BAB II
KEAMANAN SIBER MARITIM: KONSEP, ANCAMAN, DAN PERAN CYBER DIPLOMACY TOOLBOX

Sektor maritim memiliki peranan yang sangat vital bagi Uni Eropa, baik dari segi ekonomi, geopolitik, maupun keamanan. Wilayah Uni Eropa dikelilingi oleh lautan yang luas, seperti Samudra Atlantik, Laut Tengah, Laut Baltik, dan Laut Utara, yang menjadikan aktivitas kelautan sebagai bagian penting dari kehidupan dan pembangunan kawasan ini. Uni Eropa memiliki lebih dari 70.000 kilometer garis pantai dan sekitar 40% dari populasinya tinggal di wilayah pesisir, yang menggambarkan besarnya ketergantungan masyarakat Eropa terhadap sektor maritim dalam berbagai aspek kehidupan. Selain itu, lebih dari 75% perdagangan luar negeri Uni Eropa dan sekitar 30% dari pergerakan barang dalam negeri dilakukan melalui jalur laut.

Dari perspektif ekonomi, sektor maritim Eropa, yang mencakup pelabuhan, transportasi laut, perikanan, energi kelautan, dan pariwisata pantai, menyumbang secara signifikan terhadap Produk Domestik Bruto (PDB) Uni Eropa. Menurut laporan Blue Economy Report 2023 yang diterbitkan oleh Komisi Eropa, sektor ekonomi biru (blue economy) mempekerjakan lebih dari 4,45 juta orang dan menghasilkan pendapatan bruto sebesar €129 miliar. Sektor ini juga menjadi pendorong penting bagi inovasi teknologi, terutama dalam pengembangan energi terbarukan laut seperti tenaga ombak dan angin lepas pantai.

Keamanan siber maritim merupakan salah satu bidang yang semakin penting dalam konteks keamanan global dan nasional. Dengan meningkatnya ketergantungan dunia pada infrastruktur digital, khususnya di sektor maritim yang menggerakkan sekitar 80% perdagangan global, perlindungan terhadap ancaman siber menjadi sangat Penting (Bennett & Blyth, 2021). Lebih dari 80% hingga 90% volume perdagangan dunia diangkut melalui laut, dan sebagian besar jalur tersebut melintasi atau menuju pelabuhan-pelabuhan di Eropa (European Commission, 2023). Infrastruktur maritim seperti pelabuhan, kabel bawah laut, dan fasilitas energi lepas pantai memainkan peran krusial dalam menjaga kestabilan ekonomi

dan geopolitik regional (Reuters, 2025). Ketergantungan tinggi ini membuat sektor maritim menjadi target utama serangan siber, baik oleh aktor negara maupun non-negara.

Keamanan siber maritim mengacu pada serangkaian praktik, teknologi, dan kebijakan yang dirancang untuk melindungi sistem komputer, jaringan, dan data yang digunakan dalam operasi maritim dari ancaman, serangan, dan gangguan digital yang dapat merusak fungsi dan keselamatan pelayaran serta rantai pasokan (Kessler, 2020). Sektor maritim mencakup berbagai elemen mulai dari kapal, pelabuhan, sistem navigasi, manajemen logistik, hingga infrastruktur pendukung seperti terminal minyak dan gas, yang semuanya semakin bergantung pada teknologi digital dan internet untuk operasional sehari-hari (STOPFORD, 2019). Contohnya adalah penggunaan Automatic Identification System (AIS) untuk tracking kapal, Sistem Informasi Manajemen Pelabuhan (Port Management Information Systems), serta sistem kontrol otomatis untuk fasilitas bongkar muat. Ketergantungan ini membuka celah bagi serangan siber yang dapat menyebabkan gangguan besar, mulai dari keterlambatan logistik hingga kecelakaan maritim.

Ancaman siber di sektor maritim bisa datang dalam berbagai bentuk. Seperti, malware yang menyusup ke dalam sistem kendali kapal sehingga dapat mengubah jalur pelayaran, serangan ransomware yang mengenkripsi data penting pelabuhan dan menuntut tebusan, serangan Distributed Denial of Service (DDoS) yang melumpuhkan jaringan komunikasi pelabuhan, hingga manipulasi data GPS yang menyebabkan kesalahan navigasi. Ancaman ini tidak hanya berdampak pada aspek ekonomi, tetapi juga berpotensi menimbulkan bahaya keselamatan jiwa (Gill, 2022). Selain itu, keamanan siber maritim juga mencakup aspek perlindungan terhadap data pribadi dan bisnis yang sensitif, serta memastikan kontinuitas operasi selama dan setelah insiden siber. Hal ini memerlukan pendekatan berlapis, yaitu gabungan antara teknologi, sumber daya manusia yang terlatih, serta kebijakan dan regulasi yang mendukung (Liu et al., 2021). Karena karakteristik ancaman yang terus berkembang, keamanan siber maritim harus bersifat dinamis dan adaptif. Di sinilah peran teknologi pertahanan siber seperti *Cyber Diplomacy Toolbox* (CDT) menjadi sangat penting. CDT membantu memperkuat sistem dengan kemampuan

deteksi dini, respons cepat, dan pemulihan yang efektif, sekaligus mendukung kolaborasi antar pemangku kepentingan di tingkat nasional maupun internasional (ENISA, 2020).

2.1. Keamanan Siber Maritim

Keamanan siber maritim merupakan isu strategis dalam hubungan internasional seiring meningkatnya ketergantungan sektor maritim terhadap teknologi digital. Infrastruktur maritim, seperti pelabuhan, sistem navigasi, hingga operasional kapal, kini semakin terintegrasi dengan teknologi informasi, yang secara bersamaan meningkatkan risiko ancaman siber di sektor ini. Hal tersebut juga menyebabkan peningkatan serangan siber yang secara signifikan dapat mengganggu aktivitas ekonomi dan keamanan nasional, serta mengancam stabilitas global. Ancaman ini memerlukan perhatian serius dari pemerintah dan pemangku kepentingan untuk mengembangkan kebijakan yang mampu melindungi infrastruktur maritim dan menjaga stabilitas ekonomi.

Beberapa contoh nyata menunjukkan dampak besar dari serangan siber terhadap sektor maritim. Insiden ransomware NotPetya yang menimpa perusahaan pelayaran besar seperti Maersk pada 2017 misalnya, telah menyebabkan kerugian finansial dan operasional yang besar. Selain itu, kasus infiltrasi sistem pelabuhan di Antwerp antara 2011 hingga 2013 digunakan sebagai media penyelundupan barang ilegal, memperjelas bahwa ancaman siber di sektor ini juga berkaitan erat dengan aktivitas kriminal transnasional. Kompleksnya sektor maritim global memperparah risiko keamanan siber, terutama akibat konektivitas yang tinggi dan rantai pasokan internasional yang luas. Situasi ini menyebabkan kesulitan dalam penerapan standar keamanan siber yang konsisten di seluruh dunia, karena negara-negara memiliki prioritas kebijakan dan kapabilitas yang berbeda. Oleh karena itu, pendekatan koordinasi internasional menjadi sesuatu yang penting dalam mencegah ancaman siber di sektor ini.

Dalam merespons ancaman tersebut, Uni Eropa telah memperkenalkan Cyber Diplomacy Toolbox sebagai alat diplomatik dan kebijakan untuk menghadapi serangan siber berskala besar. Toolbox ini menyediakan opsi diplomatik, termasuk

penerapan sanksi dan respons kolektif negara-negara anggota terhadap pelaku serangan siber. Langkah ini merupakan bagian dari upaya Uni Eropa membangun norma internasional dalam cyberspace, khususnya terkait perlindungan infrastruktur kritis, termasuk sektor maritim. Strategi keamanan maritim Uni Eropa secara khusus menempatkan isu siber sebagai bagian penting dari keamanan keseluruhan. Strategi ini bertujuan meningkatkan kapasitas teknis negara-negara anggota serta memperkuat koordinasi antar-lembaga regional dalam menghadapi ancaman tersebut. Namun, implementasi kebijakan ini masih menghadapi tantangan yang signifikan, baik secara teknis, karena masih banyaknya infrastruktur tua yang rentan, maupun secara politis, akibat perbedaan kepentingan negara-negara anggota.

Selain negara, peran sektor swasta juga sangat penting dalam meningkatkan keamanan siber maritim. Perusahaan-perusahaan pelayaran, operator pelabuhan, dan penyedia layanan teknologi informasi memiliki tanggung jawab penting dalam memastikan sistem mereka aman dari ancaman siber. Oleh karena itu, Uni Eropa mendorong kolaborasi yang lebih erat antara sektor publik dan swasta guna menciptakan ekosistem keamanan maritim yang lebih kokoh. Dalam konteks global, kerja sama internasional melalui diplomasi siber menjadi penting, tidak hanya sebagai langkah reaksi atas insiden-insiden siber, tetapi juga sebagai mekanisme pencegahan dalam membangun kesepakatan global terkait norma dan aturan perilaku negara dalam ruang siber. Uni Eropa secara aktif terlibat dengan organisasi internasional seperti International Maritime Organization (IMO) dan NATO dalam upaya perluasan praktik keamanan siber maritim yang lebih baik.

Meski demikian, tantangan global dalam membangun norma tersebut masih nyata, terutama dalam hal menegosiasikan standar keamanan siber yang bisa diterima secara universal. Negara-negara masih cenderung memiliki pendekatan yang berbeda-beda, yang membuat kesepakatan global sulit tercapai dalam jangka pendek. Hal ini menunjukkan perlunya diplomasi siber yang lebih intensif serta kesadaran kolektif akan urgensi ancaman tersebut. perkembangan ancaman siber maritim juga menuntut inovasi teknologi dalam pertahanan siber. Teknologi-teknologi terbaru, seperti kecerdasan buatan (AI) dan analisis data, kini mulai

dimanfaatkan untuk mengantisipasi ancaman siber secara lebih efektif. Namun, pemanfaatan teknologi ini juga menghadirkan tantangan baru terkait tata kelola data, privasi, serta etika dalam penggunaannya. Dengan demikian, mengatasi tantangan keamanan siber maritim memerlukan pendekatan multidimensi, melibatkan diplomasi internasional, penguatan regulasi domestik, serta kolaborasi antara sektor publik dan swasta. Keberhasilan dalam bidang ini akan sangat tergantung pada kemampuan kolektif komunitas internasional, khususnya melalui instrumen kebijakan seperti Cyber Diplomacy Toolbox yang dikembangkan oleh Uni Eropa.

Serangan NotPetya yang melumpuhkan Maersk pada 2017 merupakan salah satu contoh paling nyata dari Supply Chain Attack dalam industri maritim. Malware disisipkan ke dalam pembaruan software akuntansi (M.E.Doc) yang digunakan cabang Maersk di Ukraina. Begitu pembaruan dijalankan, malware masuk ke jaringan internal perusahaan. Kerentanan utama terletak pada infrastruktur IT global Maersk yang sangat terhubung tanpa segmentasi ketat, sehingga malware mampu menyebar ke seluruh dunia hanya dalam hitungan jam. NotPetya memanfaatkan eksploitasi protokol lama Windows seperti SMBv1 (EternalBlue) serta pencurian kredensial melalui Mimikatz untuk melakukan lateral movement ke ribuan perangkat (Greenberg, 2018). Dampaknya, lebih dari 3.500 server dari total 6.200 hancur, 49.000 laptop rusak, dan lebih dari 1.000 aplikasi tidak bisa diakses (Palmer, 2018). NotPetya mampu menyebar cepat di seluruh jaringan internal, merusak sistem komputer pada lebih dari 45.000 perangkat di 600 lokasi di 130 negara. Berbeda dengan ransomware biasa, NotPetya bersifat destruktif karena menghapus data alih-alih memungkinkan pemulihan melalui pembayaran tebusan (Greenberg, 2018).

Lumpuhnya Maersk membuat seluruh sistem booking kontainer, operasional terminal, hingga komunikasi internal berhenti total. Aktivitas logistik di banyak pelabuhan terhenti, sementara staf harus kembali menggunakan metode manual seperti kertas dan pena untuk mencatat arus kontainer (Chirgwin, 2018). Pemulihan baru dapat dilakukan berkat ditemukannya backup Active Directory di kantor Nigeria yang kebetulan mati listrik saat serangan, sehingga selamat dari kerusakan

(Higgins, 2017). Perusahaan memperkirakan kerugian langsung sebesar $250–300 juta USD akibat gangguan operasi, dengan puluhan terminal peti kemas global, termasuk di Rotterdam (Belanda) dan Algeciras (Spanyol), berhenti beroperasi. Namun, kerugian tidak hanya dirasakan oleh perusahaan, melainkan juga oleh negara-negara. Ukraina, negara asal serangan, mengalami kerugian ekonomi sekitar $10 miliar USD secara nasional karena lumpuhnya sektor energi, perbankan, dan transportasi. Denmark, sebagai negara asal Maersk, mengalami kerugian tidak langsung bernilai ratusan juta dolar karena terganggunya perdagangan maritim yang menyumbang sekitar 25% dari PDB Denmark melalui aktivitas Maersk. Selain itu, Amerika Serikat melaporkan kerugian lebih dari $1 miliar USD, terutama dialami oleh FedEx/TNT Express yang juga terdampak. Prancis dan Belanda turut merasakan kerugian karena terhentinya layanan pelabuhan APM Terminals yang beroperasi di wilayah mereka, menyebabkan ribuan kontainer tertahan dan alur logistik terhenti (ENISA, 2018; Maersk, 2018).

Serangan siber terhadap Port of Antwerp, Belgia terjadi antara tahun 2011 hingga 2013, dan dianggap sebagai salah satu kasus paling signifikan yang memperlihatkan kerentanan sektor maritim terhadap kejahatan siber. Dalam kasus ini, sebuah kartel narkotika bekerja sama dengan kelompok peretas asal Eropa Timur untuk menyusup ke sistem manajemen terminal peti kemas. Para pelaku berhasil mengakses sistem komputer pelabuhan melalui malware yang dipasang pada jaringan internal. Dengan cara ini, mereka dapat melacak pergerakan kontainer dan memanipulasi data logistik sehingga narkoba yang diselundupkan dapat diambil tanpa menimbulkan kecurigaan aparat keamanan pelabuhan. Akibat dari serangan ini, Port of Antwerp mengalami kerugian signifikan, tidak hanya secara finansial tetapi juga dalam aspek keamanan dan reputasi. Kerugian finansial mencakup biaya pemulihan sistem, investigasi forensik, serta gangguan terhadap alur distribusi kargo yang menyebabkan keterlambatan logistik. Antwerp sendiri merupakan pelabuhan terbesar kedua di Eropa setelah Rotterdam, menangani sekitar 8,5 juta TEU (twenty-foot equivalent units) kontainer per tahun pada periode tersebut, sehingga setiap gangguan terhadap sistem digitalnya berimplikasi langsung pada rantai pasok global (Port of Antwerp, 2014). Kasus ini tidak hanya

merugikan Belgia, tetapi juga menimbulkan kerugian global dengan potensi miliaran euro akibat keterlambatan distribusi barang, meningkatnya biaya keamanan, serta risiko menurunnya kepercayaan investor pada infrastruktur pelabuhan Eropa (Caldwell, 2014).

Selain kerugian ekonomi, serangan ini juga menimbulkan implikasi strategis terhadap keamanan regional dan global. Fakta bahwa serangan dapat berlangsung selama hampir dua tahun sebelum terdeteksi memperlihatkan lemahnya mekanisme deteksi dini dan koordinasi antar lembaga keamanan di tingkat Eropa. Keterlibatan aktor non-negara dalam memanfaatkan teknologi canggih membuktikan bahwa infrastruktur kritis di sektor maritim dapat dijadikan target kriminal transnasional dengan dampak strategis. Dengan demikian, kasus *Port of Antwerp* menjadi salah satu alasan penting bagi Uni Eropa untuk mengembangkan instrumen kebijakan yang lebih komprehensif, termasuk pembentukan *Cyber Diplomacy Toolbox*, guna meningkatkan kapasitas respon diplomatik dan perlindungan terhadap infrastruktur maritim strategis (European Commission, 2017).

2.2. Cyber Diplomacy Toolbox

2.2.1. Konsep dan Fungsi dari Cyber Diplomacy Toolbox

Serangan siber terhadap sektor maritim bisa melumpuhkan aktivitas perdagangan global. Sistem logistik pelabuhan, navigasi kapal, dan jaringan komunikasi bergantung pada teknologi digital. Maka, ancaman siber terhadap infrastruktur ini tidak hanya berdampak pada ekonomi lokal, tetapi juga memiliki efek domino global (Wired, 2018). Sebagai respons, Uni Eropa membentuk Cyber Diplomacy Toolbox (CDT) pada tahun 2017 sebagai bagian dari Common Foreign and Security Policy (CFSP). CDT dirancang untuk memungkinkan UE menanggapi serangan siber asing melalui pendekatan diplomatik, termasuk pengutukan publik, kerja sama internasional, dan sanksi (European External Action Service, 2020).

Contoh implementasi nyata adalah pada tahun 2020, saat UE menjatuhkan sanksi terhadap sejumlah individu dan entitas yang terkait dengan serangan WannaCry, NotPetya, dan Cloud Hopper. Sanksi tersebut berupa pembekuan aset

dan pelarangan perjalanan ke negara-negara Uni Eropa (Council of the European Union, 2020). Pada tahun 2025, EU mengusulkan pendirian pusat keamanan maritim di Laut Hitam untuk memantau jalur perdagangan dan kabel bawah laut secara real-time. Hal ini menandai integrasi CDT ke dalam strategi keamanan maritim Uni Eropa (Reuters, 2025).

Dalam era digital yang kompleks dan saling terkoneksi, teknologi pertahanan siber atau Cyber Diplomacy Toolbox (CDT) menjadi kunci utama untuk menghadapi ancaman siber yang semakin canggih, khususnya di sektor-sektor strategis seperti maritim. CDT merujuk pada seperangkat teknologi, sistem, metode, dan alat yang dirancang untuk mendeteksi, mencegah, dan merespons ancaman siber dengan efisiensi tinggi. CDT tidak hanya melibatkan perangkat lunak keamanan biasa seperti firewall atau antivirus, tetapi juga mencakup teknologi mutakhir seperti artificial intelligence (AI), machine learning, threat intelligence systems, automated incident response, dan sensor deteksi anomali (Düzenli et al., 2024). CDT dikembangkan oleh kolaborasi antara lembaga pertahanan nasional, perusahaan teknologi, lembaga riset, dan organisasi internasional. Di Uni Eropa, pengembangan CDT banyak difasilitasi oleh European Defence Agency (EDA), European Union Agency for Cybersecurity (ENISA), serta berbagai lembaga riset seperti European Cybersecurity Competence Centre (ECCC) dan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) yang berbasis di Estonia. Negara-negara anggota juga menggandeng sektor swasta seperti Airbus Defence and Space, Leonardo, dan Thales Group yang memiliki spesialisasi dalam sistem pertahanan dan keamanan digital (European Defence Agency, 2023).

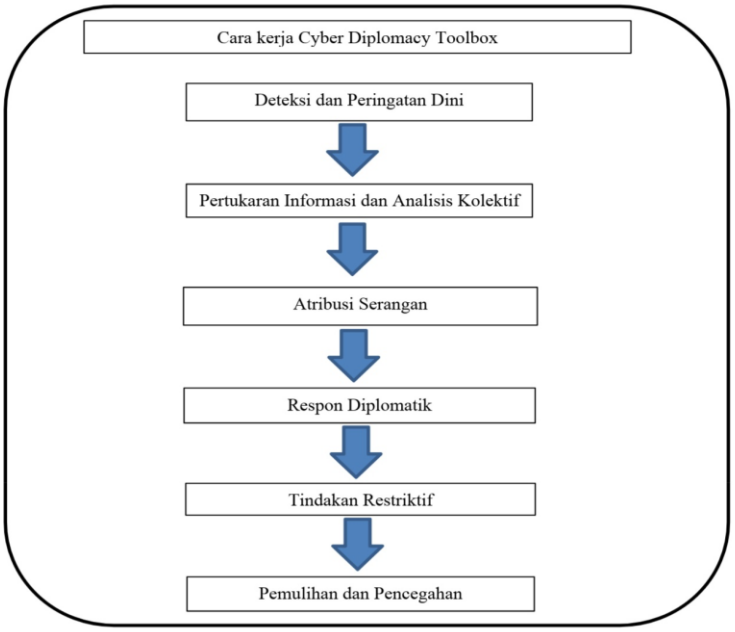
Serangan siber yang mampu dihadapi oleh CDT di sektor maritim sangat beragam. Salah satu ancaman utama adalah ransomware, di mana pelaku mengenkripsi sistem manajemen pelabuhan atau logistik kapal dan menuntut tebusan dalam bentuk crypto. Serangan seperti ini sempat terjadi di Maersk pada tahun 2017 yang menyebabkan gangguan besar dalam rantai pasokan global (Bendiek & Schulze, 2021). CDT saat ini dapat melakukan deteksi ransomware dengan mengenali pola enkripsi dan menghentikan eksekusi kode secara otomatis. Ancaman lain yang umum adalah spoofing GPS, di mana sinyal navigasi kapal

dimanipulasi untuk mengarahkan kapal ke jalur yang salah atau ke wilayah yang tidak aman. CDT sudah menggunakan teknologi multi-layered GPS verification dan threat mapping untuk mengenali sinyal palsu dan membandingkannya dengan data dari satelit atau sistem navigasi alternatif.

Selanjutnya, CDT juga dapat menghadapi serangan DDoS (Distributed Denial of Service) yang menargetkan sistem pelabuhan, terminal logistik, atau layanan e-Navigation. Dengan kapasitas analitik dan firewall dinamis, CDT mampu mendeteksi serangan masif dan secara otomatis mengalihkan trafik, menstabilkan sistem, dan menolak paket data yang berbahaya. Penerapan CDT juga memungkinkan kerja sama lintas negara dan institusi, terutama karena banyak pelabuhan dan jalur logistik maritim di Eropa saling terkoneksi. CDT mendukung sistem melalui protokol yang telah disesuaikan dengan standar Uni Eropa dan NATO, seperti NIS Directive dan Cybersecurity Act. Dengan sistem ini, data dan intelijen ancaman bisa dibagi secara aman antar negara anggota sehingga serangan siber bisa ditangani secara kolektif (European Commission, 2024). CDT juga mendukung pelaksanaan simulasi dan pelatihan keamanan siber maritim. Sistem ini digunakan dalam latihan siber seperti Cyber Europe Exercise yang secara rutin diselenggarakan oleh ENISA, di mana aktor-aktor dari berbagai negara mempraktikkan respons terhadap skenario serangan siber maritim besar-besaran. CDT memainkan peran dalam menyediakan simulasi skenario, analitik data, hingga evaluasi kelemahan sistem yang terdeteksi selama latihan (ENISA, 2022).

Sebagai teknologi yang terus berkembang, CDT di Uni Eropa tidak bersifat statis. Uni Eropa secara aktif mendorong inovasi CDT melalui program riset Horizon Europe, penguatan industri pertahanan siber dalam skema European Defence Fund (EDF), dan pendanaan untuk lembaga-lembaga kompetensi nasional. Fokus pengembangan CDT kedepan mencakup peningkatan zero-trust architecture, post-quantum cryptography, serta integrasi teknologi edge computing dan 5G dalam sistem keamanan pelabuhan dan kapal (Düzenli et al., 2024). Dengan meningkatnya jumlah dan kompleksitas serangan siber di dunia maritim, CDT menjadi bagian tak terpisahkan dalam strategi keamanan siber Uni Eropa. Teknologi ini bukan hanya menjadi alat perlindungan, tetapi juga sarana diplomasi

digital yang menunjukkan kesiapan Uni Eropa dalam melindungi sektor maritimnya dari berbagai bentuk agresi digital yang mungkin digunakan sebagai Cyber Warfare.



Gambar 2.1 Cara Kerja Cyber Diplomacy Toolbox dalam menangani serangan siber di wilayah uni eropa

Sumber : ENISA (2019) dan *European Union Council* (2020)

Dalam chart diatas, sesuai yang dijelaskan oleh ENISA dan *European Union Council* pada tahun 2019 dan 2020 disebutkan bahwa cara kerja dari *Cyber Diplomacy Toolbox* terdiri dari 6 tahap, yaitu:

1. Deteksi dan Peringatan Dini

   Proses diawali dengan identifikasi adanya serangan siber terhadap infrastruktur maritim, seperti pelabuhan, kapal, atau rantai pasok logistik. Sistem deteksi dini membantu mengurangi dampak serangan sejak awal.

2. Pertukaran Informasi dan Analisis Kolektif

   Negara anggota Uni Eropa bersama lembaga terkait saling berbagi informasi dan intelijen mengenai pola serangan. Analisis dilakukan secara kolektif untuk memahami ancaman dan menilai risiko secara menyeluruh.

3. Atribusi Serangan

   Setelah analisis, dilakukan atribusi untuk menentukan pihak pelaku

serangan, apakah berasal dari aktor negara, kelompok non-negara, atau jaringan kriminal transnasional.

4. Respon Diplomatik

   Uni Eropa kemudian mengeluarkan langkah diplomatik, seperti penyampaian nota protes (*démarches*), kecaman publik (*naming and shaming*), hingga peningkatan kerja sama internasional.

5. Tindakan Restriktif

   Jika ancaman tergolong serius, diterapkan langkah koersif berupa sanksi siber. Bentuknya bisa berupa pembekuan aset, pelarangan perjalanan, atau pembatasan kerja sama dengan pihak yang terbukti melakukan serangan.

6. Pemulihan dan Pencegahan

   Setelah insiden, dilakukan pemulihan melalui simulasi, pelatihan, serta peningkatan standar keamanan siber di sektor maritim. Proses ini juga berfungsi sebagai langkah preventif untuk menghadapi serangan serupa di masa depan.

Dengan alur kerja yang sistematis tersebut, CDT tidak hanya berfungsi sebagai instrumen reaktif terhadap insiden siber, tetapi juga sebagai perangkat preventif dan normatif yang memperkuat posisi Uni Eropa dalam diplomasi siber global, khususnya dalam melindungi sektor maritim yang vital bagi stabilitas ekonomi internasional.

2.2.2. Studi Kasus: Implementasi Cyber Diplomacy Toolbox dalam Merespons Serangan Siber

Salah satu contoh nyata penerapan Cyber Diplomacy Toolbox (CDT) adalah kasus serangan siber yang menargetkan infrastruktur kritis dan institusi pemerintah Uni Eropa pada tahun 2020. Serangan ini dikaitkan dengan kelompok Advanced Persistent Threat (APT) yang diduga memiliki afiliasi dengan Rusia, Tiongkok, dan Korea Utara. Serangan tersebut mencakup upaya penyusupan jaringan, pencurian data rahasia, serta upaya melemahkan sistem komunikasi strategis. Kasus ini menjadi penting karena untuk pertama kalinya Uni Eropa menggunakan CDT dalam bentuk pemberlakuan sanksi kolektif terhadap aktor-aktor yang diduga

bertanggung jawab (Council of the European Union, 2020).

Serangan mulai terdeteksi pada kuartal pertama 2020, investigasi berlangsung intensif hingga pertengahan tahun, dan keputusan sanksi resmi dikeluarkan pada Juli 2020. Pemulihan infrastruktur kritis berlangsung hingga akhir tahun dengan program peningkatan keamanan jaringan yang difasilitasi oleh ENISA dan koordinasi Dewan Eropa. Timeline ini menunjukkan bagaimana mekanisme CDT tidak hanya berhenti pada respons jangka pendek, tetapi juga mendorong perubahan kebijakan keamanan siber secara struktural di tingkat Uni Eropa (European Union Institute for Security Studies, 2023).

Dampak dari serangan siber 2020 ini sangat luas, mencakup dimensi ekonomi, politik, hingga keamanan. Dari sisi ekonomi, sejumlah perusahaan logistik dan pelayaran mengalami kelumpuhan sistem selama beberapa hari. Gangguan ini mengakibatkan keterlambatan distribusi barang, hilangnya data operasional, serta biaya pemulihan yang cukup besar. Beberapa pelabuhan besar di Eropa harus menunda layanan sementara demi mencegah meluasnya infeksi malware ke jaringan yang lebih luas. Secara keseluruhan, kerugian finansial yang ditimbulkan mencapai jutaan euro, yang tidak hanya merugikan sektor swasta tetapi juga menekan anggaran publik untuk mendanai pemulihan infrastruktur digital (European Maritime Safety Agency, 2022).

Dari sisi politik dan diplomasi, serangan ini menguji kredibilitas Uni Eropa sebagai aktor keamanan global. Kebocoran data diplomatik yang ditargetkan melalui sistem email dan komunikasi internal memperlihatkan bahwa motif serangan bukan semata ekonomi, melainkan juga strategis yaitu untuk memperoleh keuntungan politik dan intelijen dari kerentanan digital Eropa. Akibatnya, muncul perdebatan di antara negara anggota mengenai sejauh mana Uni Eropa harus memperkuat mekanisme kolektif melalui CDT. Beberapa negara anggota mendorong respons yang lebih keras berupa sanksi segera, sementara negara lain lebih berhati-hati karena khawatir menimbulkan eskalasi geopolitik. Perbedaan sikap ini menunjukkan bahwa serangan siber dapat memicu fragmentasi politik internal Uni Eropa (European Policy Centre, 2019).

Aktor yang terlibat dalam kasus ini diidentifikasi sebagai kelompok

Advanced Persistent Threats (APT) dengan afiliasi ke negara besar. Kelompok APT28 (Fancy Bear) yang dikaitkan dengan Rusia, APT10 yang terkait dengan Tiongkok, serta Lazarus Group dari Korea Utara terdeteksi sebagai pelaku utama. Korban dari serangan ini sangat beragam, mulai dari institusi pemerintahan Uni Eropa, kementerian luar negeri beberapa negara anggota, perusahaan teknologi, operator pelabuhan, hingga perusahaan pelayaran multinasional. Fakta bahwa serangan diarahkan pada infrastruktur maritim menunjukkan adanya upaya sistematis untuk melemahkan salah satu sektor vital Eropa yang menghubungkan perdagangan global. Dengan demikian, serangan ini tidak hanya bersifat teknis, tetapi juga strategis karena menargetkan aspek ekonomi dan politik sekaligus (Council of the European Union, 2020; European Union Institute for Security Studies, 2023).

Proses penanganan dimulai dari tahap deteksi dan peringatan dini. Melalui kerja sama antara badan keamanan siber nasional negara anggota dan EU Agency for Cybersecurity (ENISA), ditemukan indikasi serangan siber terkoordinasi sejak awal 2020. Sistem deteksi intrusi di beberapa negara anggota melaporkan pola serangan serupa yang mengarah pada pencurian data sensitif dari institusi pemerintah dan perusahaan maritim. Informasi ini kemudian disalurkan melalui mekanisme koordinasi Uni Eropa, yang memungkinkan respons awal berupa peningkatan status kewaspadaan dan penerapan langkah mitigasi darurat (European Union Institute for Security Studies, 2023).

Tahap berikutnya adalah investigasi dan atribusi. Tim forensik digital Uni Eropa bersama negara anggota mengidentifikasi bahwa serangan ini melibatkan teknik spear phishing, malware tingkat lanjut, serta eksploitasi kerentanan perangkat lunak yang sebelumnya belum ditambal (zero-day vulnerabilities). Setelah analisis mendalam, laporan teknis menyebutkan adanya keterkaitan dengan kelompok APT28 (diduga berhubungan dengan militer Rusia), APT10 (afiliasi Tiongkok), dan kelompok Lazarus (Korea Utara). Informasi atribusi ini dipresentasikan dalam rapat Dewan Uni Eropa sebagai dasar pertimbangan sanksi (European Policy Centre, 2019).

Setelah atribusi dianggap kredibel, Uni Eropa memasuki tahap pengambilan

keputusan kolektif. Proposal pemberlakuan sanksi diajukan oleh Perwakilan Tinggi Uni Eropa untuk Urusan Luar Negeri dan Kebijakan Keamanan, kemudian dibahas dalam Working Party on Cyber Issues dan Dewan Urusan Luar Negeri. Pada Juli 2020, Dewan Uni Eropa secara resmi mengadopsi Council Decision (CFSP) 2020/1127, yang menetapkan sanksi terhadap enam individu dan tiga entitas yang terkait dengan serangan siber tersebut. Keputusan ini menjadi tonggak sejarah karena untuk pertama kalinya Uni Eropa mengaktifkan rezim sanksi siber kolektifnya (Council of the European Union, 2020).

Sanksi yang dijatuhkan mencakup pembekuan aset, pelarangan perjalanan ke Uni Eropa, serta larangan bagi individu dan entitas yang terdaftar untuk menerima dukungan finansial dari warga atau perusahaan Uni Eropa. Misalnya, perusahaan teknologi asal Tiongkok Tianjin Huaying Haitai Science and Technology Development Co. Ltd dikenai sanksi karena terlibat dalam serangan Operation Cloud Hopper, sementara individu dari Rusia dan Korea Utara dikenai sanksi karena berperan langsung dalam peretasan jaringan penting di Eropa. Sanksi ini menunjukkan bahwa Uni Eropa memandang serangan siber bukan sekadar ancaman teknis, melainkan juga isu politik dan keamanan internasional (Khausar & Ras, 2023).

Tahap selanjutnya adalah pemulihan dan pencegahan. Setelah serangan terdeteksi dan sanksi dijatuhkan, Uni Eropa memperkuat koordinasi antarnegara anggota untuk memulihkan sistem yang terdampak. ENISA mengeluarkan panduan teknis mengenai patching sistem, perbaikan arsitektur keamanan jaringan, serta protokol darurat untuk sektor maritim yang menjadi salah satu target serangan. Selain itu, dilakukan simulasi serangan (cyber exercises) secara kolektif guna meningkatkan kesiapan menghadapi ancaman serupa di masa depan (European Maritime Safety Agency, 2022).

2.2.3. Cyber Diplomacy Toolbox Sebagai Rezim Uni Eropa

Cyber Diplomacy Toolbox (CDT) yang diadopsi Uni Eropa pada tahun 2017 dapat dipahami sebagai sebuah rezim dalam arti teori rezim yang dijelaskan oleh Stephen Krasner. Menurut Krasner, rezim adalah seperangkat prinsip, norma,

aturan, dan prosedur pengambilan keputusan yang disepakati oleh aktor-aktor internasional dalam suatu isu tertentu (Krasner, 1982). Dalam konteks ini, CDT lahir sebagai jawaban atas meningkatnya serangan siber yang semakin canggih dan berbahaya, termasuk serangan terhadap infrastruktur kritis dan sektor maritim (Khausar & Ras, 2023). Melalui CDT, Uni Eropa berusaha menciptakan mekanisme kolektif untuk mencegah, menanggulangi, dan merespons ancaman siber, sehingga membangun stabilitas di ruang digital yang rentan.

Sebagai rezim, CDT tidak hanya berfungsi pada level teknis, tetapi juga memperlihatkan dimensi politik dan diplomatik. Uni Eropa dan negara-negara anggotanya menyepakati serangkaian prinsip bersama, misalnya bahwa serangan siber terhadap infrastruktur vital merupakan ancaman serius terhadap keamanan, ekonomi, dan demokrasi kawasan. Norma ini kemudian diterjemahkan dalam aturan-aturan konkret seperti pemberlakuan sanksi, mekanisme berbagi informasi, serta koordinasi dalam kerangka Common Foreign and Security Policy (CFSP) (Council of the European Union, 2017). Dengan demikian, CDT mencerminkan kesepakatan kolektif yang mengikat negara-negara anggota, sekaligus menegaskan peran Uni Eropa sebagai aktor yang berusaha membentuk tatanan normatif di dunia maya.

CDT juga menunjukkan bagaimana rezim internasional dapat memengaruhi perilaku negara dan aktor non-negara. Melalui instrumen diplomatik seperti atribusi publik, nota diplomatik, hingga sanksi ekonomi, Uni Eropa berupaya memberikan efek jera bagi pihak yang melancarkan serangan siber. Pada saat yang sama, CDT juga memperkuat solidaritas digital antarnegara anggota, di mana serangan terhadap satu negara dipandang sebagai ancaman bagi seluruh kawasan. Inilah yang menjadikan CDT bukan sekadar kebijakan teknis, tetapi sebuah rezim yang mengikat, yang mampu mengarahkan arah kebijakan keamanan siber Uni Eropa, khususnya dalam menghadapi ancaman di sektor maritim yang semakin terdigitalisasi (Moret & Pawlak, 2017).

Sebelum terbentuknya Cyber Diplomacy Toolbox (CDT) pada tahun 2017, Uni Eropa telah memiliki sejumlah instrumen dan kerangka rezim yang ditujukan untuk menghadapi ancaman di ruang siber. Namun, berbagai rezim sebelumnya

dianggap masih belum memadai, baik dari segi mekanisme penegakan, koordinasi antarnegara anggota, maupun efektivitas dalam merespons serangan siber yang bersifat lintas batas. Oleh karena itu, lahirnya CDT dapat dipahami sebagai upaya Uni Eropa untuk memperkuat fondasi tata kelola siber regional dengan instrumen yang lebih komprehensif, terintegrasi, dan responsif.

1. Rezim Keamanan Siber Awal: NIS Directive

Salah satu rezim awal yang menjadi tonggak penting bagi Uni Eropa adalah Directive on Security of Network and Information Systems (NIS Directive) 2016. Regulasi ini merupakan kerangka hukum pertama di Uni Eropa yang secara khusus mengatur tentang ketahanan jaringan dan sistem informasi. Tujuan utamanya adalah memastikan tingkat keamanan siber yang tinggi dan seragam di seluruh negara anggota (Carrapico & Barrinha, 2017).

Meskipun menjadi kemajuan penting, NIS Directive masih memiliki sejumlah keterbatasan. Pertama, sifatnya lebih menekankan pada aspek preventif seperti peningkatan ketahanan infrastruktur dan kewajiban berbagi informasi antarnegara anggota namun belum menyediakan instrumen politik-diplomatik untuk merespons serangan yang bersifat geopolitik. Kedua, mekanisme implementasi NIS Directive sangat bergantung pada kapasitas masing-masing negara anggota, sehingga menimbulkan kesenjangan standar keamanan antarnegara di dalam Uni Eropa (Christou, 2018). Kondisi inilah yang menunjukkan bahwa meskipun terdapat rezim hukum yang kuat, respon Uni Eropa terhadap insiden siber berskala besar masih bersifat parsial.

2. Strategi Keamanan Siber Uni Eropa 2013 dan 2016

Sebelum NIS Directive berlaku penuh, Uni Eropa telah meluncurkan EU Cybersecurity Strategy 2013, yang merupakan visi strategis pertama dalam menyatukan kebijakan pertahanan dan keamanan siber di tingkat regional. Strategi ini menekankan lima prioritas: ketahanan siber, pengurangan kejahatan siber, pengembangan kebijakan pertahanan siber, promosi industri siber, dan mendorong kebijakan kebebasan internet global (European Commission, 2013).

Namun, strategi 2013 ini dianggap terlalu normatif dan minim instrumen

praktis untuk menghadapi serangan siber yang kian meningkat, terutama serangan dengan motif geopolitik dari aktor negara (Jensen, 2019). Oleh karena itu, Uni Eropa memperbarui strategi ini dengan EU Cybersecurity Strategy 2016, yang lebih menekankan kolaborasi dengan badan keamanan seperti ENISA (European Union Agency for Network and Information Security) dan peningkatan kapasitas negara anggota dalam deteksi serta respons insiden. Akan tetapi, strategi ini pun masih sebatas arahan kebijakan tanpa memberikan mekanisme sanksi atau instrumen diplomasi kolektif terhadap aktor negara yang dianggap bertanggung jawab atas serangan.

3. Rezim Pertahanan dan Kebijakan Luar Negeri: CFSP dan PESCO

Selain rezim teknis, Uni Eropa juga mengandalkan Common Foreign and Security Policy (CFSP) serta kerangka Permanent Structured Cooperation (PESCO) untuk merespons ancaman siber dalam kerangka pertahanan kolektif. CFSP memungkinkan Uni Eropa untuk menggunakan instrumen diplomatik, termasuk sanksi, dalam merespons ancaman eksternal. Sementara PESCO memberi ruang bagi negara anggota untuk berkolaborasi dalam proyek-proyek pertahanan bersama, termasuk yang terkait dengan keamanan siber (Fiott, 2018).

Namun, keterbatasan utama dari kedua rezim ini adalah sifatnya yang bersifat umum dan tidak secara spesifik dirancang untuk domain siber. CFSP memang membuka kemungkinan penggunaan sanksi, tetapi pada masa sebelum CDT, belum ada mekanisme operasional yang jelas mengenai bagaimana dan kapan sanksi dapat dijatuhkan terhadap serangan siber (Maurer, 2018). Sementara itu, PESCO lebih berorientasi pada pembangunan kapabilitas militer jangka panjang, sehingga tidak dapat memberikan respons cepat terhadap insiden siber yang membutuhkan keputusan segera.

Kondisi di atas melatarbelakangi lahirnya Cyber Diplomacy Toolbox (CDT) pada tahun 2017. CDT merupakan mekanisme kebijakan luar negeri Uni Eropa yang menyediakan spektrum instrumen diplomasi mulai dari pernyataan politik, tindakan pembatasan (restrictive measures), hingga sanksi terhadap aktor negara atau non-negara yang terlibat dalam serangan siber (European Council, 2017).

Dengan adanya CDT, Uni Eropa untuk pertama kalinya memiliki instrumen yang secara eksplisit menghubungkan isu keamanan siber dengan kebijakan luar negeri dan keamanan kolektif.

CDT bukan hanya melengkapi kekurangan rezim sebelumnya, tetapi juga mencerminkan kesadaran baru bahwa serangan siber memiliki implikasi geopolitik yang serius. Keputusan untuk membentuk CDT juga menandai pergeseran pendekatan Uni Eropa dari sekadar regulasi teknis ke arah diplomasi koersif yang lebih tegas dalam mempertahankan kepentingan strategisnya di ruang siber (Pawlak, 2020). Dengan demikian, CDT menjadi representasi transformasi Uni Eropa dari rezim yang terpecah menuju rezim cyber diplomasi yang terstruktur.

2.2.4. Kondisi Keamanan Siber Uni Eropa Sebelum dan Sesudah Munculnya *Cyber Diplomacy Toolbox*

Sebelum Uni Eropa mengadopsi Cyber Diplomacy Toolbox (CDT) pada tahun 2017, kebijakan keamanan siber di tingkat regional masih bersifat umum dan belum diarahkan secara khusus pada sektor maritim. EU Cybersecurity Strategy 2013, misalnya, menekankan pentingnya meningkatkan ketahanan infrastruktur penting, mendorong kerja sama dengan sektor swasta, dan memperkuat penegakan hukum terhadap kejahatan siber (European Commission, 2013). Meskipun pelabuhan dan rantai pasok maritim termasuk dalam kategori critical infrastructures, dokumen ini tidak memberikan kerangka regulasi yang secara khusus menyasar keamanan digital sektor maritim. Hal serupa terlihat dalam EU Maritime Security Strategy 2014 yang lebih berfokus pada ancaman tradisional seperti pembajakan, terorisme, dan keamanan jalur perdagangan. Isu siber hanya disebut sebagai salah satu risiko baru tanpa adanya instrumen kebijakan yang memadai untuk mengatasinya (European Union, 2014).

Langkah yang lebih konkret mulai diambil melalui pengesahan Directive on Security of Network and Information Systems (NIS Directive) pada tahun 2016. Regulasi ini merupakan instrumen hukum pertama Uni Eropa di bidang keamanan siber yang mewajibkan negara anggota meningkatkan kesiapan siber, membentuk Computer Security Incident Response Teams (CSIRTs), serta menunjuk operator

infrastruktur penting yang harus menerapkan standar keamanan minimum (European Union, 2016). Namun, implementasi NIS Directive sangat bergantung pada masing-masing negara anggota, sehingga terjadi ketidakseragaman standar keamanan di sektor maritim. Dengan kata lain, sebelum CDT lahir, Uni Eropa memang telah memiliki kerangka hukum terkait keamanan siber, tetapi sifatnya masih terfragmentasi dan belum menyediakan mekanisme kolektif yang kuat untuk merespons ancaman lintas batas.

Perubahan signifikan terjadi setelah lahirnya CDT pada Juni 2017. Mekanisme ini menyediakan alat diplomatik baru bagi Uni Eropa untuk menghadapi serangan siber, yaitu atribusi kolektif, kecaman publik, serta sanksi terhadap individu atau entitas yang dinilai bertanggung jawab. Dampaknya terlihat jelas pada tahun 2020 ketika Uni Eropa untuk pertama kalinya menggunakan sanksi siber terhadap enam individu dan tiga entitas asal Rusia, Tiongkok, dan Korea Utara, termasuk terkait serangan NotPetya yang melumpuhkan perusahaan pelayaran Maersk (Council of the European Union, 2020). Tindakan ini menandai tonggak penting, karena untuk pertama kalinya Uni Eropa menerapkan diplomasi siber secara nyata dengan konsekuensi politik dan hukum yang langsung dirasakan oleh sektor maritim.

Integrasi diplomasi siber semakin terlihat dalam revisi EU Maritime Security Strategy pada tahun 2018, yang untuk pertama kalinya secara eksplisit mengakui ancaman siber sebagai risiko utama bagi sektor maritim. Infrastruktur pelabuhan, sistem logistik, dan navigasi laut diidentifikasi sebagai target strategis yang membutuhkan perlindungan bukan hanya melalui solusi teknis, tetapi juga lewat koordinasi politik dan diplomatik di tingkat Uni Eropa (European Union, 2018). Kesadaran ini kemudian diperkuat dengan lahirnya NIS2 Directive pada tahun 2020, yang memperluas cakupan sektor serta menetapkan standar keamanan yang lebih ketat bagi entitas penting, termasuk pelabuhan besar dan perusahaan pelayaran (European Union, 2020). Perubahan ini tidak dapat dilepaskan dari pengalaman Uni Eropa menghadapi serangan besar seperti NotPetya, yang memperlihatkan betapa rapuhnya rantai pasok Eropa ketika diserang secara digital.

Sebelum Terbentuk *Cyber Diplomacy Toolbox* (Sebelum tahun 2017) :

Tabel 2.1 Contoh Kasus Serangan Siber yang Menyerang Uni Eropa Berdasarkan Data dari *Council Of The European Union* (2020)

Kasus	Tahun	Jenis Serangan	Pelaku Terduga	Respon Uni Eropa
Estonia Cyberattack	2007	DdoS Terhadap Infrastruktur negara	Rusia	Respon masih terbatas dan meminta bantuan terhadap NATO
Stuxnet	2010	Malware SCADA industri	AS dan Israel (dugaan)	Peningkatan Kesadaran terhadap ancaman siber
Operation Shady RAT	2006 - 2011	Spionase Siber	Tidak Diketahui, aktor negara Asia Timur (Dugaan)	Dilakukan penyelidikan namun terbatas
Peretasan Pelabuhan Rotterdam	2011 - 2013	Penyusupan Sistem Logistik kontainer untuk penyeludupan narkoba	Kartel Narkoba	Tidak terdapat respon diplomatik kolektif
Peretasan Sistem AIS kapal eropa di	2014 - 2015	Manipulasi Automatic Identification	Rusia (dugaan)	Dilakukan penyelidikan namun

laut hitam		System (AIS) Kapl		terbatas

sumber: Council Of The European Union (2020)

Setelah Terbentuk *Cyber Diplomacy Toolbox* :

Tabel 2.2 Contoh Kasus Serangan Siber yang Menyerang Uni Eropa Berdasarkan Data dari *Council Of The European Union* (2020)

Kasus	Tahun	Jenis Serangan	Pelaku Terduga	Respon Uni Eropa
Operation Ghostwritter	2019 - 2021	Peretasan dan Disinformasi Politik	APT28 (Rusia)	Nota diplomatik dan Atribusi Kolektif
UE Cyber Sanction (NotPetya, Wannacry, APT10)	2020	Malware, Spionase, Ransomware	Rusia, China, Korea Utara	Sanksi Resmi (pembekuan aset dan Larangan visa)
SolarWinds	2020	Supply Chain Attack	APT29 (Rusia)	Koordinasi dengan AS dan NATO
Serangan pada sistem IT pelabuhan Antwerp (Belgia)	2022	Malware dan sabotase logistik kontainer	Kelompok kriminal yang terhubung dengan kartel narkoba	Investigasi dan peningkatan pengamanan pelabuhan Uni Eropa
GPS Spoofing dan Jamming terhadap kapal	2021 - 2023	Intervensi sinyal navigasi kapal	Dugaan keterlibatan aktor negara	Pemberian peringatan dari EMSA

dagang Eropa di Mediterania Timur			(Rusia/Turki) di zona konflik	dan integrasi dalam strategi keamanan maritim siber dibawah Uni Eropa

sumber: Council Of The European Union (2020)

Sebelum hadirnya *Cyber Diplomacy Toolbox* (CDT) sebagai pendekatan dalam menghadapi ancaman siber, Uni Eropa menghadapi berbagai tantangan serius dalam keamanan digital, terutama di sektor maritim yang sangat vital bagi ekonomi kawasan. Kawasan Eropa, dengan lebih dari 1.200 pelabuhan aktif dan ribuan kapal komersial yang beroperasi di perairan internal maupun internasional, menjadi target yang mudah bagi serangan siber karena minimnya perlindungan infrastruktur digital pada masa awal digitalisasi (Bendiek & Schulze, 2021). Pada dasarnya, sebelum sekitar tahun 2016 sampai 2017, banyak negara Uni Eropa belum memiliki strategi keamanan siber nasional yang terintegrasi untuk sektor maritim. Keamanan digital sebagian besar masih dianggap urusan internal perusahaan pelayaran atau operator pelabuhan. Kebijakan keamanan siber bersifat terpecah, dengan pendekatan yang bervariasi antara satu negara dengan negara lain. Beberapa negara seperti Jerman dan Belanda memang lebih maju dengan membentuk lembaga perlindungan infrastruktur digital, namun banyak negara anggota lainnya masih tertinggal dalam kesiapan menghadapi ancaman siber (Carrapico & Barrinha, 2017).

Ketidaksiapan ini menjadi semakin terlihat saat insiden besar terjadi. Seperti, serangan siber NotPetya pada tahun 2017 yang melumpuhkan berbagai sistem logistik dan pelayaran global, termasuk kantor Maersk Line di berbagai pelabuhan Eropa. Serangan ini tidak hanya menyebabkan kerugian hingga USD 300 juta, tetapi juga memperlihatkan bahwa perusahaan maupun negara tidak memiliki respons cepat atau sistem pertahanan yang efektif untuk mengatasi dampak siber secara sistemik (Bendiek & Schulze, 2021). Ketiadaan CDT membuat negara dan aktor

industri maritim hanya bisa mengandalkan antivirus konvensional atau sistem teknologi manual yang tidak mampu mengenali skala ancaman yang kompleks dan cepat menyebar. Sebelum CDT diperkenalkan, upaya yang dilakukan bersifat reaktif, bukan proaktif. Misalnya, ketika sistem pelabuhan mengalami anomali atau kelumpuhan, respons yang dilakukan adalah pemadaman sistem (*shutdown*), pemulihan data secara manual, atau pelaporan ke lembaga keamanan nasional yang terkadang tidak memiliki spesialisasi siber maritim. Pendekatan ini tentu berisiko tinggi dan lambat, serta menyulitkan pemulihan yang cepat.

Ketiadaan sistem intelijen ancaman (*threat intelligence system*) membuat banyak pelabuhan atau kapal tidak mengetahui sumber, pola, atau metode serangan yang terjadi di lokasi lain. Hal ini menimbulkan efek domino, karena satu serangan berhasil menargetkan satu sistem, lalu menyebar dengan cepat ke sistem terhubung lainnya di negara berbeda tanpa koordinasi regional yang memadai untuk mengatasinya (Pernik, 2018). Selain itu, sebelum adanya CDT, pelatihan keamanan siber untuk pekerja di sektor maritim juga sangat minim. Operator kapal, petugas pelabuhan, dan manajer logistik tidak dilengkapi dengan pemahaman dasar tentang ancaman siber, teknik phishing, atau protokol enkripsi data. Banyak sistem yang menggunakan software versi lama, tidak diperbarui, dan bahkan memiliki kata sandi default yang merupakan kondisi yang ideal bagi serangan siber (ENISA, 2016).

Regulasi dan kerangka hukum Uni Eropa pun masih dalam tahap pengembangan. Sebelum 2016, belum ada kerangka hukum yang secara khusus mengatur standar keamanan siber maritim atau kerja sama antar lembaga keamanan digital di seluruh Uni Eropa. Baru pada 2016 Uni Eropa mengesahkan NIS Directive (*Directive on Security of Network and Information Systems*), yang kemudian menjadi dasar untuk penguatan kerjasama antarnegara dalam perlindungan infrastruktur digital penting, termasuk sektor maritim (European Commission, 2022). Kondisi ini mendorong perlunya transformasi pendekatan keamanan digital dari nasional ke supranasional, serta dari sistem pasif menjadi aktif dan adaptif. Kesenjangan inilah yang kemudian mengarahkan pada penciptaan dan pengadopsian *Cyber Diplomacy Toolbox* (CDT) yang lebih canggih, berbasis

AI dan threat intelligence, serta mampu mendeteksi, menganalisis, merespons, dan memulihkan sistem dari serangan siber secara otomatis dan lintas batas negara. Hadirnya CDT juga merupakan respons terhadap pergeseran ancaman global: dari konflik bersenjata tradisional ke peperangan hybrid dan serangan digital. Dalam konteks geopolitik saat ini, Uni Eropa tidak hanya menghadapi serangan dari kelompok kriminal terorganisir, tetapi juga dari aktor negara (state-sponsored) seperti yang ditunjukkan dalam insiden spionase digital dan serangan pada rantai pasok logistik energi serta pelabuhan-pelabuhan strategis (Carrapico & Barrinha, 2017).

2.2.5. Peran Negara-Negara Uni Eropa Dalam Mengadopsi *Cyber Diplomacy Toolbox*

Seiring dengan meningkatnya frekuensi dan kompleksitas serangan siber yang mengancam infrastruktur kritis, negara-negara anggota Uni Eropa mulai memperkuat sistem pertahanan digital mereka melalui adopsi *Cyber Diplomacy Toolbox* (CDT). Meskipun implementasi CDT berbeda-beda antarnegara, terdapat pola umum berupa kolaborasi antara pemerintah, industri, dan lembaga riset yang menjadi kunci kesuksesan pengembangan sistem pertahanan siber maritim yang kuat.

1. Estonia

Estonia menjadi negara Uni Eropa pertama yang serius mengembangkan CDT, terutama setelah mengalami serangan siber besar-besaran pada tahun 2007 yang melumpuhkan sistem perbankan, pemerintahan, dan infrastruktur komunikasi. Pengalaman ini mendorong pembentukan NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) di Tallinn, yang kini menjadi pusat pelatihan dan pengembangan CDT untuk negara-negara NATO dan mitra Uni Eropa (Pernik, 2018). Estonia memanfaatkan CDT untuk sistem e-Government, pelabuhan, dan keamanan maritim berbasis digital. Teknologi seperti intrusion detection systems (IDS) dan AI-based anomaly detection telah digunakan untuk memantau jalur komunikasi antar kapal dan pelabuhan. Negara ini juga memimpin dalam

penggunaan blockchain untuk perlindungan data logistik maritim dan koordinasi informasi lintas instansi (Tikk et al., 2022).

2. Belanda: Pusat Inovasi Maritim dan Keamanan Siber Pelabuhan

Sebagai salah satu negara pelabuhan terbesar di Eropa dengan Rotterdam sebagai pelabuhan tersibuk di benua ini, Belanda memiliki kepentingan strategis dalam pengembangan CDT. Pemerintah Belanda bekerja sama dengan sektor swasta dan universitas melalui program seperti *Cyber Security Innovation Platform* untuk mengembangkan teknologi keamanan pelabuhan otomatis, termasuk threat intelligence sharing platforms, sistem monitoring real-time untuk aktivitas logistik, serta sistem kontrol berbasis machine learning. Belanda juga menjadi negara pertama yang menguji coba *maritime cyber range*, yaitu laboratorium simulasi serangan siber maritim, untuk melatih operator pelabuhan dan pengemudi kapal dalam menanggapi serangan digital. Hal ini menjadikan Belanda sebagai pusat pengujian dan pengembangan CDT berbasis maritim (Karas, 2023).

3. Prancis dan Jerman

Sebagai dua negara besar Uni Eropa dengan kapasitas industri pertahanan yang kuat, Prancis dan Jerman berperan penting dalam mendanai dan mengembangkan CDT melalui perusahaan besar seperti *Thales* (Prancis) dan *Siemens Defence* (Jerman). Keduanya memproduksi perangkat keras dan lunak untuk keamanan digital pelabuhan, kapal tanker, serta sistem kontrol energi laut. Jerman, misalnya, telah memasukkan CDT sebagai bagian dari strategi keamanan siber nasional melalui *Federal Office for Information Security* (BSI). Pelabuhan-pelabuhan besar seperti Hamburg kini menggunakan sistem multi-layered firewall, behavioural analytics, dan sensor deteksi GPS spoofing untuk memastikan jalur distribusi logistik tetap aman dari sabotase digital (Bendiek & Schulze, 2021). Di sisi lain, Prancis mengintegrasikan CDT dalam strategi maritim nasionalnya, dengan membentuk Pôle d'Excellence Cyber (PEC) untuk menghubungkan kebutuhan militer dan sipil dalam keamanan siber. Prancis juga berperan penting dalam mendorong European Cyber Situational Awareness Platform, yang membantu negara-negara Eropa saling berbagi informasi ancaman secara real time

(Carrapico & Barrinha, 2017).

4. Italia dan Spanyol

Italia dan Spanyol, sebagai dua negara pesisir dengan pelabuhan besar di Mediterania, mulai mengadopsi CDT terutama untuk sektor logistik dan perdagangan laut. Italia, melalui badan pertahanannya, telah mengembangkan sistem predictive analytics dan monitoring cyber-physical systems untuk pelabuhan Genoa dan Napoli. Spanyol meluncurkan program nasional untuk memperkuat cyber resilience sektor maritim melalui pelatihan berbasis CDT dan pelibatan perusahaan pelayaran seperti Navantia dan Repsol. Negara ini juga menekankan pada aspek legal melalui regulasi keamanan TI di pelabuhan yang diperbarui secara berkala berdasarkan rekomendasi ENISA dan European Commission (ENISA, 2022).

5. Negara-Negara Nordik

Negara-negara Nordik seperti Swedia, Finlandia, dan Denmark memiliki pendekatan kolaboratif dalam pengembangan CDT, khususnya di wilayah laut Arktik dan Baltik. Karena tantangan iklim ekstrem dan ancaman geopolitik yang meningkat, mereka membentuk *Nordic-Baltic Cybersecurity Collaboration Framework*, sebuah platform lintas negara untuk pengembangan CDT bersama, pertukaran data intelijen, dan pelatihan *cyber wargames maritim*. Swedia memiliki sistem keamanan pelabuhan berbasis AI dan autonomous response system, sementara Finlandia mengintegrasikan CDT dengan satellite-based surveillance dan sistem deteksi penipuan sinyal kapal. Denmark, sebagai markas besar Maersk, sangat aktif dalam membangun sistem CDT terdesentralisasi di seluruh jaringan logistik lautnya (Tikk et al., 2022).

2.2.6. Komitmen Uni Eropa

Uni Eropa telah menunjukkan komitmen yang kuat dan berkelanjutan dalam memperkuat keamanan siber, khususnya dalam sektor maritim, melalui pengembangan dan pemeliharaan Cyber Diplomacy Toolbox (CDT). Komitmen ini diwujudkan dalam bentuk kerangka kebijakan, pendanaan riset, pembentukan pusat

kolaborasi, serta pelatihan dan penguatan kapabilitas teknis di tingkat negara anggota maupun regional.

Komitmen Uni Eropa dalam pengembangan CDT dimulai dengan kerangka strategis yang terdefinisi dengan baik. Salah satunya adalah dokumen EU Cybersecurity Strategy for the Digital Decade (2020) yang menetapkan keamanan siber sebagai bagian integral dari kedaulatan digital Uni Eropa. Di dalamnya, CDT disebut sebagai salah satu prioritas untuk melindungi infrastruktur kritis, termasuk pelabuhan dan jalur pelayaran strategis (Bendiek & Schulze, 2021). Di tingkat regulasi, Uni Eropa mengesahkan NIS2 Directive (2022) pembaruan dari NIS Directive yang mewajibkan negara anggota dan operator sektor esensial untuk menerapkan sistem pertahanan siber canggih, termasuk CDT. Aturan ini tidak hanya memperkuat standar minimum, tetapi juga mendorong penggunaan teknologi mutakhir seperti AI-based threat detection, automated response, dan resilience testing terhadap seluruh infrastruktur digital maritim (European Commission, 2022).

Uni Eropa menyediakan berbagai skema pendanaan untuk mendukung pengembangan CDT secara berkelanjutan. Program seperti Horizon Europe dan Digital Europe Programme mengalokasikan miliaran euro untuk riset dan pengembangan teknologi keamanan siber, termasuk untuk aplikasi di sektor maritim. Salah satu contoh konkret adalah proyek Cyber-MAR, sebuah proyek penelitian yang berfokus pada penerapan CDT berbasis AI untuk perlindungan rantai pasok maritim dan pelatihan simulasi serangan siber (Cyber-MAR Project, 2021). Selain itu, European Defence Fund (EDF) menyediakan dana khusus untuk CDT yang terkait pertahanan dan keamanan, termasuk pelabuhan militer, jalur logistik pertahanan, serta sistem pelacakan kapal berbasis satelit. Program ini membantu mempercepat integrasi CDT dalam lingkungan operasional dan mendukung kolaborasi antara perusahaan pertahanan, lembaga riset, dan pemerintah (European Commission, 2022).

Uni Eropa juga membentuk sejumlah lembaga yang didedikasikan untuk pengembangan dan pemeliharaan CDT. Salah satu yang paling penting adalah European Cybersecurity Competence Centre (ECCC) yang berbasis di Bucharest,

Rumania. Lembaga ini menjadi pusat koordinasi riset dan inovasi keamanan siber, termasuk pengembangan CDT lintas sektor, serta sebagai penghubung antara negara anggota dan aktor industri (ECCC, 2023). Di samping itu, European Union Agency for Cybersecurity (ENISA) secara rutin menerbitkan panduan, rekomendasi teknis, dan laporan ancaman untuk sektor maritim. ENISA juga melakukan cybersecurity exercises, audit teknologi CDT, serta mendorong standardisasi perangkat lunak dan perangkat keras keamanan digital di lingkungan pelabuhan dan logistik laut (ENISA, 2022).

CDT yang digunakan oleh Uni Eropa tidak hanya dikembangkan sekali lalu dibiarkan berjalan secara otomatis. Salah satu wujud nyata komitmen Uni Eropa adalah proses pemeliharaan berkala, termasuk pembaruan sistem, penambahan fitur proteksi, serta pemantauan adaptif terhadap jenis serangan baru. Contohnya, sistem Maritime Cyber Security Monitoring (MCSM) di pelabuhan Rotterdam secara berkala diperbarui setiap triwulan berdasarkan laporan threat intelligence global dan hasil simulasi lokal (Karas, 2023). Banyak sistem CDT modern di Eropa dirancang untuk melakukan self-healing dan predictive patching, yakni kemampuan untuk mengidentifikasi potensi kerentanan sebelum digunakan oleh aktor jahat, serta menerapkan perbaikan secara otomatis berdasarkan pembelajaran mesin.

Komitmen Uni Eropa juga tercermin dari keterlibatannya dalam kolaborasi internasional yang memperkuat keamanan maritim global. Uni Eropa, melalui ENISA dan CCDCOE (Cooperative Cyber Defence Centre of Excellence), berpartisipasi dalam latihan siber maritim berskala besar seperti Locked Shields, Cyber Europe, dan Blue OLEx, yang melibatkan simulasi serangan siber terhadap sistem pelayaran, navigasi kapal, dan pengendalian pelabuhan (CCDCOE, 2022). Latihan ini menjadi sarana evaluasi terhadap keefektifan CDT yang sedang digunakan, sekaligus tempat pengujian teknologi baru dalam skenario realistis. Latihan juga menciptakan pemahaman bersama lintas negara tentang protokol respons cepat, sistem cadangan digital, dan koordinasi komunikasi darurat.

Tanpa SDM yang kompeten, CDT tidak akan bekerja maksimal. Oleh karena itu, Uni Eropa mendukung program pelatihan untuk operator pelabuhan, pelaut, dan teknisi IT di sektor maritim melalui inisiatif seperti EU Cybersecurity Skills

Academy. Pelatihan ini tidak hanya mencakup penggunaan teknologi, tetapi juga prinsip cyber hygiene, prosedur tanggap darurat, dan protokol otentikasi berlapis di kapal dan pelabuhan (Bendiek & Schulze, 2021). Banyak pelatihan juga melibatkan penggunaan simulator siber maritim, di mana peserta dilatih menghadapi berbagai skenario, seperti pengambilalihan sistem navigasi oleh hacker, sabotase perangkat IoT pelabuhan, hingga pencurian data logistik.

Komitmen Uni Eropa terhadap CDT bersifat multidimensi: dari aspek kebijakan, pembiayaan, pengembangan teknologi, pembaruan sistem, hingga pelatihan sumber daya manusia. Pendekatan holistik ini tidak hanya meningkatkan keamanan siber maritim secara teknis, tetapi juga memperkuat ketahanan digital secara institusional. Dengan perkembangan teknologi dan dinamika ancaman yang terus berubah, Uni Eropa tidak berhenti pada pengadopsian CDT, melainkan terus berinvestasi dalam pengembangan lanjutan (next-gen CDT) yang lebih adaptif, otomatis, dan bersifat prediktif. Ini menjadi bukti bahwa keamanan siber maritim bukan hanya kebutuhan teknis, tetapi juga bagian dari strategi geopolitik dan ketahanan kawasan yang lebih luas.