

BAB 2

TINJAUAN PUSTAKA

2.1. Landasan Teori

Landasan teori pada penelitian ini bertujuan untuk memberikan pemahaman mendalam terkait kerangka konseptual yang menjadi dasar penelitian mengenai pengaruh ISPS Code terhadap ancaman non tradisional Pelabuhan Kuala Tanjung di Selat Malaka. Teori-teori tersebut meliputi teori Keamanan Maritim, Ancaman Non Tradisional, Konsep *International Ship and Port Security Code* dan Legitimasi Hukum Terhadap Hadirnya ISPS Code di Indonesia.

2.1.1 Teori Keamanan Maritim

Dalam beberapa tahun terakhir, keamanan maritim (*maritime security*) telah menjadi konsep yang semakin populer. Konsep keamanan maritim melibatkan perlindungan terhadap wilayah perairan laut, sumber daya laut, dan kegiatan maritim dari berbagai tindakan seperti terorisme, perompakan, penyelundupan, proliferasi senjata, penangkapan ikan ilegal, kejahatan lingkungan hidup, dan kejahatan lainnya (Chapsos, 2016).

Dalam konteks ini, (Onuoha, 2010) mendefinisikan keamanan maritim sebagai kebebasan dari atau tidak adanya tindakan-tindakan yang dapat berdampak negatif terhadap integritas alami dan ketahanan wilayah maritim atau melemahkan keselamatan orang, infrastruktur, kargo, kapal, dan alat angkut lainnya yang secara sah berada di, melakukan transaksi yang sah di, atau transit melalui perairan teritorial dan laut. saluran air internasional. Intrinsik dan ekstrinsik merupakan dua dimensi utama keamanan maritim (Okafor-Yarwood & Onuoha, 2023). Penelitian ini termasuk pada dimensi ekstrinsik. Dimensi ekstrinsik yang dimaksud mencakup keselamatan setiap entitas atau objek apa pun yang menggunakan batas maritim. Hal ini kemudian berkaitan dengan keselamatan, antara lain, kapal, orang, dan aset yang tidak melekat pada ekosistem laut tetapi memiliki nilai bagi

negara atau entitas yang memiliki hak hukum untuk memanfaatkan lingkungan laut.

Table 2. Summary of dimensions of maritime security and associated common threats.⁶

Dimensions	Core element	Primary beneficiary	Major interest promoted	Common threats	Culprits
Intrinsic	The integrity of the pristine state of waters and marine resources	Local people and their livelihoods	Livelihood security	Pollution (oil spills and dumping of toxic or e-wastes), IUU or poaching	State actors and foreign capital
Extrinsic	Safety of foreign objects/ persons	States/foreign capital (multinationals, shipping companies)	Assets and personnel security	Piracy, terrorism, accidents	Non-state actors and criminal groups

Gambar 2.1 Dimensi Keamanan Maritim dan Ancaman Umum Terkait

Sumber: Onuoha (2020)

Dimensi ekstrinsik keamanan maritim baru-baru ini mendapat penekanan baru karena dua alasan. Yang pertama adalah ancaman kejahatan terorganisir transnasional yang terus berlanjut – keamanan maritim non tradisional antara lain pembajakan maritim, perdagangan narkoba, pembuangan limbah, dan penyelundupan senjata – yang difasilitasi melalui saluran maritim. Alasan kedua dan yang lebih penting adalah meningkatnya ancaman terorisme, terutama sejak serangan 11 September 2001 (sering disebut sebagai serangan 9/11). Dengan latar belakang ini, muncul kekhawatiran bahwa peristiwa 9/11 berikutnya dapat terjadi di laut. Sebagai hasilnya, beberapa langkah keamanan maritim seperti Kode Keamanan Kapal dan Fasilitas Pelabuhan Internasional (ISPS), Inisiatif Keamanan Proliferasi (PSI), Inisiatif Keamanan Peti Kemas (CSI), dan Kemitraan Bea Cukai-Perdagangan Melawan Terorisme telah diimplementasikan (Onuoha, 2010). Meskipun terorisme maritim telah terbukti menjadi ancaman yang belum terwujud, pembajakan merupakan ancaman utama yang mendorong sebagian besar sekuritisasi global domain maritim. Bahaya pembajakan terhadap perdagangan internasional membawa dimensi keamanan maritim ke dalam konteks global (Bueger,

2015).

Keamanan maritim berkembang secara drastis karena peristiwa bencana 11 September 2001 (9/11), ketika serangkaian serangan teroris yang disinkronkan terjadi di Amerika Serikat, khususnya di *World Trade Center* dan Pentagon oleh kelompok teroris Islam ekstremis Al-Qaeda. Insiden terorisme yang belum pernah terjadi sebelumnya dan merupakan bencana besar ini mengejutkan dunia, tetapi yang terpenting adalah menarik perhatian otoritas keamanan maritim internasional terhadap kerentanan pelabuhan terhadap tindakan terorisme dan ancaman kriminal lainnya. Majelis Umum Perserikatan Bangsa-Bangsa mengadakan sidang darurat pada 12 September 2001 yang bertujuan untuk mengutuk serangan 9/11 di Amerika Serikat dan mengadopsi resolusi untuk meningkatkan keamanan maritim global. Setelah itu, terdapat berbagai *platform* yang membahas metode untuk meningkatkan keamanan maritim. Diputuskan bahwa metode terbaik untuk meningkatkan keamanan maritim di seluruh dunia adalah dengan mengembangkannya di tingkat internasional.

Keamanan maritim merupakan tanggung jawab kolektif internasional dan untuk memastikan keberhasilan lingkungan maritim yang aman, sangat penting untuk menerapkan langkah-langkah keamanan yang konsisten dan terstandardisasi. Konvensi Internasional untuk Keselamatan Kehidupan di Laut (1974) adalah salah satu perjanjian maritim internasional yang paling signifikan yang berkaitan dengan keamanan dan keselamatan. Konvensi ini pertama kali diadaptasi pada tahun 1914 sebagai reaksi terhadap bencana Titanic, kemudian adaptasi kedua pada tahun 1929, adaptasi ketiga pada tahun 1948, adaptasi keempat pada tahun 1960, dan akhirnya adaptasi kelima dan yang terbaru pada tahun 1974. SOLAS telah diamandemen dalam berbagai kesempatan untuk memenuhi kebutuhan industri maritim dan saat ini dinamai SOLAS 1974, sebagaimana telah diamandemen. Setelah insiden tragis serangan 9/11, Konvensi penting ini kembali diamandemen untuk memasukkan Kode Keamanan Fasilitas Pelabuhan dan Internasional (ISPS) oleh Organisasi Maritim Internasional (IMO), yang

memimpin dalam merumuskan berbagai rekomendasi dan Konvensi terkait keamanan dengan melibatkan negara-negara dalam diskusi untuk mengembangkan konvensi internasional yang dirancang untuk meningkatkan keamanan maritim internasional.

2.1.2 Teori Ancaman Non Tradisional

Ancaman keamanan non-tradisional telah didefinisikan ulang sebagai ancaman yang disebut bukan ancaman keamanan tradisional dan merupakan konflik nonmiliter, politik, dan taktis yang dapat menjadi penyebab ancaman terhadap perkembangan negara berdaulat dan manusia secara keseluruhan. Ancaman keamanan non-tradisional adalah ancaman yang dapat membahayakan lembaga pemerintah dan warga sipil dan ini dapat berasal dari berbagai alasan non-negara, manusia, dan alam. Ancaman tersebut dapat muncul dari tindakan tertentu oleh orang atau kelompok, sampai batas tertentu daripada tindakan negara. Ancaman ini dapat menjadi penyebab kerugian ekonomi yang sangat besar bagi wilayah tertentu atau seluruh dunia. (Syed & Javed, 2017).

Salah satu pendekatan yang memungkinkan untuk merancang sistem klasifikasi ancaman non tradisional adalah dengan mempertimbangkan berbagai faktor seperti sifat ancaman, individu atau kelompok yang bertanggung jawab, lokasi geografis, dan tingkat potensi bahaya yang dapat mereka timbulkan. Klasifikasi ancaman non tradisional berdasarkan tipe 2 menurut (Pandey, 2023), yaitu untuk sistem klasifikasi yang lebih beragam dengan menambahkan lapisan kompleksitas pada kategori berdasarkan dimensi seperti ruang lingkup, aktor yang terlibat, tingkat dampak, wilayah geografis, dan modus operasi, akan dijelaskan sebagai berikut:

- a. Jenis Ancaman: dengan mengklasifikasikan ancaman menurut sifatnya, seperti kegiatan ilegal, ancaman lingkungan, dan ancaman teknologi.
- b. Aktor yang Terlibat:

- 1) Aktor negara: Ancaman yang ditimbulkan oleh negara-bangsa, seperti sengketa teritorial, manuver angkatan laut yang agresif, dan pembajakan atau terorisme yang disponsori negara.
 - 2) Aktor Non-negara: Ancaman dari sindikat kejahatan terorganisir, organisasi teroris, bajak laut, dan operator penangkapan ikan ilegal.
 - 3) Aktor perorangan: Ancaman dari individu, seperti teroris *lone wolf* atau peretas individu.
- c. Cakupan Geografis:
- 1) Global: Ancaman yang memiliki dampak global, seperti perubahan iklim atau ancaman siber yang menargetkan rute pelayaran internasional.
 - 2) Regional: Ancaman yang spesifik pada wilayah tertentu, seperti pembajakan di Teluk Aden.
 - 3) Lokal: Ancaman yang mempengaruhi area lokal tertentu, seperti penangkapan ikan ilegal atau polusi di pelabuhan tertentu.
- d. Tingkat Dampak:
- 1) Dampak Tinggi: Ancaman dengan konsekuensi yang berpotensi parah, seperti serangan teroris berskala besar, tumpahan minyak yang besar, atau serangan siber yang signifikan terhadap infrastruktur maritim yang penting.
 - 2) Dampak Sedang: Ancaman dengan konsekuensi yang signifikan, tetapi tidak sampai menimbulkan bencana, seperti tumpahan minyak berukuran sedang atau serangan bajak laut lokal.
 - 3) Dampak Rendah: Ancaman dengan konsekuensi langsung yang relatif kecil tetapi berpotensi menimbulkan efek jangka panjang yang parah, seperti penangkapan ikan ilegal atau masuknya spesies invasif secara bertahap.

e. Modus operasi:

- 1) Fisik: Ancaman yang melibatkan bahaya atau kerusakan fisik, seperti pembajakan, terorisme, atau pencemaran lingkungan.
- 2) Siber: Ancaman yang melibatkan serangan digital terhadap sistem dan infrastruktur, seperti peretasan sistem pelabuhan atau sistem navigasi.
- 3) Hibrida: Ancaman yang melibatkan kombinasi elemen fisik dan siber. Misalnya, serangan siber yang menyebabkan konsekuensi fisik, seperti peretasan ke dalam sistem navigasi kapal untuk menyebabkan tabrakan.

Dalam hal ini adanya klasifikasi tersebut dapat membantu menangani berbagai ancaman. Misalnya, ancaman keamanan mungkin memerlukan peningkatan patroli angkatan laut atau penjaga bersenjata di kapal, sementara tindakan keamanan siber yang lebih baik untuk kapal dan pelabuhan mungkin diperlukan untuk ancaman teknologi (Pandey, 2023). Namun pada penelitian ini, fokus peneliti hanya pada ancaman non tradisional dengan mengamati masalah pembajakan dan perampokan bersenjata sebagai prioritas terhadap isu keamanan yang menjadi perhatian utama di Selat Malaka. Sehingga tidak mencakup isu-isu lain seperti penangkapan ikan secara ilegal (*IUU Fishing*), penyelundupan manusia, perdagangan narkoba, atau bentuk ancaman lainnya yang sering diidentifikasi dalam kajian keamanan maritim.

Ancaman non tradisional dalam konteks jalur komunikasi maritim Asia Tenggara (SLOC) tidak menggunakan pendekatan militer. SLOC yang merupakan jalur penting bagi perdagangan dunia dimana sepertiga perdagangan dunia dan setengah dari lalu lintas pasokan minyak terjadi di Selat Malaka, kapal-kapal yang transit di perairan ini sangat rentan ketika memasuki selat yang sempit seperti tanker kecil dan kapal penangkap ikan yang secara khusus menjadi sasaran empuk bagi kapal perompak. Tingginya volume lalu lintas di wilayah maritim negara-negara Asia

Tenggara juga mendorong para perompak untuk melakukan penyerangan (Zara dalam Kwa dan Guan, 2007:65). Ancaman seperti pembajakan dan perampokan bersenjata di wilayah perairan Selat Malaka telah memberikan kontribusi kerugian yang besar bagi para pelaku usaha yang melintas dan telah menjadi salah satu ancaman yang paling signifikan dalam beberapa tahun terakhir.

Menurut Pasal 101 UNCLOS menentukan bahwa definisi “Pembajakan” terdiri dari salah satu tindakan berikut:

- a. segala tindakan kekerasan atau penahanan yang melanggar hukum, atau segala tindakan perampasan apa pun, yang dilakukan untuk tujuan pribadi oleh awak kapal atau penumpang kapal atau pesawat udara pribadi, dan ditujukan kepada:
 1. di laut lepas, terhadap kapal atau pesawat udara lain, atau terhadap orang atau harta benda yang ada di atas kapal atau pesawat udara tersebut;
 2. terhadap kapal, pesawat udara, orang atau properti di suatu tempat di luar yurisdiksi Negara mana pun;
- b. setiap tindakan partisipasi sukarela dalam pengoperasian kapal atau pesawat udara dengan pengetahuan tentang fakta-fakta yang menjadikannya kapal atau pesawat udara bajak laut;
- c. segala tindakan yang menghasut atau secara sengaja memfasilitasi suatu tindakan sebagaimana diuraikan dalam sub-ayat (a) atau (b).

Mengenai Kode Praktik IMO untuk Investigasi Kejahatan Pembajakan dan Perampokan Bersenjata terhadap Kapal, menentukan bahwa perampokan bersenjata terhadap kapal terdiri dari salah satu tindakan berikut:

- a. setiap perbuatan kekerasan atau penahanan yang melanggar hukum atau setiap perbuatan perampasan, atau ancaman kekerasan tersebut, selain dari perbuatan pembajakan, yang dilakukan untuk tujuan pribadi dan ditujukan terhadap suatu

kapal atau terhadap orang atau harta benda yang ada di atas kapal tersebut, di dalam perairan pedalaman suatu Negara, perairan kepulauan, dan laut teritorial;

- b. segala tindakan yang memicu atau secara sengaja memfasilitasi suatu tindakan sebagaimana diuraikan di atas.”

Berdasarkan definisi Pembajakan dan Perampokan Bersenjata, IMB RRT melaporkan insiden-insiden sebagai berikut:

- a. Naik ke kapal (*Boarded*): Tindakan illegal yang dilakukan oleh pelaku yang berhasil mendapatkan akses ke kapal.
- b. Dibajak (*Hijacked*): Tindakan illegal yang dilakukan oleh pelaku yang berhasil mendapatkan akses ke kapal dan mengambil alih kendali kapal dari nahkoda dan awak kapal.
- c. Ditembaki (*Fired Upon*): Tindakan illegal yang dilakukan oleh pelaku dengan menembakkan senjata ke arah kapal ketika mencoba mendapatkan akses ke kapal.
- d. Percobaan (*Attempted*): Tindakan illegal yang dilakukan oleh pelaku yang mencoba mendekati kapal dengan kemungkinan niat untuk naik ke kapal, namun tidak berhasil karena tindakan awak kapal yang tepat waktu.

Konsekuensi terhadap awak kapal, kapal, atau kargo, sebagai akibat dari tindakan illegal di atas:

- a. Kru: Penculikan, penyanderaan, kematian, ancaman, penyerangan, cedera, hilang.
- b. Kapal: Kerusakan, terutama akibat pelepasan senjata atau ketika pelaku dengan sengaja merusak peralatan dan properti kapal.
- c. Kargo: Pencurian atau kerusakan kargo.

Tingkat keparahan insiden spesifik wilayah pada Awak, Kapal dan Kargo, IMB melaporkan di bawah tiga Tingkat Keparahannya umum – I, II, dan III yang ditentukan oleh dampak insiden awak kapal, kapal dan kargo.

- a. Tingkat Keparahannya 1: Setiap insiden yang berdampak langsung

pada awak kapal. Termasuk:

- b. Tingkat Keparahan II: Mencakup kapal yang ditembaki, tim keamanan yang menembaki ancaman yang mendekat, perampok/bajak laut yang terindikasi membawa senjata jenis apa pun (ada kekerasan) baik di atas kapal maupun tidak.
- c. Tingkat Keparahan III: Untuk memasukkan insiden yang tidak termasuk dalam Tingkat I atau Tingkat II.

Dalam hal pembajakan dan perampokan bersenjata, ancaman ini bukanlah fenomena baru di Asia Tenggara. Pembajakan dan perampokan bersenjata telah lama dihadapi oleh industri pelayaran yang berlangsung selama berabad-abad dan terus meningkat sejak awal tahun 1970-an. Meskipun pembajakan di masa lalu memiliki peran struktural yang berbeda dalam interaksi global dan lokal dibandingkan dengan pembajakan kontemporer saat ini. Sejumlah perkembangan besar memicu maraknya pembajakan kontemporer, seperti kemajuan globalisasi dan intensifikasi ekonomi dunia telah membawa perubahan besar di kawasan Asia Tenggara, terutama pasca perang dingin. Transformasi politik dan ekonomi menjadi salah satu faktor yang memicu meningkatnya lalu lintas perdagangan maritim sehingga menjadi target potensial bagi para perampok dan bajak laut. Di satu sisi, perkembangan ekonomi global yang signifikan memberikan keuntungan bagi sebagian orang, namun di sisi lain, sebagian lainnya mengalami kemalangan karena hal ini juga menghasilkan kesenjangan sosial dimana perompakan dan perampokan menjadi alternatif untuk menghidupi keluarga yang kelaparan (Rosnani et al., 2022).

Selama beberapa dekade, pemerintah dan asosiasi pemilik kapal telah mengeluarkan peraturan dan instruksi dalam upaya membantu pelaut menghadapi bahaya tersebut. Sekitar 30 tahun yang lalu, dengan munculnya pembajakan modern, IMO dan Kamar Pelayaran Internasional mengeluarkan pedoman (Bergqvist, Lars H., 2014). Pada tahun 1957, sebuah konvensi internasional terkait penumpang gelap diadopsi, meskipun belum berlaku, dan ada kebijakan yang dikeluarkan tentang cara

menangani penumpang gelap. Akan tetapi, instruksi khusus tentang cara melindungi kapal dari teroris, sebelum adanya ISPS Code, tidak pernah dikeluarkan. Konvensi tentang Pemberantasan Tindakan Melawan Hukum terhadap Keselamatan Navigasi Maritim, yang disepakati setelah pembajakan kapal modern pertama yang menarik perhatian internasional adalah pembajakan kapal penumpang Portugis Santa Maria pada Januari 1961. Kemudian pada tahun 1985, pembajakan kapal pesiar Achille *Lauro*, hanya membahas hukuman atas tindakan yang dapat mengancam keselamatan navigasi maritim.

2.1.3 Konsep *International Ship and Port Facility Security Code*

Ketentuan-ketentuan baru dalam SOLAS, 1974 sebagaimana telah diamandemen dan penyertaan Kode Keamanan Kapal dan Fasilitas Pelabuhan Internasional (ISPS) diadopsi dalam Konferensi Diplomatik tentang Keamanan Maritim pada bulan Desember 2002 di London. Rezim keamanan baru untuk perlindungan kapal dagang dan pelabuhan ini diimplementasikan pada tanggal 1 Juli 2004 dan berlaku efektif di 147 negara. Saat ini, langkah-langkah keamanan baru ini berlaku untuk 162 Negara Anggota SOLAS yang dikontrak untuk mematuhi persyaratan yang ditetapkan dalam ISPS Code. Pada Konferensi Kelompok Kerja Intersessional tentang Keamanan Maritim pada tanggal 9-13 September 2002, ISPS Code digambarkan sebagai pembentukan kerangka kerja di seluruh dunia yang mencakup kerja sama antara berbagai pemain peran utama seperti pemerintah yang mengontrak, instansi pemerintah, pejabat daerah, perusahaan pelayaran dan pelabuhan. Kode ini pada dasarnya menyediakan deteksi dan pencegahan ancaman keamanan serta metodologi untuk menilai keamanan sambil menetapkan peran dan tanggung jawab berbagai pihak. Kode ISPS memungkinkan pengumpulan dan pertukaran informasi keamanan. Kode ini juga memastikan bahwa langkah-langkah keamanan yang memadai telah tersedia (Radonja & Glujić, 2020).

ISPS Code terbatas pada kapal dengan berat lebih dari 500 g.r.t. dan mewajibkan untuk disertifikasi. Kode tersebut dibagi menjadi dua bagian, menurut *Internasional Maritime Organization (2016) ISPS Code Guidelines for Ship Suppliers*, London: IMO), Kode Bagian A bersifat wajib, sedangkan Bagian B sebagai anjuran. Adapun tujuan Kode Etik sebagaimana dinyatakan dalam Bagian A (imo.org):

- a. Untuk menetapkan *framework* internasional yang melibatkan kolaborasi antara Pemerintah Pihak, layanan publik, pemerintah daerah, dan perusahaan industri perkapalan untuk mengidentifikasi ancaman keamanan dan menerapkan langkah-langkah keamanan.
- b. Menentukan peran dan tanggung jawab yang relevan dari pemerintah yang berkolaborasi, layanan publik, pemerintah daerah, dan perusahaan perkapalan, baik secara nasional maupun global untuk mewujudkan keamanan maritim.
- c. Memastikan pengambilan dan penukaran informasi yang tepat waktu dan efisien berkaitan dengan keamanan;
- d. Persiapan prosedur untuk evaluasi keamanan, dengan membuat rencana dan prosedur untuk berbagai bentuk keamanan
- e. Menciptakan kepercayaan yang diperlukan untuk mengambil langkah-langkah keamanan yang tepat dan khusus di laut.

Untuk mencapai tujuan di atas, pemerintah yang termasuk dalam kode ini, dan untuk mengatur pelabuhan, kantor kurir dan kantor pelabuhan yang bersangkutan, baik secara global maupun lokal, untuk memastikan keamanan maritim dan untuk berbagi/menerapkan data terkait keamanan guna memastikan pemilik kapal melakukan upaya keselamatan maritim yang memadai dan koheren untuk kapal-kapal mereka. Sehubungan dengan kode ISPS, perusahaan pelayaran, pelabuhan dan terminal harus menunjuk pejabat/otoritas keamanan yang sesuai di setiap kapal, di setiap kantor pelabuhan dan di setiap angkutan yang tertib untuk menyiapkan dan melaksanakan rancangan keselamatan yang akan dilaksanakan. Kode

ISPS harus dilaksanakan dalam strukturnya yang lengkap untuk memastikan keamanan dan kepastian bagi semua yang terlibat (Akram Elentably, 2020). IMO dapat memberikan dukungan kepada negara-negara Anggota yang membutuhkan bantuan dalam menerapkan Kode, melalui lokakarya nasional dan regional, seminar, misi penilaian kebutuhan, dll (IMO, 2024).

Implementasi kode dengan persyaratan yang harus diikuti oleh setiap orang akan berbeda, tidak hanya dari satu negara ke negara lain, tetapi juga dari satu pelabuhan ke pelabuhan lain di dalam satu negara dan dalam kasus yang ekstrim bahkan di dalam satu pelabuhan. Sebagai contoh, beberapa pelabuhan besar akan memiliki banyak operasi yang berbeda seperti terminal feri, terminal curah, dermaga kimia dan minyak, tempat berlabuh peti kemas, dan lainnya. Di lokasi-lokasi seperti itu, sangat mungkin untuk memiliki “tingkat” keamanan yang berbeda dalam operasi pada saat yang bersamaan. Ada tiga tingkat keamanan yang wajib diterapkan di semua kapal dan pelabuhan. Pengaturan tingkat keamanan ini adalah tanggung jawab pemerintah yang membuat kontrak. Isi dari ketiga tingkat keamanan Kode Etik tersebut, yaitu:

- a. Tingkat Keamanan 1: Normal: Ini adalah tingkat operasional kapal dan fasilitas pelabuhan pada umumnya. Tingkat ini menyediakan langkah-langkah keamanan perlindungan minimum yang harus dipertahankan setiap saat. Untuk tingkat keamanan 1, aktivitas berikut harus dilakukan:
 - 1) Akses terhadap fasilitas pelabuhan harus dikontrol.
 - 2) Semua tugas fasilitas pelabuhan harus dilaksanakan.
 - 3) Pengawasan terhadap penanganan gudang dan muatan kapal (kargo).
 - 4) Area terlarang harus dipantau untuk memastikan bahwa hanya orang-orang yang memiliki izin yang sesuai yang dapat aksesnya.
 - 5) Komunikasi terkait keamanan harus tersedia.

- 6) Fasilitas pelabuhan harus dipantau.
- b. Tingkat Keamanan 2: Ditingkatkan: Tingkat ini berlaku selama periode peningkatan risiko insiden keamanan. Tingkat ini menyediakan tindakan perlindungan keamanan tambahan yang akan dipertahankan untuk jangka waktu tertentu.
 - c. Tingkat Keamanan 3: Luar Biasa: Tingkat ini berlaku selama risiko insiden keamanan yang mungkin terjadi atau akan terjadi. Tingkat ini menyediakan tindakan keamanan perlindungan khusus tambahan yang harus dipertahankan untuk jangka waktu tertentu. Menetapkan tingkat keamanan 3, menurut Kode Etik, yang pertama hanya boleh diterapkan jika ada informasi yang dapat dipercaya bahwa insiden keamanan mungkin terjadi atau akan segera terjadi dan yang kedua, hanya boleh ditetapkan untuk jangka waktu ancaman keamanan yang teridentifikasi/insiden keamanan yang terjadi.

Tiga level yang didefinisikan di atas adalah sebagaimana yang dinyatakan dalam ISPS Code; namun, pemahaman dasar tentang level-level tersebut adalah Level 1 sama dengan situasi ancaman rendah, sementara Level 2 adalah situasi ancaman sedang dan Level 3 adalah situasi ancaman tinggi. Karena setiap kapal dan setiap fasilitas pelabuhan akan memiliki risiko yang berbeda, maka merupakan tanggung jawab Pemerintah Negara Pihak untuk menentukan dan menetapkan tingkat keamanan. Tingkat keamanan yang ditetapkan pada kenyataannya menciptakan hubungan antara kapal dan fasilitas pelabuhan karena memicu penerapan langkah-langkah keamanan tertentu untuk kapal dan fasilitas pelabuhan sesuai dengan peraturan ISPS Code.

Selanjutnya, ISPS Code mengharuskan pelabuhan untuk menyediakan organisasi keamanan yang diakui (RSO), penilaian keamanan kapal (SSA), dan rencana keamanan kapal (SSP). RSO adalah sebuah perusahaan yang terdiri dari orang-orang intelektual yang memiliki pengetahuan tentang keamanan, manajemen risiko, dan aktivitas intelijen

di kapal dan pelabuhan. SSP adalah rencana tindakan keamanan di atas kapal yang dikembangkan untuk memastikan perlindungan terhadap manusia, kargo, alat muat, penyimpanan, dan kapal. Selain itu, SSA merupakan bagian penting dan integral dari pengembangan dan pembaruan SSP. Adapun SSA harus memperhatikan elemen-elemen berikut saat di atas kapal atau di dalam kapal, yaitu (a) keamanan fisik kapal, (b) integritas struktural kapal, (c) sistem perlindungan bagi semua awak kapal, (d) kebijakan dan prosedur pengamanan, (e) sistem radio dan telekomunikasi, termasuk sistem dan jaringan komputer, serta (f) area lain yang mungkin jika dirusak atau digunakan untuk pengamatan terlarang, dapat menimbulkan risiko terhadap orang, properti, atau operasi di atas kapal atau di dalam fasilitas pelabuhan.

Pelabuhan juga diharuskan untuk memiliki rencana keamanan fasilitas pelabuhan (PFSP), yang merupakan rencana untuk implementasi langkah-langkah keamanan di pelabuhan dan fasilitas; dan penilaian keamanan fasilitas pelabuhan (PFSA), yang merupakan rencana untuk pengembangan dan pembaruan keamanan untuk fasilitas pelabuhan dengan memperhatikan elemen-elemen berikut, seperti (a) keamanan fisik, (b) integritas struktural, (c) sistem perlindungan personel, (d) kebijakan prosedural, (e) sistem radio dan telekomunikasi, termasuk sistem dan jaringan komputer, (f) infrastruktur transportasi yang relevan, (g) utilitas, serta (h) area lain yang mungkin, jika dirusak atau digunakan untuk pengamatan terlarang, menimbulkan risiko terhadap orang, properti atau operasi dalam fasilitas pelabuhan.

Di sisi lain, perusahaan pelayaran harus memiliki petugas keamanan perusahaan (CSO) atau orang yang ditunjuk oleh perusahaan untuk memastikan bahwa prosedur SSA dilakukan, perencanaan keamanan kapal dikembangkan, diimplementasikan dan dipelihara. Petugas ini juga bertanggung jawab untuk berkoordinasi dengan PSO dan SSO. Direktur Jenderal Perhubungan Laut akan melakukan review terhadap hasil SSA, SSP, PFSA dan PFSP. Adapun SSA dan PFSA harus mempertimbangkan

semua ancaman yang mungkin terjadi, yang dapat mencakup jenis insiden keamanan berikut:

- a. kerusakan atau penghancuran kapal atau fasilitas pelabuhan, misalnya dengan bahan peledak, pembakaran, sabotase atau vandalisme;
- b. pembajakan atau penyitaan kapal atau orang-orang yang ada di dalamnya;
- c. merusak kargo, peralatan atau sistem penting kapal, atau perbekalan/gudang kapal;
- d. akses atau penggunaan yang tidak sah, termasuk keberadaan penumpang gelap;
- e. menyelundupkan senjata atau peralatan, termasuk senjata pemusnah massal;
- f. penggunaan kapal untuk mengangkut orang-orang yang berniat menyebabkan insiden keamanan dan/atau perlengkapannya;
- g. penggunaan kapal itu sendiri sebagai senjata atau sebagai sarana untuk menimbulkan kerusakan atau kehancuran;
- h. serangan dari arah laut ketika sedang bersandar atau berlabuh; dan
- i. serangan saat berada di laut.
- j. penyumbatan; pintu masuk pelabuhan, kunci, pendekatan, dll; dan
- k. serangan nuklir, biologi dan kimia.

Selanjutnya, kapal-kapal yang telah ditinjau akan diberikan sertifikasi keamanan kapal sementara (jangka pendek) (ISSC) dan pelabuhan akan memiliki fasilitas keamanan fasilitas pelabuhan sementara (SoCPF) yang berlaku selama lima bulan. Kapal dan pelabuhan harus melalui proses pemeriksaan dan verifikasi internal. Jika dinyatakan bersih, kapal dan pelabuhan akan diberikan ISSC dan SoCPF permanen yang berlaku selama lima tahun.

ISPS Code juga mengharuskan pelabuhan dan kapal untuk

melakukan program pelatihan tentang ISPS Code kepada awak kapal. SSO akan memberikan pelatihan untuk awak kapal dan PFSO memberikan pelatihan dalam hal manajemen fasilitas pelabuhan. Petugas keamanan juga harus melakukan drill atau program pelatihan praktis untuk menguji prosedur yang tertulis dalam SSP dan PFSP. Pelatihan ini melibatkan pihak internal yang bertanggung jawab atas kapal dan fasilitas pelabuhan. Terakhir petugas keamanan harus melakukan program Latihan atau pelatihan komunikasi. Program ini bertujuan untuk menguji koordinasi, ketersediaan dan kapasitas sumber daya untuk mengkomunikasikan ancaman keamanan. Pelatihan komunikasi harus melibatkan pihak internal yang bekerja untuk kapal dan fasilitas pelabuhan serta pihak lain yang bergabung dengan PSC.

Dalam hal ini, ketentuan ISPS Code cukup komprehensif dalam memberikan panduan tentang cara meningkatkan keamanan maritim. Ketentuan ISPS Code menciptakan platform bagi komunitas maritim internasional untuk berada di level yang sama dalam hal mengamankan pelabuhan, fasilitas, dan kapalnya. Bagian A berisi ketentuan wajib sementara Bagian B berisi pedoman khusus untuk setiap peraturan yang dapat digunakan oleh negara-negara selama tahap penyusunan undang-undang keamanan maritim domestik mereka sendiri. Penerapan ISPS Code sangat penting karena akan meningkatkan keamanan nasional dan internasional, karena keamanan lingkungan maritim merupakan tantangan transnasional, yang membutuhkan upaya regional dan internasional.

2.1.4 Legitimasi Hukum Terhadap Hadirnya ISPS Code di Indonesia

Sebagai negara maritim, Indonesia merupakan anggota dari beberapa konvensi internasional yang berhubungan dengan keamanan maritim, termasuk keselamatan pelayaran. Indonesia sebagai anggota penandatanganan IMO, telah menandatangani dan meratifikasi ISPS Code, oleh karena itu Indonesia berkewajiban untuk menerapkan ketentuan-ketentuan dalam ISPS Code secara konsisten. Saat ini penerapan ISPS

Code di Indonesia telah memasuki fase akhir lima tahun keempat. Indonesia meratifikasi ISPS Code dan menerapkannya melalui ketentuan perundang-undangan domestiknya, yaitu Undang-Undang Nomor 17 Tahun 2008 tentang Pelayaran, yang merupakan hukum tertinggi di Indonesia dan memberikan landasan hukum bagi keberadaan negara dan harus dipatuhi oleh semua hukum di Indonesia. Kerangka hukum yang mengatur kewajiban pemerintah dan pelaku usaha dalam menjaga keamanan di laut, termasuk pencegahan dan penanganan kejahatan maritim seperti perompakan dan penyelundupan. Undang-undang ini mengatur berbagai aspek pelayaran, termasuk keselamatan dan keamanan pelayaran, pendaftaran dan kebangsaan kapal, perlindungan lingkungan maritim, serta kewajiban dan tanggung jawab dari semua pihak yang terlibat dalam kegiatan pelayaran.

Kemudian, turunan dari undang-undang tersebut dijelaskan lebih spesifik pada Peraturan Pemerintah Nomor 31 Tahun 2021 tentang Penyelenggaraan Bidang Pelayaran. Peraturan ini mengatur lebih detail mengenai pelaksanaan pelayaran di Indonesia, termasuk aspek teknis dan administratif dalam operasional pelayaran. Terkait keamanan maritim, peraturan ini mengatur mengenai tanggung jawab otoritas pelabuhan, operator pelayaran, dan pengguna jasa pelabuhan dalam menjamin keamanan kapal dan keamanan fasilitas pelabuhan serta menetapkan standar keamanan yang harus dipenuhi oleh semua pihak yang terlibat dalam pelayaran, termasuk penerapan sistem manajemen keamanan yang harus sesuai dengan standar internasional.

Selanjutnya, Permenhub PM 134 Tahun 2016 tentang Manajemen Keamanan Kapal dan Fasilitas Pelabuhan, yang merupakan pedoman teknis bertujuan untuk penerapan ISPS Code agar Indonesia dapat memenuhi kewajiban internasionalnya berdasarkan Bab XI-2 Konvensi Keselamatan. Dalam konteks keamanan maritim, peraturan ini menetapkan kewajiban operator kapal dan fasilitas pelabuhan untuk menerapkan sistem manajemen keamanan yang meliputi identifikasi ancaman, penilaian risiko,

dan langkah-langkah mitigasi. Kemudian mengatur pelaksanaan audit, inspeksi, dan sertifikasi keamanan kapal serta fasilitas pelabuhan guna memastikan kepatuhan terhadap standar keamanan yang telah ditetapkan serta memberikan panduan dalam penanganan insiden keamanan, seperti pembajakan, perompakan, dan kegiatan ilegal lainnya di lingkungan pelabuhan dan kapal. Ketiga regulasi ini membentuk kerangka hukum yang saling terkait untuk menjamin keamanan maritim di Indonesia, mulai dari aspek legal, operasional, hingga implementasi teknis lapangan.

2.2 Hasil Penelitian Terdahulu

Pemahaman yang mendalam tentang penelitian terdahulu dalam bidang studi yang relevan merupakan langkah krusial dalam pengembangan pengetahuan dan pemecahan masalah yang signifikan. Dalam konteks ini, penelitian terdahulu menyediakan landasan teoritis yang kuat dan merangkum temuan-temuan yang sebelumnya pernah dilakukan oleh para peneliti terdahulu. Penelitian sebelumnya dalam bidang ini telah menghasilkan sejumlah temuan yang berharga. Dalam rangka menyusun penelitian ini, studi literatur telah dilakukan untuk memahami perkembangan pengetahuan yang ada. Melalui referensi tersebut, peneliti dapat mempelajari temuan serta penemuan yang sebelumnya pernah dilakukan, penggunaan metode penelitian, serta disimilaritas penelitian sebelumnya dengan riset yang sedang dilakukan. Dengan menggunakan penelitian sebelumnya sebagai acuan, peneliti dapat mengidentifikasi kesenjangan pengetahuan yang masih ada dan menentukan pendekatan yang tepat dalam penelitian yang sedang dilakukan. Peneliti juga dapat memperoleh wawasan mengenai isu-isu yang perlu diperhatikan, metodologi yang berhasil, dan saran-saran yang diberikan oleh penelitian sebelumnya, sehingga dapat memberikan kontribusi signifikan dalam bidang ini. Penelitian-penelitian yang memiliki relevansi dengan penelitian ini, yaitu:

- a. Penelitian oleh (Papageorgiou et al., 2024) dengan judul "*Using*

a Proposed Risk Computation Procedure and the Bow-Tie diagram as a method for Maritime Security Assessment". Hasil penelitian ini mengusulkan kerangka kerja secara efektif mengkonsolidasikan informasi tentang ancaman, tindakan pencegahan, dan pihak yang bertanggung jawab, sehingga memfasilitasi pengambilan keputusan yang tepat dalam keamanan maritim. Selain itu, perangkat lunak yang mudah digunakan meningkatkan proses penghitungan risiko, memberikan umpan balik visual langsung tentang nilai risiko dan efektivitas langkah-langkah yang diterapkan. Persamaannya, yaitu pembahasan mengenai ISPS Code dan aspek keamanan maritim. Perbedaannya terletak pada metode dan fokus yang diteliti, yaitu penilaian risiko keamanan maritim menggunakan alat bantu diagram *Bow-Tie*, sedangkan fokus peneliti pada pengaruh ISPS Code terhadap ancaman non tradisional menggunakan analisis statistik regresi linier sederhana dengan 2 pengujian hipotesis penelitian. Relevansinya, yaitu berhubungan dengan ISPS Code yang bertujuan untuk mengatasi masalah keamanan maritim.

- b. Penelitian oleh (Ibrahim, 2024) dengan judul "*The Influence of Computerized Simulation Techniques on Maritime Security Exercises: ISPS Code*". Hasil penelitian menunjukkan bahwa dengan mengintegrasikan teknologi imersif ke dalam latihan meja dapat meningkatkan eksposur realistis terhadap skenario. Simulasi terkomputerisasi menawarkan pengalaman praktis dan interaktif untuk personel khusus keamanan. Kurangnya simulasi imersif dapat menunda kualifikasi dan persiapan personel keamanan. Persamaannya, yaitu membahas mengenai ISPS Code dan aspek keamanan maritim. Perbedaannya, yaitu penelitian ini berfokus pada pengaruh teknik simulasi terkomputerisasi pada latihan keamanan maritim sedangkan

peneliti berfokus pada pengaruh ISPS Code secara menyeluruh termasuk keamanan kapal dan fasilitas pelabuhan. Relevansinya, yaitu berhubungan dengan pembahasan mengenai ISPS Code dan aspek keamanan maritim.

- c. Penelitian oleh (Da Rosa et al., 2023) dengan judul "*Safety risk assessment of port facilities*". Hasil penelitian menunjukkan bahwa risiko keamanan di fasilitas pelabuhan, khususnya di Terminal Pelabuhan Santa Catarina (TESC) di Brasil, berada dalam kendali yang baik, dengan skor kinerja global sebesar 79,91 poin dari 100. Ini mencerminkan manajemen yang efektif dan langkah-langkah perlindungan yang diterapkan. Penelitian ini juga mengidentifikasi 17 risiko keamanan spesifik dan mengembangkan konsep untuk mengelola risiko tersebut secara efektif, dengan tujuan meningkatkan manajemen keamanan pelabuhan dan memastikan kontinuitas operasional. Persamaannya, yaitu sama-sama menekankan pentingnya struktur perlindungan yang sesuai dengan regulasi internasional, yaitu *ISPS Code* untuk meningkatkan keamanan di fasilitas pelabuhan. Perbedaannya, terletak pada lokasi studi, fokus dan konteks yang diteliti. Penelitian ini lebih menekankan pada analisis risiko keamanan di Terminal Pelabuhan Santa Catarina (TESC) di Brasil, sedangkan peneliti berfokus pada pengaruh ISPS Code secara menyeluruh termasuk keamanan kapal dan fasilitas pelabuhan dalam konteks keamanan maritim. Relevansinya, yaitu berhubungan dengan penerapan ISPS Code yang merupakan standar internasional utama yang mengatur keamanan pelabuhan dan bahwa penerapannya di Brasil telah mempengaruhi konteks keamanan pelabuhan di negara tersebut.
- d. Penelitian oleh Abdurrasyid, M. R., Nur, H. I., & Lazuardi, S. D. (2023) dengan judul "*Analisis Penerapan International Ship and*

Port Facility Security (ISPS) Code di Indonesia". Hasil penelitian menunjukkan bahwa penerapan ISPS Code setelah dianalisis di tiga lokasi berikut, yaitu Terminal Tanjung Priok: Prioritaskan tindakan 'Dokumen' untuk semua kriteria, risiko sangat rendah. Terminal Gapura Surya: Perlu perbaikan, risiko tinggi dalam beberapa skenario dan kriteria tidak dilaksanakan sesuai dengan ISPS Code. PT. ISM Bogasari: Membutuhkan langkah-langkah keamanan yang ditingkatkan untuk fasilitas pelabuhan. Persamaannya, yaitu sama-sama penelitian kuantitatif menggunakan kuesioner dan membahas mengenai penerapan ISPS Code di Indonesia. Perbedaanya terletak pada lokasi studi penelitian ini, yaitu di pelabuhan utama Indonesia, yaitu Pelabuhan Tanjung Priok dan Pelabuhan Tanjung Perak sedangkan lokus peneliti di Pelabuhan kecil dan menengah seperti Pelabuhan Kuala Tanjung. Selain itu, penelitian ini berfokus pada tingkat penerapan berdasarkan analisis risiko ancaman, kerentanan, dan dampak untuk kepatuhan Kode ISPS, sedangkan peneliti berfokus pada pengaruh ISPS Code dengan variabel dependen keamanan kapal dan fasilitas pelabuhan terhadap variabel independen, yaitu keamanan Maritim. Relevansinya, yaitu berhubungan dengan penerapan ISPS Code di Indonesia dan pembahasan mengenai pengembangan keamanan dan keselamatan pada kapal dan pelabuhan.

- e. Penelitian oleh (Ávila-Zúñiga-nordfjeld et al., 2023) dengan judul "*Proposing a Mathematical Dynamic Model to Develop a National Maritime Security Assessment and Build a National Maritime Security Plan*". Penelitian ini menunjukkan bahwa hasil dari pendekatan berbasis risiko dalam implementasi dan penegakan Kode ISPS yang diterapkan di tingkat fasilitas pelabuhan dan kapal, akan sangat bermanfaat untuk mengembangkannya lebih

lanjut ke tingkat nasional dengan menerapkan pendekatan nasional dan holistik tidak hanya untuk meningkatkan penilaian risiko keamanan tetapi juga mengelola sumber daya manusia, ekonomi, dan material terkait ancaman keamanan maritim yang telah diidentifikasi. Persamaannya, yaitu sama-sama penelitian kuantitatif, yang membahas penerapan ISPS Code dan menunjukkan perhatian yang sama terhadap keamanan maritim. Perbedaannya, yaitu penelitian ini melibatkan lima negara dan masing-masing tiga pelabuhan dengan mengusulkan model matematis untuk melakukan penilaian risiko keamanan maritim yang berlandaskan pada ISPS Code, yang bertujuan untuk meningkatkan perencanaan keamanan maritim nasional dan kesadaran situasional di pelabuhan-pelabuhan suatu negara sedangkan peneliti fokus pada Pelabuhan Kuala Tanjung dan menganalisis pengaruh ISPS Code terhadap aspek keamanan maritim. Relevansinya, yaitu berhubungan dengan pembahasan mengenai ISPS Code dan aspek keamanan maritim.

- f. Penelitian oleh (Wiko et al., 2023) dengan judul "*Tanjungpura Port as an International Hub Port to Improve Economic Competitiveness: an Overview from International Law*". Hasil penelitian menunjukkan bahwa konsekuensi dari status "hub internasional" adalah diperlukannya sistem pengelolaan dan pengaturan pelabuhan internasional yang terbaik untuk diterapkan di Pelabuhan Tanjungpura Terminal Kijing. Rencana pengembangan meliputi Smelter Bauksit, Kawasan Industri Kijing, dan KEK. Agar tata kelola yang efisien di Pelabuhan Tanjungpura membutuhkan reposisi peran pemerintah dalam pengelolaan dan pengembangan pelabuhan dengan fokus mendukung mekanisme pasar. Persamaannya terletak pada pembahasan mengenai peraturan nasional dan internasional terkait pelabuhan. Perbedaannya, yaitu lokasi studi pada

penelitian ini berbeda dengan peneliti, yaitu di Pelabuhan Tanjungpura dengan fokus penelitian mempelajari rencana pembangunan Terminal Kijing untuk meningkatkan daya saing daerah sedangkan peneliti berfokus pada keamanan kapal dan fasilitas pelabuhan di Kuala Tanjung. Relevansinya, yaitu berhubungan dengan peraturan nasional dan internasional terkait pelabuhan, termasuk keselamatan dan keamanan kapal, peraturan lalu lintas manajemen kapal dan pemeriksaan kapal yang berlabuh, serta penanganan kargo yang berbahaya.

- g. Penelitian oleh (Kapalidis et al., 2022) dengan judul “*A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships*”. Hasil penelitian menunjukkan bahwa sektor maritim, khususnya pelabuhan dan kapal, memiliki ekosistem siber yang kompleks dengan ancaman yang signifikan, terutama pada sistem teknologi operasional (OT). Penelitian ini mengidentifikasi bahwa kejadian siber dapat menyebabkan konsekuensi serius. Temuan juga menekankan perlunya pendekatan manajemen risiko yang holistik untuk mengatasi ancaman lanskap siber yang terus berkembang di sektor maritim. Selain itu, penelitian ini mengungkapkan bahwa banyak komponen sektor maritim semakin rentan terhadap ancaman siber, yang dapat memiliki dampak sosial-ekonomi yang signifikan. Persamaannya, yaitu terletak pada fokus keduanya terhadap aspek keamanan maritim. Perbedaan penelitian ini dapat dilihat dari fokusnya, yaitu penelitian ini lebih menekankan pada kerentanan siber dan manajemen risiko sedangkan peneliti berfokus pada pengaruh ISPS Code. Relevansinya, yaitu berhubungan dengan penerapan ISPS Code di Indonesia dan pembahasan mengenai pengembangan keamanan dan keselamatan pada kapal dan pelabuhan.

Penelitian ini juga relevan dengan penerapan ISPS Code yang bertujuan untuk meningkatkan keamanan di pelabuhan dan kapal dengan menekankan perlunya langkah-langkah proaktif untuk melindungi infrastruktur maritim dari berbagai ancaman.

- h. Penelitian oleh (Hasanov & Alsulaiman, 2021) dengan judul "*Evaluating the implementation framework of the International Ship and Port Facility Security Code in the Republic of Azerbaijan*". Penelitian menghasilkan evaluasi implementasi Kode ISPS di fasilitas pelabuhan Azerbaijan dengan survei menunjukkan pandangan yang beragam tentang tingkat keamanan. Langkah-langkah keamanan di fasilitas pelabuhan umumnya efektif. Penjaga keamanan menerima pelatihan dan terlibat dalam latihan keamanan. Kemudian pelaut menemukan fasilitas pelabuhan aman dan memiliki staf yang memadai. Selain itu perlu perbaikan untuk masa depan termasuk meningkatkan komunikasi dan kerja sama di antara para pemangku kepentingan. Azerbaijan melebihi persyaratan IMO untuk keamanan maritim di Laut Kaspia. Secara keseluruhan, implementasi ISPS Code di Azerbaijan telah berhasil, dan tingkat keamanan telah dipertahankan pada tingkat yang tinggi; namun ada beberapa area yang perlu ditingkatkan. Persamaannya, yaitu membahas implementasi ISPS Code berdasarkan peraturan dan pedoman terkait dengan responden penelitian adalah orang yang bertanggung jawab atas keamanan kapal dan fasilitas pelabuhan. Perbedaannya, pada lokasi studi penelitian ini berbeda dengan peneliti, yaitu di Azerbaijan. Fokus penelitian ini, yaitu untuk mengevaluasi kerangka kerja implementasi spesifik ISPS Code dan memeriksa langkah-langkah keamanan yang berbeda di berbagai fasilitas pelabuhan (melibatkan beberapa fasilitas pelabuhan) di Republik Azerbaijan, sedangkan peneliti berfokus pada keamanan kapal dan fasilitas

di satu pelabuhan, yaitu Pelabuhan Kuala Tanjung. Relevansinya, yaitu bhubungan dengan pembahasan mengenai penerapan ISPS Code.

- i. Penelitian oleh (Onwuegbuchunam et al., 2021) dengan judul "*Maritime Security Regimes and Impacts on Nigerian Seaports*". Hasil penelitian menunjukkan bahwa penerapan langkah-langkah keamanan yang tepat dapat mengurangi insiden keamanan pelabuhan dan meningkatkan kinerja pelabuhan Nigeria. Hubungan yang signifikan antara langkah-langkah keamanan pelabuhan, insiden, dan kinerja pelabuhan. Nilai statistik F yang tinggi menunjukkan efek substansial pada keamanan dan kinerja pelabuhan. Persamaannya, yaitu membahas mengenai rezim keamanan maritim termasuk ISPS Code dan sama-sama penelitian kuantitatif menggunakan kuesioner dengan populasi penelitian operator pelabuhan termasuk petugas keamanan fasilitas pelabuhan. Perbedaannya terletak pada lokasi studi penelitian ini, yaitu di Pelabuhan Nigeria. Variabel yang digunakan pada penelitian ini berbeda dengan peneliti, yaitu langkah-langkah keamanan pelabuhan sebagai variabel eksogen laten dan variabel endogen laten terdiri dari dua, yaitu kinerja pelabuhan dan insiden keamanan pelabuhan. variabel manifes ada 14, yaitu ada langkah-langkah keamanan yang memadai di pelabuhan, pelabuhan/terminal sesuai dengan implementasi kode ISPS, terdapat langkah-langkah untuk memastikan kepatuhan terhadap kode ISPS, perdagangan manusia, perdagangan gelap narkoba, senjata dan amunisi, barang selundupan, pencurian kargo, perampokan bersenjata, serangan terhadap kapal, hilangnya kargo peti kemas, penumpang gelap, hasil muatan kargo, dan lalu lintas kapal. Namun penelitian ini masih memiliki relevansi, yaitu berhubungan dengan pembahasan rezim keamanan maritim

pada pelabuhan.

- j. Penelitian yang dilakukan oleh (Radonja & Glujić, 2020) dengan judul “*Safety Aspects of ISPS Code Onboard Practice*”. Hasil penelitian menunjukkan bahwa prosedur yang diterapkan untuk meningkatkan keamanan di atas kapal dapat membahayakan keselamatan awak kapal jika tidak dilaksanakan secara memadai. Dalam hal ini, tanggung jawab atas implementasi yang buruk tidak selalu berada di tangan awak kapal, karena perusahaan juga harus terlibat pengecekan dan perbaikan. Pelaut dalam latihan 'Pencarian Bom' tahu apa yang mereka cari sedangkan Pelaut dalam latihan 'Deteksi objek tak teridentifikasi' mungkin kurang sadar. Persamaan penelitian dengan tesis ini adalah sama-sama penelitian kuantitatif menggunakan kuesioner dan membahas mengenai penerapan ISPS Code. Perbedaannya terletak pada lokasi studi penelitian ini, yaitu di Kroasia sedangkan peneliti mengambil lokasi studi di Pelabuhan Kuala Tanjung. Selain itu, fokus penelitian ini terbatas pada masalah keamanan di atas kapal saja, sedangkan peneliti berfokus pada pengaruh ISPS Code secara menyeluruh termasuk keamanan kapal dan fasilitas pelabuhan. Responden penelitian juga terbatas pada peserta kursus pelatihan 'Kepemimpinan dan kerja sama tim' yang diselenggarakan di Fakultas Maritim di Rijeka, Kroasia pada tahun 2016. Variabel yang diteliti mengenai 'prosedur pelaksanaan' untuk setiap pelatihan yang dilakukan oleh responden seperti 'Pencarian bom' dan 'Deteksi objek tak dikenal'. Relevansinya yaitu berhubungan dengan pembahasan mengenai keselamatan awak kapal dan keamanan kapal dan praktik ISPS Code di atas kapal serta kasus terkait keamanan maritim.
- k. Penelitian yang dilakukan oleh (Elentably, 2020) dengan judul “*The ISPS code gap requirements costs and related financing by*

the implementation in Saudi Ports". Hasil penelitian ini menjelaskan implikasi Kode ISPS pada perdagangan internasional dan langkah-langkah keamanan. Tantangan dalam pembiayaan implementasi ISPS di pelabuhan dan pentingnya menyesuaikan hubungan untuk rantai pasokan fleksibel. Persamaan penelitian dengan tesis ini adalah sama-sama membahas mengenai ISPS Code. Perbedaannya terletak pada lokasi studi penelitian, yaitu lokasi implementasi pada penelitian ini di Pelabuhan Saudi. Fokus penelitian ini terkait pada kesenjangan biaya persyaratan ISPS Code dan pembiayaan terkait dengan implementasi di Pelabuhan Saudi. Namun penelitian ini masih memiliki relevansi, yaitu berhubungan dengan pembahasan mengenai ISPS Code.

- I. Penelitian oleh (Farisi et al., 2020) dengan judul "*Facility Security Measures at Ujung Jabung Port: a Review in Terms of The International Ship and Port Facility Security Code*". Hasil penelitian menunjukkan bahwa konsep pengembangan dan pembangunan Pelabuhan Samudera Ujung Jabung dibagi menjadi dua kategori. Pelabuhan dikategorikan untuk pengembangan pelabuhan internasional atau pelabuhan pengumpul dan aplikasi Kode ISPS penting untuk pembangunan pelabuhan Ujung Jabung. Meskipun dua kategori pelabuhan telah ditetapkan untuk Pelabuhan Ujung Jabung, pemerintah harus mempertahankan penerapan ISPS Code dalam pembangunan pelabuhan. Dengan lokasi pelabuhan yang strategis dan nilai ekonomi dari kegiatan pelayaran di sekitar pelabuhan, ada peluang untuk meningkatkan status pelabuhan menjadi pelabuhan utama untuk melayani kegiatan perdagangan dan pelayaran internasional. Persamaannya, yaitu membahas penerapan ISPS Code di Indonesia. Perbedaannya, pada lokasi studi penelitian ini, yaitu di Pelabuhan Ujung Jabung dan fokus

penelitian ini pada pengembangan dan pembangunan Pelabuhan Ujung Jabung dengan metode penelitian kualitatif sedangkan peneliti menggunakan metode kuantitatif yang berfokus pada pengaruh ISPS Code di Pelabuhan Kuala Tanjung dengan variabel dependen keamanan kapal dan fasilitas pelabuhan terhadap variabel independen, yaitu keamanan Maritim. Relevansinya yaitu berhubungan dengan pembahasan mengenai ISPS Code.

Berdasarkan penjelasan tersebut, maka bisa dilihat pada tabel di bawah ini adalah matriks perbandingan dari beberapa penelitian terdahulu:

Tabel 2.1 Penelitian Terdahulu

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
1.	Papageorgiou et al., (2024)	<i>Using a Proposed Risk Computation Procedure and the Bow-Tie diagram as a method for Maritime Security Assessment</i>	Penelitian Kuantitatif	Hasil penelitian mengusulkan kerangka kerja secara efektif mengkonsolidasikan informasi tentang ancaman, tindakan pencegahan, dan pihak yang bertanggung jawab, sehingga memfasilitasi pengambilan keputusan yang tepat dalam keamanan maritim. Selain itu, perangkat lunak yang mudah digunakan meningkatkan proses penghitungan risiko, memberikan umpan balik visual langsung tentang nilai risiko dan efektivitas langkah-langkah yang diterapkan.	Sama-sama membahas mengenai ISPS Code dan aspek keamanan maritim.	Perbedaan terletak pada metode dan fokus yang diteliti, yaitu penilaian risiko keamanan maritim melalui identifikasi risiko, analisis risiko dan evaluasi risiko, dengan menggunakan alat bantu diagram Bow-Tie, sedangkan fokus peneliti pengaruh ISPS Code terhadap ancaman non tradisional menggunakan analisis statistik regresi linier sederhana dengan 2 pengujian hipotesis penelitian.	Berhubungan dengan ISPS Code yang bertujuan untuk mengatasi masalah keamanan maritim.

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
2	Ahmed Mohy Ibrahim (2024)	<i>The Influence of Computerized Simulation Techniques on Maritime Security Exercises: ISPS Code</i>	Penelitian Kuantitatif.	Mengintegrasikan teknologi imersif ke dalam latihan meja dapat meningkatkan eksposur realistis terhadap skenario. Simulasi terkomputerisasi menawarkan pengalaman praktis dan interaktif untuk personel khusus keamanan. Kurangnya simulasi imersif menunda kualifikasi dan persiapan personel keamanan.	Membahas mengenai ISPS Code dan aspek keamanan maritim	Penelitian ini berfokus pada pengaruh teknik simulasi terkomputerisasi pada latihan keamanan maritim sedangkan peneliti berfokus pada pengaruh ISPS Code secara menyeluruh termasuk keamanan kapal dan fasilitas pelabuhan.	Berhubungan dengan pembahasan mengenai ISPS Code dan aspek keamanan maritim
3	Izaias Otacilio da Rosa, et al. (2023)	<i>Safety risk assessment of port facilities</i>	Penelitian eksplorasi dengan studi kasus dan metodologi MCDA-C.	Hasil penelitian menunjukkan bahwa risiko keamanan di fasilitas pelabuhan, khususnya di Terminal Pelabuhan Santa Catarina (TESC) di Brasil, berada dalam kendali yang baik, dengan skor kinerja global sebesar 79,91 poin dari 100. Ini mencerminkan manajemen yang efektif dan langkah-langkah perlindungan yang diterapkan.	Menekankan pentingnya struktur perlindungan yang sesuai dengan regulasi internasional, yaitu ISPS Code untuk meningkatkan keamanan di fasilitas pelabuhan.	Fokus dan konteks yang diteliti. Penelitian ini lebih menekankan pada analisis risiko keamanan di Terminal Pelabuhan Santa Catarina (TESC) di Brasil, termasuk identifikasi 17 risiko keamanan spesifik dan pengembangan konsep manajemen risiko.	Berhubungan dengan penerapan ISPS Code, standar internasional utama yang mengatur keamanan pelabuhan dan bahwa penerapannya di Brasil telah

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
							mempengaruhi konteks keamanan pelabuhan di negara tersebut.
4	Muhammad Raihan Abdurrasyid, dkk. (2023)	Analisis Penerapan <i>International Ship and Port Facility Security (ISPS) Code</i> di Indonesia	Penelitian kuantitatif menggunakan analisis risiko ancaman, kerentanan, dan dampak untuk kepatuhan	Terminal Tanjung Priok: Prioritaskan tindakan 'Dokumen' untuk semua kriteria, risiko sangat rendah. Terminal Gapura Surya: Perlu perbaikan, risiko tinggi dalam beberapa skenario dan kriteria tidak dilaksanakan sesuai dengan ISPS Code. PT. ISM Bogasari: Membutuhkan langkah-langkah keamanan yang ditingkatkan untuk fasilitas pelabuhan.	Membahas mengenai penerapan ISPS Code. Penelitian kuantitatif menggunakan kuesioner	Lokus pada penelitian ini di pelabuhan utama Indonesia, yaitu Pelabuhan Tanjung Priok dan Pelabuhan Tanjung Perak sedangkan lokus peneliti di Pelabuhan kecil dan menengah seperti Pelabuhan Kuala Tanjung. Penelitian ini berfokus pada tingkat penerapan berdasarkan analisis risiko ancaman, kerentanan, dan dampak untuk kepatuhan Kode ISPS, sedangkan peneliti berfokus pada pengaruh ISPS Code dengan variabel dependen keamanan kapal dan fasilitas pelabuhan terhadap variabel	Berhubungan dengan penerapan ISPS Code di Indonesia dan pembahasan mengenai pengembangan keamanan dan keselamatan pada kapal dan pelabuhan.

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
						independen, yaitu keamanan Maritim.	
5	Adriana Avila-Z' u'niga-Nordfjeld, et al. (2023)	<i>Proposing a Mathematical Dynamic Model to Develop a National Maritime Security Assessment and Build a National Maritime Security Plan</i>	Penelitian kuantitatif dengan menggunakan model matematika untuk perhitungan risiko waktu nyata	Hasil dari pendekatan berbasis risiko dalam implementasi dan penegakan Kode ISPS yang diterapkan di tingkat fasilitas pelabuhan dan kapal, akan sangat bermanfaat untuk mengembangkannya lebih lanjut ke tingkat nasional dengan menerapkan pendekatan nasional dan holistik tidak hanya untuk meningkatkan penilaian risiko keamanan tetapi juga mengelola sumber daya manusia, ekonomi, dan material terkait ancaman keamanan maritim yang telah diidentifikasi	Penelitian kuantitatif, yang membahas penerapan ISPS Code dan menunjukkan perhatian yang sama terhadap keamanan maritim	Penelitian ini melibatkan lima negara dan masing-masing tiga pelabuhan dengan mengusulkan model matematis untuk melakukan penilaian risiko keamanan maritim yang berlandaskan pada ISPS Code, yang bertujuan untuk meningkatkan perencanaan keamanan maritim nasional dan kesadaran situasional di pelabuhan-pelabuhan suatu negara sedangkan peneliti fokus pada Pelabuhan Kuala Tanjung dan menganalisis pengaruh ISPS Code terhadap aspek keamanan maritim	Berhubungan dengan pembahasan mengenai ISPS Code dan aspek keamanan maritim
6	Garuda Wiko, et al. (2023)	<i>Tanjungpura Port as an International Hub Port to</i>	Penelitian normatif dengan pendekatan	Hasil penelitian menunjukkan bahwa konsekuensi dari status "hub internasional" adalah diperlukannya sistem	Membahas peraturan nasional dan internasional	Lokus pada penelitian ini berbeda dengan peneliti, yaitu di Pelabuhan Tanjungpura dengan fokus	Berhubungan dengan peraturan nasional dan

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
		<i>Improve Economic Competitiveness: an Overview from International Law</i>	studi hukum in-concreto	manajemen dan regulasi pelabuhan internasional terbaik untuk diterapkan di Terminal Kijing Pelabuhan Tanjungpura. Adanya rencana pengembangan meliputi Smelter Bauksit, Kawasan Industri Kijing, dan KEK. Agar tata kelola yang efisien di Pelabuhan Tanjungpura membutuhkan reposisi peran pemerintah dalam manajemen dan pengembangan pelabuhan dengan berfokus pada dukungan terhadap mekanisme pasar.	terkait pelabuhan.	penelitian mempelajari rencana pembangunan Terminal Kijing untuk meningkatkan daya saing daerah sedangkan peneliti berfokus pada keamanan kapal dan fasilitas pelabuhan di Kuala Tanjung.	internasional terkait pelabuhan, termasuk keselamatan dan keamanan kapal, peraturan lalu lintas manajemen kapal dan pemeriksaan kapal yang berlabuh, serta penanganan kargo yang berbahaya
7	Kapalidis et al., (2022)	<i>A Vulnerability Centric System of Systems Analysis on</i>	Metode penelitian kualitatif, yang terdiri dari tiga tahap: (1)	Hasil penelitian menunjukkan bahwa sektor maritim, khususnya pelabuhan dan kapal, memiliki ekosistem siber yang kompleks dengan ancaman yang signifikan,	Membahas aspek keamanan maritim.	Penelitian ini dapat dilihat dari fokusnya yang lebih menekankan pada kerentanan siber dan manajemen risiko sedangkan	Berhubungan dengan penerapan ISPS Code yang bertujuan

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
		<i>the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships</i>	Penelitian kepustakaan, (2) Keterlibatan pemangku kepentingan dan (3) Validasi temuan	terutama pada sistem teknologi operasional (OT). Penelitian ini mengidentifikasi bahwa kejadian siber dapat menyebabkan konsekuensi serius. Temuan juga menekankan perlunya pendekatan manajemen risiko yang holistik untuk mengatasi ancaman lanskap siber yang terus berkembang di sektor maritim. Selain itu, penelitian ini mengungkapkan bahwa banyak komponen sektor maritim semakin rentan terhadap ancaman siber, yang dapat memiliki dampak sosial-ekonomi yang signifikan		peneliti berfokus pada pengaruh ISPS Code.	untuk meningkatkan keamanan di pelabuhan dan kapal dengan menekankan perlunya langkah-langkah proaktif untuk melindungi infrastruktur maritim dari berbagai ancaman.
8	Hasanov & Alsulaiman, (2021)	<i>Evaluating the implementation framework of the International Ship</i>	Teknik penelitian kualitatif dan kuantitatif digunakan	Penjaga keamanan menerima pelatihan dan terlibat dalam latihan keamanan. Pelaut menemukan fasilitas pelabuhan aman dan memiliki staf yang memadai. Perbaikan masa depan	Membahas implementasi ISPS Code berdasarkan peraturan dan pedoman terkait.	Lokus penelitian ini berbeda dengan peneliti, yaitu di Azerbaijan. Fokus penelitian ini, yaitu untuk mengevaluasi kerangka kerja implementasi spesifik ISPS Code dan memeriksa langkah-langkah	Berhubungan dengan pembahasan mengenai penerapan ISPS Code

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
		<i>and Port Facility Security Code in the Republic of Azerbaijan</i>	untuk evaluasi.	termasuk meningkatkan komunikasi dan kerja sama di antara para pemangku kepentingan. Azerbaijan melebihi persyaratan IMO untuk keamanan maritim di Laut Kaspia. Secara keseluruhan, implementasi ISPS Code di Azerbaijan telah berhasil, dan tingkat keamanan telah dipertahankan pada tingkat yang tinggi; namun ada beberapa area yang perlu ditingkatkan.	Responden penelitian adalah orang yang bertanggung jawab atas keamanan kapal dan fasilitas pelabuhan.	keamanan yang berbeda di berbagai fasilitas pelabuhan (melibatkan beberapa fasilitas pelabuhan) di Republik Azerbaijan, sedangkan peneliti berfokus pada keamanan kapal dan fasilitas di satu pelabuhan, yaitu Pelabuhan Kuala Tanjung.	
9	Donatus E. Onwuegbuchunam, et al. (2021)	<i>Maritime Security Regimes and Impacts on Nigerian Seaports</i>	Penelitian kuantitatif menggunakan kuesioner skala Likert. Model Partial Least Squares diterapkan	Hasil penelitian menunjukkan bahwa penerapan langkah-langkah keamanan yang tepat dapat mengurangi insiden keamanan pelabuhan dan meningkatkan kinerja pelabuhan Nigeria. Hubungan yang signifikan antara langkah-langkah keamanan pelabuhan, insiden,	Membahas mengenai rezim keamanan maritim termasuk ISPS Code. Penelitian kuantitatif menggunakan	Lokus penelitian ini berbeda dengan peneliti, yaitu di Pelabuhan Nigeria. Fokus penelitian ini terbatas pada variabel yang digunakan pada penelitian ini berbeda dengan peneliti, yaitu langkah-langkah keamanan pelabuhan sebagai variabel eksogen laten dan variabel	Berhubungan dengan pembahasan rezim keamanan maritim pada pelabuhan

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
			untuk menguji hipotesis.	dan kinerja pelabuhan. Nilai statistik F yang tinggi menunjukkan efek substansial pada keamanan dan kinerja pelabuhan.	n kuesioner dengan populasi penelitian operator pelabuhan termasuk petugas keamanan fasilitas pelabuhan	endogen laten terdiri dari dua, yaitu kinerja pelabuhan dan insiden keamanan pelabuhan. variabel manifes ada 14, yaitu ada langkah-langkah keamanan yang memadai di pelabuhan, pelabuhan/terminal sesuai dengan implementasi kode ISPS, terdapat langkah-langkah untuk memastikan kepatuhan terhadap kode ISPS, perdagangan manusia, perdagangan gelap narkoba, senjata dan amunisi, barang selundupan, pencurian kargo, perampokan bersenjata, serangan terhadap kapal, hilangnya kargo peti kemas, penumpang gelap, hasil muatan kargo, dan lalu lintas kapal	

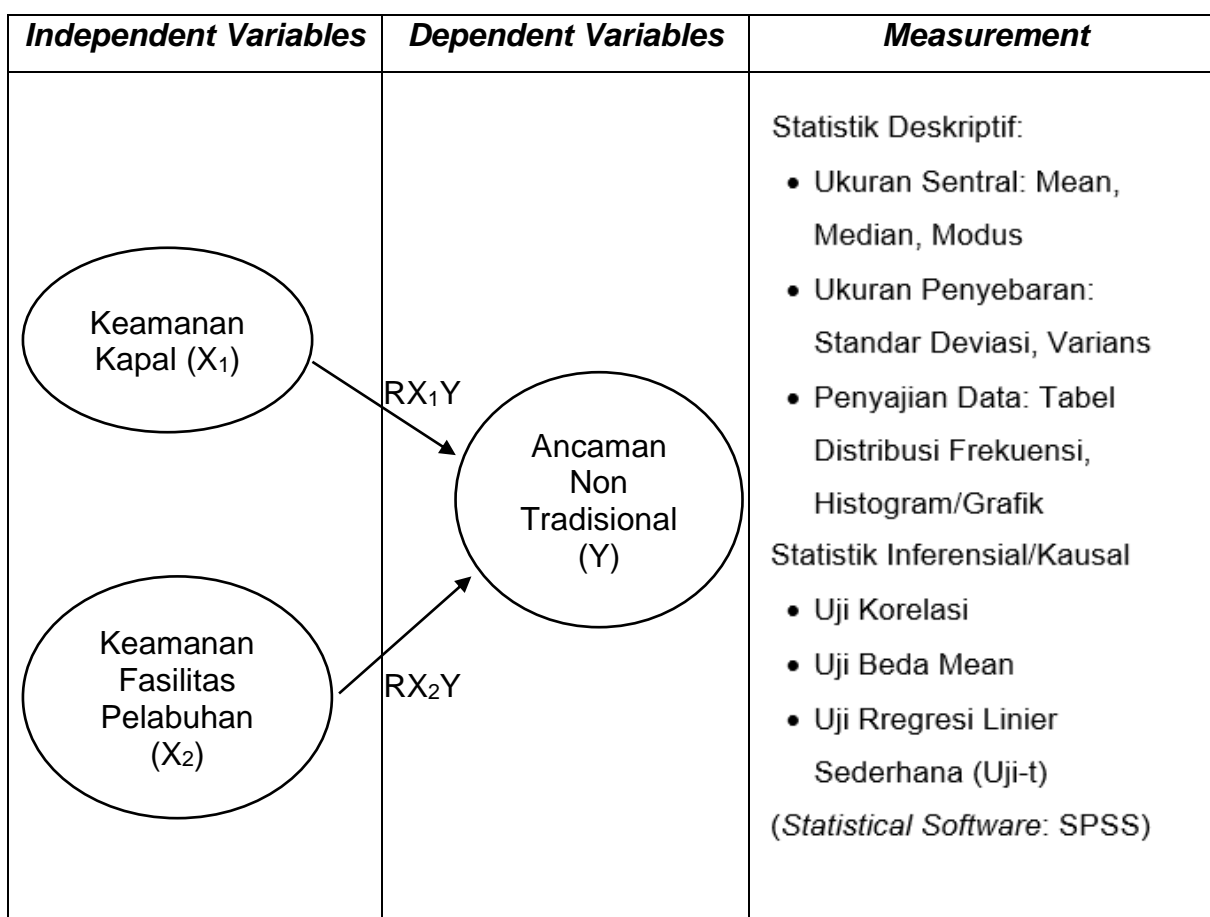
No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
10	Radoslav Radonja and Darko Glujić (2020)	<i>Safety Aspects of ISPS Code Onboard Practice</i>	Penelitian ini menggunakan metode kuantitatif. Data dianalisis dari kuesioner dan diskusi dengan petugas maritim	Hasil penelitian menunjukkan bahwa prosedur yang diterapkan untuk meningkatkan keamanan di atas kapal dapat membahayakan keselamatan awak kapal jika tidak dilaksanakan secara memadai. Dalam hal ini, tanggung jawab atas implementasi yang buruk tidak selalu berada di tangan awak kapal, karena perusahaan juga harus terlibat pengecekan dan perbaikan. Pelaut dalam latihan 'Pencarian Bom' tahu apa yang mereka cari. Pelaut dalam latihan 'Deteksi objek tak teridentifikasi' mungkin kurang sadar	Membahas mengenai penerapan ISPS Code. Penelitian kuantitatif menggunakan kuesioner	Lokus penelitian ini berbeda dengan peneliti, yaitu di Kroasia. Fokus penelitian ini terbatas pada masalah keamanan di atas kapal saja, sedangkan peneliti berfokus pada pengaruh ISPS Code secara menyeluruh termasuk keamanan kapal dan fasilitas pelabuhan. Responden penelitian juga terbatas pada peserta kursus pelatihan 'Kepemimpinan dan kerja sama tim' yang diselenggarakan di Fakultas Maritim di Rijeka, Kroasia pada tahun 2016. Variabel yang diteliti mengenai 'prosedur pelaksanaan' untuk setiap pelatihan yang dilakukan oleh responden seperti 'Pencarian bom' dan 'Deteksi objek tak dikenal'.	Berhubungan dengan pembahasan mengenai keselamatan awak kapal dan keamanan kapal dan praktik ISPS Code di atas kapal serta kasus terkait keamanan maritim.

No	Nama Peneliti dan Tahun	Judul Penelitian	Metode Penelitian	Ringkasan Hasil Penelitian	Persamaan	Perbedaan	Relevansi
11	Akram Elentably (2020)	<i>The ISPS code gap requirements costs and related financing by the implementati on in Saudi Ports</i>	Penelitian kualitatif menggunakan evaluasi akuisisi data	Tantangan dalam pembiayaan implementasi ISPS di pelabuhan Saudi, yaitu pentingnya menyesuaikan hubungan untuk rantai pasokan fleksibel. Implikasi Kode ISPS pada perdagangan internasional dan langkah-langkah keamanan dijelaskan	Membahas mengenai ISPS Code	Lokasi implementasi pada penelitian ini di Pelabuhan Saudi. Fokus penelitian ini terkait pada kesenjangan biaya persyaratan ISPS Code dan pembiayaan terkait dengan implementasi di Pelabuhan Saudi	Berhubungan dengan pembahasan mengenai ISPS Code
12	Mochammad Farisi, et al. (2020)	<i>Facility Security Measures at Ujung Jabung Port: a Review in Terms of The International Ship and Port Facility Security Code</i>	Penelitian kualitatif. Studi pustaka dengan menggunakan beberapa dokumen hukum, termasuk implementasi	Hasil penelitian menunjukkan bahwa konsep pengembangan dan pembangunan Pelabuhan Samudera Ujung Jabung dibagi menjadi dua kategori. Pelabuhan dikategorikan untuk pengembangan pelabuhan internasional atau pelabuhan pengumpul dan aplikasi Kode ISPS penting untuk pembangunan pelabuhan Ujung Jabung.	Membahas penerapan ISPS Code di Indonesia	Lokus pada penelitian ini di Pelabuhan Ujung Jabung. Fokus penelitian ini pada pengembangan dan pembangunan Pelabuhan Ujung Jabung sedangkan peneliti berfokus pada pengaruh ISPS Code dengan variabel dependen keamanan kapal dan fasilitas pelabuhan terhadap variabel independen, yaitu keamanan Maritim	Berhubungan dengan pembahasan mengenai ISPS Code

Sumber: diolah oleh peneliti

2.3 Kerangka Pemikiran

Dalam penelitian ini langkah-langkah yang dilakukan oleh penulis dalam melakukan penelitian, yaitu pencarian jurnal maupun makalah yang berkaitan dengan topik yang akan penulis teliti. Setelah mencari data-data yang dibutuhkan, kemudian mengolahnya menjadi data dan menganalisis data, sehingga didapat hasil dari penelitian tersebut. Dalam kerangka berfikir ini terdapat dua variabel yaitu dependen dan independen. Variabel Independen adalah variabel yang dimanipulasi atau dikendalikan dalam percobaan, sedangkan variabel dependen adalah variabel yang diukur atau diamati dalam percobaan (Habeck, C. G., & Brickman, A. M. 2018). Berikut adalah bagan dari kerangka berfikir.



Bagan 2.1 Kerangka Pemikiran

Sumber: diolah oleh peneliti

Dalam penelitian ini terdapat dua variabel independent dan satu variabel dependen yang akan diuraikan sebagai berikut:

- a. Keamanan Kapal (X_1): Variabel ini mengacu pada aspek-aspek yang berkaitan dengan perlindungan kapal dari ancaman atau risiko keamanan. Elemen-elemen yang terkait dengan variabel ini mencakup:
 - 1) keamanan fisik kapal;
 - 2) integritas struktural kapal;
 - 3) sistem perlindungan bagi semua awak kapal;
 - 4) kebijakan dan prosedur pengamanan;
 - 5) sistem radio dan telekomunikasi, termasuk sistem dan jaringan komputer; serta
 - 6) area lain yang mungkin jika dirusak atau digunakan untuk pengamatan terlarang, dapat menimbulkan risiko terhadap orang, properti, atau operasi di atas kapal atau di dalam fasilitas pelabuhan.
- b. Keamanan Fasilitas Pelabuhan (X_2): Variabel ini mengacu pada aspek-aspek untuk memastikan keamanan di fasilitas pelabuhan agar tidak menjadi target atau tempat aktivitas ilegal dari ancaman keamanan. Elemen-elemen yang terkait dengan variabel ini mencakup:
 - 1) keamanan fisik;
 - 2) integritas struktural;
 - 3) sistem perlindungan personel;
 - 4) kebijakan prosedural;
 - 5) sistem radio dan telekomunikasi, termasuk sistem dan jaringan komputer;
 - 6) infrastruktur transportasi yang relevan;
 - 7) kegunaan (utilitas), serta
 - 8) area lain yang mungkin jika dirusak atau digunakan untuk pengamatan terlarang, dapat menimbulkan risiko terhadap

orang, properti, atau operasi dalam fasilitas pelabuhan.

c. Ancaman Non Tradisional (Y): Variabel ini merujuk pada ancaman keamanan yang tidak konvensional, seperti pembajakan dan perampokan bersenjata. Dalam penelitian ini, ancaman non-tradisional berfokus pada aktivitas yang dapat mengganggu operasi maritim atau pelabuhan dengan mempertimbangkan semua ancaman yang mungkin terjadi, yang berdasarkan pedoman ISPS Code dapat mencakup jenis insiden keamanan berikut:

- 1) kerusakan atau penghancuran kapal atau fasilitas pelabuhan, misalnya dengan bahan peledak, pembakaran, sabotase atau vandalisme;
- 2) pembajakan atau penyitaan kapal atau orang-orang yang ada di dalamnya;
- 3) merusak kargo, peralatan atau sistem penting kapal, atau perbekalan/gudang kapal;
- 4) akses atau penggunaan yang tidak sah, termasuk keberadaan penumpang gelap;
- 5) menyelundupkan senjata atau peralatan, termasuk senjata pemusnah massal;
- 6) penggunaan kapal untuk mengangkut orang-orang yang berniat menyebabkan insiden keamanan dan/atau perlengkapannya;
- 7) penggunaan kapal itu sendiri sebagai senjata atau sebagai sarana untuk menimbulkan kerusakan atau kehancuran;
- 8) serangan dari arah laut ketika sedang bersandar atau berlabuh; dan
- 9) serangan saat berada di laut.
- 10) penyumbatan; pintu masuk pelabuhan, kunci, pendekatan, dll; dan
- 11) serangan nuklir, biologi dan kimia.

2.4 Hipotesis

Berdasarkan atas kerangka pemikiran tersebut, maka dapat dilakukan perumusan hipotesis penelitiannya sebagai berikut:

- a. Terdapat pengaruh nyata antara keamanan kapal terhadap ancaman non tradisional Pelabuhan Kuala Tanjung di Selat Malaka.
- b. Terdapat pengaruh nyata antara keamanan fasilitas pelabuhan terhadap ancaman non tradisional Pelabuhan Kuala Tanjung di Selat Malaka.