BAB I
PENDAHULUAN

1.1 Latar Belakang

Sektor maritim memegang peranan fundamental dalam mendukung aktivitas ekonomi global. Lebih dari 90% perdagangan dunia dilakukan melalui jalur laut, dengan volume barang yang terus meningkat seiring globalisasi (Stopford, 2019). Jalur laut bukan sekadar sarana transportasi, tetapi juga penopang utama global supply chain yang menghubungkan produsen, konsumen, dan pasar lintas benua. Bagi negara maritim seperti Indonesia, jalur laut adalah nadi perekonomian nasional sekaligus penghubung vital antarwilayah. Perdagangan komoditas ekspor–impor, distribusi energi, serta logistik bahan pangan sangat bergantung pada kelancaran sektor ini.

Seiring meningkatnya kompleksitas perdagangan global, sektor maritim mengalami transformasi digital yang signifikan. Penerapan smart port, automated terminal operation systems, hingga penggunaan Internet of Things (IoT) di kapal dan pelabuhan menjadikan rantai logistik semakin efisien (Gill, 2022). Namun, digitalisasi yang pesat ini juga menciptakan kerentanan baru. Sistem maritim yang terkoneksi ke jaringan global tidak hanya berfungsi sebagai tulang punggung ekonomi, tetapi sekaligus menjadi target empuk bagi aktor jahat di ruang siber. Dengan demikian, risiko serangan siber di sektor maritim bukan lagi kemungkinan abstrak, melainkan ancaman nyata yang terbukti menimbulkan kerugian besar.

Beberapa kasus insiden siber maritim memperlihatkan besarnya dampak yang bisa ditimbulkan. Kasus serangan NotPetya pada tahun 2017 melumpuhkan Maersk Line, perusahaan pelayaran terbesar di dunia, sehingga menyebabkan 76 terminal kontainer di berbagai negara terhenti operasionalnya (Bendiek & Schulze, 2021). Kerugian yang ditaksir mencapai USD 300 juta tersebut menunjukkan betapa rapuhnya rantai pasok global ketika satu aktor utama diserang. Dampaknya merembet ke berbagai sektor, termasuk keterlambatan distribusi bahan baku industri, barang konsumsi, hingga komoditas pertanian

Kasus lain adalah serangan ransomware di Pelabuhan Rotterdam, Belanda,

yang melumpuhkan terminal kontainer dan menghambat arus perdagangan internasional. Insiden ini tidak hanya menimbulkan kerugian ekonomi langsung, tetapi juga mengurangi tingkat kepercayaan mitra dagang terhadap stabilitas rantai pasok Eropa (Daniel E., 2023). Di sisi lain, kasus Port of Antwerp (2011–2013) memperlihatkan bagaimana infiltrasi jaringan komputer pelabuhan dimanfaatkan untuk penyelundupan narkoba. Selama hampir dua tahun, para pelaku berhasil memanipulasi sistem kontainer untuk menyelundupkan barang terlarang sebelum akhirnya terbongkar (Port of Antwerp, 2014; Caldwell, 2014). Kasus ini menegaskan bahwa ancaman siber tidak hanya berdimensi ekonomi, tetapi juga berdampak pada keamanan sosial dan kriminalitas lintas negara.

Jenis ancaman yang dihadapi sektor maritim sangat beragam, mulai dari ransomware, Distributed Denial of Service (DDoS), manipulasi data navigasi GPS, hingga pencurian data sensitif (Liu et al., 2021). Ancaman ini dapat dilancarkan oleh berbagai aktor, baik negara, kelompok kriminal, maupun peretas independen. Motivasi mereka juga beragam: keuntungan finansial, sabotase geopolitik, spionase industri, bahkan terorisme. Dengan kata lain, sektor maritim kini menjadi arena baru bagi perebutan kepentingan strategis di ruang siber.

Pada sektor maritim, kasus seperti NotPetya yang melumpuhkan Maersk pada 2017, serangan ransomware di Pelabuhan Rotterdam, serta infiltrasi Port of Antwerp oleh kartel narkotika memperlihatkan betapa beragamnya aktor pelaku yang terlibat. NotPetya secara resmi ditangani oleh Rusia, khususnya unit intelijen militer GRU, karena penyebarannya bermula di Ukraina dan skalanya sulit dilakukan tanpa dukungan negara (Greenberg, 2018; Council of the European Union, 2020). Serangan ini bersifat destruktif, bukan sekadar pemerasan, sehingga konsisten dengan operasi geopolitik. Sebaliknya, ransomware yang menyerang Rotterdam diatribusikan pada kelompok kriminal siber, yang jelas menuntut uang tebusan demi keuntungan finansial (Daniel, 2023). Sementara itu, kasus Antwerp memperlihatkan keterlibatan kartel narkotika yang bekerja sama dengan peretas asal Eropa Timur untuk menyusup ke sistem manajemen kontainer dan memfasilitasi penyelundupan barang ilegal (Caldwell, 2014; Port of Antwerp, 2014). Kompleksitas ini menunjukkan bahwa isu keamanan siber tidak bisa

dipandang hanya dari lensa negara, melainkan melibatkan interaksi berbagai tipe aktor dengan motivasi yang berbeda-beda.

Keberagaman aktor yang menjadikan kerjasama internasional penting. dalam penelitian, regime theory digunakan untuk memahami alasan negara-negara memilih bekerja sama dalam menghadapi ancaman siber di sektor maritim. Teori ini berangkat dari asumsi bahwa di tingkat internasional, negara butuh prinsip, norma, aturan dan prosedur pengambilan keputusan (Krasner, 1983). Dalam isu siber, rezim internasional berfungsi menciptakan konsensus tentang perilaku yang dapat diterima, cara merespons pelanggaran, dan mekanisme atribusi terhadap pelaku. Tanpa rezim, respon tiap negara cenderung parsial, sebagaimana yang terjadi sebelum 2017 ketika Eropa belum punya instrumen kolektif dalam menghadapi serangan siber (Miadzvetskaya & Wessel, 2022).

Dampak serangan siber maritim tidak bisa dipandang sebelah mata. Dari sisi ekonomi, biaya kerugian yang ditimbulkan mencapai ratusan juta hingga miliaran dolar, serta menambah biaya logistik akibat keterlambatan distribusi. Dari sisi sosial, serangan siber berpotensi mengganggu distribusi kebutuhan pokok, energi, dan obat-obatan. Sementara itu, dari sisi geopolitik, serangan yang melumpuhkan pelabuhan utama dapat memengaruhi stabilitas kawasan, menurunkan daya saing global, serta melemahkan kepercayaan investor (Gill, 2022).

Demi mengatasi ancaman siber yang semakin banyak, telah ada beberapa rezim internasional yang berada di bidang keamanan siber. Seperti, ITU (International Telecommunication Union) yang mengatur telekomunikasi global, tetapi lebih berfokus teknis ketimbang keamanan. kemudian terdapat Budapest Convention on Cybercrime (2001) yang menjadi instrumen hukum internasional pertama, tetapi efektivitasnya terbatas karena negara-negara besar seperti Rusia dan Tiongkok menolak bergabung (Carrapico & Barrinha, 2017). Di kawasan Asia Tenggara, ASEAN Regional Forum (ARF) memang mulai mengangkat isu siber, tetapi forum ARF kurang menghasilkan aturan yang mengikat (Miadzvetskaya & Wessel, 2022).

Keterbatasan ini jelas terlihat ketika serangan besar benar-benar terjadi. NotPetya pada 2017 memperlihatkan lemahnya kesiapan baik negara maupun

perusahaan: sistem logistik global lumpuh, kerugian mencapai USD 250–300 juta hanya bagi Maersk, sementara ribuan perangkat di ratusan lokasi rusak permanen (ENISA, 2018; Chirgwin, 2018). Kasus Antwerp memperlihatkan bahwa kejahatan terorganisir bisa bertahan hampir dua tahun tanpa terdeteksi, yang berarti mekanisme deteksi dini dan koordinasi Eropa saat itu nyaris tidak berfungsi (European Commission, 2017). Rotterdam pun menunjukkan tidak adanya respons diplomatik kolektif, meskipun dampaknya jelas berskala Eropa (Daniel, 2023).

Menyadari kompleksitas ancaman tersebut, berbagai negara dan organisasi internasional mulai merumuskan kebijakan khusus untuk memperkuat ketahanan siber. Uni Eropa, misalnya, meluncurkan Cyber Diplomacy Toolbox (CDT) pada tahun 2017 sebagai instrumen diplomatik untuk merespons serangan siber. CDT mencakup koordinasi politik antarnegara anggota, mekanisme penjatuhan sanksi, hingga penguatan kerja sama internasional (European Commission, 2017; EEAS, 2020; European Union, 2023). Langkah ini menegaskan bahwa isu keamanan siber tidak dapat hanya dihadapi melalui solusi teknis, tetapi juga memerlukan pendekatan diplomasi multilateral.

CDT merupakan instrumen kebijakan yang dikembangkan dalam kerangka Common Foreign and Security Policy (CFSP) oleh Uni Eropa dan ditujukan untuk mencegah, menghalangi, serta merespons tindakan berbahaya di dunia maya melalui mekanisme diplomatik yang terkoordinasi. Berbeda dari sebuah lembaga organisasi, CDT bersifat kolaboratif dan terdesentralisasi. Keputusan strategis berada di tangan negara-negara anggota, sementara European External Action Service (EEAS) bertindak sebagai koordinator utama dalam pelaksanaan kebijakan. Kerja sama ini diperkuat oleh peran badan-badan pendukung seperti Komisi Eropa, Political and Security Committee (PSC), serta Horizontal Working Party on Cyber Issues (HWPCI), yang menyediakan forum untuk pertukaran intelijen dan pembangunan kesadaran situasional kolektif (European External Action Service, 2020).

CDT mengadopsi prinsip fleksibilitas dan proporsionalitas, yang berarti bahwa setiap respons disesuaikan dengan tingkat bahaya serta konsekuensi dari serangan yang terjadi. Rangkaian prosesnya meliputi deteksi dini, pertukaran

informasi antarnegara anggota, analisis kolektif untuk atribusi pelaku, hingga perumusan serta penerapan tindakan balasan yang dianggap sesuai. Alat yang tersedia dalam kerangka ini mencakup berbagai spektrum tindakan diplomatik, mulai dari penyampaian nota protes (démarches) dan kecaman publik (naming and shaming), hingga tindakan restriktif yang bersifat koersif seperti pembekuan aset dan pelarangan perjalanan melalui sanksi siber (Bendiek & Pawlak, 2019).

Dalam konteks sektor maritim, pendekatan CDT memiliki relevansi yang signifikan mengingat infrastruktur pelabuhan, sistem navigasi, dan rantai pasok maritim semakin terdigitalisasi dan rentan terhadap gangguan siber. Serangan terhadap sistem informasi pelabuhan atau pelacakan kargo, misalnya, tidak hanya menimbulkan kerugian ekonomi, tetapi juga dapat mengganggu stabilitas dan keamanan kawasan. Oleh karena itu, kerangka CDT dapat berfungsi sebagai instrumen diplomatik yang mendukung upaya mitigasi dan respons terhadap insiden siber yang menargetkan sektor maritim, sekaligus menegaskan posisi Uni Eropa dalam menegakkan norma dan hukum internasional di ruang siber (European Union Council, 2019). Walaupun demikian, fokus kebijakan di tingkat nasional maupun internasional masih dominan pada aspek teknis dan regulasi internal. Sementara itu, dimensi diplomasi siber, kerja sama internasional, serta koordinasi lintas aktor di sektor maritim masih jarang dikaji secara komprehensif.

Dengan kondisi tersebut, tampak jelas adanya kesenjangan antara meningkatnya ancaman siber dengan kesiapan sektor maritim dalam menghadapinya. Kajian akademik mengenai diplomasi siber maritim masih terbatas, dan sebagian besar penelitian menitikberatkan pada aspek teknologi atau hukum semata. Padahal, sektor maritim merupakan simpul vital dalam perekonomian global yang keberlanjutannya sangat bergantung pada kerja sama lintas negara. Oleh karena itu, penelitian yang mengangkat dimensi diplomasi siber di sektor maritim menjadi penting, baik sebagai kontribusi teoritis dalam bidang hubungan internasional, maupun sebagai masukan praktis bagi pembuat kebijakan dalam memperkuat ketahanan siber di tingkat regional dan global.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka rumusan masalah yang didefinisikan pada penelitian ini adalah "*Mengapa Uni Eropa menerapkan Cyber Diplomacy Toolbox dalam merespons serangan siber, serta apa efek dari penerapan Cyber Diplomacy Toolbox terhadap transformasi kebijakan keamanan siber maritim Uni Eropa?* ".

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka Penelitian ini memiliki tujuan utama untuk menganalisis mengenai implementasi *Cyber Diplomacy Toolbox* terhadap kebijakan keamanan siber di Uni Eropa. Selain itu, penelitian ini juga bertujuan untuk mengetahui bagaimana pengaruh dari *Cyber Diplomacy Toolbox* terhadap perubahan kebijakan keamanan siber maritim Uni Eropa. Melalui penelitian ini, diharapkan dapat tercipta pemahaman yang lebih mendalam mengenai Pengaruh dari implementasi *Cyber Diplomacy Toolbox* terhadap kebijakan keamanan siber maritim di Uni Eropa.

1.4 Kegunaan Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi dalam kegunaan akademis serta juga praktis bagi para pembaca sebagaimana yang telah dijelaskan pada sub bab berikutnya.

1.5 Kerangka Penelitian

Kerangka pemikiran pada penelitian yang dilakukan penulis bertujuan untuk menganalisis penelitian terlebih dahulu yang relevan dengan penelitian yang dilakukan oleh penulis. Landasan teori yang kuat akan membuat analisis dan pembahasan yang akan dilakukan oleh penulis.

1.5.1 Tinjauan Pustaka

Tinjauan pustaka berfungsi untuk memetakan penelitian-penelitian terdahulu

yang relevan dengan topik penelitian sekaligus menegaskan posisi penelitian dalam mengisi kesenjangan yang ada. Kajian mengenai *Cyber Diplomacy Toolbox* (CDT) telah banyak dilakukan, terutama dalam kaitannya dengan keamanan siber Uni Eropa, namun masih jarang yang menyinggung secara spesifik keterkaitannya dengan sektor maritim.

Penelitian oleh Miftahul Khausar dan Abdul Rivai Ras (2023) dalam artikel Establishment of the Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union Against the Threat of Cyber Attack Activity menyoroti urgensi meningkatnya serangan siber terhadap infrastruktur penting, lembaga pemerintahan, dan sektor swasta di Eropa. Dengan menggunakan pendekatan kualitatif terhadap kebijakan Uni Eropa, penelitian oleh Miftahul Khausar dan Abdul Rivai menekankan bahwa pendekatan unilateral negara anggota tidak cukup untuk menghadapi ancaman yang bersifat lintas batas. Oleh karena itu, CDT dipandang sebagai instrumen kolektif yang menyediakan mekanisme koordinasi diplomatik. Miftahul Khausar dan Abdul Rivai juga menggarisbawahi dimensi politik dan ekonomi dari serangan siber, meskipun belum menjangkau isu sektoral seperti maritim.

Kajian lain dari Yuliya Miadzvetskaya dan Ramses A. Wessel (2022) berjudul The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox memberikan perspektif berbeda dengan membahas eksternalisasi CDT ke ranah global. Menurut Yuliya Miadzvetskaya dan Ramses A. Wessel, Uni Eropa tidak hanya menggunakan CDT untuk kepentingan internal, tetapi juga sebagai alat diplomasi luar negeri guna memperkuat posisi dalam tata kelola siber global. Artikel Yuliya Miadzvetskaya dan Ramses A. Wessel penting karena menegaskan dimensi multilateral dari CDT. Namun, fokus kajian masih bersifat umum dan belum secara mendalam menyinggung implikasi bagi sektor-sektor spesifik, termasuk maritim.

Selain itu, Schulze (2021) meneliti penerapan sanksi siber dalam kerangka CDT. Schulze menunjukkan bahwa sanksi digunakan sebagai bentuk naming and shaming sekaligus instrumen pencegahan terhadap aktor pelaku serangan. Penelitian Schulze memperlihatkan aspek hard power dari kebijakan Uni Eropa.

Akan tetapi, sama seperti penelitian sebelumnya, studi ini tidak menelusuri relevansinya secara sektoral, padahal dampak serangan siber kerap paling nyata terlihat pada sektor transportasi dan maritim.

Beberapa literatur juga mengaitkan CDT dengan perlindungan infrastruktur kritis. Laporan Advancing the EU's Cyber Posture yang diterbitkan oleh EUISS (2021) menegaskan pentingnya meningkatkan resiliensi infrastruktur digital, termasuk energi, transportasi, dan telekomunikasi. Laporan oleh EUISS menunjukkan bahwa ancaman siber dapat menimbulkan efek domino terhadap rantai pasok global. Walaupun isu maritim sempat disebut, fokus utama laporan lebih pada kebijakan umum. Dokumen kebijakan yang dikeluarkan oleh European External Action Service (2020) turut menjelaskan prosedur penggunaan CDT, mulai dari demarches hingga penerapan sanksi. Namun, pendekatan dalam dokumen kebijakan EEAS masih bersifat normatif dan belum banyak ditopang data empiris mengenai implementasi di sektor maritim.

Selain studi mengenai CDT, terdapat pula literatur yang secara langsung menyoroti ancaman siber di sektor maritim. Liu et al. (2021) mengidentifikasi berbagai bentuk serangan yang mengancam keamanan pelabuhan, seperti manipulasi data navigasi GPS, penyusupan ke sistem logistik, dan serangan ransomware pada terminal kontainer. Kajian oleh Liu et al memperlihatkan bahwa serangan terhadap pelabuhan tidak hanya mengganggu kegiatan ekonomi, tetapi juga membahayakan keselamatan pelayaran. Hal serupa ditekankan oleh Bendiek dan Schulze (2021) melalui analisis kasus NotPetya yang melumpuhkan Maersk. Bendiek dan Schulze menunjukkan bahwa satu serangan siber mampu menyebabkan gangguan global, sehingga diperlukan respons kolektif di tingkat Uni Eropa. Akan tetapi, penelitian Bendiek dan Schulze masih bersifat studi kasus dan tidak secara eksplisit menghubungkannya dengan CDT sebagai kerangka kebijakan.

Penelitian Daniel (2023) mengenai serangan ransomware di Pelabuhan Rotterdam menambah bukti empiris betapa rentannya sektor maritim terhadap ancaman siber. Daniel menjelaskan kerugian ekonomi besar serta implikasi gangguan terhadap stabilitas rantai pasok global. Meskipun relevan, penelitian Daniel tidak mengkaji lebih jauh keterkaitan dengan instrumen diplomasi Uni

Eropa. Sementara itu, Gill (2022) dan Vanberghen (2025) melihat isu ini dari perspektif tata kelola global. Gill menyoroti tren globalisasi ancaman siber serta kebutuhan akan standar internasional, sedangkan Vanberghen membahas persaingan model tata kelola siber antara Uni Eropa dan Tiongkok. Literatur ini penting karena menegaskan bahwa keamanan siber harus dipandang dalam dinamika geopolitik global yang lebih luas.

Berdasarkan uraian di atas, terlihat bahwa penelitian mengenai CDT cukup banyak, baik dari perspektif internal Uni Eropa maupun eksternalisasi global. Demikian pula, literatur mengenai ancaman siber maritim juga mulai berkembang, menyoroti kasus-kasus besar dan kerentanan infrastruktur pelabuhan. Akan tetapi, masih sangat jarang kajian yang secara khusus menghubungkan CDT dengan keamanan siber maritim. Padahal, sektor maritim merupakan simpul vital dalam ekonomi global sekaligus salah satu sektor paling terdampak oleh digitalisasi. Dengan demikian, terdapat kesenjangan penelitian yang perlu dijawab, yaitu analisis mengenai bagaimana CDT berperan dalam memperkuat keamanan maritim di Uni Eropa. Penelitian ini berupaya mengisi celah tersebut dengan memberikan perspektif baru yang mengaitkan diplomasi siber Uni Eropa dengan keamanan sektor maritim, sehingga dapat memberikan kontribusi baik secara akademis maupun praktis.

1.6 Kerangka Teori

Kerangka teori dalam penelitian ini berfungsi sebagai landasan konseptual yang mengarahkan serta mendasari analisis data dan interpretasi penelitian. Pada bagian ini, penulis menggunakan teori yaitu ;

1.6.1 Regime Theory

Regime Theory fokus pada bagaimana negara-negara mampu membentuk kerja sama dalam sistem internasional yang bersifat anarki, yaitu tanpa adanya otoritas pusat yang berdaulat atas semua aktor. Teori ini menjadi sangat relevan ketika membahas isu-isu global seperti perdagangan internasional, perubahan iklim, serta keamanan siber di mana tidak ada satu negara pun yang mampu mengatasi

tantangan tersebut secara unilateral (Krasner, 1983).

Regime Theory mulai berkembang secara signifikan pada tahun 1970-an hingga 1980-an sebagai respons terhadap tantangan terhadap pendekatan realis yang menekankan pada konflik dan persaingan kekuasaan. Salah satu tokoh utama dalam pengembangan teori ini adalah Stephen D. Krasner, yang mendefinisikan rezim internasional sebagai:

"Sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given issue-area."
(Krasner, 1983)

Berdasarkan definisi tersebut, rezim bukanlah organisasi formal seperti PBB atau WTO, melainkan seperangkat aturan dan norma yang membentuk ekspektasi bersama antarnegara dalam suatu bidang isu tertentu. Rezim internasional membantu menciptakan keteraturan, transparansi, dan kepercayaan dalam hubungan antarnegara, terutama dalam bidang yang memerlukan kerja sama jangka panjang dan koordinasi lintas batas (Krasner, 1983).

Dalam kerangka pemikiran Stephen D. Krasner, terdapat empat komponen penting yang membentuk suatu rezim internasional, yaitu prinsip, norma, aturan, dan prosedur pengambilan keputusan. Keempat elemen ini saling berkaitan dan membentuk struktur dasar dari bagaimana aktor-aktor internasional terutama negara berperilaku dan bekerja sama dalam suatu bidang isu tertentu. Prinsip merujuk pada keyakinan dasar yang mendasari rezim, seperti nilai-nilai atau asumsi bersama tentang bagaimana dunia bekerja atau seharusnya bekerja. Misalnya, dalam rezim keamanan siber, terdapat prinsip bahwa ruang siber merupakan wilayah strategis yang harus dijaga secara kolektif dan tidak boleh dimonopoli oleh satu negara saja (Krasner, 1983).

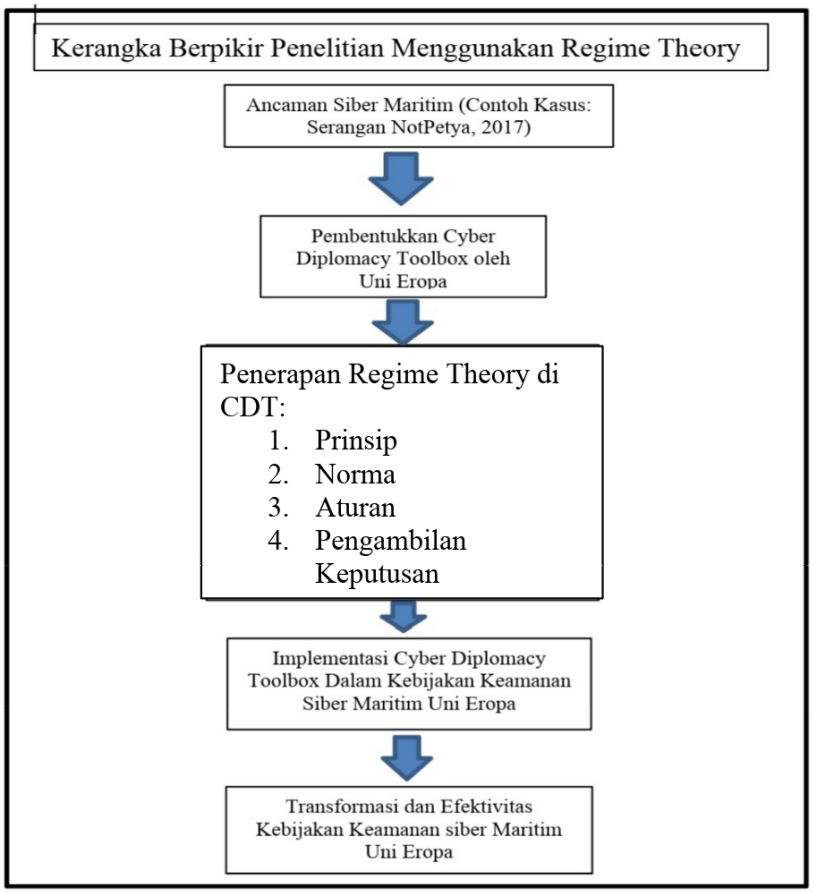
Selanjutnya, norma merupakan standar perilaku yang disepakati oleh para anggota rezim sebagai pedoman bertindak. Dalam konteks keamanan siber, norma bisa berupa kesepakatan bahwa serangan terhadap infrastruktur sipil digital adalah tindakan yang tidak dapat diterima dalam hubungan internasional. Sementara itu, aturan menjabarkan bagaimana prinsip dan norma tersebut diimplementasikan

secara operasional. Aturan ini menentukan apa yang boleh dan tidak boleh dilakukan oleh aktor dalam suatu rezim, serta bagaimana mereka dapat menanggapi pelanggaran terhadap aturan tersebut. Misalnya, aturan mengenai sanksi diplomatik terhadap negara atau entitas yang melakukan serangan siber (Krasner, 1983).

Terakhir, prosedur pengambilan keputusan mengatur mekanisme teknis atau institusional yang digunakan untuk menyelesaikan persoalan dalam rezim, seperti forum dialog, sistem voting, atau konsultasi teknis antarpemerintah. Dalam Uni Eropa, lembaga seperti European Union Agency for Cybersecurity (ENISA) berperan dalam menjalankan prosedur ini dalam bidang keamanan siber. Keempat komponen ini tidak berdiri sendiri, melainkan bekerja secara terintegrasi untuk menciptakan stabilitas, keteraturan, dan ekspektasi bersama dalam interaksi internasional. Oleh karena itu, dalam analisis Regime Theory, memahami hubungan antar elemen ini menjadi kunci untuk menilai kekuatan dan efektivitas suatu rezim, termasuk rezim keamanan siber seperti Cyber Diplomacy Toolbox milik Uni Eropa (Krasner, 1983).

Dalam konteks keamanan siber, rezim internasional sangat diperlukan karena serangan siber bersifat lintas batas, tidak terlihat, dan sulit distribusikan. Negara-negara tidak bisa bertindak sendiri karena ancaman yang dihadapi cenderung global dan menyasar infrastruktur penting yang saling terhubung. Di sinilah peran “rezim keamanan siber” menjadi krusial untuk mengatur norma, berbagi informasi, dan merespons ancaman secara kolektif (Keohane, 1984).

Cyber Diplomacy Toolbox (CDT) yang dibentuk oleh Uni Eropa pada 2017 dapat dikategorikan sebagai bagian dari rezim keamanan siber regional. CDT menciptakan mekanisme tanggapan diplomatik terhadap serangan siber, baik dalam bentuk sanksi, koordinasi kebijakan, maupun pertukaran intelijen ancaman. CDT juga mencerminkan konvergensi ekspektasi antarnegara anggota UE mengenai pentingnya menghadapi serangan siber dengan cara yang terkoordinasi dan legal.



Gambar 1.1 Kerangka Pemikiran Penelitian Berlandaskan Regime Theory oleh Krasner (1983)

Chart kerangka berpikir penelitian menggunakan Regime Theory sebagai pandangan analisis. Menurut Krasner (1983), rezim internasional terbentuk dari prinsip, norma, aturan, dan prosedur yang disepakati bersama. Sementara itu, Keohane (1984) menekankan bahwa rezim berfungsi mengurangi ketidakpastian dan memfasilitasi koordinasi antarnegara. Dengan dasar itu, chart kerangka berpikir penelitian disusun untuk menunjukkan bagaimana ancaman siber di sektor maritim mendorong terbentuknya sebuah rezim yang diwujudkan melalui Cyber Diplomacy Toolbox (CDT) Uni Eropa.

Bagian pertama chart memperlihatkan kondisi awal, yaitu meningkatnya ancaman siber di sektor maritim. Digitalisasi pelabuhan, kapal, dan sistem logistik membuka peluang serangan berupa ransomware, manipulasi data, dan infiltrasi jaringan. Karena ancaman ini bersifat lintas batas, negara tidak dapat menanganinya

sendiri. Dari titik ini terlihat adanya kebutuhan bersama untuk menciptakan koordinasi. Dalam kerangka teori rezim, kebutuhan kolektif lah yang menjadi pemicu munculnya kesepakatan antar aktor internasional.

Bagian kedua chart menggambarkan munculnya kebutuhan rezim internasional. Uni Eropa berperan sebagai aktor yang mencoba merumuskan seperangkat aturan dan mekanisme untuk merespons serangan siber. Proses ini sesuai dengan gagasan Scholte (2011) bahwa tata kelola global muncul ketika aktor menghadapi masalah yang tidak bisa diselesaikan secara unilateral. Kebutuhan akan rezim kemudian menjadi dasar pembentukan instrumen kebijakan yang lebih terarah.

Bagian ketiga chart menempatkan Cyber Diplomacy Toolbox (CDT) sebagai instrumen rezim tersebut. CDT menyediakan seperangkat mekanisme diplomatik, mulai dari demarches, koordinasi antarnegara, kerja sama teknis, hingga sanksi. CDT memungkinkan Uni Eropa memberikan respons yang lebih terkoordinasi terhadap serangan siber. Dalam perspektif Regime Theory, CDT merepresentasikan seperangkat aturan dan prosedur yang dipakai bersama oleh negara anggota.

Bagian terakhir chart menunjukkan hasil yang diharapkan dari Cyber Diplomacy Toolbox sebagai rezim, yaitu peningkatan keamanan siber di sektor maritim dan terjaganya stabilitas rantai pasok global. Dengan adanya koordinasi melalui CDT, respons terhadap serangan siber tidak lagi bersifat parsial, melainkan kolektif. Regime Theory membantu menjelaskan bagaimana ancaman nyata dapat mendorong pembentukan rezim, bagaimana instrumen rezim bekerja, dan bagaimana hasil akhirnya mendukung stabilitas internasional.

1.7 Operasionalisasi Konsep

1.7.1 Definisi Konseptual

Definisi konseptual dalam penelitian ini berfungsi untuk memberikan pemahaman yang jelas dan terukur mengenai rumusan masalah yang diteliti oleh penulis. Konsep yang dipakai yaitu;

1.7.2 Keamanan

Keamanan merupakan konsep fundamental dalam studi hubungan internasional dan ilmu politik yang merujuk pada kondisi bebas dari ancaman yang dapat membahayakan eksistensi, stabilitas, atau kesejahteraan suatu entitas, baik individu, masyarakat, maupun negara. Konsep ini tidak bersifat statis, melainkan bersifat dinamis dan kontekstual, tergantung pada persepsi aktor terhadap ancaman yang dihadapi. Tradisionalnya, keamanan dipahami dalam kerangka militer dan pertahanan negara dari serangan fisik oleh negara lain. Namun, sejak akhir Perang Dingin, konsep keamanan mengalami perluasan (*widening*) dan pendalaman (*deepening*), mencakup berbagai dimensi seperti keamanan ekonomi, keamanan lingkungan, keamanan manusia, hingga keamanan siber (Buzan, Waever, & de Wilde, 1998). Dalam konteks modern, keamanan juga berarti upaya preventif dan responsif dalam menghadapi ancaman non-tradisional, termasuk terorisme, kejahatan transnasional, dan serangan siber, yang dapat mengganggu stabilitas nasional maupun internasional. Negara dan aktor internasional dituntut untuk membangun mekanisme perlindungan, termasuk kerjasama multilateral dan penyusunan kebijakan yang adaptif terhadap perkembangan bentuk-bentuk ancaman tersebut.

1.7.3 Diplomasi

Diplomasi adalah proses komunikasi dan negosiasi antara aktor-aktor internasional, terutama negara, yang dilakukan secara damai untuk mencapai tujuan politik luar negeri, menyelesaikan konflik, membangun aliansi, serta memelihara stabilitas hubungan internasional. Diplomasi tidak hanya melibatkan perwakilan resmi suatu negara seperti duta besar atau menteri luar negeri, tetapi juga mencakup peran organisasi internasional, aktor non-negara, dan bahkan individu dalam beberapa kasus tertentu (Barston, 2019). Diplomasi menjadi alat vital dalam menjaga kepentingan nasional melalui jalur non-militer, baik dalam konteks bilateral maupun multilateral. Dalam era globalisasi dan interdependensi yang semakin tinggi, diplomasi telah berkembang ke dalam berbagai bentuk, seperti diplomasi ekonomi, diplomasi publik, diplomasi lingkungan, dan diplomasi digital. Salah satu bentuk kontemporer yang penting adalah diplomasi siber, di mana

negara-negara berusaha membentuk norma, aturan, dan mekanisme kerja sama untuk menghadapi ancaman dan tantangan yang muncul di ranah digital. Dengan demikian, diplomasi tidak hanya menjadi instrumen penyelesaian konflik, tetapi juga strategi proaktif dalam mencegah krisis dan membangun tatanan internasional yang stabil dan kooperatif.

1.7.4 Serangan Siber

Serangan Siber adalah tindakan yang dilakukan oleh individu, kelompok, atau negara dengan tujuan untuk mengganggu, merusak, atau mendapatkan akses tanpa izin ke sistem komputer, jaringan, atau data. Serangan ini dapat dilakukan dengan berbagai metode, seperti peretasan, phishing, serangan malware, serangan DDoS *(Distributed Denial-of-Service)*, hingga eksploitasi kerentanan perangkat lunak atau perangkat keras. *Cyber attack* sering kali bertujuan untuk mencuri informasi sensitif, seperti data keuangan, rahasia dagang, atau data pribadi, tetapi juga dapat digunakan untuk sabotase, spionase, atau bahkan manipulasi sistem kritis seperti infrastruktur energi dan komunikasi. Dalam beberapa kasus, serangan ini dilakukan oleh pelaku non-negara seperti kelompok kriminal atau aktivis (*hacktivist*), sementara dalam konteks geopolitik, serangan siber juga dapat dilakukan oleh negara untuk mencapai tujuan strategis atau militer, yang sering disebut sebagai state-sponsored cyber attacks. Dampak dari serangan siber bisa sangat luas, mencakup kerugian finansial, pelanggaran privasi, kerusakan reputasi, gangguan operasional, hingga ancaman terhadap keselamatan masyarakat. Oleh karena itu, *cyber attack* menjadi salah satu ancaman utama dalam era digital, yang mendorong perlunya penguatan keamanan siber melalui teknologi, regulasi, dan kolaborasi internasional (Li, Y., & Liu, Q. 2021).

1.7.5 Rezim

Rezim dapat dipahami sebagai seperangkat aturan, norma, prinsip, dan prosedur pengambilan keputusan yang disepakati oleh aktor-aktor tertentu dalam suatu sistem internasional atau politik domestik untuk mengatur perilaku mereka. Stephen D. Krasner (1982) mendefinisikan rezim internasional sebagai “aturan,

norma, prinsip, dan prosedur pengambilan keputusan di mana ekspektasi aktor dalam isu tertentu bertemu satu sama lain" (Krasner, 1982). Dengan demikian, rezim bukan hanya sekadar pemerintahan yang berkuasa, tetapi mencakup kerangka aturan formal maupun informal yang memandu interaksi aktor dalam bidang tertentu, baik itu dalam konteks politik internasional, keamanan, ekonomi, maupun lingkungan.

1.7.6 Diplomasi Siber

Diplomasi siber pada dasarnya merupakan perpanjangan dari praktik diplomasi tradisional ke dalam ruang digital. Konsep ini mencakup segala bentuk interaksi diplomatik yang berkaitan dengan isu siber, baik dalam hal keamanan, tata kelola internet, maupun pembangunan kapasitas negara. Diplomasi siber tidak hanya terbatas pada pencegahan konflik atau penyelesaian sengketa, tetapi juga mencakup pembangunan norma internasional mengenai bagaimana negara seharusnya berperilaku di dunia maya. Bendiek dan Schulze (2021) menyebut diplomasi siber sebagai pemanfaatan instrumen diplomasi klasik seperti dialog, negosiasi, dan sanksi, namun diarahkan secara khusus untuk merespons dinamika dan ancaman yang lahir dari ruang siber. Dengan demikian, diplomasi siber tidak berdiri sendiri, melainkan berada dalam kerangka hubungan internasional yang lebih luas, di mana ruang digital semakin dianggap sebagai domain strategis yang setara dengan darat, laut, udara, dan luar angkasa.

1.7.7 Definisi Operasional

Definisi Operasional dalam penelitian ini berfungsi untuk memberikan pemahaman yang jelas dan terukur mengenai rumusan masalah yang diteliti oleh penulis. Konsep yang dipakai yaitu;

1.7.8 Keamanan

Dalam penelitian ini, keamanan dioperasikan sebagai kondisi terlindungnya sistem teknologi informasi dan komunikasi yang digunakan dalam sektor maritim

dari berbagai bentuk serangan siber yang dapat mengancam keselamatan, operasi, dan stabilitas infrastruktur pelabuhan, navigasi, serta rantai pasok laut. Keamanan tidak hanya mencakup pencegahan terhadap gangguan teknis, tetapi juga ketahanan institusi maritim dalam merespon insiden siber melalui kerangka hukum, kelembagaan, dan kerja sama internasional. Pengukuran keamanan dalam konteks ini dilakukan dengan menilai efektivitas mekanisme perlindungan yang digunakan oleh negara-negara atau institusi terkait, seperti sistem deteksi dini, regulasi nasional, dan protokol penanganan insiden. Dengan demikian, definisi operasional keamanan yang mencakup ancaman non-tradisional dan multi-dimensi (Buzan et al., 1998) menjadi dasar dalam mengevaluasi seberapa siap dan tanggap sektor maritim terhadap tantangan siber melalui instrumen diplomatik dan teknis.

1.7.9 Diplomasi

Diplomasi dalam penelitian ini dioperasionalkan sebagai serangkaian tindakan yang dilakukan oleh negara, baik secara bilateral maupun multilateral, dalam rangka membangun norma, membentuk kesepakatan, dan menjalankan mekanisme kerja sama internasional untuk menghadapi ancaman siber di sektor maritim. Fokus utama adalah pada penggunaan cyber diplomacy toolbox yang dikeluarkan oleh Uni Eropa sebuah instrumen kebijakan luar negeri yang mencakup sanksi, dialog diplomatik, serta kerja sama internasional di bidang siber. Diplomasi dalam penelitian ini diukur melalui seberapa efektif alat-alat tersebut digunakan dalam merespon serangan siber terhadap infrastruktur maritim, mendorong akuntabilitas negara pelaku, serta memperkuat ketahanan siber maritim secara kolektif. Definisi operasional diplomasi dijelaskan sebagai alat negosiasi damai dan pembentukan tatanan internasional (Barston, 2019) digunakan sebagai dasar dalam menganalisis bagaimana diplomasi siber berfungsi dalam kerangka keamanan maritim global.

1.7.10 Serangan Siber

Dalam konteks penelitian ini, serangan siber dijelaskan sebagai segala bentuk tindakan yang bersifat merusak, mengganggu, atau mengeksploitasi sistem

teknologi informasi dan komunikasi (TIK) yang digunakan di sektor maritim, baik oleh aktor negara maupun non-negara. Serangan ini dapat mencakup *malware*, *ransomware, distributed denial-of-service* (DDoS), peretasan sistem navigasi, serta gangguan pada sistem manajemen pelabuhan dan logistik laut. Serangan siber diukur berdasarkan intensitas (skala kerusakan), frekuensi, aktor pelaku, serta respons yang dihasilkan, termasuk keterlibatan diplomasi internasional dalam menangani kasus tersebut. Dalam penelitian ini, serangan siber diposisikan sebagai variabel yang menguji efektivitas respon diplomatik yang dimiliki suatu negara atau organisasi regional, seperti Uni Eropa, dalam konteks kerja sama keamanan maritim. Definisi ini memperluas pemahaman terhadap penelitian tentang ancaman siber terhadap keamanan nasional (Buzan et al., 1998), sekaligus menggaris bawahi urgensi diplomasi siber sebagai instrumen mitigasi dan pencegahan. Serangan siber dalam sektor maritim menjadi tantangan nyata yang menguji kemampuan cyber diplomacy toolbox dalam mengoordinasikan respons kolektif, mendorong akuntabilitas pelaku, serta memperkuat kerangka kerja hukum internasional di domain siber.

1.7.11 Rezim

Dalam Penelitian, rezim dapat dipahami sebagai seperangkat aturan, norma, dan mekanisme yang secara nyata digunakan untuk mengatur praktik dan perilaku aktor dalam suatu bidang tertentu. Dalam konteks penelitian, rezim dioperasionalkan melalui identifikasi aturan dan norma yang berlaku, implementasi kebijakan yang diterapkan, serta tingkat kepatuhan aktor terhadap aturan tersebut. Misalnya, dalam rezim perdagangan internasional, pengaturan dilakukan melalui lembaga seperti WTO dengan seperangkat aturan yang mengikat negara anggota, sementara dalam rezim lingkungan global, aturan diwujudkan melalui perjanjian internasional seperti Protokol Kyoto atau Paris Agreement. Dengan demikian, operasionalisasi rezim dalam penelitian dapat dilihat dari bagaimana aturan-aturan itu diterjemahkan ke dalam kebijakan keamanan, dijalankan dalam praktik, serta memengaruhi perilaku negara atau aktor lain di tingkat internasional maupun domestik (Keohane, 1984).

1.7.12 Diplomasi Siber

Dalam penelitian ini, diplomasi siber dipahami secara operasional sebagai cara Uni Eropa menggunakan saluran diplomatik untuk merespons serangan siber lintas batas. Praktik ini terlihat melalui penerapan Cyber Diplomacy Toolbox (CDT) yang menjadi kerangka kebijakan bersama negara anggota. Diplomasi siber dalam konteks CDT dapat diidentifikasi dari sejumlah tindakan nyata, seperti atribusi kolektif terhadap pelaku serangan, penyampaian kecaman resmi melalui pernyataan publik Uni Eropa, serta pemberlakuan sanksi yang disepakati secara bersama terhadap individu atau entitas yang dinilai bertanggung jawab. Contoh paling jelas adalah pada tahun 2020 ketika Uni Eropa untuk pertama kalinya menjatuhkan sanksi terhadap enam individu dan tiga entitas asal Rusia, Tiongkok, dan Korea Utara yang terlibat dalam serangan besar, termasuk NotPetya (Council of the European Union, 2020). Keputusan ini menandai transformasi diplomasi siber Uni Eropa dari sekadar wacana ke tindakan nyata yang dapat dirasakan implikasinya dalam hubungan internasional. Dengan batasan tersebut, diplomasi siber dalam penelitian ini tidak hanya dipahami sebagai konsep abstrak, tetapi juga sebagai praktik konkret yang dapat diamati, diukur, dan dianalisis melalui respons Uni Eropa terhadap kasus-kasus besar yang menargetkan infrastruktur penting di kawasan maupun secara global.

1.8 Argumen Penelitian

Penelitian ini berargumen bahwa Cyber Diplomacy Toolbox (CDT) merupakan instrumen diplomasi kolektif yang tidak hanya berfungsi secara teknis dalam merespons serangan siber, tetapi juga memiliki peran transformasional dalam membentuk kebijakan keamanan siber maritim Uni Eropa. Melalui kerangka Regime Theory, CDT dapat dipahami sebagai seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan yang mengikat negara anggota. Dengan mekanisme ini, Uni Eropa berupaya menghadirkan tata kelola keamanan siber yang bersifat lintas batas, di mana ancaman terhadap sektor maritim dipandang sebagai isu strategis yang membutuhkan respons politik, diplomatik, dan regulatif secara

kolektif.

Transformasi kebijakan yang dihasilkan CDT dapat dilihat pada tiga dimensi. Pertama, dimensi regulatif, dengan lahirnya kebijakan baru seperti NIS2 Directive dan EU Cybersecurity Act yang memperluas perlindungan terhadap infrastruktur maritim. Kedua, dimensi institusional, melalui penguatan peran lembaga seperti ENISA serta koordinasi antarnegara anggota di bawah kerangka Common Foreign and Security Policy (CFSP). Ketiga, dimensi diplomatik, yang ditunjukkan dengan penerapan atribusi kolektif, kecaman diplomatik, dan sanksi terhadap aktor negara maupun non-negara sebagai upaya penegakan norma internasional. Tiga dimensi ini memperlihatkan bahwa CDT bukan hanya instrumen kebijakan reaktif, tetapi juga mekanisme normatif yang memperkuat ketahanan siber maritim sekaligus posisi Uni Eropa sebagai aktor normatif global.

Selain itu, penelitian ini menegaskan adanya kesenjangan penelitian di mana kajian terdahulu tentang CDT cenderung membahasnya secara umum tanpa menghubungkannya secara khusus dengan sektor maritim. Padahal, maritim merupakan salah satu sektor paling terdigitalisasi sekaligus paling vital bagi perekonomian dan keamanan Eropa. Dengan menempatkan sektor maritim sebagai fokus, penelitian ini menunjukkan bahwa CDT memiliki dampak langsung terhadap perlindungan rantai pasok global, stabilitas ekonomi regional, serta legitimasi Uni Eropa dalam diplomasi siber internasional. Dengan demikian, argumen penelitian ini menekankan bahwa CDT bukan hanya alat penanganan serangan siber, tetapi juga instrumen strategis dalam transformasi kebijakan keamanan maritim Uni Eropa.

1.8.1 Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif yang digunakan untuk memberikan pemahaman yang komprehensif mengenai topik yang diteliti. Penelitian kualitatif menurut Creswell adalah pendekatan untuk mengeksplorasi dan memahami makna individu atau kelompok terhadap suatu masalah sosial atau kemanusiaan. Metode ini bertujuan untuk memperoleh pemahaman mendalam mengenai pengalaman, perilaku, atau pandangan partisipan dari perspektif mereka

sendiri. Dalam penelitian kualitatif, peneliti berperan sebagai instrumen utama dalam proses pengumpulan data, yang dapat berupa wawancara, observasi, atau analisis dokumen. Pendekatan ini sering kali bersifat fleksibel dan adaptif, memungkinkan peneliti untuk mengeksplorasi data secara mendalam sesuai dengan konteks penelitian. Creswell menekankan pentingnya aspek interpretatif dalam penelitian kualitatif, di mana peneliti berupaya memahami dan menafsirkan makna yang muncul dari interaksi dengan partisipan atau analisis teks (Creswell, 2014).

1.8.2 Tipe Penelitian

Penelitian ini menggunakan tipe penelitian Kualitatif-Deskriptif Analitis. Penelitian kualitatif-deskriptif analitis dipilih karena mampu memberikan gambaran mendalam dan sistematis mengenai penerapan Cyber Diplomacy Toolbox dalam merespons serangan siber, serta apa efek penerapannya terhadap transformasi kebijakan keamanan siber maritim Uni Eropa. Tipe penelitian ini memungkinkan peneliti untuk menganalisis fenomena, fakta, dan hubungan antar variabel terkait implementasi kebijakan keamanan siber maritim di Uni Eropa. Melalui penelitian Kualitatif-Deskriptif Analitis dapat memberikan analisis mendalam terhadap kebijakan, regulasi, dan implementasi *Cyber Diplomacy Toolbox*. Dengan demikian, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai pengaruh *Cyber Diplomacy Toolbox* yang terlibat dalam kebijakan siber maritim Uni Eropa.

1.8.3 Situs Penelitian

Penelitian ini dilakukan dengan mengambil situs penelitian pada institusi Uni Eropa dan lembaga-lembaga terkait yang memiliki otoritas dalam pengembangan dan implementasi kebijakan keamanan siber maritim.

1.8.4 Subjek Penelitian

Subjek dalam penelitian ini adalah *Cyber Diplomacy Toolbox* sebagai perangkat kebijakan Uni Eropa yang diimplementasikan untuk menghadapi

ancaman siber di sektor maritim. *Cyber Diplomacy Toolbox* merupakan seperangkat langkah-langkah diplomatik, ekonomi, dan strategis yang dikembangkan oleh Uni Eropa sebagai respons terhadap aktivitas siber yang mengancam kepentingan dan infrastruktur maritim Uni Eropa. perangkat kebijakan ini mencakup berbagai mekanisme, mulai dari langkah-langkah pencegahan hingga sanksi terhadap subjek yang melakukan serangan siber.

Penelitian ini juga berfokus pada kebijakan siber maritim Uni Eropa sebagai subjek yang dipengaruhi oleh implementasi *Cyber Diplomacy Toolbox*. Kebijakan ini meliputi kerangka regulasi, strategi keamanan, dan protokol pertahanan siber yang diterapkan di sektor maritim Uni Eropa, termasukpelabuhan, kapal, sistem navigasi, dan infrastruktur maritim lainnya. Analisis akan dilakukan terhadap perubahan dan perkembangan kebijakan siber maritim sebelum dan sesudah penerapan *Cyber Diplomacy Toolbox*, serta efektivitasnya dalam meningkatkan ketahanan siber sektor maritim Uni Eropa.

1.8.5 Jenis Data

Penelitian ini menggunakan jenis data kualitatif-deskriptif analitis yang berfokus pada pengumpulan dan analisis informasi mendalam mengenai *Cyber* Diplomacy *Toolbox* dan kebijakan siber maritim Uni Eropa. Data kualitatif yang digunakan mencakup deskripsi komprehensif tentang kebijakan, proses implementasi, mekanisme koordinasi, dan dampak dari penerapan *Cyber Diplomacy Toolbox* terhadap sektor maritim. Jenis data ini dipilih karena mampu memberikan pemahaman yang kuat tentang bagaimana pengaruh *cyber diplomacy toolbox* memberikan pengaruh kebijakan terhadap perkembangan keamanan siber maritim di Uni Eropa.

Pendekatan deskriptif analitis dalam pengumpulan data memungkinkan penelitian ini untuk mengeksplorasi berbagai aspek dari fenomena yang diteliti, termasuk pola-pola implementasi kebijakan, dinamika hubungan antar institusi, dan faktor-faktor yang mempengaruhi efektivitas *Cyber Diplomacy Toolbox*. Data yang dikumpulkan mencakup deskripsi detail tentang struktur kebijakan, mekanisme implementasi, proses adaptasi, dan respons terhadap ancaman siber di sektor

maritim. Analisis data dilakukan secara sistematis untuk mengidentifikasi implementasi *Cyber Diplomacy Toolbox* terhadap perubahan dalam kebijakan siber maritim Uni Eropa. Pendekatan ini memungkinkan peneliti untuk membangun pemahaman yang mendalam tentang fenomena yang diteliti.

1.8.6 Sumber Data

Penelitian ini menggunakan dua jenis data, yaitu data primer dan data sekunder yang relevan dengan implementasi *Cyber Diplomacy Toolbox* dan kebijakan siber maritim Uni Eropa. Data primer yang digunakan dalam penelitian ini meliputi dokumen-dokumen resmi Uni Eropa seperti Framework Cyber Diplomacy Toolbox, regulasi kebijakan siber maritim, laporan implementasi kebijakan, dokumen strategis keamanan siber, serta protokol dan pedoman keamanan maritim yang dikeluarkan oleh institusi-institusi Uni Eropa seperti EEAS, EMSA, dan ENISA. Data primer ini memberikan informasi langsung dan otoritatif mengenai kebijakan dan implementasinya di tingkat Uni Eropa.

Data sekunder dalam penelitian ini diperoleh dari berbagai sumber akademis dan profesional yang mengkaji implementasi Cyber Diplomacy Toolbox dan kebijakan siber maritim Uni Eropa. Sumber-sumber ini mencakup artikel jurnal ilmiah, laporan analisis kebijakan, studi kasus, buku-buku akademik, laporan penelitian independen. Data sekunder ini berfungsi untuk memperkaya analisis dengan menyediakan perspektif dan interpretasi dari para ahli dan peneliti tentang efektivitas kebijakan yang diterapkan. Selain itu, data sekunder juga mencakup laporan media, dokumentasi konferensi, dan publikasi industri maritim yang memberikan konteks aktual terhadap implementasi kebijakan tersebut.

1.8.7 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilaksanakan dengan menganalisis jurnal-jurnal penelitian internasional yang membahas tentang *Cyber Diplomacy Toolbox* dan kebijakan siber maritim Uni Eropa. Penelitian yang menggunakan metode kualitatif-deskriptif analitis ini berfokus pada pengumpulan data dari jurnal-jurnal akademik terpercaya yang memuat analisis mendalam

tentang implementasi *Cyber Diplomacy Toolbox*, strategi keamanan siber maritim, serta dampaknya terhadap kebijakan Uni Eropa. Selain jurnal penelitian, pengumpulan data juga dilakukan melalui analisis buku-buku yang membahas tentang diplomasi siber, keamanan maritim, dan kebijakan strategis Uni Eropa dalam menghadapi ancaman siber.

Proses pengumpulan data dilakukan secara sistematis dengan mengidentifikasi, mengkategorisasi, dan menganalisis konten dari sumber-sumber tersebut untuk memperoleh pemahaman menyeluruh tentang topik penelitian. Peneliti melakukan penelusuran terhadap jurnal-jurnal internasional, serta mengakses buku-buku referensi yang relevan. Data yang terkumpul kemudian diklasifikasikan berdasarkan tema-tema utama penelitian untuk memudahkan proses analisis kualitatif yang mendalam tentang bagaimana *Cyber Diplomacy Toolbox* mempengaruhi perkembangan kebijakan siber maritim di Uni Eropa.

1.8.8 Analisis dan Interpretasi Data

Analisis dan interpretasi data dalam penelitian ini dilakukan dengan menggunakan pendekatan kualitatif-deskriptif analitis untuk mengkaji penerapan Cyber Diplomacy Toolbox dalam merespons serangan siber, serta apa efek penerapannya terhadap transformasi kebijakan keamanan siber maritim Uni Eropa. Proses analisis dimulai dengan mengorganisir data yang telah dikumpulkan dari jurnal-jurnal penelitian dan buku-buku referensi ke dalam topik yang relevan dengan rumusan masalah penelitian. Data tersebut kemudian dianalisis secara sistematis untuk mengidentifikasi hubungannya antara implementasi *Cyber Diplomacy Toolbox* dengan perkembangan kebijakan keamanan siber maritim. Analisis dilakukan dengan memperhatikan konteks historis, keamanan, dan kebijakan yang mempengaruhi pembentukan dan implementasi kebijakan tersebut.

Interpretasi data dilakukan dengan mengintegrasikan temuan-temuan dari berbagai sumber literatur untuk membangun pemahaman yang menyeluruh tentang *Cyber Diplomacy Toolbox* dalam memperkuat keamanan siber maritim Uni Eropa. Proses interpretasi mencakup analisis mendalam terhadap mekanisme implementasi

kebijakan, tantangan yang dihadapi, dan dampak yang dihasilkan terhadap sektor maritim. Hasil analisis dan interpretasi data kemudian disusun secara sistematis untuk menjawab pertanyaan penelitian tentang Bagaimana pengaruh dari implementasi *Cyber Diplomacy Toolbox* terhadap perubahan pembentukan kebijakan keamanan di Uni Eropa, serta mengidentifikasi implikasi strategis dari implementasi kebijakan tersebut terhadap keamanan siber maritim di Uni Eropa.

1.8.9 Kualitas Data

Untuk memastikan kualitas data dalam penelitian ini, peneliti menerapkan beberapa kriteria keabsahan data yang penting. Pertama, peneliti memastikan kredibilitas data dengan menggunakan jurnal-jurnal penelitian internasional dan buku-buku yang sudah diakui dalam bidang diplomasi siber dan keamanan maritim. Keabsahan data dijamin melalui pencatatan yang teratur dan teliti dari setiap sumber yang digunakan. Peneliti juga melakukan pengindentifikasi antar sumber untuk memastikan keakuratan informasi yang didapat. Untuk mendukung penerapan hasil penelitian yang lebih luas, peneliti menggunakan berbagai sudut pandang dari jurnal dan buku yang berbeda-beda. Selain itu, peneliti memperhatikan keterbaruan sumber dengan mengutamakan publikasi-publikasi terbaru yang membahas tentang *Cyber Diplomacy Toolbox* dan kebijakan siber maritim Uni Eropa. Dengan menerapkan kriteria-kriteria ini, peneliti dapat menjamin bahwa data yang digunakan dalam penelitian bersifat valid dan dapat dipercaya.