelemahan ditemukan, langkah selanjutnya yang akan diambil peretas adalah

[70] Armour, Gr. Maritime Cyber Security, (Athena: Nato Cage Code,2008), hlm.14.

menembus batas keamanan cyber (keamanan dasar yang diadopsi sebagian besar perusahaan) dan mendapatkan akses yang bagi kebanyakan penyerang mudah untuk dilakukan.

4.4.2.1 *Information Security Handbook* untuk Aplikasi Inaportnet

Banyaknya hal yang harus diatur dalam aplikasi Inaportnet membuat perlunya hal-hal yang bersifat krusial untuk dibuatkan *handbook* sebagai panduan bagi para *stakeholder* yang terlibat dalam aplikasi Inaportnet. Saat ini panduan yang dimiliki Inaportnet adalah panduan untuk pendaftaran Inaportnet yaitu Buku Manual Inaportnet, serta edaran mengenai alur operasional pelayanan Inaportnet di pelabuhan. Sebagai referensi pembuatan *handbook* ini dapat mengadopsi *handbook* khusus untuk keamanan infomasi di pelabuhan dimiliki oleh New York dan New Jersey.

Handbook tersebut[71] berisi siapa saja yang bertanggung jawab dengan tugas yang menjadi wewenangnya, kategori atau level informasi, siapa yang berhak mengakses (hak akses), dan pembatasan akses. Juga terdapat hal-hal yang berkaitan dengan cara menyimpan, melindungi, trasmisi untuk informasi, hingga proses *monitoring* dan penyesuaian kemudian ada beberapa kebijakan tentang pelanggaran dan konsekuensi hingga materi pelatihan edukasi kesadaran keamanan informasi.

Menurut teori implementasi keamanan infomasi yang dikemukakan oleh Timothy (2007) dalam 9 komponen yang ada, keberadaan *handbook* untuk keamanan informasi termasuk kedalam komponen 7. Pengaturan tentang Keamanan Informasi. Isi dari *handbook* tersebut merupakan sebuah representatif dari kebijakan-kebijakan keamanan informasi yang diterapkan dalam aplikasi Inaportnet sembilan komponen implementasi keamanan informasi. Keberadaan *handbook* ini juga akan memperjelas posisi setiap *stakeholder* dalam aplikasi Inaportnet dan bagaimana cara mengatasi permasalahan ketika terjadi sehingga siapa yang bertanggung

[71] The Ports Authority of New York and New Jersey, “Information Security *Handbook*”

jawab dari tiga aspek dasar keamanan informasi dapat ditentukan. *Handbook* ini seharusnya dapat dibuat oleh Direktorat Jenderal Perhubungan Laut melalui Direktorat Lalu Lintas dan Angkutan Laut sebagai tingkatan regulator dan penanggung jawab untuk aplikasi Inaportnet.

Mengingat Inapornet merupakan aplikasi untuk mengintegrasikan seluruh aplikasi milik *stakeholder* yang berkepentingan dalam kegiatan kepelabuhanan. Maka pembuatan *handbook* ini dimaksudkan untuk menjamin status keamanan dari setiap masing-masing aplikasi yang terintegrasi dengan Inaportnet. Selain itu, konsep *handbook* untuk keamanan informasi ini dimaksudkan untuk menetapkan dan mendokumentasikan serangkaian kunci utama di mana setiap organisasi harus mempertimbangkannya untuk menerapkan efektifitas yang tinggi dalam operasi Inaportnet.

Menurut Timothy P. Layton (2007) *handbook* untuk keamanan informasi digunakan sebagai dokumen untuk kontrol kebijakan keamanan informasi dengan penunjukkan persyaratan yang jelas dalam pengembangan dan penerbitan dokumen kebijakan keamanan informasi. Dokumen ini juga dapat menjadi kontrol untuk penekanan pentingnya mengkomunikasikan kebijakan kepada semua pihak secara tepat termasuk karyawan, pihak eksternal, dan organisasi lain yang termasuk didalamnya. Kode praktik tidak memberikan panduan khusus bagaimana mencapai hal ini, tetapi menyarankan kebijakan yang dikomunikasikan secara efektif akan mendapatkan penerimaan dan kepatuhan pengguna target.

Dokumen pedoman ini akan menyediakan instruksi dasar dalam aplikasi Inaportnet yang membuat pernyataan paling jelas juga harus dimasukkan kedalam dokumen kebijakan keamanan infomasi secara formal. Salah satu bagian yang sering dilupakan, namun harus tetap dimasukkan adalah penilaian resiko dan hubunganya dengan manajemen resiko. Ada sedikit panduan yang berisi hal apa saja yang harus dimasukkan kedalam dokumen pedoman ini. Panduan tersebut adalah

ISO/IEC 27001 yang memberikan panduan tentang pengembangan dan pemeliharaan kebijakan dan program keamanan. Namun tetap tidak ada hal yang baku mengenai isi dokumen pedoman ini karena hal ini menyangkut kebijakan keamanan informasi tiap-tiap organisasi, akan tetapi yang jelas komponen dasar harus menjadi bagian dari semua kebijakan keamanan informasi.

BAB V
KESIMPULAN DAN REKOMENDASI

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dijelaskan pada Bab satu hingga empat serta ditambah dengan analisa SSM, maka dapat ditarik kesimpulan yang menjawab rumusan masalah pada penelitian ini yaitu sebagai berikut:

a. Implementasi sistem keamanan informasi Inaportnet di lapangan sudah berjalan dengan baik namun belum berjalan secara efektif dan efisien. Hal ini dikarenakan salah satu aspek pendukung sistem keamanan informasi yang juga penting yaitu kesadaran tentang pentingnya keamanan informasi (*awareness*) dapat dikatakan masih kurang. Hal ini dibuktikan dengan temuan dilapangan yaitu tidak adanya jadwal rutin untuk kegiatan *penetration test* dan *patch*. Jadwal secara rutin untuk *penetration test* dan *patch* selain untuk mengetahui kelemahan-kelemahan dalam sistem pengamanan informasi di Inaportnet juga untuk meminimalisir ancaman cyber yang dapat berevolusi setiap waktu.
b. Keamanan informasi dalam aplikasi Inaportnet belum dijadikan sebagai salah satu prioritas oleh Direktorat Lalu Lintas dan Angkutan Laut. Hal ini berdasarkan temuan di lapangan yang kemudian diolah dalam analisa. Hal ini juga dibuktikan dengan tidak adanya Inaportnet *Information Security Handbook* untuk para pemangku kepentingan dalam kegiatan kepelabuhanan. Handbook ini tidak hanya berfungsi sebagai *standard* atau *guidance* bagi para pemangku kepentingan dalam aplikasi Inaportnet akan tetapi *handbook* ini juga sebagai representatif kebijakan-kebijakan keamanan informasi yang diimplementasikan dalam aplikasi Inaportnet.

5.2 Rekomendasi

Peneliti memberikan rekomendasi yang didapat dari hasil penelitian ini. Rekomendasi ini diajukan sesuai dengan permasalahan yang muncul pada latar belakang penelitian dengan harapan isu yang diangkat dalam penelitian ini dapat dijadikan bahan pertimbangan oleh pihak-pihak yang berkepentingan dalam aplikasi Inaportnet, serta secara akademis dapat dilanjutkan dalam penelitian selanjutnya.

5.2.1 Rekomendasi Teoritis

Di dalam penelitian ini telah dibuktikan bahwa teori implementasi, teori keamanan nasional, konsep keamanan maritim, teori *cyber security*, dan teori keamanan informasi dapat digunakan dalam penelitian terkait dengan implementasi sistem pengamanan informasi dalam aplikasi Inaportnet untuk mendukung *maritime cyber security*. Penggunaan SSM dan NVivo sangat membantu dalam penelitian ini, sehingga dapat menghasilkan analisa yang tajam serta terstruktur. Metode ini direkomendasikan untuk digunakan dalam penelitian kualitatif lainnya. *Gap* yang ditemukan dalam penelitian ini dalam perbandingan model konseptual dengan realitas dapat dikembangkan menjadi penelitian lebih lanjut. Pembahasan yang dapat diambil diantaranya adalah *cyber security awareness* dalam aplikasi Inaportnet, penelitian lebih lanjut tentang efektifitas adanya *informasi security handbook* dalam aplikasi Inaportnet. Rekomendasi teoritis penelitian selanjutnya tentang topik *Maritime Cyber Security* adalah penelitian yang mengkaji tentang *cyber security on ship* atau *cyber security* untuk sistem IT perusahaan perkapalan. Saat ini, banyak kapal telah dikendalikan oleh komputer, hal ini yang menjadikannya rentan terhadap ancaman *cyber*. Keamanan *cyber* di kapal harus juga diperhatikan karena dapat memunculkan era pembajakan kapal yang baru, yaitu pembajakan kapal dengan menggunakan teknologi.

5.2.2 Rekomendasi Praktis

Berdasarkan hasil dari Root Definition dalam penelitian ini maka dapat pula ditarik beberapa saran teoritis terhadap owners.

Rekomendasi praktis yang pertama ditujukan kepada Direktorat Jenderal Perhubungan Laut sebagai penanggung jawab aplikasi Inaportnet. Hal yang direkomendasikan berupa pembuatan Inaportnet *Information Security Handbook* yang dibuat khusus untuk para pemangku kepentingan di pelabuhan. *Handbook* ini akan berisi siapa saja yang bertanggung jawab, pengkategorian level informasi, siapa dan apa yang dapat mengakses informasi dalam inaportnet (akses kontrol), manual prosedur yang digunakan ketika terjadi *error/trouble*, pembatasan akses, teknis perlindungan informasi, *monitoring*, audit, *self-assesment*, hingga materi pelatihan tentang pengetahuan dan kesadaran akan pentingnya keamanan informasi.

Rekomendasi praktis yang kedua adalah kerjasama dengan pihak ketiga terutama untuk aplikasi pelayanan untuk publik seperti Inaportnet memang dirasa tepat. Selain memang terbukti professional, kerjasama ini akan mengurangi biaya yang dikeluarkan jika dibandingkan dengan menyiapkan semuanya sendiri dengan sumber daya sendiri mulai dari hardwarenya, *software*nya, tenaga kerja, lingkungan, serta standar-standar yang harus dipenuhi dan membutuhkan biaya jauh lebih besar. Pihak ketiga, seperti Telkomsigma memang terbukti mempunyai kredibilitas dalam bidang pengamanan informasi, dibuktikan dengan seluruh aspek yang diperhatikan mulai dari keamanan lingkungan, perangkat lunak, perangkat keras, hingga keamanan personal.

GLOSARIUM

Cyber Security	:	Merupakan segala tindakan yang dilakukan untuk melindungi dan mencegah sistem informasi dan komunikasi serta perangkat komputer lainnya dari kerusakan, serta penggunaan atau modifikasi tidak sah baik dalam perangkat itu sendiri maupun dalam jaringan internet.
Cloud Computing	:	Teknologi yang menggabungkan teknologi komputer dan pengembangan berbasis internet dan menjadikannya sebagai pusat pengelolaan data dan aplikasi.
Cyber Attack	:	Segala jenis maneuver ofensi yang menargetkan sistem IT, jaringan komputer atau perangkat komputer pribadi yang berusaha untuk berkompromi, menghancurkan atau mengakses sistem dan data perusahaan.
Cyber Space	:	Merupakan media elektronik dalam jaringan komputer yang banyak digunakan untuk keperluan komunikasi satu arah maupun timbal balik secara langsung (*online*)
Cyber System	:	Merupakan kombinasi fasilitas, peralatan, personel, prosedur dan komunikasi yang terintegrasi untuk menyediakan layanan *cyber*, seperti sistem bisnis, sistem kontrol, dan sistem kontrol akses.
Data Base	:	Merupakan kumpulan data yang disimpan secara sistematis dalam komputer yang dapat diolah atau dimanipulasi menggunakan perangkat lunak untuk menghasilkan informasi

Data Center	:	Merupakan suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya seperti sistem telekomunikasi dan penyimpanan data.
Demilitarized Zone (DMZ)	:	Merupakan zona *buffer* antara internet dan *internal network*. DMZ menyediakan lapisan perlindungan untuk *internal network.*
Enkripsi	:	Merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.
Firewall	:	Merupakan penyaring yang dirancang untuk mencegah akses tidak sah ke dalam infrastruktur dan informasi TI. Firewall juga akan melindungi jaringan dari lalu lintas yang tidak wajar, di mana lalu lintas yang tidak wajar ini kemungkinan besar dilakukan oleh penyerang.
Kontrol Akses	:	Pembatasan secara selektif kemampuan dan sarana untuk berkomunikasi atau berinteraksi dengan suatu sistem dalam menggunakan sumber daya, menangani informasi, memperoleh pengetahuan tentang informasi yang terdapat di sistem serta mengontrol komponen dan fungsi sistem.
Kriptografi	:	Ilmu mengenai teknik enkripsi di mana naskah asili diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit untuk dibaca
Malware	:	Istilah umum untuk berbagai perangkat lunak berbahaya yang dapat menginfeksi sistem komputer dan akan berdampak pada kinerjanya.
Proses Deteksi	:	Merupakan sebuah metode untuk mendeteksi intrusi ke dalam komputer dan jaringan.

Server	:	Merupakan sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Didukung dengan prosesor yang bersifat scalable dan RAM yang besar, serta dilengkapi dengan sistem operasi khusus yang disebut sebagai sistem operasi jaringan (*Network Operating System*)
Transmisi data	:	Merupakan proses saat melakukan pengiriman data dari salah satu sumber data ke penerima data menggunakan komputer/media elektronik lainnya.
Virtual Private Network (VPN)	:	Suatu koneksi antara satu jaringan dengan jaringan lainnya secara pribadi (private) melalui jaringan publik (internet). VPN digunakan untuk menghindari penyusup saat melakukan transmisi data yang sewaktu-waktu bisa masuk ke lalu lintas jaringan.
Virus	:	Bagian dari perangkat lunak komputer tersembunyi yang mereplikasi diri sendiri untuk menginfeksi dan memanipulasi pengoperasian program atau sistem komputer secara tidak sah dan berbahaya.

DAFTAR PUSTAKA

Buku

Awad, Ali Ismail. 2018. *Introduction to Information Security Foundations and Applications*. London: The Institution of Engineering and Technology.

Armour, Gr. 2008. *Maritime Cyber Security*. Athena: Nato Cage Code.

Bandur, Agustinus. 2016. *Penelitian Kualitatif: Metodologi, Desain, dan Teknik Analisis Data dengan NVIVO 11 plus*. Jakarta: Mitra Wacana Media.

Checkland, Peter. 1991. *Soft System Methodology in Action*. Denmark: University of Aalborg.

Clarke, Richard A. dan Robert K. Knake. 2012. *Cyber war: the next threat to national security and what to do about it*. USA: ECCO Harper Collin Publishers.

Creswell, John W. 2009. *Research Design: Pendekatan Metode Kualitiatif, Kuantitatif dan Campuran: Edisi 4*. Yogyakarta: Pustaka Pelajar.

Drew, Dennis M. dan Donald M.Snow. 2006. *Making Twenty First Century Strategy: An Introduction to Modern National Security Processes and Problems*. Alabama: Air University Press.

Fung, Kwok T. 2005. *Network Security Technologies: Second edition*. New York: Auerbach Publication, A CRC Press Company.

Gibson, Darril. 2011. *CompTIA Security+ Get Certified Get Ahead: SY0-301 Study Guide*. North Charleston, South Carolina: CreateSpace.

Hardjosoekarto, Suharsono. 2012. *Soft System Methodology: Metode serba sistem lunak*. Jakarta: UI Press.

Horne, Craig A., Atif Ahmad, and Sean B. Maynard. 2016. *A Theory on Information Security*. Australia: Australasian Conference on Information Systems.

Kamus Besar Bahasa Indonesia. 2016. Pusat Bahasa Kementerian Pendidikan Nasional.

Klein, A. dan L. Storme. 2011. *Application of finite geopmetry in coding theory and cryptography*. Amsterdam: IOS Press.

Kementerian Pertahanan Republik Indonesia. 2015. *Buku Putih Pertahanan Indonesia*. Jakarta: Kementerian Pertahanan Indonesia.

Layton, Timothy P. 2007. *Informaton Security: Design, Implementation, Measurement, and Compliance*. Florida: Auerbach Publications, Taylor & Francis Group.

Miller, Lawrence C. 2014. *Cybersecurity for Dummies*. New Jersey: John Wiley & Sons, Inc.

Rahman, Chris. 2009. *Concepts of Maritime Security*. New Zealand: The Centre for Strategic Studies.

Sloan, Elinor C. 2012. *Modern Military Strategy: An Introduction*. London: Routledge.

Springer, Paul J. 2013. *Cyber Warfare: a reference handbook*. USA : ABC-CLIO, LLC.

Stallings, William. 2005. *Crytography and Network Security Principles and Practices: Fourth Edition*. New Jersey: Prentice Hall, 2005), hlm.8.

Sujarweni, Wiratna. 2014. *Metodologi Penelitian*. Yogyakarta: PT. Pustaka Baru.

Till, Geoffrey. 2015. *Sea Power*. New York : Routledge.

Vacca, John R. 2009. *Computer and Information Security Handbook*. USA: Morgan Kaufmann Publishers imprint of Elsevier.

Venkataraman, Karthik, H Raghav Rao, dan David Dewitt. 2007. *Handbooks in Information Systems Vol.2 National Security: National Information Technology (IT) Security Policies An Overview of Issues*. Amsterdam: Elsevier.

Tesis

Hayes, Christopher R. 2016. “Maritime *Cyber* Security: the future of national security”, *Tesis Magister*, (California: Homeland Security and Defense, Naval Postgraduate School.

Jurnal

Ahokas, Jenna dan Tuomas Kiiski. 2017. ”*Cybersecurity*in Ports”. *Publication of the Hazard Project*: Volume 3.

Bilgin, Begul, Svetla Nikova, dan Vincent Rljmen. 2016. “Theory of Implementation Security (TIs 2016)”. *Proceedings of the 2016 ACM SIGCAC Conference on Computer and Communications Security*.

Bueger, Christian. 2014. “What is Maritime Security?”. *Marine Policy*, Volume 53.

Darmono, Bambang. 2010. “Konsep dan Sistem Keamanan Nasional Indonesia”. *Jurnal Ketahanan Nasional*. Volume 15 (1).

Fitton, Oliver *et al*. 2015. “The Future of Maritime *Cyber* Security”, *Lancaster University*. Security Lancaster.

Grozdanoska, Natasha.2014. “National Defence and Security”. *European Scientific Journal*. Volume.1. ISSN-1857-7431

Sitorus, Budi, Tulus Irpan H. Sitorus, dan Prasadja Ricardianto. 2016. "Evaluasi Manajemen Sistem Informasi dan Teknologi Informasi Pelabuhan", *Jurnal Manajemen Transportasi & Logistik* (JMTransLog). Volume 3 (3).

Vleeschhouwer, S. 2017. "Safety of data: The risks of *Cybersecurity*in the maritime sector". *Netherlands Maritime Technology*.

Undang-undang

Undang-undang Nomor 17 tentang Pelayaran tahun 2008

Peraturan

Peraturan Menteri Perhubungan Nomor 192 Tahun 2015 tentang perubahan atas PM Nomor 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan.

Peraturan Menteri Perhubungan RI Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan

Lampiran II Peraturan Presiden Republik Indonesia Nomor 16 Tahun 2017 Tentang Kebijakan Kelautan Indonesia

ISPS Code tahun 2003 International Ship and Port Facility Security Code and SOLAS Amendments 2002

Majalah

Dwyer, Maria. "*Cyber*crime – is it a threat to Australia's Marine Industry?.". *Ausmarine Magazine*, 25 Oktober 2015.

Website

Rouse, Margaret. "Information Security", dalam https://searchsecurity.techtarget.com/definition/information-security-infosec, 2018, diakses pada 17 Agustus 2018.

Riri. “Apa saja Peran Audit Internal dalam *Cyber* Security?” dalam IT Governance Indonesia https://itgid.org/apa-saja-peran-audit-internal-dalam-*cyber*-security/ diakses pada 07 November 2018.

IPC dan HUBLA. “Inapornet: Apa dan Mengapa” dalam http://portal.inaportnet.com/about.html diakses pada 07 November 2018.

Direktorat Jenderal Perhubungan Laut. “Struktur Organisasi Direktorat Lalu Lintas dan Angkutan Laut” dalam http://hubla.dephub.go.id/unit/ditlala/Pages/Struktur-Organisasi.aspx diakses pada 27 November 2018.

Direktorat Jenderal Perhubungan Laut. “Tugas dan Fungsi Direktorat Lalu Lintas Angkutan Laut” dalam http://hubla.dephub.go.id/unit/ditlala/Pages/Tugas-Fungsi.aspx diakses pada 27 November 2018.

Djawahir, Kusnan dan Yosa Maulana. “Telkomsigma Fokus Kembangkan Aplikasi untuk Transportasi” dalam http://www.telkomsigma.co.id/telkomsigma-fokus-kembangkan-aplikasi-untuk-transportasi/ diakses pada 27 November 2018.

Press Release News. “Telkomsigma Dinobatkan sebagai The Best Disruptor Company” dalam http://www.telkomsigma.co.id/telkomsigma-dinobatkan-sebagai-best-distruptor-company/ diakses pada 27 November 2018.

Anita Chandraker,”*How can you improve cyber security awareness in your organization*?” dalam https://www.paconsulting.com/insights/how-can-you-improve-*cyber*-security-awareness-in-your-organisation/ diakses pada 27 November 2018

Lain-Lain

International Maritime Organization, ‘Interim Guidelines on Maritime *Cyber* Risk Management: IMO-MSC1/CICC 1526,2016

International Maritime Organization, “Guidelines on Maritime *Cyber* Risk Management”, IMO-MSC-FAL.1/CICC 3,2017.

Octavian,A. “Teknik Analisa Data Kualitatif”. Pada kuliah FIMP di Universitas Pertahanan, tanggal 13 Oktober 2017.

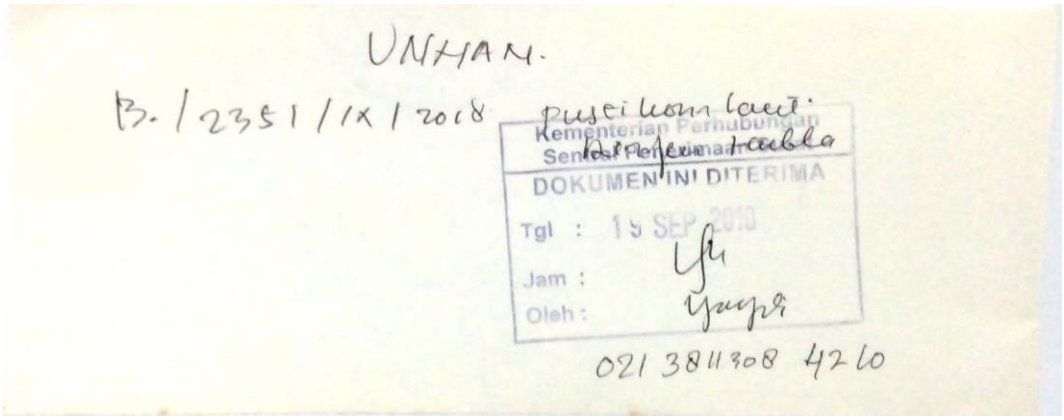
Setiawan, Anton. “Technology Utilization to Uncover Terrorist Networks in Indonesia and Regionally”. Pada seminar IIDSS 2018 di Hotel Grand Mercure Kemayoran, tanggal 13 Juli 2018.

Surat Keputusan Menteri Perhubungan RI Nomor KP. 336 Tahun 2018 tanggal 20 Februari 2018 Tentang Reviu Rencana Strategis Sekretariat Jenderal Kementerian Perhubungan Tahun 2015-2019.

Pronichkin, Alexey. “Marine Cyber Security”. Pada Seminar IIDSS 2018 di Hotel Grand Mercure Kemayoran, tanggal 13 Juli 2018.

LAMPIRAN

Lampiran 1 : Surat Keterangan Penelitian



Lampiran 2 : Pedoman Wawancara

Judul : Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk *Maritime Cyber Security*

Pertanyaan Penelitian 1	**Sekretariat Jenderal Perhubungan**	**Direktorat Jenderal Perhubungan Laut**	**Telkomsigma**
	Pusat Teknologi dan Komunikasi Perhubungan	**Direktorat Lalu Lintas dan Angkutan Laut**	***Data Center Site Operation***
Pertanyaan Penelitian 1 (Teori Implementasi Keamanan Informasi) Bagaimana implementasi sistem pengamanan informasi dalam aplikasi Inaportnet untuk mendukung *Maritime Cyber Security*? 1. Apa yang diketahui tentang *Maritime Cyber Security*? 2. Bagaimana mekanisme pengamanan data dalam aplikasi Inaportnet? 3. Bagaimana mekanisme pengamanan aplikasi Inaportnet secara personal komputer? 4. Mengapa memilih Telkom sebagai penyedia jasa pengamanan data untuk Kementerian Perhubungan? 5. Apa yang menjadi keunggulan Telkom sehingga menjadi pilihan bagi Kementerian Perhubungan? 6. Bagaimana mendeteksi apabila terjadi serangan *cyber*? 7. Sistem manakah yang paling sering diserang oleh *attacker*?			

8. Bagaimana pelaksanaan *maintenance* yang dilakukan dalam memelihara keamanan sistem Inaportnet? 9. Apa saja kendala yang dihadapi dalam memelihara sistem keamanan dalam aplikasi Inaportnet? 10. Bagaimana cara meyakinkan *customer* bahwa data yang ada pada sistem Inaportnet aman? 11. Bagaimana persiapan Dirjen Perhubungan Laut dalam mempersiapkan SDM-nya khusus menangani dalam domain *cyber*? 12. Apa saja hambatan yang kemungkinan terjadi saat mengimplementasikan sistem keamanan dalam aplikasi Inaportnet? 13. Hal apa saja yang idealnya diperlukan untuk menerapkan sistem pengamanan informasi yang ideal? 14. Bagaimana dengan kondisi fasilitas sarana dan prasarana untuk mendukung kelancaran pelaksanaan aplikasi Inaportnet? (*control room*, komputer, dll) 15. Berapa lama waktu yang dibutuhkan untuk menstablikan kembali operasional Inaportnet akibat dari kejadian kebakaran? 16. Apa dampak yang diakibatkan oleh kebakaran pada juli 2018 terhadap sistem inaportnet? 17. Apakah ada buku panduan khusus yang dibuat untuk keamanan informasi dalam aplikasi Inaportnet dan dibagikan kepada para *stakeholder* yang sistem aplikasinya terintegrasi dengan Inapornet? 18. Bagaimana pembagian peran antara ditlala, pustikom, dan telkomsigma mengenai hak akses kontrol untuk aplikasi Inaportnet serta para pegawai?			

Pertanyaan Penelitian 2	Sekretariat Jenderal Perhubungan	Direktorat Jenderal Perhubungan Laut	Telkomsigma
	Kepala Pusat Teknologi dan Komunikasi Perhubungan	Direktorat Lalu Lintas dan Angkutan Laut	Data Center Site Operation
Pertanyaan Penelitian 2 (Teori Keamanan Informasi) Bagaimana aspek pendukung dan penghambat dalam sistem pengamanan informasi yang terdapat dalam aplikasi Inaportnet? 1. Siapa saja yang bertanggung jawab atas operasional dari aplikasi Inaportnet? 2. Adakah lembaga-lembaga yang tergabung dalam aplikasi Inaportnet ini diluar dari Kementerian Perhubungan? 3. Apa saja kelebihan dan kelemahan dari aplikasi Inaportnet? 4. Apa saja kendala yang dihadapi dalam memelihara sistem keamanan dalam aplikasi Inaportnet? 5. Bagaimana penanganan yang dilakukan apabila hal tersebut terjadi? 6. Apakah pernah terjadi serangan *cyber* terhadap sistem Inaportnet? 7. Apa dampak dari serangan ini terhadap operasional Inaportnet? 8. Bagaimana SOP yang dilakukan ketika terjadi serangan *cyber*? 9. Berapa jumlah SDM yang khusus untuk mengelola aplikasi Inaportnet? 10. Bagaimana ketersediaan tenaga ahli dalam pengelolaan aplikasi Inaportnet?serta berapa jumlahnya?			

11. Bagaimana dengan kondisi peralatan fisik untuk mendukung kelancaran pelaksanaan aplikasi Inaportnet? 12. Bagaimana dengan kondisi peralatan non-fisik (jaringan integrasi, jaringan internet *software*) untuk mendukung kelancaran pelaksanaan aplikasi Inaportnet			

Lampiran 3 : Dokumen Pendukung

Gambar 6.1 Wawancara dengan Direktorat Lalu Lintas dan Angkutan Laut

Gambar 6.2 Wawancara dengan Pustikom Perhubungan

RIWAYAT HIDUP PENELITI

Asmaul Mufidasari, Lahir di Malang pada 03 Januari 1994. Anak ke-3 dari 3 bersaudara dari pasangan Muhammad Su'ud dan Komariatul Qurfi (almh). Menyelesaikan pendidikan SDN Turirejo 02 Lawang lulus tahun 2005, SMP Negeri 03 Lawang lulus tahun 2008, SMA PGRI Lawang lulus tahun 2011, Sarjana (S-1) Universitas Brawijaya Malang, Program Studi Ilmu Kelautan lulus tahun 2015, dan pada tahun 2017 melanjutkan program Magister (S-2) di Universitas Pertahanan.

Selama kuliah masa sarjana penulis aktif disejumlah kegiatan akademik maupun non-akademik. Kegiatan akademik yang pernah dilakukan adalah menjadi asisten praktikum untuk mata kuliah Kawasan Perlindungan Laut, Ekowisata Bahari, Konservasi, Pencemaran Laut, dan Pengelolaan Wilayah Pesisir dan Laut Terpadu. Serta menjadi finalis untuk tampil dalam makalah ilmiah di Universitas Diponegoro Semarang.

Kegiatan non-akademik yang pernah diikuti penulis antara lain tergabung dalam organisasi selam POSSI, organisasi KSR (Korps Sukarela) Universitas Brawijaya, Himpunan Mahasiswa Jurusan PSPK, Himpunan Mahasiswa Program Studi Ilmu Kelautan serta banyak kegiatan lainnya.