BAB IV
KESIMPULAN DAN SARAN

4.1 Kesimpulan

Penelitian ini membahas mengenai keamanan siber maritim dalam kerangka Uni Eropa melalui implementasi Cyber Diplomacy Toolbox (CDT). Hasil kajian menunjukkan bahwa sektor maritim memiliki posisi strategis dalam perekonomian global, tetapi juga menghadapi kerentanan serius akibat digitalisasi yang masif. Serangan siber seperti NotPetya terhadap Maersk, ransomware di Pelabuhan Rotterdam, dan infiltrasi di Port of Antwerp menegaskan bahwa ancaman siber di sektor maritim dapat menyebabkan dampak ekonomi, sosial, hingga geopolitik yang luas. Kondisi ini menjadi latar belakang Uni Eropa untuk mengadopsi pendekatan diplomasi siber melalui CDT sebagai instrumen kolektif menghadapi ancaman lintas batas.

Pertama, penelitian ini menemukan bahwa Cyber Diplomacy Toolbox terbukti efektif dalam memperkuat kebijakan keamanan siber maritim di Uni Eropa. CDT berfungsi sebagai wadah koordinasi antarnegara anggota dalam merespons serangan, baik melalui nota diplomatik, kecaman publik, hingga penerapan sanksi kolektif. Sebelum CDT hadir pada 2017, respons negara anggota cenderung parsial dan tidak terkoordinasi, sehingga banyak insiden siber tidak tertangani secara memadai. Setelah CDT diberlakukan, Uni Eropa mampu mengadopsi mekanisme atribusi kolektif dan mengeluarkan sanksi resmi, misalnya terhadap aktor negara yang terlibat dalam serangan NotPetya, WannaCry, dan Cloud Hopper pada tahun 2020. Hal ini menandakan adanya perubahan mendasar dalam cara Uni Eropa merespons ancaman siber, dari pendekatan individual menuju koordinasi supranasional.

Kedua, CDT dapat dipahami sebagai sebuah rezim keamanan siber regional dalam kerangka teori rezim Stephen Krasner. Rezim ini terbentuk melalui prinsip, norma, aturan, dan mekanisme pengambilan keputusan yang disepakati bersama. Prinsip utama CDT adalah bahwa serangan siber terhadap satu negara anggota dipandang sebagai ancaman terhadap seluruh Uni Eropa. Norma yang lahir adalah

solidaritas digital, di mana negara anggota wajib bekerja sama menghadapi serangan lintas batas. Aturannya tercermin dalam kerangka sanksi yang diatur dalam Council Decision (CFSP) 2019/797, sedangkan mekanisme pengambilan keputusan dijalankan melalui konsensus di Dewan Uni Eropa. Dengan demikian, CDT tidak hanya bersifat normatif, tetapi juga memiliki dasar hukum yang konkret untuk menegakkan keamanan digital di kawasan. Dalam konteks maritim, rezim ini berfungsi menjaga stabilitas rantai pasok global melalui koordinasi kolektif menghadapi ancaman yang menyasar pelabuhan, kapal, maupun sistem navigasi.

Ketiga, penelitian ini memperlihatkan bahwa CDT berkontribusi besar terhadap harmonisasi kebijakan siber antarnegara anggota Uni Eropa. Sebelum hadirnya CDT, terdapat kesenjangan kemampuan dan prioritas antarnegara, di mana negara maju seperti Jerman atau Belanda relatif lebih siap dibanding negara lain. Kehadiran CDT mendorong penerapan standar bersama melalui regulasi seperti NIS2 Directive, Cybersecurity Act, dan Cyber Resilience Act, yang mengikat seluruh negara anggota untuk memperkuat perlindungan infrastruktur kritis. Harmonisasi ini penting, karena serangan siber di satu negara dapat berdampak pada kawasan secara keseluruhan. Dengan CDT, Uni Eropa berhasil menyatukan negara anggota dalam kerangka kerja diplomasi kolektif yang mempersempit celah keamanan antarnegara.

Keempat, CDT memainkan peran strategis dalam diplomasi global dan hubungan internasional. Uni Eropa tidak hanya menggunakan CDT untuk melindungi kepentingan internal, tetapi juga untuk memengaruhi tata kelola siber global. Melalui forum multilateral seperti PBB, OSCE, maupun kemitraan strategis dengan Amerika Serikat, Jepang, dan India, Uni Eropa memanfaatkan CDT untuk mempromosikan norma internasional bahwa hukum internasional berlaku pula di dunia maya. Hal ini memperkuat posisi Uni Eropa sebagai aktor normatif global, sekaligus menandingi model tata kelola digital yang lebih tertutup seperti yang dipromosikan Tiongkok. Dalam konteks maritim, CDT juga memperkuat kerja sama internasional melalui latihan siber global, kolaborasi dengan IMO, dan pengembangan standar keamanan rantai pasok lintas batas.

Kelima, penelitian ini menegaskan bahwa transformasi kebijakan keamanan

siber maritim Uni Eropa pasca 2017 semakin komprehensif dan multidimensi. Kebijakan teknis seperti NIS2 Directive, Cyber Resilience Act, serta penguatan peran ENISA kini dipadukan dengan instrumen diplomasi kolektif melalui CDT. Integrasi ini membuat Uni Eropa tidak hanya tangguh secara teknis, tetapi juga kuat secara politik dan diplomatik. CDT memungkinkan Uni Eropa memberikan respons yang terukur, proporsional, dan berbasis hukum internasional. Dengan demikian, ancaman siber tidak lagi dipandang sebagai isu teknis semata, melainkan juga sebagai isu politik luar negeri yang menuntut solidaritas regional dan keterlibatan global.

Keenam, penelitian ini menghasilkan sintesis bahwa CDT merupakan instrumen strategis Uni Eropa dalam menghadapi ancaman siber maritim. CDT berfungsi ganda: sebagai mekanisme teknis untuk mendeteksi, merespons, dan memulihkan insiden, serta sebagai instrumen diplomasi kolektif untuk memperkuat solidaritas internal dan memengaruhi norma global. Keberadaannya memperlihatkan bagaimana Uni Eropa mampu mentransformasikan tantangan siber menjadi peluang untuk memperkokoh integrasi regional sekaligus meningkatkan pengaruhnya di tingkat internasional. Bagi sektor maritim, CDT menjadi kunci untuk menjaga stabilitas rantai pasok global, melindungi infrastruktur kritis, dan memperkuat daya saing kawasan di tengah kompetisi geopolitik digital yang semakin tajam.

Secara keseluruhan, kesimpulan penelitian ini menunjukkan bahwa CDT bukan hanya sekadar respons kebijakan teknis, melainkan juga representasi dari visi politik Uni Eropa dalam membangun tata kelola siber yang terbuka, aman, dan berbasis hukum internasional. Dengan demikian, CDT tidak hanya penting bagi Uni Eropa, tetapi juga bagi stabilitas global, khususnya di sektor maritim yang menjadi tulang punggung perdagangan dunia.

4.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, terdapat beberapa saran yang dapat diajukan. Bagi Uni Eropa, penguatan kapasitas koordinasi dan atribusi kolektif dalam kerangka CDT perlu terus dilakukan, mengingat perbedaan kemampuan teknis antarnegara anggota sering kali menjadi hambatan dalam merespons serangan siber secara cepat dan efektif. Investasi yang lebih besar dalam program pelatihan, peningkatan kapasitas intelijen ancaman, serta pembentukan pusat koordinasi regional yang dapat bergerak cepat ketika terjadi insiden akan sangat bermanfaat. Selain itu, Uni Eropa juga perlu memastikan bahwa regulasi seperti NIS2 Directive dan Cyber Resilience Act benar-benar diimplementasikan secara konsisten di seluruh negara anggota. Kesenjangan dalam implementasi regulasi berpotensi menimbulkan titik lemah yang dapat dimanfaatkan oleh aktor jahat untuk melancarkan serangan.

Dalam konteks sektor maritim, perhatian lebih besar perlu diberikan pada penguatan regulasi yang berhubungan langsung dengan keamanan pelabuhan dan rantai pasok global. Program Maritime Cybersecurity Guidelines yang saat ini bersifat rekomendatif dapat ditingkatkan menjadi regulasi yang lebih mengikat, misalnya dengan mewajibkan audit keamanan siber secara berkala di setiap pelabuhan utama. Kerja sama internasional dengan organisasi seperti International Maritime Organization (IMO) dan NATO juga penting diperluas, sehingga standar keamanan maritim dapat berlaku secara global, bukan hanya terbatas di kawasan Eropa. Di samping itu, pemanfaatan teknologi baru seperti kecerdasan buatan, big data analytics, dan quantum-resistant cryptography sebaiknya mulai diprioritaskan agar sistem pertahanan siber maritim memiliki daya tahan yang lebih tinggi terhadap bentuk-bentuk ancaman baru yang semakin kompleks.

Sementara itu, dari sisi akademis, penelitian ini membuka peluang bagi kajian lanjutan mengenai perbandingan antara CDT dengan instrumen diplomasi siber di kawasan lain, seperti Amerika Serikat atau Tiongkok, untuk mengetahui bagaimana pendekatan regional yang berbeda dapat memengaruhi efektivitas tata kelola siber global. Peran aktor non-negara seperti perusahaan pelayaran, operator

pelabuhan, dan penyedia teknologi juga layak mendapat perhatian lebih dalam penelitian ke depan, mengingat mereka adalah bagian integral dari sistem pertahanan maritim yang tidak bisa dilepaskan dari kebijakan regional. Selain itu, perkembangan teknologi berbasis kecerdasan buatan, deepfake, dan serangan hibrida menghadirkan tantangan baru yang juga perlu diteliti lebih mendalam. Dengan memperluas lingkup kajian akademis ke arah tersebut, kontribusi penelitian di bidang keamanan siber maritim dan diplomasi siber akan semakin signifikan, baik secara teoritis maupun praktis.