Pengambilan Kebijakan Kerjasama Estonia-NATO dalam Mendirikan *Cooperative Cyber Defense Center of Excellence* 2007-2008

SKRIPSI

UNIVERSITAS
ISLAM
INDONESIA

Oleh:

ALIF HAFIZ

20323010

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL BUDAYA

UNIVERSITAS ISLAM INDONESIA

2025

Pengambilan Kebijakan Kerjasama Estonia-NATO dalam Mendirikan

***Cooperative Cyber Defense Center of Excellence* 2007-2008**

SKRIPSI

Diajukan kepada Program Studi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia
Untuk memenuhi sebagian dari syarat guna memperoleh

Derajat Sarjana S1 Hubungan Internasional

Oleh:

ALIF HAFIZ

20323010

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL BUDAYA

UNIVERSITAS ISLAM INDONESIA

2025

HALAMAN PENGESAHAN

Pengambilan Kebijakan Kerjasama Estonia-NATO dalam Mendirikan

***Cooperative Cyber Defense Center of Excellence* 2007-2008**

Dipertahankan di depan Dewan Penguji Skripsi Prodi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia

Untuk memenuhi sebagian dari syarat-syarat dalam memperoleh
derajat Sarjana S1 Hubungan Internasional

Pada Tanggal
02 Oktober 2025

Mengesahkan

Program Studi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia
Ketua Program Studi

Karina Utami Dewi, S.I.P, M.A.

	Dewan Penguji	Tanda Tangan
1	Ayu Heryati Naqsabandiyah, S.IP., M.A.	
2	Irawan Jati, S.IP., M.Hum., M.S.S., Ph.D.	
3	Mohamad Rezky Utama, S.IP., M.Si.	

iii

PERNYATAAN INTEGRITAS AKADEMIK

Dengan ini saya menyatakan bahwa skripsi ini adalah hasil karya ilmiah independen saya sendiri, dan bahwa semua materi dari karya orang lain (dalam buku, artikel, esai, disertasi, dan di internet) telah dinyatakan, serta kutipan dan parafrase diindikasikan dengan jelas.

Tidak ada materi selain yang digunakan selain yang termuat. Saya telah membaca dan memahami peraturan dan prosedur universitas terkait plagiarisme.

Memberikan pernyataan yang tidak benar dianggap sebagai pelanggaran integritas akademik.

02 Oktober 2025,

Alif Hafiz

iv

DAFTAR ISI

DAFTAR TABEL

DAFTAR SINGKATAN

CCDCOE : Cooperative Cyber Defence Centre of Excellence

CDU : Cyber Defence Unit

EIC : Estonian Informatics Centre

EGDI : *E-Government Development Index*

EKRE : *Estonian Conservative People's Party*

KAPO : *Kaitsepolitseiamet (Estonian Internal Security Service)*

MFA : *Ministry of Foreign Affairs (Kementerian Luar Negeri Estonia)*

MoD : *Ministry of Defence (Kementerian Pertahanan Estonia)*

NATO : *North Atlantic Treaty Organization*

RIA : *Estonian Information System Authority*

Riigikogu : *Parlemen Estonia*

GAPR : *Governmental as Political Resultant*

DAFTAR GAMBAR

ABSTRAK

Serangan siber besar-besaran pada April–Mei 2007, dikenal sebagai *Estonia Shutdown*, mengganggu infrastruktur digital vital dan menegaskan bahwa serangan siber adalah ancaman politik serta keamanan nasional. Estonia menyadari perlunya menempatkan isu ini dalam kerangka keamanan kolektif NATO. Penelitian ini menjelaskan proses pengambilan kebijakan kerja sama Estonia–NATO dalam pendirian Cooperative Cyber Defense Center of Excellence (CCDCOE) pada 2007–2008 dengan menggunakan metode kualitatif deskriptif dan analisis Governmental Politics Model Graham T. Allison yang menyoroti peran aktor dan lembaga dengan kepentingan berbeda. Pemilihan tema ini didasarkan alasan karena studi kasus Estonia masih jarang dikaji di Indonesia, padahal relevan untuk memahami diplomasi dan pertahanan siber. Analisis penelitian ini menunjukkan bahwa proses pengambilan kebijakan kerja sama pendirian CCDCOE menjadi bukti bagaimana keputusan strategis dalam isu non-konvensional dapat lahir dari dinamika politik pemerintahan, sehingga penelitian ini tidak hanya memberi kontribusi akademis tetapi juga menawarkan pembelajaran praktis bagi negara lain, termasuk Indonesia.

Kata-kata kunci: Estonia, Estonia Shutdown, Governmental Politics Model, NATO, pertahanan siber.

ABSTRACT

TThe large-scale cyberattack in April–May 2007, known as the *Estonia Shutdown*, disrupted vital digital infrastructure and underscored that cyber threats are political and national security challenges rather than merely technical issues. Estonia recognized the necessity of addressing this matter within NATO's collective security framework. This study examines the policy-making process of Estonia–NATO cooperation in establishing the Cooperative Cyber Defense Center of Excellence (CCDCOE) during 2007–2008, employing a qualitative descriptive method and Graham T. Allison's Governmental Politics Model, which highlights the roles of actors and institutions with differing interests. The choice of this topic is justified since Estonia's case remains underexplored in Indonesia, despite its relevance to diplomacy and cyber defense. The analysis shows that the policy-making process behind CCDCOE illustrates how strategic decisions in non-conventional security issues emerge from governmental political dynamics, making this research not only academically valuable but also a practical lesson for other states, including Indonesia.

Keywords: Cyber Defense, Estonia, Estonia Shutdown, Governmental Politics Model, NATO.

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada tahun 2008, Estonia menempati posisi ke-13 dalam United Nations E-Government Development Index (EGDI) sebagai salah satu negara digital paling maju di dunia (United Nations 2008). Capaian ini bukan terjadi secara kebetulan, melainkan merupakan hasil dari kebijakan strategis yang dimulai sejak awal kemerdekaannya dari Uni Soviet pada tahun 1991. Estonia merupakan salah satu negara pertama yang mengadopsi sistem pemerintahan berbasis digital secara menyeluruh, dan memperkenalkan infrastruktur layanan publik daring mulai dari sistem pajak elektronik, e-residency, hingga e-voting. Dengan pendekatan "digital by default", Estonia menjadikan transformasi digital sebagai bagian inti dari identitas nasional dan strategi pembangunan (Frost & Sullivan Institute 2023; Kütt 2020; Deutsche Welle 2023; Government of Estonia 2024; Vinkel and Martens 2004).

Namun, kemajuan pesat di bidang digital justru membuat Estonia menjadi target rentan terhadap bentuk ancaman baru: serangan siber. Puncaknya terjadi pada musim semi tahun 2007, ketika Estonia mengalami serangan siber besar-besaran yang kemudian dikenal sebagai "Estonia Shutdown" (BBC News 2007). Peristiwa Estonia Shutdown pada April–Mei 2007 berakar pada ketegangan politik antara Estonia dan Rusia, terutama setelah keputusan Pemerintah Estonia untuk memindahkan patung peringatan Tentara Soviet, "Bronze Soldier", dari pusat Kota Tallinn ke kompleks pemakaman militer. Kebijakan ini dipandang sebagai

penghinaan oleh komunitas etnis Rusia di Estonia serta pemerintah Rusia, yang sebelumnya menjunjung tinggi simbol peran Soviet dalam Perang Dunia II. Situasi tersebut segera memicu gelombang protes besar, kerusuhan di jalanan, hingga akhirnya bereskalasi ke serangan digital yang melumpuhkan berbagai layanan vital seperti situs pemerintah, media, dan sistem perbankan (BBC 2007; BBC News 2017; Kompas 2022).

Serangan ini memanfaatkan teknik Distributed Denial of Service (DDoS) untuk melumpuhkan infrastruktur digital vital negara, termasuk situs pemerintahan, layanan keuangan, media berita daring, dan sistem komunikasi internal lembaga negara (Ottis 2008; Sarwindaningrum 2024). Serangan DDoS, atau *Distributed Denial of Service*, adalah upaya melumpuhkan sebuah layanan digital dengan membanjiri server target menggunakan permintaan palsu dalam jumlah sangat besar. Permintaan palsu ini misalnya berupa “klik” berulang atau akses palsu ke sebuah halaman situs web, yang jika datang dari jutaan komputer sekaligus akan membuat server kewalahan dan tidak bisa membedakan mana pengguna asli dan mana serangan. Untuk melancarkan serangan, pelaku biasanya menggunakan *botnet*, yaitu jaringan komputer yang sebelumnya sudah diretas dan dipasang program berbahaya tanpa sepengetahuan pemiliknya. Komputer-komputer dalam botnet ini bisa tersebar di berbagai negara, namun semuanya dikendalikan dari jarak jauh untuk menyerang target pada waktu yang sama. Dampaknya, layanan penting seperti situs pemerintah, perbankan, atau media bisa menjadi sangat lambat, bahkan sepenuhnya tidak dapat diakses (BBC 2007; BBC News 2017; Kompas 2022).

Selama lebih dari dua minggu, Estonia menghadapi gelombang serangan terkoordinasi yang berdampak serius terhadap stabilitas nasional dan ekonomi

domestik. Kerusakan akibat serangan ini sangat konkret. Sistem perbankan terganggu hingga transaksi daring tidak dapat dilakukan, mesin ATM tidak berfungsi, serta situs resmi pemerintahan tidak dapat diakses baik oleh masyarakat maupun antar instansi (Gross 2017). Salah satu bank terbesar, Hansabank, harus membekukan seluruh operasional digitalnya selama lebih dari satu jam dan menderita kerugian sekitar US$1 juta hanya dalam kurun waktu singkat (Gross 2017). Di sektor pemerintahan, terganggunya sistem email internal menyebabkan koordinasi antar instansi lumpuh, sementara sistem administrasi sipil seperti pendaftaran dokumen publik dan pelayanan pajak daring juga terhenti (Ottis 2008).

Lebih jauh lagi, Estonia juga menderita kerugian strategis berupa menurunnya reputasi internasional sebagai negara digital. Ketidakmampuan sementara untuk menjaga keberlanjutan sistem elektronik publik menimbulkan pertanyaan terhadap kesiapan infrastruktur keamanan digital negara. Di tingkat domestik, masyarakat mulai meragukan kemampuan pemerintah dalam melindungi data pribadi dan layanan dasar mereka. Sementara di ranah internasional, serangan ini memicu ketegangan diplomatik antara Estonia dan Rusia. Meskipun tidak ada bukti langsung yang dapat mengaitkan pemerintah Rusia sebagai dalang utama serangan, berbagai alamat IP asal Rusia tercatat sebagai sumber lalu lintas berbahaya (BBC News 2007), dan pemerintah Rusia menolak bekerja sama dalam proses investigasi internasional (Ottis 2008).

Menghadapi situasi ini, pemerintah Estonia menyadari bahwa ancaman digital tidak bisa hanya ditangani melalui pendekatan domestik. Presiden Toomas Hendrik Ilves dan Perdana Menteri Andrus Ansip segera meluncurkan strategi diplomasi digital yang bertujuan untuk menjadikan keamanan siber sebagai bagian

dari kerangka keamanan kolektif NATO. Hal ini dilatarbelakangi oleh fakta bahwa serangan terhadap infrastruktur digital sebuah negara anggota sejatinya dapat mengancam stabilitas seluruh aliansi (Laasme 2011).

Upaya lobi dimulai melalui serangkaian pertemuan tingkat tinggi. Pada 14 Juni 2007, Estonia berhasil membawa isu ini ke meja pertemuan Menteri Pertahanan NATO di Brussels. Tak lama setelahnya, pada 25 Juni 2007, Presiden Ilves bertemu langsung dengan Presiden Amerika Serikat George W. Bush di Washington D.C., untuk mempertegas bahwa serangan siber dapat memiliki dampak strategis yang setara dengan serangan militer konvensional (Schmidt 2007). Dalam pertemuan tersebut, Estonia menekankan bahwa jika Pasal 5 NATO menganggap serangan terhadap satu anggota adalah serangan terhadap semua, maka serangan siber harus termasuk dalam definisi ancaman tersebut.

Diplomasi juga dilakukan melalui forum-forum internasional seperti Uni Eropa, OSCE, dan NATO Parliamentary Assembly, dengan tujuan mendorong perubahan paradigma ancaman keamanan dari yang bersifat tradisional ke arah digital (Aday et al. 2019). Estonia terus menekankan bahwa pertahanan digital harus menjadi bagian integral dari sistem keamanan kolektif internasional, dan bahwa pendekatan ini harus dikodifikasikan ke dalam kebijakan NATO secara resmi.

Langkah ini kemudian menghasilkan hasil nyata. Pada 14 Mei 2008, NATO meresmikan pembentukan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di ibu kota Estonia, Tallinn. CCDCOE menjadi pusat unggulan pertama NATO yang dikhususkan untuk pertahanan siber, dengan mandat menyelenggarakan pelatihan, riset, dan simulasi pertahanan digital seperti Locked

Shields (CCDCOE 2020). Pusat ini didukung oleh tujuh negara pemrakarsa, yakni Estonia, Jerman, Italia, Latvia, Lithuania, Slovakia, dan Spanyol. Estonia tidak hanya menjadi tuan rumah, tetapi juga memainkan peran utama dalam inisiatif pendirian lembaga ini, baik secara diplomatik, administratif, maupun teknis (Laasme 2011).

Alasan Penulis mengambil judul ini dikarenakan peristiwa serangan siber yang dialami Estonia pada tahun 2007 yang bernama Estonia Shutdown sendiri merupakan serangan siber skala negara pertama di dunia dan Estonia cukup berhasil dalam pemulihan bencana nirmiliter ini dengan cukup serta menghimpun dukungan internasional untuk strategi mitigasi di masa depan. Serangan Estonia Shutdown 2007 tidak hanya menjadi titik balik dalam kebijakan keamanan nasional Estonia, tetapi juga membawa perubahan dalam strategi keamanan internasional. Estonia berhasil mengubah krisis domestik menjadi momentum diplomasi strategis dengan hasil konkret berupa integrasi keamanan digital ke dalam doktrin kolektif NATO. Hal ini menjadikan Estonia bukan hanya sebagai korban serangan siber pertama berskala nasional di dunia, tetapi juga sebagai pionir global dalam pertahanan digital abad ke-21.

1.2 Rumusan Masalah

Bagaimana proses pengambilan kebijakan Estonia untuk bekerjasama dengan NATO (*North Atlantic Treaty Organization*) dalam mendirikan *Cooperative Cyber Defense Center of Excellence* (CCDCoE)?

1.3 Tujuan Penelitian

Riset ini memiliki tujuan sebagai berikut:

1. Untuk menjelaskan proses pengambilan kebijakan kerjasama Estonia dan NATO dalam mendirikan *CCDCoE* pasca *Estonia Shutdown* 2007-2008.

1.4 Cakupan penelitian

Penelitian ini mencakup kerjasama yang terjalin antara Estonia dan juga NATO dalam sektor keamanan siber dengan disepakatinya kerjasama dalam bidang tersebut pada tanggal 14 Mei 2008 lalu, serta didirikannya kantor pusat keamanan siber NATO bernama *CCDCoE* (*Cooperative Cyber Defense Center of Excellence*) di Estonia pada saat yang sama (CCDCoE 2020). Kerjasama ini sendiri diinisiasi oleh Estonia setelah serangan siber yang cukup masif dirasakan oleh negaranya setahun sebelum kerjasama ini dibuat atau tepatnya pada bulan April 2007 (McGuinness 2017). Dengan begitu maka penelitian ini akan berfokus pada 2 tahun krusial tersebut yang menjadikan kerjasama ini terbentuk untuk menjawab rumusan masalah yang ada yakni pada tahun 2007 sebagai pemicu kerjasama antara Estonia dan NATO untuk urusan keamanan siber serta tahun 2008 dimana kerjasama tersebut terbentuk.

1.5 Tinjauan Pustaka

Kajian mengenai keamanan siber dan kerjasama internasional dalam lingkup NATO telah banyak dilakukan, namun terdapat variasi fokus serta kedalaman analisis. Beberapa studi awal berusaha menjelaskan serangan siber terhadap Estonia pada tahun 2007 sebagai momentum penting yang menandai pergeseran isu siber menjadi agenda utama keamanan kolektif. Salah satu penelitian menguraikan latar belakang serangan tersebut sekaligus menegaskan urgensi pembentukan Cooperative Cyber Defense Center of Excellence (CCDCOE) di

Tallinn. Artikel ini menekankan dimensi historis dan motivasional, dimana Estonia dianggap pionir yang berhasil mengangkat ancaman siber ke forum internasional (Efthymiopoulos 2019). Akan tetapi, keterbatasannya terletak pada absennya pembahasan detail mengenai dinamika internal dalam pemerintahan Estonia, terutama bagaimana aktor-aktor domestik melakukan tawar-menawar kebijakan hingga tercapai kesepakatan dengan NATO.

Literatur lain lebih berfokus pada perkembangan peran NATO dalam menghadapi ancaman multi domain, termasuk siber. Kajian tersebut memperlihatkan bagaimana CCDCOE kemudian diposisikan sebagai bagian integral dari strategi NATO dalam memperkuat interoperabilitas dan kesiapan menghadapi ancaman non-konvensional (Army University Press 2024). Kontribusi kajian ini penting karena memberikan kerangka yang lebih luas untuk memahami posisi CCDCOE sebagai instrumen aliansi, bukan sekadar respons lokal Estonia. Namun, kelemahannya adalah tidak menyentuh secara mendalam faktor politik domestik yang membuat Estonia begitu aktif mendorong NATO. Hubungan antara kepentingan domestik dan strategi kolektif aliansi masih terabaikan.

Selain itu, terdapat pula kajian perbandingan strategi keamanan siber nasional dari sejumlah negara, termasuk Estonia. Studi ini bermanfaat dalam mengungkapkan variasi pendekatan negara terhadap ancaman digital, sekaligus menunjukkan posisi Estonia sebagai pelopor dalam digital governance (ArXiv 2023). Namun, kelemahan mendasarnya adalah fokus yang terbatas pada isi dokumen kebijakan dan strategi formal. Analisis ini tidak mampu menangkap interaksi antar aktor politik maupun dinamika negosiasi domestik dan internasional

yang mendasari kebijakan tersebut, termasuk dalam kaitannya dengan pembentukan CCDCOE.

Secara umum, literatur yang tersedia memberikan pemahaman cukup komprehensif mengenai konteks eksternal, mekanisme NATO, serta latar belakang serangan siber Estonia 2007. Namun, masih terdapat kesenjangan penelitian yang signifikan. Pertama, belum banyak studi yang secara eksplisit membahas proses politik domestik di Estonia, khususnya bagaimana aktor-aktor utama—seperti presiden, perdana menteri, kementerian pertahanan, serta lembaga keamanan—berinteraksi dalam merumuskan kebijakan kerja sama dengan NATO. Kedua, hubungan antara kepentingan nasional Estonia sebagai negara kecil dan dinamika institusional dalam NATO masih jarang diteliti melalui perspektif politik pemerintahan. Ketiga, terdapat kekurangan dalam melihat keterkaitan antara keputusan formal pembentukan CCDCOE dengan proses implementasinya, yang kerap melibatkan negosiasi ulang, resistensi, maupun adaptasi dari aktor-aktor pelaksana.

Gap ini penting karena justru pada titik inilah studi mengenai Estonia menjadi relevan bagi konteks akademik maupun praktis. Bagi akademisi, penelitian yang menyoroti proses politik internal akan memperkaya kajian hubungan internasional yang selama ini cenderung menitikberatkan pada peran organisasi internasional atau kebijakan negara besar. Sementara bagi praktisi, khususnya di Indonesia, pengalaman Estonia dapat menjadi pembelajaran strategis mengenai bagaimana sebuah negara kecil mampu mengubah krisis domestik menjadi peluang untuk memperkuat posisi internasional melalui kerja sama pertahanan siber. Oleh sebab itu, penelitian ini memiliki kontribusi penting dalam mengisi kekosongan

literatur, dengan menggunakan pendekatan *Governmental Politics Model* untuk menelaah pengambilan kebijakan kerjasama pendirian CCDCOE.

1.6 Kerangka Pemikiran

Untuk menjelaskan tentang pemetaan tujuan dari penelitian ini dan menjawab rumusan masalah, peneliti berorientasi kepada model analisis yang cukup ideal dan sudah cukup umum digunakan dalam analisis interaksi sosial yang berujung kepada terbentuknya suatu kebijakan yakni model analisis "*The Governmental Politics*". Model analisis *The Governmental Politics* ini yang akan peneliti ambil didasarkan pada karya Graham T. Allison dengan judul "*Essence of Decision: Explaining the Cuban Missile Crisis*" (1971). Model ini umumnya memberikan sudut pandang bagaimana proses birokrasi berjalan dengan melibatkan beberapa aktor yang mempengaruhinya sehingga suatu kebijakan dapat terbentuk. Di dalam buku ini sendiri, Allison (1971), menjelaskan bahwa meskipun terkadang suatu keputusan memiliki sifat absolut dan diambil oleh satu orang saja, namun bukan berarti suatu keputusan tidak melibatkan berbagai macam faktor serta pengaruh dari pihak eksternal maupun internal. Allison (1971), sendiri meyakini bahwa dalam krisis yang terjadi di Kuba memiliki kompleksitas yang tinggi dalam pengambilan keputusan serta strategi yang mendalam.

Model The *Governmental Politics* ini sendiri berfokus pada politik pemerintahan dengan kaitan erat pemain (*player*) atau tokoh yang memiliki peran dalam kegiatan tawar-menawar internal pemerintahan. Menurut model ini, peristiwa dalam urusan luar negeri tidak dicirikan sebagai pilihan tunggal atau hasil organisasi. Sebaliknya, apa yang terjadi dipahami sebagai hasil dari permainan tawar-menawar di antara para pemain dalam pemerintahan nasional. Dalam

menghadapi masalah yang ditimbulkan oleh rudal Soviet di Kuba, Allison sendiri menyusun teka-teki: Hasil tawar-menawar seperti apa di antara para pemain yang menghasilkan keputusan dan tindakan kritis? Ia memfokuskan perhatian pada konsep-konsep tertentu: para pemain yang kepentingan dan tindakannya mempengaruhi masalah yang dimaksud, faktor-faktor yang membentuk persepsi dan pendirian para pemain, prosedur yang ditetapkan atau "penyaluran aksi" untuk menggabungkan preferensi yang bersaing, dan kinerja para pemain. Analis tersebut menggunakan pola inferensi tertentu: jika pemerintah melakukan suatu tindakan, tindakan tersebut merupakan hasil tawar-menawar di antara para pemain dalam permainan ini. Seorang analis Model III telah "menjelaskan" peristiwa ini ketika ia telah menemukan siapa yang melakukan apa kepada siapa yang menghasilkan tindakan yang dimaksud. Prediksi dibuat dengan mengidentifikasi permainan di mana suatu masalah akan muncul, pemain yang relevan, dan kekuatan relatif serta keterampilan tawar-menawar mereka.

Paradigma *Governmental Politics* yang digunakan dalam penelitian ini bersumber dari pemikiran Graham T. Allison, dengan landasan pada karya Neustadt yang kemudian diperluas sehingga tidak hanya menekankan keputusan presiden, melainkan juga melihat keputusan pemerintah sebagai hasil tawar-menawar politik antar aktor yang relatif independen. Paradigma ini telah banyak diaplikasikan sejak diperkenalkan dalam *Essence of Decision* pada tahun 1971, baik secara eksplisit maupun implisit, sehingga memberikan pijakan konseptual yang kuat bagi analisis kebijakan luar negeri.

I. Basic Unit of Analysis: Governmental Action as Political Resultant.

Paradigma ini berangkat dari asumsi bahwa tindakan pemerintah bukanlah solusi rasional tunggal atas suatu masalah, melainkan *political resultants* yang lahir dari kompromi, konflik, dan tarik-menarik antar pejabat dengan kepentingan serta pengaruh berbeda. Disebut *political* karena keputusan muncul dari proses tawar-menawar melalui saluran formal di antara aktor dalam pemerintahan. Perilaku negara di panggung internasional dipahami sebagai keluaran dari permainan politik internal yang kompleks, simultan, tumpang tindih, dan dipengaruhi hirarki aktor yang ada. Proses ini tidak berjalan acak, tetapi dibatasi oleh saluran formal dan tenggat waktu yang memaksa isu-isu masuk dalam agenda aktor kunci. Dengan demikian, gerak politik suatu negara dapat dijelaskan melalui interaksi antar aktor dengan tujuan, kepentingan, dan kapasitas yang berbeda.

II. Organizing Concepts.

Kerangka ini dijabarkan melalui empat pertanyaan kunci: siapa pemainnya, faktor apa yang membentuk persepsi dan sikap pemain, apa yang menentukan pengaruh pemain, dan bagaimana proses menghasilkan keputusan.

A. Who Plays?

Pemerintah dipandang bukan sebagai aktor tunggal, melainkan kumpulan individu dalam posisi tertentu yang membentuk arena pengambilan keputusan. Pemain bisa berupa pemimpin politik, pejabat birokrasi, staf ahli, hingga aktor ad hoc seperti parlemen, media, atau kelompok kepentingan. Posisi menentukan kewajiban, kewenangan, serta batasan mereka, tetapi kepribadian dan pengalaman individu juga mempengaruhi peran yang dijalankan.

B. What Factors Shape Players` Perceptions?

Setiap pemain menafsirkan isu melalui kacamata organisasinya (*parochial priorities*), tujuan nasional, kepentingan politik domestik, maupun ambisi pribadi. Tarik-menarik antara kepentingan tersebut membentuk sikap masing-masing aktor. Tenggat waktu atau momentum tertentu juga memberi wajah berbeda pada sebuah isu, sehingga menuntut respon yang cepat dari para pemain.

C. What Determines Each Player's Impact on Result?

Kekuatan seorang aktor tidak hanya berasal dari otoritas formal, tetapi juga dari kontrol atas sumber daya, akses informasi, kemampuan persuasi, jaringan politik, dan reputasi keberhasilan sebelumnya. Pemain yang mampu menggabungkan faktor-faktor tersebut memiliki pengaruh lebih besar dalam menentukan arah kebijakan.

D. What is the Game?

Keputusan lahir melalui *action-channels*, yaitu saluran formal yang sudah terstruktur, seperti mekanisme anggaran, prosedur diplomasi, atau koordinasi antar lembaga. Aturan permainan ditetapkan melalui hukum, konstitusi, maupun norma politik yang berlaku. Dengan demikian, kebijakan pemerintah dipandang bukan sebagai keputusan tunggal pemimpin, melainkan sebagai hasil tarik-menarik antar aktor dalam sistem politik. Keputusan formal seringkali hanya menjadi titik antara, karena implementasi masih dipengaruhi oleh aktor-aktor lain yang dapat mempercepat, menunda, atau bahkan mengubah pelaksanaannya.

Dalam konteks penelitian ini, paradigma *Governmental Politics* dipandang relevan untuk menganalisis proses pengambilan kebijakan kerja sama antara Estonia dan NATO dalam pendirian Cooperative Cyber Defense Center of

Excellence (CCDCOE) pada 2007–2008. Serangan siber *Estonia Shutdown* tahun 2007 menunjukkan bahwa keputusan strategis dalam isu non-konvensional tidak lahir dari satu aktor tunggal, melainkan merupakan hasil interaksi politik di antara presiden, perdana menteri, kementerian terkait, lembaga keamanan, serta dukungan mitra internasional. Dinamika tarik-menarik kepentingan, batasan institusional, serta prosedur formal dan informal dalam pemerintahan Estonia mencerminkan logika model ini. Dengan demikian, penggunaan *Governmental Politics Model* memungkinkan penelitian ini untuk mengurai bagaimana keputusan pendirian CCDCOE terbentuk melalui kompromi, negosiasi, dan distribusi kekuasaan antar aktor yang berperan dalam kebijakan pertahanan siber Estonia. Keseluruhan dari faktor ini akan dipakai oleh penulis untuk membantu menganalisis penelitian ini.

1.7 Argumen Sementara

Dalam kasus Estonia, proses pengambilan kebijakan untuk mendirikan Cooperative Cyber Defense Center of Excellence (CCDCOE) pada 2008 tidak terlepas dari dinamika politik internal yang melibatkan presiden, perdana menteri, kementerian pertahanan, lembaga keamanan nasional, hingga dukungan aktor eksternal melalui NATO (Efthymiopoulos 2019).

Argumen sementara penelitian ini adalah bahwa pendirian CCDCOE bukan semata respons teknis terhadap ancaman digital, melainkan keputusan strategis yang lahir dari permainan politik pemerintahan Estonia yang kemudian beresonansi ke tingkat aliansi (Crandall and Allan 2015). Dengan kata lain, peristiwa ini menunjukkan bagaimana negara kecil dapat memanfaatkan krisis untuk memperluas pengaruhnya melalui kerja sama multilateral. Peneliti berpendapat bahwa penggunaan *Governmental Politics Model* relevan karena model ini mampu

menjelaskan mekanisme bagaimana aktor dengan posisi dan kepentingan berbeda dapat menghasilkan kebijakan bersama, meskipun terdapat konflik dan perbedaan pandangan (Allison and Zelikow 1999).

1.8 Metode Penelitian

1.8.1 Jenis Penelitian

Metode dalam penulisan hasil penelitian yang dipilih oleh penulis adalah kualitatif deskriptif, yaitu penelitian yang menekankan pada pemahaman makna, proses, serta dinamika yang melatarbelakangi suatu fenomena politik internasional. Penelitian kualitatif dalam Hubungan Internasional digunakan untuk mengeksplorasi peran aktor, interaksi antar lembaga, serta konstruksi kebijakan yang terjadi dalam konteks tertentu (Creswell 2014). Pendekatan ini sesuai dengan fokus penelitian karena bertujuan menjelaskan proses pengambilan kebijakan kerja sama antara Estonia dan NATO dalam pendirian Cooperative Cyber Defense Center of Excellence (CCDCOE). Dengan kata lain, penelitian ini menekankan pada kedalaman analisis daripada kuantifikasi data, sehingga lebih mampu menangkap dinamika politik pemerintahan yang melibatkan negosiasi antar aktor (Yin 2018).

1.8.2 Subjek dan Objek Penelitian

Subjek penelitian ini mencakup Estonia sebagai negara yang paling banyak mendapatkan dampak serta memberikan dampak dari serangan siber yang terjadi pada tahun 2007 di negaranya. Untuk objek penelitian sendiri adalah proses pengambilan kebijakan pemerintah Estonia terkait kerjasama di bidang siber dengan NATO serta pendirian *CCDCoE* di Estonia pada tahun 2008.

1.8.3 Metode Pengumpulan Data

Untuk pengumpulan data penelitian ini, penulis mengambil sumber data sekunder yang berorientasi kepada riset literatur. Sumber data yang diambil berfokus kepada data yang memiliki kredibilitas melalui buku, artikel, jurnal, laporan resmi pemerintahan serta media nasional maupun internasional yang relevan.

1.8.4 Proses Penelitian

Dalam proses pengumpulan data yang akan dianalisa nantinya, penulis memiliki tiga tahapan pengumpulan data yang terdiri dari koleksi, seleksi, dan eliminasi. Pada tahapan koleksi, penulis akan mengambil sebanyak mungkin sumber data yang memiliki relevansi dengan topik yang akan dibahas. Selanjutnya tahapan seleksi yakni penulis akan memisahkan data berdasarkan tingkat kredibilitas serta relevansinya terhadap topik penelitian. Terakhir penulis akan melakukan eliminasi terhadap data yang dianggap tidak bisa dipakai dalam menjawab rumusan masalah yang telah penulis ajukan.

1.9 Sistematika Pembahasan

Demi memudahkan penulis dalam mendalami isi pembahasan serta menjelaskan pembahasan dari topik penelitian ini, maka sistematika penulisan akan disusun kedalam empat bab yang sistematis sebagai berikut:

Bab I yang berisi pendahuluan yang di dalamnya berisi latar belakang dari topik penelitian yang dibahas, rumusan masalah, tujuan penelitian, cakupan penelitian, tinjauan pustaka, kerangka pemikiran, argumen sementara, metode penelitian, dan sistematika pembahasan.

Bab II yang berisi tentang Peristiwa *Estonia Shutdown* 2007 dengan cakupan motif serangan, dampak serangan, skala serangan dan implikasinya, serta respons pemerintah terhadap serangan.

Bab III berisi tentang analisis proses pengambilan kebijakan kerjasama Estonia dengan NATO dalam pendirian *CCDCoE* 2007-2008 menggunakan model analisis “The Governmental Politics” Graham T. Allison.

Bab IV memuat kesimpulan yang didapatkan dari poin-poin pokok pembahasan yang termuat dalam bab-bab sebelumnya pada penelitian ini, serta rekomendasi untuk penelitian di kemudian hari.

BAB 2

LANGKAH DE-ESKALASI SERTA PEMULIHAN KONDISI SOSIAL DAN POLITIK ESTONIA PASCA PERISTIWA ESTONIA SHUTDOWN

Bab ini membahas langkah-langkah de-eskalasi dan pemulihan kondisi sosial serta politik Estonia pasca peristiwa Estonia Shutdown 2007, sebuah serangan siber besar yang mengguncang sektor digital, pemerintahan, dan masyarakat Estonia. Fokus pembahasan mencakup dampak serangan terhadap keamanan nasional, respons pemerintah dalam memperkuat sistem digital, serta strategi diplomasi Estonia untuk menghimpun dukungan negara-negara NATO dalam pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), yang menjadi tonggak penting dalam penguatan pertahanan siber internasional.

2.1. Dampak Peristiwa Estonia Shutdown 2007 terhadap Keamanan Nasional Estonia

Pada musim semi di tahun 2007, tepatnya bulan April hingga Mei di Estonia telah terjadi serangan siber pertama dan salah satu yang terbesar di dunia. Serangan ini membuktikan bagaimana suatu bentuk ketegangan antara negara yang bermusuhan dapat saling menjatuhkan dengan mengeksploitasi potensi terbesar dari negara lawannya. Tepat setelah pemerintah Estonia memutuskan untuk memindahkan monumen bersejarah bernama “Bronze Soldier Monument” atau Monumen Prajurit Perunggu dari pusat kota Tallinn ke pemakaman militer di pinggir kota tersebut ternyata berhasil dimanfaatkan oleh pihak oposisi Estonia untuk menyulut konflik di negara tersebut (McGuinness 2017; Ottis 2008).

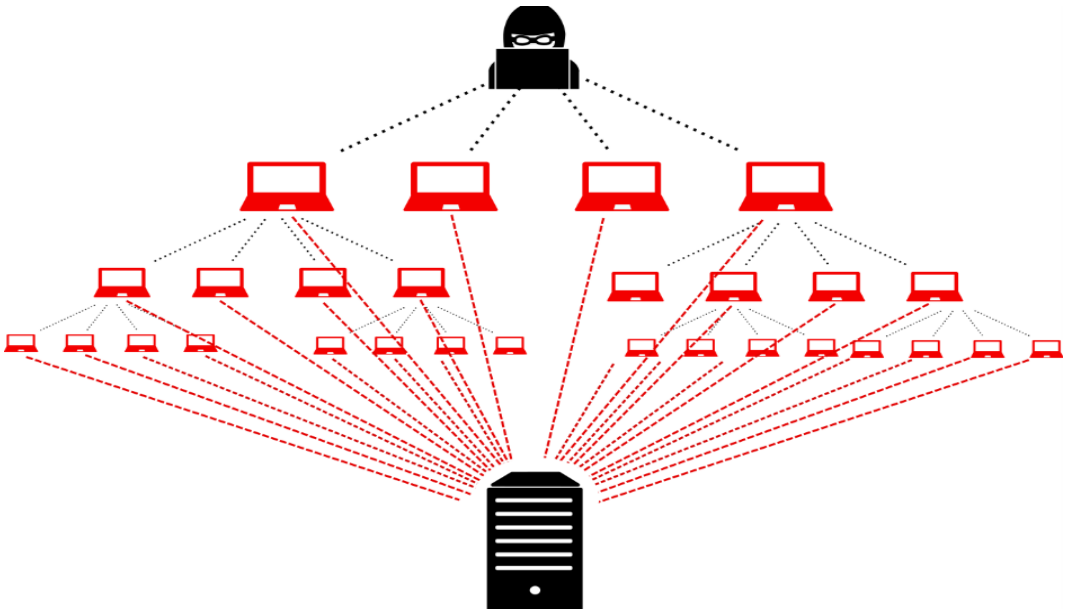
Tentunya Etnis Rusia yang tinggal di Estonia yang memandang bahwa monumen ini sangat bersejarah langsung memberikan reaksi sehingga berbagai media berbahasa Rusia serta masyarakat Estonia yang beretnis Rusia langsung bereaksi dengan kemarahan (Sarwindaningrum 2024). “Monumen Tentara Perunggu” atau “Bronze Soldier Monument” sendiri bukan hanya sekedar monumen peringatan biasa, namun membawa pesan sejarah yang cukup penting bagi Estonia dan juga Rusia. Bagi Rusia sendiri, monumen tersebut merupakan simbol kemenangan Soviet atas Nazi Jerman sekaligus bentuk penghormatan terhadap tentara Soviet yang gugur dalam Perang Dunia II, sehingga pemindahan monumen itu dianggap sebagai penghinaan terhadap sejarah dan pengorbanan mereka (BBC 2007; BBC News 2017). Dengan hadirnya isu penghancuran monumen tersebut oleh pemerintah Estonia, kemarahan publik semakin memuncak. Etnis Rusia di Estonia tentunya langsung melakukan protes dengan turun ke jalan dan tidak berhenti disitu, kerusuhan pun melanda Estonia pada tanggal 26 April 2007 dengan total 156 orang terluka, 1 orang dilaporkan tewas, serta 1000 orang berhasil ditahan oleh otoritas keamanan Estonia (Ottis 2008; Sarwindaningrum 2024).

Tidak berhenti disitu, kekerasan dan kerusuhan juga tertuju pada kedutaan besar Estonia di Moskow serta diperparah dengan sanksi ekonomi secara tidak langsung oleh Rusia (McGuinness 2017). Puncak serangan yang dipercaya sebagai salah satu pukulan telak yang dialami oleh Estonia terjadi tepat sehari setelah kerusuhan tersebut yakni pada tanggal 27 April 2007 dimana sektor digital Estonia mendapatkan serangan siber dengan teknik Distributed Denial-of-Service (DDoS) (Ottis 2008; Sarwindaningrum 2024).

2.1.1 Skala Serangan Siber dan Implikasinya

Serangan siber di Estonia pada April 2007 yang sekaligus menjadi bentuk serangan siber pertama ini dapat dikatakan sebagai serangan telak meskipun tidak melibatkan sektor militer. Hal ini dikarenakan Estonia sendiri cukup banyak bergantung pada sektor digital. Teknik serangan DDoS menjadi pilihan dari pihak oposisi untuk menjatuhkan sistem digital baik itu sistem informasi, komunikasi, perbankan, maupun pemerintahan Estonia. Lebih detail, yang mendapatkan serangan yakni website kepresidenan, parlemen, perbankan, serta kantor berita Estonia (Crandall & Allan 2015).

Gambar 1. Ilustrasi Serangan DDoS



Sumber: Gudang SSL (2019).

Pada tanggal 28 April 2007 atau sehari setelah serangan siber tersebut pecah, akhirnya diketahui bahwa serangan tersebut bukanlah bentuk serangan siber asal seperti yang sering terjadi di dunia digital sebelumnya. Serangan ini dipercaya merupakan serangan terstruktur yang bahkan tingkat serangannya berada di level

nasional (Kash 2008). Teknik DDoS ini sendiri merupakan salah satu bentuk serangan digital atau siber dengan cara memenuhi server dengan lalu lintas internet yang berlebih sehingga kinerja sistem menurun karena kewalahan dan akhirnya akses terhadap server terhenti yang menyebabkan efek domino.

Serangan DDoS, atau *Distributed Denial of Service*, adalah upaya melumpuhkan sebuah layanan digital dengan membanjiri server target menggunakan permintaan palsu dalam jumlah sangat besar. Permintaan palsu ini misalnya berupa “klik” berulang atau akses palsu ke sebuah halaman situs web, yang jika datang dari jutaan komputer sekaligus akan membuat server kewalahan dan tidak bisa membedakan mana pengguna asli dan mana serangan. Untuk melancarkan serangan, pelaku biasanya menggunakan *botnet*, yaitu jaringan komputer yang sebelumnya sudah diretas dan dipasang program berbahaya tanpa sepengetahuan pemiliknya. Komputer-komputer dalam botnet ini bisa tersebar di berbagai negara, namun semuanya dikendalikan dari jarak jauh untuk menyerang target pada waktu yang sama. Dampaknya, layanan penting seperti situs pemerintah, perbankan, atau media bisa menjadi sangat lambat, bahkan sepenuhnya tidak dapat diakses (BBC 2007; BBC News 2017; Kompas 2022). Efek domino yang terjadi dikarenakan serangan ini diantaranya adalah berhentinya transaksi perbankan ditandai dengan sistem anjungan tunai mandiri (ATM) yang tidak dapat digunakan untuk mengambil uang serta perbankan daring yang juga tidak dapat digunakan, terhentinya komunikasi antar anggota pemerintahan Estonia melalui surat elektronik, dan yang terakhir adalah aktivitas media berita daring yang tidak berjalan dikarenakan para wartawan tidak bisa mengunggah berita pada portal daring mereka (Sarwindaningrum 2024).

Dikarenakan serangan siber pertama, tentunya Estonia tidak memiliki acuan atau contoh mitigasi bencana digital ini. Meskipun begitu, Estonia sendiri merupakan negara yang dapat dikatakan cukup maju dalam urusan sektor digital. Adopsi besar-besaran terhadap sistem digital sedari awal kemerdekaan Estonia memberikan negara tersebut fleksibilitas dalam menghadapi ancaman dunia digital. Hal ini dapat dilihat dari sistem perbankan yang ada di negara tersebut yang tentunya memiliki sistem mitigasi bencana-nya sendiri. Sebut saja salah satu bank terbesar milik Estonia yakni Hansabank yang turut menjadi sasaran serangan siber kala itu. Menghadapi serangan siber yang diterima pihaknya, Hansabank melaksanakan langkah mitigasi seperti membekukan sistem operasional mereka. Hal ini berdampak kepada berhentinya sistem operasional Hansabank selama lebih dari 1 jam. Keputusan membekukan sistem operasional demi mitigasi bencana serangan digital ini membuat Estonia Hansabank kehilangan US$1 juta menurut laporan bank tersebut. Meskipun begitu, langkah ini dianggap sebagai langkah paling rasional dalam menghadapi arus lalu lintas data yang cukup masif melanda sistem digital Estonia. Sebesar 4 juta data per detik dilaporkan menyerang berbagai sektor di Estonia termasuk perbankan yang tentunya langsung mematikan kinerja sistem digital di sana (Gross 2017).

Selain sektor finansial, sektor pemerintahan juga tentunya terkena imbas dari serangan siber ini. Situs-situs website krusial milik parlemen Estonia juga terkena arus serangan lalu lintas data ini. Baik sistem komunikasi internal maupun sistem pelayanan publik yang dimiliki pemerintah turut terdampak serangan ini. Pada sektor internal sendiri, sistem komunikasi yang terganggu di Estonia membuat koordinasi antar instansi di Estonia kala itu mengalami hambatan. Untuk sektor

eksternal sendiri yakni tidak bisa diaksesnya situs resmi pemerintah baik dari pihak pemerintah maupun masyarakat Estonia sehingga memperparah kondisi kala itu. Hal ini kian memburuk dengan berhentinya proses administratif digital seperti perputaran dan pengajuan dokumen sipil serta pelayanan publik digital (Ottis 2008).

Selanjutnya pemerintah Estonia juga menghadapi kerugian lain yang sifatnya strategis dan juga risiko reputasi negaranya. Hal ini muncul dikarenakan dengan terekseposnya peristiwa ini kepada masyarakat dunia turut memberikan dampak menurunnya pandangan internasional terhadap sistem keamanan digital Estonia. Hal ini juga berlaku pada lingkungan domestik yang memunculkan spekulasi kekhawatiran masyarakat Estonia terhadap kemampuan pemerintahannya dalam melindungi sistem vital mencakup infrastruktur nasional dan juga data masyarakatnya (Aday et al. 2019).

Tidak berhenti di situ, kerugian Estonia berlanjut pada sektor internasional di mana berkat peristiwa ini, ketegangan politik dan diplomatik yang dihadapi Estonia terhadap Rusia dapat dikatakan semakin memanas. Meskipun pemerintah Estonia tidak secara eksplisit menuduh aktor dari pihak Rusia sebagai dalang di balik serangan ini, namun serangan digital yang terjadi tepat setelah munculnya isu pemindahan Patung Prajurit Perunggu memberikan sinyal yang cukup dapat dibaca serta bagaimana pada akhirnya kementerian luar negeri merilis beberapa alamat IP (Internet Protocol) yang berasal dari Rusia (BBC News 2007). Hal ini semakin diperparah dengan pernyataan pihak Rusia yang menolak kerja sama dalam penyelidikan digital internasional terhadap isu ini sehingga kesempatan penyelesaian bilateral antara dua negara ini menjadi terputus. Kejadian ini tentunya

memperburuk hubungan diplomatik Estonia dengan Rusia yang pada kala itu dapat dikatakan sudah sangat sensitif (Ottis 2008).

Demi mengatasi mimpi buruk yang dialami negaranya, tentu Estonia pada akhirnya meminta bantuan yang bersifat darurat kepada NATO dan juga penyedia layanan internet internasional untuk memulihkan layanan digital serta memperkuat keamanan sibernya (Schmidt 2007). Tentu hal tersebut menelan biaya yang cukup besar. Ditambah lagi dengan langkah reaksi pemerintah Estonia terhadap kasus ini dengan memperkuat sistem digital negaranya serta pembentukan CDU (Cyber Defense Unit) dan juga peningkatan infrastruktur digitalnya membuat Estonia mau tidak mau kehilangan dana yang cukup besar (Aday et al. 2019).

2.1.2 Proses Estonia dalam Menghimpun Dukungan Pendirian CCDCOE dengan negara-negara NATO Pasca Peristiwa Estonia Shutdown

Setelah serangan siber besar pada April–Mei 2007, Estonia menyadari bahwa menghadapi ancaman digital secara unilateral tidaklah cukup. Pemerintah Estonia segera mengambil langkah proaktif dengan melobi aliansi keamanan kolektif seperti NATO untuk memperluas ranah pertahanan mereka ke domain siber. Presiden Toomas Hendrik Ilves dan Perdana Menteri Andrus Ansip menjadi tokoh kunci dalam upaya diplomasi ini, memanfaatkan momentum krisis sebagai alat untuk mendorong reformasi sistem keamanan internasional (Tikk, Kaska, & Vihul 2010; Rõigas 2014).

Langkah awal lobi dimulai dengan membawa isu keamanan siber ke forum NATO. Dalam pertemuan Menteri Pertahanan NATO di Brussels pada 14 Juni 2007, Estonia menyampaikan bahwa serangan siber dapat berdampak sistemik pada stabilitas negara anggota dan karenanya perlu menjadi bagian dari kerangka kerja

Pasal 5 NATO (Ottis 2008; Tikk et al. 2010). Estonia juga menyuarakan perlunya solidaritas digital dalam berbagai forum seperti NATO Parliamentary Assembly dan Uni Eropa (Rõigas 2014).

Sebagai bagian dari strategi lobi, pada 25 Juni 2007 Presiden Ilves bertemu langsung dengan Presiden AS George W. Bush di Washington D.C. Dalam pertemuan tersebut, Ilves menyampaikan kekhawatiran tentang potensi ancaman digital terhadap stabilitas demokrasi dan infrastruktur negara anggota NATO. Diskusi ini membantu meningkatkan kesadaran Amerika Serikat terhadap urgensi pengembangan kebijakan pertahanan siber NATO (Schmidt 2007).

Puncak keberhasilan diplomasi Estonia terlihat pada awal 2008, ketika proposal pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) secara resmi disetujui. CCDCOE diresmikan pada 14 Mei 2008 di Tallinn dengan dukungan dari tujuh negara pendiri, yakni Estonia, Jerman, Italia, Latvia, Lithuania, Slovakia, dan Spanyol (Rõigas 2014; NATO CCDCOE 2022). Estonia tidak hanya menjadi tuan rumah, tetapi juga memberikan kontribusi besar dalam penyusunan visi strategis, infrastruktur teknis, dan kerangka hukum CCDCOE.

Dengan pendekatan diplomatik yang agresif dan koordinasi lintas sektor yang kuat, Estonia berhasil mengubah krisis domestik menjadi pijakan untuk reformasi keamanan global. Respons NATO yang diwujudkan melalui pendirian CCDCOE menjadi bukti konkret keberhasilan lobi Estonia dalam menjadikan keamanan siber sebagai komponen penting dalam arsitektur pertahanan kolektif internasional (Tikk et al. 2010; Gross 2017).

BAB 3

ANALISIS KEBIJAKAN PEMERINTAH ESTONIA DALAM MENDIRIKAN NATO CCDCoE PASCA PERISTIWA ESTONIA SHUTDOWN 2007

Dalam bab ini, penulis menggunakan kerangka analisis *Governmental Politics Model* dari Graham T. Allison yang menekankan bahwa kebijakan luar negeri merupakan hasil tawar-menawar politik di antara aktor-aktor dalam pemerintahan, bukan keputusan tunggal yang rasional. Model ini relevan untuk menganalisis pembentukan kerja sama Estonia–NATO dalam pendirian *Cooperative Cyber Defense Center of Excellence* (CCDCOE) di Tallinn pada 2008. Analisis difokuskan pada dua elemen utama, yaitu *Basic Unit of Analysis: Governmental Action as Political Resultant* serta *Organizing Concepts*, yang mencakup identifikasi faktor, faktor pembentuk persepsi, pengaruh relatif antara aktor, dan dinamika permainan politik yang membentuk keputusan.

Proses pembentukan kebijakan pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Tallinn pada tahun 2008 merupakan salah satu studi kasus paling menarik dalam melihat bagaimana mekanisme *Basic Unit of Analysis: Governmental as Political Resultant (GAPR)* bekerja dalam sistem politik Estonia. Setelah serangan siber masif pada April–Mei 2007, Estonia tidak hanya menghadapi kerentanan teknis, tetapi juga harus menjawab pertanyaan strategis mengenai arah kebijakan keamanan nasionalnya. Dalam konteks ini, keputusan untuk mendorong pembentukan CCDCOE tidak lahir dari satu otoritas tunggal, melainkan merupakan hasil tarik-menarik kepentingan, negosiasi, serta

dinamika politik di antara berbagai lembaga pemerintahan, sektor swasta, hingga elemen masyarakat sipil (Ottis 2008; Tikk et al. 2010).

3.1. Political Resultant

Dalam kerangka *Governmental Politics Model* (Model III) yang diperkenalkan oleh Graham T. Allison, analisis kebijakan luar negeri tidak dilihat sebagai hasil keputusan seorang aktor rasional tunggal, melainkan sebagai *political resultant*, yakni hasil dari tarik-menarik kepentingan, kompromi, konflik, dan negosiasi antar aktor yang memiliki otoritas serta pengaruh berbeda dalam pemerintahan (Allison & Zelikow 1999, 255). Dengan demikian, suatu keputusan negara pada level internasional tidak pernah sepenuhnya lahir dari logika rasional institusional, tetapi merupakan hasil interaksi dinamis di dalam lingkaran politik domestik yang kompleks.

Penerapan konsep *governmental action as political resultant* menjadi penting untuk memahami kebijakan Estonia pasca-serangan siber 2007. Serangan yang dikenal sebagai *Estonia Shutdown* bukan sekadar gangguan teknis terhadap infrastruktur digital, tetapi telah menantang otoritas negara secara menyeluruh. Pemerintah Estonia menghadapi tekanan signifikan untuk segera merespons, tidak hanya demi stabilitas internal, melainkan juga untuk menjaga kredibilitasnya di mata komunitas internasional, khususnya NATO dan Uni Eropa (Czosseck, Ottis, & Taliharm 2011). Dalam kondisi seperti ini, keputusan untuk mendorong pembentukan *Cooperative Cyber Defense Center of Excellence* (CCDCOE) di Tallinn tidak bisa dipahami hanya sebagai reaksi logis terhadap ancaman keamanan, melainkan sebagai hasil tarik-menarik antaraktor dalam lingkaran

politik pemerintahan Estonia, interaksi dengan sekutu NATO, serta pertimbangan domestik dan internasional yang saling bersinggungan.

Sebagaimana dicontohkan Allison ketika membahas *Cuban Missile Crisis*, keputusan penting negara lahir dari interaksi aktor yang berbeda kepentingan dan posisinya (Allison & Zelikow 1999, 307). Analogi ini dapat diterapkan untuk kasus Estonia: keputusan mendorong NATO agar membangun pusat pertahanan siber bukanlah keputusan tunggal Presiden Toomas Hendrik Ilves, melainkan hasil interaksi antara Kementerian Pertahanan Estonia, pejabat keamanan nasional, militer, parlemen, serta jaringan diplomatik di NATO. Setiap aktor memiliki persepsi dan kalkulasi politik berbeda, yang pada akhirnya dipadukan dalam proses tawar-menawar hingga menghasilkan satu bentuk kebijakan yang dapat dijalankan.

Lebih jauh, pendekatan *political resultant* menjelaskan bahwa hasil kebijakan Estonia tidak semata-mata mengikuti pola *cause-effect* linear, melainkan sebuah agregasi dari berbagai keputusan kecil yang diambil aktor berbeda. Misalnya, Kementerian Pertahanan Estonia mendorong kerja sama siber karena melihatnya sebagai bagian dari modernisasi pertahanan; sementara Kementerian Luar Negeri melihatnya sebagai kesempatan memperkuat posisi diplomatik Estonia di NATO. Di sisi lain, pejabat parlemen tertentu menekankan pentingnya biaya dan manfaat domestik yang akan diterima Estonia dari kehadiran lembaga internasional seperti CCDCOE di ibu kota negara (Jackson 2013). Maka, keputusan final tidak lahir dari satu preferensi dominan, melainkan dari kombinasi serta keseimbangan kepentingan yang berhasil dinegosiasikan.

Dalam praktiknya, proses kebijakan ini memperlihatkan sifat khas dari *governmental politics*: adanya “pulling and hauling” antar aktor yang ingin

memajukan perspektifnya. Misalnya, dalam merespons serangan 2007, sebagian aktor menekankan urgensi membangun mekanisme pertahanan siber yang bersifat domestik, seperti *Cyber Defence Unit* (CDU). Namun, kelompok lain mendorong agar isu ini dinaikkan ke tingkat NATO dengan argumen bahwa serangan siber bersifat lintas batas dan tidak mungkin ditangani secara unilateral. Tarik-menarik inilah yang akhirnya menghasilkan kompromi berupa penguatan unit domestik sekaligus pendirian CCDCOE sebagai inisiatif kolektif NATO dengan basis di Tallinn (Pamment et al. 2019).

Pendekatan ini menegaskan bahwa kebijakan CCDCOE tidak semata dilihat sebagai keberhasilan strategi luar negeri Estonia, tetapi juga sebagai hasil akumulasi dari fragmentasi birokrasi, koordinasi lintas kementerian, hingga keberhasilan diplomasi Estonia di NATO. Konsep *political resultant* dengan demikian memungkinkan peneliti untuk melihat dimensi kebijakan secara lebih kaya, karena menyoroti bahwa apa yang tampak sebagai keputusan strategis tunggal sesungguhnya adalah hasil kompromi dan konflik yang terjadi di balik layar.

Di sisi lain, penerapan model ini juga menunjukkan keterbatasan pendekatan rasional tradisional dalam menjelaskan kasus Estonia. Jika hanya menggunakan model aktor rasional, keputusan mendirikan CCDCOE akan dipandang sebagai pilihan logis untuk memperkuat keamanan nasional pasca-serangan siber. Namun, kenyataannya, proses ini penuh dengan negosiasi politik, termasuk dalam hal mendapatkan dukungan dari negara anggota NATO lain yang bersedia menjadi sponsor pendirian CCDCOE seperti Jerman, Italia, Spanyol, dan Slovakia (Cheskin & Kasekamp 2019). Tanpa adanya keberhasilan Estonia

mengarahkan dinamika internal NATO, CCDCOE mungkin tidak akan terealisasi secepat itu.

Dengan demikian, analisis *governmental action as political resultant* memperlihatkan bahwa kebijakan Estonia–NATO terkait CCDCOE tidak bisa dilepaskan dari proses politik domestik Estonia, interaksi birokrasi, serta diplomasi multilateral. Hasil kebijakan yang muncul adalah *resultant* dari tarik-menarik kepentingan yang berbeda, namun justru dalam kompleksitas inilah strategi pertahanan siber Estonia menemukan bentuknya. Puncaknya pada tahun 2008 tepatnya pada tanggal 14 Mei, akhirnya Estonia berhasil menginisiasi pendirian NATO *CCDCoE* di Tallinn atau ibu kota negaranya bersama dengan 6 negara anggota NATO lainnya yakni Jerman, Italia, Latvia, Lithuania, Republik Slovakia dan Spanyol yang merupakan *Political Resultant* (CCDCoE 2024).

3.2. Organizing Concept

Dalam konteks pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Estonia, keputusan pemerintah merupakan hasil interaksi multi-aktor dengan kepentingan berbeda. Organizing concepts ini memungkinkan analisis terhadap empat aspek: siapa aktor yang terlibat, faktor yang membentuk persepsi dan preferensi, faktor yang menentukan pengaruh aktor, dan bagaimana interaksi serta strategi mereka menghasilkan keputusan.

Setiap aktor memiliki kepentingan spesifik yang mempengaruhi peran dan strategi mereka. Misalnya, Presiden Estonia dan pejabat senior menekankan legitimasi internasional dan keamanan nasional, Kementerian Luar Negeri fokus pada hubungan diplomatik dan citra Estonia di NATO, sedangkan badan keamanan

menekankan kesiapan teknis, kapasitas intelijen, dan kemampuan melindungi infrastruktur kritis (Czosseck, Ottis, and Taliharm 2011; Schmidt 2007). Aktor eksternal, termasuk diplomat NATO, penasihat teknis, dan negara sponsor, juga mempengaruhi jalannya proses negosiasi melalui masukan teknis dan politik, serta dukungan sumber daya.

Data serangan siber Estonia 2007 menunjukkan urgensi tindakan pemerintah dan menambah tekanan terhadap bargaining antaraktor. Serangan ini melumpuhkan layanan publik, sektor keuangan, dan institusi negara, sehingga menciptakan kondisi di mana pemerintah Estonia harus segera mengembangkan kemampuan cyber defence yang berkelanjutan (Pamment et al. 2019; Efthymiopoulos 2019; Gross 2017). Kejadian ini tidak hanya mempengaruhi prioritas aktor internal, tetapi juga memicu dukungan internasional, mendorong kolaborasi dengan NATO, dan menegaskan pentingnya pendirian CCDCOE sebagai pusat riset dan latihan siber (Rõigas 2014; NATO CCDCOE 2022).

Organizing concepts menekankan bahwa persepsi dan preferensi aktor dipengaruhi oleh sejumlah faktor. Pertama, prioritas parokial dan persepsi posisi, di mana setiap aktor melihat isu melalui mandat dan orientasi organisasi mereka. Kementerian Luar Negeri menekankan citra Estonia di panggung internasional, badan keamanan fokus pada kesiapan teknis, sedangkan Presiden mempertimbangkan legitimasi politik dan reputasi nasional (Herzog 2011; Sarwidaningrum 2024). Kedua, tujuan dan kepentingan, baik nasional maupun organisasi, mempengaruhi preferensi. Aktor dapat menekankan program yang memperkuat reputasi atau posisi tawar mereka di internal maupun eksternal pemerintahan (Crandall and Allan 2015; Kaska, Beckvard, and Minárik 2019).

Ketiga, tenggat waktu dan bentuk masalah memainkan peran. Tekanan dari serangan siber sebelumnya, deadline NATO, atau konferensi internasional memaksa aktor memprioritaskan isu tertentu, sehingga persepsi masalah menjadi lebih konkret dan strategis (Ottis 2008; Studia Securitatis 2023).

Selanjutnya, pengaruh aktor terhadap keputusan tidak semata ditentukan oleh posisi formal. Faktor seperti kontrol atas sumber daya dan informasi, kemampuan persuasif, hubungan personal, serta strategi investasi kekuasaan menentukan seberapa besar aktor dapat mempengaruhi hasil akhir. Pejabat dengan akses ke intelijen siber atau data teknis memiliki leverage tinggi dalam proses negosiasi. Aktor yang dihormati dan memiliki hubungan baik dengan pihak lain dapat memobilisasi dukungan lebih efektif. Selain itu, aktor memilih isu yang mereka yakini dapat dimenangkan untuk meningkatkan reputasi atau efektivitas mereka (Neustadt 1960; Pamment et al. 2019).

Permainan politik terjadi melalui integrasi posisi, pengaruh, dan langkah aktor melalui berbagai action-channel. Rutin dan subchannel digunakan untuk memproses proposal teknis dan diplomatik, misalnya jalur Kementerian Luar Negeri → Presiden → Staf NATO. Konflik dan kompromi terjadi ketika aktor menarik dan menekan untuk mencapai hasil yang mendekati kepentingan mereka, sambil menyesuaikan kompromi antar-pemain (Czosseck and Tikk 2011; Laasme 2011). Selain itu, implementasi keputusan formal melibatkan interaksi berkelanjutan, dari pemilihan lokasi, penunjukan staf, hingga pengembangan kerangka kerja kerja sama, sehingga dinamika multi-aktor tetap berlangsung sepanjang proses (Kalvet 2007; Schmidt 2013).

Dengan memahami organizing concepts ini, analisis pendirian NATO CCDCOE menjadi lebih rinci. Keputusan akhir bukan sekadar produk Presiden atau Kementerian Luar Negeri, tetapi hasil interaksi kompleks antara aktor formal, staf pendukung, aktor ad hoc, dan pemain eksternal, yang dipandu oleh preferensi, persepsi, pengaruh, dan strategi masing-masing.

3.2.1. Who Plays?

Dalam pembentukan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Estonia pada 2007–2008, peran masing-masing aktor tidak dapat dilepaskan dari konteks serangan siber Estonia Shutdown 2007 yang memicu urgensi kebijakan keamanan siber nasional dan internasional. Ottis (2008) dan Gross (2017) menekankan bahwa pengalaman Estonia menghadapi serangan siber tersebut menjadi pemicu utama bagi pemerintah untuk memperkuat kapasitas pertahanan digital dan mendorong kerja sama internasional. Pemerintah Estonia sendiri bukan entitas tunggal, melainkan kumpulan individu yang menempati posisi strategis, dengan kepentingan, prioritas, dan pengalaman berbeda yang mempengaruhi pengambilan keputusan (Allison 1971; Allison & Zelikow 1999).

- Pemain Utama Domestik

Rapat-rapat darurat yang digelar pasca serangan 2007 memperlihatkan bahwa otoritas pengambilan keputusan tersebar di antara banyak institusi negara. Kantor Presiden, Kantor Perdana Menteri, Kementerian Pertahanan, Kementerian Luar Negeri, Kementerian Ekonomi dan Komunikasi, Estonian Informatics Centre (EIC), hingga lembaga keamanan dalam negeri (Kaitsepolitseiamet/KAPO) semuanya hadir dengan mandat, keprihatinan, dan usulan yang berbeda (Ottis 2008; Tikk et al. 2010). Presiden Toomas Hendrik Ilves, misalnya, memandang krisis ini

terutama sebagai isu diplomasi dan reputasi internasional. Ia menekankan bahwa tanpa dukungan sekutu NATO, Estonia akan kesulitan mengembalikan kredibilitas digitalnya. Sebaliknya, Perdana Menteri Andrus Ansip lebih fokus pada aspek stabilisasi domestik, yakni bagaimana memastikan sistem keuangan, komunikasi pemerintahan, dan pelayanan publik dapat kembali berjalan untuk mencegah ketidakpercayaan masyarakat. Distribusi kekuasaan ini menimbulkan konsekuensi penting: tidak ada aktor tunggal yang dapat memaksakan kehendak secara sepihak, dan setiap lembaga harus meyakinkan pihak lain melalui argumentasi dan negosiasi. Inilah yang membuat proses pembentukan CCDCOE menjadi cerminan nyata *Basic Unit of Analysis: Governmental as Political Resultant,* dimana keputusan akhir merupakan hasil interaksi seluruh lembaga (Allison 1999).

Presiden Toomas Hendrik Ilves memimpin diplomasi internasional untuk mendorong pendirian CCDCOE di Tallinn. Dalam berbagai pertemuan dengan negara sponsor NATO, Ilves menekankan bahwa Estonia, sebagai salah satu negara digital paling maju di Eropa, membutuhkan pusat pelatihan dan riset keamanan siber untuk melindungi infrastruktur kritis dan mendukung aliansi NATO secara kolektif (McGuinness 2017; Deutsche Welle 2023). Ilves pernah menyatakan dalam forum NATO, “Pengalaman Estonia dalam serangan siber tahun 2007 menekankan perlunya pusat internasional khusus untuk mempelajari, melatih, dan mengkoordinasikan pertahanan siber” (Ilves, dikutip dalam Schmidt 2013). Peran Ilves di arena internasional juga memastikan bahwa negara-negara Baltik lain, seperti Latvia dan Lithuania, mendukung lokasi Tallinn sebagai markas CCDCOE.

Perdana Menteri Andrus Ansip memfokuskan perannya pada politik domestik dan koordinasi internal. Ansip memimpin rapat kabinet darurat untuk

merespons serangan 2007, melibatkan semua kementerian yang relevan: Pertahanan, Luar Negeri, Keuangan, Dalam Negeri, dan Komunikasi. Dalam rapat pertama pasca-serangan, Ansip menekankan urgensi kerja sama internasional: "Kita harus bertindak tegas. Infrastruktur digital kita telah menjadi target, dan hanya melalui koordinasi NATO kita dapat memastikan keamanan di masa depan" (Ansip, dikutip dalam Gross 2017).

Ansip menghadapi tekanan dari oposisi, khususnya EKRE dan partai Sosial-Demokrat, yang mempertanyakan biaya dan relevansi strategis pendirian CCDCOE. Seorang anggota EKRE menyatakan, "Mengapa Estonia harus menanggung beban finansial dan politik untuk menjadi tuan rumah pusat NATO? Prioritas kita seharusnya fokus pada ketahanan siber domestik terlebih dahulu" (EKRE, dikutip dalam Sarwindaningrum 2024). Ansip merespons bahwa partisipasi Estonia dalam CCDCOE justru memperkuat pertahanan nasional dengan memanfaatkan jaringan NATO dan akses ke keahlian internasional (Ansip, dikutip dalam Kaska, Beckvard, dan Minárik 2019).

Menteri Pertahanan dan Menteri Luar Negeri memainkan peran teknis dan diplomatis. Menteri Pertahanan menilai kesiapan militer dan infrastruktur untuk mendukung CCDCOE, sedangkan Menteri Luar Negeri memimpin negosiasi dengan NATO terkait alokasi dana, dukungan teknis, dan validasi lokasi (Ottis 2008; Czosseck, Ottis, dan Taliharm 2011).

1. Pemain legislatif dan oposisi

Riigikogu (Parlemen Estonia) menjadi arena penting bagi legitimasi kebijakan. Selain EKRE, partai-partai oposisi lain mengekspresikan kekhawatiran tentang kemungkinan intervensi asing dan biaya tambahan. Dalam rapat parlemen

bulan Desember 2007, seorang anggota Sosial-Demokrat menyatakan, “Menjadi tuan rumah pusat siber NATO dapat menempatkan Estonia dalam konflik siber internasional. Pemerintah harus memberikan penilaian risiko yang terperinci” (Sosial-Demokrat, dikutip dalam Sarwindaningrum 2024).

Meskipun mayoritas aktor politik mendukung pembentukan CCDCOE, terdapat pula suara skeptis dari sebagian kalangan parlemen Estonia. Estonian Centre Party (Keskerakond), yang secara tradisional menjadi representasi politik komunitas berbahasa Rusia, khawatir pendirian pusat NATO akan memperbesar ketergantungan Estonia pada agenda keamanan Barat sekaligus menimbulkan sensitivitas baru dalam hubungan dengan Rusia, mengingat basis politik mereka yang kuat di kalangan etnis Rusia (Ehin and Berg 2009). Selain itu, kalangan nasionalis konservatif yang kemudian berkembang menjadi *Estonian Conservative People’s Party* (EKRE) juga mengekspresikan keraguan. Mereka menilai penempatan lembaga multinasional di Tallinn berpotensi mengurangi kedaulatan digital nasional karena kebijakan pertahanan siber lebih banyak diatur oleh NATO ketimbang oleh pemerintah Estonia sendiri (Kasekamp 2010). Pandangan skeptis ini menunjukkan adanya perdebatan internal yang relevan dengan konsep GAPR, dimana keputusan kebijakan luar negeri Estonia merupakan hasil interaksi dan kompromi antar lembaga, bukan produk satu otoritas tunggal.

Pihak pro, termasuk partai Reformasi yang mendukung Ansip, menekankan bahwa pendirian CCDCOE adalah peluang strategis untuk menempatkan Estonia sebagai pusat keamanan siber internasional, meningkatkan reputasi, dan memberikan perlindungan infrastruktur digital yang kritis. Argumen ini akhirnya

menyeimbangkan tekanan oposisi dan mempermudah persetujuan di parlemen (Kaljurand 2023, 123).

2. Pemain NATO dan internasional

Negara-negara sponsor CCDCOE, yaitu Amerika Serikat, Jerman, Spanyol, Latvia, dan Lithuania, memberikan dukungan politik, teknis, dan finansial (Studia Securitatis 2023; Army University Press 2024). Mereka menilai Estonia sebagai lokasi strategis karena pengalaman langsungnya menghadapi serangan siber dan kapasitas digital nasional yang tinggi. Prancis dan Italia sempat ragu karena pertimbangan biaya dan prioritas nasional masing-masing, sehingga tidak termasuk blok pemrakarsa awal (Schmidt 2007; NATO 2008).

Koalisi negara Baltik—Estonia, Latvia, Lithuania—digunakan sebagai tekanan diplomatik untuk mempercepat persetujuan NATO. Estonia, melalui Presiden Ilves dan PM Ansip, mengkoordinasikan posisi Baltik agar pesan yang disampaikan kepada NATO lebih kuat dan konsisten, menekankan urgensi keamanan kolektif dan pengalaman Estonia sebagai contoh nyata kerentanan digital (Crandall dan Allan 2015; Kaska, Beckvard, dan Minárik 2019).

3. Pemain akademisi

Selain di level pemerintahan, sejumlah aktor domestik juga memperlihatkan sikap ragu. Sebagian akademisi dari Universitas Tartu dan Tallinn University menekankan pentingnya mengintegrasikan riset ilmiah ke dalam kebijakan, namun memperingatkan risiko menjadikan CCDCOE sekadar “etalase diplomasi” tanpa substansi penelitian yang memadai (Rõigas 2014).

Tallinn University dan University of Tartu memainkan peran sebagai penyedia data teknis dan penelitian. Mereka menganalisis serangan Estonia 2007,

menilai metode serangan hybrid, dan memberikan rekomendasi mitigasi risiko siber (Pamment et al. 2019; Efthymiopoulos 2019). Akademisi ini menghadirkan argumen berbasis bukti yang digunakan pemerintah untuk membenarkan urgensi CCDCOE kepada NATO dan legislatif domestik, sehingga narasi kebijakan tidak hanya bersifat politis tetapi juga ilmiah.

4. Pemain sektor swasta

Beberapa bank besar yang mengalami kerugian signifikan akibat serangan siber 2007 sempat menyoroti bahwa alih-alih membangun struktur multinasional baru, pemerintah seharusnya memprioritaskan investasi pada sistem keamanan siber domestik, firewall finansial, serta redundansi jaringan perbankan (Gross 2017). Sektor swasta, terutama Hansa Bank, memberikan input terkait dampak operasional serangan siber dan kebutuhan mitigasi infrastruktur kritis (Blank 2008; Gross 2017). Perusahaan teknologi lokal lainnya terlibat sebagai konsultan teknis, menjembatani gap antara kebutuhan praktis dan kebijakan formal, memastikan CCDCOE dapat mendukung sektor swasta maupun publik.

5. Pemain media

Media nasional dan internasional memainkan peran penting dalam membentuk opini publik dan memberi tekanan pada pemerintah. Media dan kantor berita besar di Estonia memainkan peran kritis, mempertanyakan apakah NATO benar-benar akan menjadikan keamanan siber sebagai prioritas, atau hanya memandang CCDCOE sebagai proyek simbolis (Aday, Farrell, and Lynch 2019). Media Estonia seperti Postimees, media internasional seperti BBC, serta media opini di kawasan Baltik menyoroti serangan siber dan menekankan kebutuhan pusat keamanan siber (BBC News 2007; Sarwindaningrum 2024). Liputan ini

memperkuat posisi Ilves di forum internasional, sekaligus menekan oposisi domestik agar kebijakan diterima publik.

6. Kronologi interaksi pemain

Pada bulan April 2007, Serangan siber besar pertama terhadap situs pemerintah dan perbankan memaksa Ansip mengadakan rapat darurat dengan Menteri Pertahanan, Menteri Luar Negeri, dan badan keamanan siber untuk menilai dampak, kebutuhan mitigasi, dan opsi kerja sama internasional.

+ April 2007 – Serangan siber besar pertama terhadap situs pemerintah dan perbankan memaksa Ansip mengadakan rapat darurat dengan Menteri Pertahanan, Menteri Luar Negeri, dan badan keamanan siber untuk menilai dampak, kebutuhan mitigasi, dan opsi kerja sama internasional (Ottis 2008; Gross 2017).
+ Mei–Juni 2007 – Presiden Ilves melakukan perjalanan diplomatik ke NATO dan negara sponsor untuk mempromosikan pendirian CCDCOE (Schmidt 2007; NATO 2008).
+ Juli–Agustus 2007 – Koordinasi internal Ansip dengan kabinet untuk menyusun draft proposal pendirian CCDCOE, termasuk estimasi biaya, dampak politik, dan persetujuan legislatif (Sarwindaningrum 2024).
+ September 2007 – Rapat parlemen dengan oposisi (EKRE dan Sosial-Demokrat) menekankan risiko dan biaya. Pemerintah menegaskan manfaat strategis CCDCOE, termasuk perlindungan infrastruktur digital nasional (Sosial-Demokrat, dikutip dalam Sarwindaningrum 2024).
+ Oktober–Desember 2007 – Negosiasi akhir dengan NATO; koalisi Baltik menekan negara sponsor untuk menyetujui Tallinn sebagai lokasi

CCDCOE. Ilves dan Ansip mengatur briefing, menyediakan laporan akademik, dan menggalang dukungan sektor swasta (Crandall & Allan 2015; Kaska, Beckvard, & Minárik 2019).

+ Januari 2008 – Persetujuan resmi NATO terhadap pendirian CCDCOE di Tallinn, dilanjutkan dengan perencanaan implementasi teknis dan administratif (NATO 2008; Rõigas 2014).

Interaksi antar pemain mencerminkan dinamika bargaining, lobbying, dan persuasi, dimana presiden memimpin diplomasi eksternal, PM Ansip menyeimbangkan kepentingan domestik, oposisi memaksa klarifikasi, akademisi menyediakan dasar teknis, sektor swasta memberikan perspektif praktis, dan media menekan opini publik (Pamment et al. 2019; Sarwindaningrum 2024).

3.2.2. What Factors Shape Players' Perceptions?

Persepsi, preferensi, dan sikap para pemain terhadap pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Estonia pada 2007–2008 sangat dipengaruhi oleh berbagai faktor struktural, institusional, politik, dan personal. Dalam konteks ini, pemain utama termasuk Presiden Toomas Hendrik Ilves, Perdana Menteri Andrus Ansip, anggota parlemen dari partai pro-pemerintah maupun oposisi seperti EKRE, pejabat Kementerian Pertahanan dan Kementerian Luar Negeri, pejabat NATO dari negara sponsor (Amerika Serikat, Jerman, Latvia, Lithuania, Spanyol), serta akademisi dari Tallinn University dan pihak swasta seperti Hansa Bank. Interaksi mereka dalam rapat darurat, diskusi bilateral dengan NATO, dan konsultasi domestik membentuk persepsi tentang urgensi, risiko, dan manfaat pendirian CCDCOE (Kaljurand 2023, 238).

1. Posisi dan prioritas organisasi

Para pejabat pemerintah Estonia memiliki persepsi yang dipengaruhi oleh posisi formal mereka. Misalnya, Kementerian Pertahanan menekankan keamanan nasional dan kemampuan pertahanan siber sebagai prioritas utama, sementara Kementerian Luar Negeri fokus pada legitimasi internasional dan dukungan aliansi NATO. Presiden Ilves, yang lebih aktif di kancah internasional, menekankan pentingnya Estonia sebagai negara digital maju dan pionir dalam keamanan siber, sebagaimana tercermin dalam pidatonya di Brussels dan Washington (Hommik 2007; Schmidt 2007). Sebaliknya, Perdana Menteri Ansip lebih berfokus pada koordinasi internal pemerintahan dan penyusunan anggaran untuk memastikan implementasi pendirian CCDCOE berjalan lancar. Posisi-posisi ini membentuk cara masing-masing pemain menilai isu dan menetapkan prioritas mereka dalam rapat koordinasi darurat dan pertemuan bilateral dengan NATO (Ottis 2008; Laasme 2011).

2. Kepentingan nasional dan pribadi

Kepentingan pemain tidak hanya bersifat institusional tetapi juga personal. Pemain senior di Kementerian Pertahanan dan Kementerian Luar Negeri memiliki tanggung jawab untuk melindungi reputasi institusi mereka sekaligus menjaga kredibilitas personal di mata presiden dan publik. Dalam hal ini, Presiden Ilves memanfaatkan kredibilitas internasionalnya untuk menekan negara-negara sponsor NATO agar mendukung Estonia, sementara Ansip berfokus pada stabilitas domestik dan konsensus politik internal (Czosseck, Ottis, & Taliharm 2011). Di tingkat parlemen, anggota dari partai oposisi EKRE dan beberapa anggota sosial-demokrat mengekspresikan kekhawatiran tentang biaya pendirian CCDCOE dan risiko keterlibatan Estonia dalam konflik siber internasional, sehingga

mempengaruhi sikap dan strategi komunikasi pemerintah. EKRE menekankan, “Estonia harus berhati-hati agar tidak terlalu mengikat diri dengan NATO tanpa konsensus penuh di dalam negeri” (Sarwindaningrum 2024).

3. Deadline, krisis, dan tekanan eksternal

Serangan siber 2007 yang menimpa Estonia menjadi krisis yang mempercepat proses pengambilan keputusan. Dalam rapat darurat yang diadakan di Tallinn pada Mei 2007, para pemain utama harus menilai dampak langsung terhadap infrastruktur kritis, termasuk perbankan (Hansa Bank), media, dan pemerintahan elektronik. Rapat ini melibatkan Presiden Ilves, PM Ansip, Menteri Pertahanan, Menteri Luar Negeri, dan pejabat keamanan siber nasional, dengan kehadiran terbatas dari perwakilan NATO melalui telekonferensi. Tekanan dari masyarakat dan media nasional untuk menemukan solusi segera memperkuat urgensi pendirian CCDCOE (BBC News 2007; Gross 2017). Deadline yang muncul akibat krisis ini membuat pemain lebih pragmatis, memaksa mereka menyesuaikan persepsi dan mengambil keputusan cepat meskipun ada perbedaan prioritas internal.

4. Persepsi risiko dan manfaat

Setiap pemain menilai risiko dan manfaat berdasarkan pengalaman, akses informasi, dan posisi dalam jaringan pengambilan keputusan. Kementerian Pertahanan melihat pendirian CCDCOE sebagai peluang memperkuat pertahanan kolektif NATO dan meningkatkan kemampuan Estonia menghadapi ancaman siber. Sementara itu, Kementerian Luar Negeri menekankan manfaat diplomatik, termasuk peningkatan profil internasional dan peluang untuk memimpin inisiatif keamanan siber global (Crandall & Allan 2015). Di sisi lain, pihak oposisi

menyoroti potensi eksposur Estonia terhadap konflik siber lebih lanjut dan keterlibatan dalam politik aliansi yang lebih kompleks. Perbedaan ini menciptakan "multi-face" issue, di mana satu masalah dapat dilihat sebagai peluang strategis, risiko politik, atau beban anggaran tergantung perspektif masing-masing pemain (Allison & Zelikow 1999).

5. Interaksi antar pemain dan negosiasi

Persepsi juga dibentuk melalui interaksi antar pemain. Rapat koordinasi internal antara PM Ansip, Presiden Ilves, dan menteri terkait melibatkan diskusi intensif tentang strategi komunikasi dengan NATO, negosiasi mengenai kontribusi Estonia, serta koordinasi untuk meredam oposisi parlemen (Ottis 2008; Laasme 2011). Pada level NATO, perwakilan AS, Jerman, Latvia, Lithuania, dan Spanyol berdiskusi mengenai kontribusi dana dan personel. Prancis dan Italia awalnya menunjukkan keraguan karena mempertanyakan relevansi dan beban administratif CCDCOE, namun tekanan dari koalisi negara Baltik dan diplomasi Ilves mendorong mereka menyetujui konsep pendirian (Schmidt 2007; NATO 2008). Interaksi ini menekankan bahwa persepsi pemain terbentuk bukan hanya oleh kepentingan internal tetapi juga oleh dinamika bargaining dan persuasi antar pihak.

6. Pengaruh akademisi dan pihak swasta

Akademisi Tallinn University berperan sebagai konsultan teknis dan penyedia analisis risiko siber. Mereka menyuplai data empiris mengenai serangan 2007, rekomendasi mitigasi, dan blueprint operasional awal CCDCOE (Rõigas 2014). Pihak swasta, seperti Hansa Bank, berkontribusi dalam evaluasi risiko terhadap infrastruktur kritis ekonomi dan memberikan masukan terkait protokol keamanan yang diperlukan. Informasi ini mempengaruhi persepsi menteri dan

pembuat keputusan, membantu mereka menyeimbangkan risiko keamanan dengan kepentingan nasional dan domestik (Ottis 2008; Kalvet 2007).

7. Media dan opini publik

Media domestik Estonia dan internasional memainkan peran signifikan dalam membentuk persepsi dan menekan pengambilan keputusan pemerintah terkait pendirian CCDCOE. Media domestik, seperti *Postimees*, melaporkan dampak langsung serangan siber terhadap infrastruktur pemerintahan dan perbankan, menyoroti kerentanan Estonia, serta menekankan urgensi respons strategis. Sementara itu, media internasional, seperti BBC dan Kompas, memberitakan serangan Estonia 2007 secara luas, menempatkan Estonia dalam sorotan global dan menunjukkan perlunya kerja sama multinasional dalam keamanan siber (BBC News 2007; Sarwindaningrum 2024).

Presiden Ilves menggunakan liputan media ini untuk memperkuat pesan diplomatiknya di forum internasional, sedangkan Perdana Menteri Andrus Ansip memanfaatkan opini publik domestik sebagai alat lobbying internal. Ansip secara aktif mendorong publik Estonia memahami urgensi pendirian CCDCOE, menekankan bahwa keterlibatan negara dalam pusat siber NATO bukan hanya meningkatkan keamanan nasional, tetapi juga meningkatkan reputasi Estonia sebagai pionir digital di Eropa. Strategi ini bertujuan agar opini publik memberikan tekanan tambahan kepada anggota parlemen, khususnya pihak oposisi, agar proposal pendirian CCDCOE dapat disetujui lebih cepat (Gross 2017; McGuinness 2017).

Dengan demikian, opini publik Estonia dan liputan media domestik maupun internasional membentuk lingkungan eksternal yang mempengaruhi persepsi

legislatif. Tekanan ini menambah legitimasi keputusan pemerintah, mempermudah proses negosiasi internal, dan memperkuat posisi Estonia dalam persuasi kepada negara-negara sponsor NATO serta dalam diplomasi multilateral.

Faktor-faktor yang membentuk persepsi para pemain Estonia dalam pendirian CCDCOE bersifat multidimensi seperti posisi formal, kepentingan nasional dan pribadi, tekanan krisis, interaksi antar pemain, input akademisi dan swasta, serta opini publik dan media. Kombinasi faktor ini menghasilkan pandangan yang berbeda-beda terhadap urgensi, risiko, dan strategi pendirian CCDCOE. Misalnya, persepsi Ilves lebih bersifat strategis-internasional, Ansip lebih domestik-administratif, sementara oposisi seperti EKRE menyoroti risiko politik dan anggaran. Interaksi antar pemain, negosiasi dengan NATO, serta masukan akademik, swasta, dan opini publik membentuk kerangka persepsi yang akhirnya menghasilkan konsensus untuk melanjutkan pendirian CCDCOE, meskipun tidak semua pihak sepenuhnya puas dengan kompromi yang dicapai (Sarwidaningrum 2023, 245).

3.2.3. What Determines Each Player's Impact on Result?

Dalam konteks pembentukan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Estonia pada 2007–2008, dampak atau pengaruh masing-masing pemain terhadap hasil kebijakan tidak hanya ditentukan oleh jabatan formal, tetapi juga oleh kombinasi dari kewenangan institusional, keahlian, jaringan relasi, reputasi personal, dan kemampuan negosiasi. Pemahaman faktor-faktor ini penting untuk menjelaskan bagaimana keputusan untuk mendirikan CCDCOE dapat dicapai meskipun terdapat perbedaan prioritas, kepentingan, dan sikap di antara aktor domestik dan internasional (Allison 1971, 21).

1. Kekuatan posisi formal (positional power)

Pengaruh formal berasal dari kewenangan yang melekat pada posisi jabatan masing-masing pemain. Presiden Toomas Hendrik Ilves memiliki kapasitas signifikan untuk mempengaruhi keputusan melalui legitimasi simbolik dan jaringan internasional. Perannya sebagai pemimpin Estonia dalam forum internasional, termasuk pertemuan NATO dan kunjungan bilateral ke Washington dan Brussels, memberikan bobot diplomatik yang tinggi (Hommik 2007; Schmidt 2007). Ilves dapat membentuk persepsi negara sponsor mengenai kepentingan strategis Estonia, mendorong dukungan pro-CCDCOE, dan menekan pihak yang ragu seperti Prancis dan Italia melalui argumen diplomatik berbasis keamanan siber dan profil Estonia sebagai negara digital terdepan.

Sementara itu, Perdana Menteri Andrus Ansip memiliki pengaruh yang lebih domestik-administratif. Sebagai kepala eksekutif, Ansip mengontrol koordinasi antar kementerian, penyusunan anggaran, dan proses legislasi internal. Posisi ini membuatnya mampu mengarahkan implementasi keputusan, menyeimbangkan kepentingan menteri, dan menjaga konsensus internal meskipun ada tekanan dari oposisi seperti EKRE. Contohnya, dalam rapat darurat Mei 2007, Ansip memimpin diskusi tentang alokasi dana keamanan siber dan prosedur koordinasi antar kementerian, yang menjadi dasar mekanisme operasional CCDCOE (Sarwindaningrum 2024).

2. Keahlian dan kontrol informasi (expertise and informational power)

Selain posisi formal, pengaruh pemain ditentukan oleh tingkat keahlian dan akses terhadap informasi yang relevan. Kementerian Pertahanan dan akademisi Tallinn University menyediakan data teknis tentang serangan siber 2007, analisis

risiko, serta rekomendasi mitigasi, yang menjadi landasan argumen pemerintah pro-CCDCOE. Informasi ini memperkuat posisi Ansip dan Ilves dalam negosiasi dengan NATO karena mereka dapat menyajikan bukti konkret terkait ancaman dan kesiapan Estonia (Ottis 2008; Crandall & Allan 2015).

Negara sponsor NATO—AS, Jerman, Latvia, Lithuania, dan Spanyol—memiliki kontrol informasi terkait standar keamanan siber NATO, prosedur pendanaan, dan pengalaman operasional di negara lain. Pemain Estonia yang mampu mengakses dan memahami informasi ini secara efektif, seperti Ilves dan pejabat Kementerian Luar Negeri, mampu memanfaatkan data untuk meyakinkan pihak yang awalnya ragu, yaitu Prancis dan Italia, tentang manfaat pendirian CCDCOE (Laasme 2011, 58).

3. Jaringan relasi dan koalisi (network and coalition building)

Pengaruh pemain juga dipengaruhi oleh kemampuan membangun koalisi dan jaringan relasi. Estonia membentuk koalisi dengan negara Baltik lainnya (Latvia dan Lithuania) untuk menekan keraguan dari negara sponsor yang lain. Koalisi ini memperkuat posisi bargaining Estonia, menegaskan kepentingan kolektif kawasan Baltik, dan memberikan legitimasi tambahan dalam forum NATO (Schmidt 2007; NATO 2008).

Untuk bagian domestik, Ansip dan Ilves perlu membangun dukungan mayoritas di parlemen, menghadapi oposisi seperti EKRE dan beberapa anggota sosial-demokrat yang khawatir tentang biaya dan risiko keterlibatan internasional. Diskusi dan kompromi dilakukan untuk memastikan dukungan legislatif, misalnya dengan menekankan manfaat diplomatik dan keamanan jangka panjang CCDCOE,

yang pada akhirnya meningkatkan pengaruh kedua pemimpin Estonia terhadap hasil keputusan (Laasme 2011, 60).

4. Reputasi dan kredibilitas personal (reputation and credibility)

Reputasi personal dan kredibilitas juga mempengaruhi dampak pemain. Presiden Ilves memiliki reputasi internasional sebagai advokat keamanan siber dan pionir digitalisasi, yang membuatnya lebih dipercaya oleh negara sponsor NATO dibanding pejabat lain. Ansip, dengan reputasi efektif dalam manajemen internal, mampu memastikan implementasi keputusan berjalan lancar. Sebaliknya, anggota oposisi seperti EKRE memiliki pengaruh terbatas terhadap keputusan akhir karena posisi mereka lebih lemah dalam jaringan internasional, meski tetap mempengaruhi persepsi publik dan menuntut kompromi anggaran (Sarwindaningrum 2024).

5. Kemampuan negosiasi dan persuasi (bargaining skill and persuasion)

Kemampuan negosiasi memainkan peran kunci dalam menentukan pengaruh. Dalam pertemuan bilateral dengan NATO, Ilves memanfaatkan diplomasi persuasif dengan menekankan pengalaman Estonia menghadapi serangan siber 2007 dan kesiapan institusi lokal. Strategi ini berhasil membalik keraguan awal Prancis dan Italia menjadi persetujuan konseptual, sementara koalisi Baltik menambah tekanan kolektif. Ansip menggunakan pendekatan administratif dan politis dalam rapat internal untuk menyeimbangkan kepentingan menteri dan mengurangi resistensi oposisi, dengan mengalokasikan anggaran dan membagi tanggung jawab kementerian secara jelas (Ottis 2008, 5).

6. Faktor institusional dan aturan permainan (institutional and rule-based factors)

Pengaruh pemain tidak dapat dilepaskan dari aturan institusional. Posisi formal menentukan siapa yang memiliki kewenangan untuk memutuskan, siapa yang harus diajak berkonsultasi, dan jalur legal untuk mengimplementasikan kebijakan (Tikk, Kaska, dan Vihul 2010, 15). Misalnya, pengaruh Ilves dalam diplomasi internasional dibatasi oleh kapasitas legislatif untuk menyetujui alokasi anggaran CCDCOE, sehingga koordinasi dengan Ansip dan parlemen menjadi vital (Ottis 2008, 7). Rangkaian rapat darurat, konsultasi NATO, dan negosiasi internal ini mengikuti "aturan permainan" yang ditentukan oleh undang-undang nasional, prosedur NATO, dan norma diplomatik, yang pada gilirannya mempengaruhi seberapa besar setiap pemain dapat memaksimalkan pengaruhnya (Laasme 2011, 61).

7. Interaksi antar pemain dan dampaknya terhadap hasil

Interaksi antar pemain, baik domestik maupun internasional, menentukan dampak nyata terhadap keputusan (Ottis 2008, 9). Misalnya, rapat darurat Mei 2007 di Tallinn melibatkan Ansip, Ilves, Menteri Pertahanan, Menteri Luar Negeri, dan pejabat keamanan siber (Laasme 2011, 60). Perbedaan perspektif—Ilves fokus pada diplomasi internasional, Ansip pada koordinasi internal—diharmonisasikan melalui negosiasi (Tikk, Kaska, dan Vihul 2010, 18). Oposisi parlementer, walau memiliki kekuatan terbatas, memaksa pemerintah untuk memberikan justifikasi publik dan transparansi anggaran (Sarwidaningrum 2023, 245). Di forum NATO, interaksi dengan negara sponsor memungkinkan Estonia mengamankan komitmen dana, personel, dan legitimasi formal untuk pendirian CCDCOE (Ottis 2008, 12).

Dampak masing-masing pemain terhadap hasil kebijakan pendirian CCDCOE ditentukan oleh kombinasi posisi formal, keahlian dan kontrol informasi,

kemampuan membangun jaringan dan koalisi, reputasi personal, keterampilan negosiasi, serta aturan institusional (Tikk, Kaska, dan Vihul 2010, 20). Pemain yang mampu menggabungkan faktor-faktor ini secara efektif—seperti Ilves dan Ansip—memiliki pengaruh lebih besar terhadap keputusan akhir, sedangkan pemain dengan posisi lebih lemah, seperti anggota oposisi, tetap berperan dalam menyeimbangkan dan memvalidasi keputusan melalui tekanan legislatif dan opini publik (Sarwidaningrum 2023, 247). Dinamika ini menunjukkan bahwa pengaruh pemain tidak bersifat linear; melainkan hasil interaksi kompleks antara struktur formal dan kemampuan personal, yang secara kolektif membentuk jalannya pengambilan keputusan Estonia–NATO CCDCOE 2007–2008 (Laasme 2011, 61).

3.2.4. What is the Game?

Permainan politik yang menghasilkan pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Estonia pada 2007–2008 merupakan rangkaian kompleks interaksi antara aktor domestik, regional, dan internasional, dengan kepentingan, strategi, dan tekanan yang saling bertumpuk. Konsep "game" dalam kerangka Governmental Politics Model (Allison 1971; Allison & Zelikow 1999) menekankan bahwa keputusan akhir bukan sekadar hasil konsensus tunggal atau preferensi formal pemerintah, melainkan produk interaksi, negosiasi, kompromi, dan tekanan struktural yang dijalankan oleh pemain dengan kekuasaan dan agenda berbeda.

Menghadapi interaksi dalam proses pengambilan kebijakan, dinamika rapat berjalan melalui proses negosiasi yang intens. Kementerian Pertahanan mengajukan argumen bahwa CCDCOE tidak akan mengurangi kedaulatan Estonia, justru memperkuat kapasitas nasional melalui akses ke teknologi, pelatihan, dan

jaringan intelijen siber NATO (Tikk et al. 2010). Presiden Ilves secara aktif mendorong dimensi diplomasi dengan menekankan bahwa tanpa dukungan sekutu, Estonia berisiko dipandang sebagai negara kecil yang gagal mengelola infrastruktur digitalnya sendiri. Dengan adanya CCDCOE, Estonia dapat bertransformasi menjadi pelopor solusi global, sebuah narasi yang menenangkan kekhawatiran parlemen dan sebagian sektor bisnis (Schmidt 2013).

Perdana Menteri Ansip memainkan peran kunci sebagai jembatan antara kelompok pro dan kontra. Ia menekankan bahwa penguatan domestik dan kerja sama multinasional bukanlah pilihan yang saling meniadakan, melainkan dapat berjalan beriringan. Ansip mengusulkan bahwa sebagian pendanaan CCDCOE dapat diarahkan untuk program pelatihan teknis bagi bank, perusahaan swasta, dan akademisi domestik, sehingga manfaatnya dapat langsung dirasakan oleh aktor non-pemerintah Estonia (Laasme 2011). Strategi kompromi ini menjadi salah satu faktor yang membuat usulan CCDCOE dapat diterima lebih luas.

Proses rapat yang berlangsung sepanjang pertengahan hingga akhir 2007 menghasilkan konsensus bahwa CCDCOE akan memberikan lebih banyak keuntungan strategis dibandingkan kerugiannya. Kesepakatan ini tidak dicapai dalam satu kali pertemuan, melainkan melalui serangkaian kompromi, lobi internal, dan penyusunan narasi bersama. Kementerian Ekonomi dan Komunikasi mendapat jaminan bahwa penguatan infrastruktur domestik tetap menjadi prioritas melalui paket kebijakan terpisah. Bank dan sektor bisnis diberi ruang dalam agenda pelatihan CCDCOE, sementara akademisi dilibatkan dalam kerangka penelitian yang menjadi basis publikasi internasional.

Dengan demikian, lahirnya CCDCOE dapat dipahami bukan sebagai hasil keputusan top-down dari Presiden atau Perdana Menteri semata, melainkan sebagai buah dari *Basic Unit of Analysis: Governmental as Political Resultant*, dimana setiap aktor memiliki kapasitas untuk menahan, mempengaruhi, atau mempercepat jalannya kebijakan. Tarik-menarik kepentingan antar lembaga pemerintahan, tekanan dari sektor swasta, kritik media, serta partisipasi akademisi semuanya berkontribusi dalam membentuk kebijakan final yang kemudian disepakati (Tikk et al. 2010; Rõigas 2014). Studi kasus ini memperlihatkan bahwa dalam konteks Estonia, pembuatan kebijakan luar negeri terkait keamanan siber tidak bisa dilepaskan dari dinamika domestik yang kompleks. Rapat-rapat pembentukan CCDCOE menjadi arena dimana kekuasaan tersebar di antara berbagai institusi yang memiliki kepentingan berbeda. Proses tersebut memperlihatkan dengan jelas bagaimana *GAPR* bekerja: keputusan lahir dari interaksi, kompromi, dan sinergi antar pihak, bukan dari satu otoritas tunggal.

1. Pemicu permainan: Estonia Shutdown 2007

Permainan ini dimulai dari peristiwa Estonia Shutdown pada April–Mei 2007, ketika serangan siber besar-besaran menargetkan infrastruktur vital Estonia, termasuk bank, media, dan institusi pemerintah (Pamment et al. 2019; Czosseck et al. 2011). Peristiwa ini mengekspos kerentanan Estonia, memicu krisis nasional, dan menuntut respons cepat dari pemerintah. Presiden Ilves menekankan bahwa serangan tersebut bukan sekadar gangguan teknis, tetapi ancaman strategis yang menuntut langkah internasional. Analisis serangan oleh Tallinn University dan Kementerian Pertahanan menyediakan data teknis yang memperkuat argumen pro-CCDCOE, termasuk bukti bahwa Estonia membutuhkan pusat kerjasama

multinasional untuk mengkoordinasikan tanggapan dan meningkatkan kapasitas nasional (Ottis 2008; Gross 2017).

2. Rapat darurat domestik: koordinasi internal

Segera setelah serangan, Perdana Menteri Andrus Ansip menginisiasi serangkaian rapat darurat di Tallinn, melibatkan Menteri Pertahanan, Menteri Luar Negeri, pejabat keamanan siber, dan kepala birokrasi terkait (Ottis 2008, 7). Dalam rapat ini, Ansip berperan sebagai koordinator, memastikan seluruh kementerian berbagi informasi, menyusun skenario respons, dan menilai kemampuan Estonia untuk menangani serangan (Sarwidaningrum 2024, 236). Sementara itu, oposisi parlemen, termasuk EKRE, menuntut transparansi dan memperingatkan risiko anggaran (Sarwidaningrum 2024, 238). Ansip menyeimbangkan tekanan oposisi dengan argumentasi teknis dan kepentingan strategis nasional, menekankan bahwa keterlibatan NATO akan memperkuat pertahanan dan reputasi Estonia (Schmidt 2007, 5).

Selama rapat, muncul dinamika tarik-menarik: menteri pertahanan fokus pada kesiapan teknis (Ottis 2008, 9), menteri luar negeri menekankan implikasi diplomatik (Tikk, Kaska, dan Vihul 2010, 18), sedangkan Ansip bertindak sebagai mediator, merumuskan strategi yang dapat mengakomodasi kepentingan berbagai pihak sekaligus menjaga konsensus internal (Laasme 2011, 61). Dokumentasi rapat menunjukkan bahwa perdebatan tidak hanya mengenai urgensi pendirian CCDCOE, tetapi juga pembagian anggaran, koordinasi lembaga, dan penyusunan mandat operasional yang realistis (Sarwidaningrum 2024, 241).

3. Lobi domestik dan pembentukan koalisi parlemen

Ansip melakukan lobi intensif di dalam negeri untuk mengamankan persetujuan legislatif (Sarwidaningrum 2024, 244). Ia membangun koalisi mayoritas dengan partai-partai pro-pemerintah, termasuk partai sosialis-liberal dan sebagian anggota sosial-demokrat yang mendukung agenda digitalisasi dan keamanan siber (Laasme 2011, 62). Oposisi, seperti EKRE dan beberapa anggota konservatif, tetap skeptis, menekankan risiko keterlibatan internasional dan biaya pendirian CCDCOE (Sarwidaningrum 2024, 246). Ansip menggunakan data teknis, proyeksi risiko serangan siber, dan legitimasi internasional untuk menekan oposisi secara persuasif (Ottis 2008, 12). Negosiasi mencakup kompromi anggaran dan penyusunan prosedur pengawasan legislatif, sehingga meskipun oposisi tetap menentang sebagian kebijakan, keputusan pendirian CCDCOE tetap memperoleh dukungan parlemen (Tikk, Kaska, dan Vihul 2010, 20).

4. Lobi internasional: diplomasi Presiden Ilves

Sementara Ansip fokus pada koordinasi internal, Presiden Ilves menjalankan lobi diplomatik di forum internasional (Schmidt 2007, 6). Ia bertemu dengan perwakilan NATO, pejabat negara sponsor seperti AS, Jerman, Spanyol, Latvia, dan Lithuania, serta melakukan kunjungan bilateral ke Brussels dan Washington (NATO 2008, 14). Ilves menekankan pengalaman Estonia dalam menghadapi serangan siber, kapasitas digital nasional, dan kesiapan institusi untuk menjadi tuan rumah CCDCOE (Rõigas 2014, 55). Strategi ini dirancang untuk mengatasi keraguan awal Prancis dan Italia, yang mempertanyakan relevansi pusat siber tambahan dan alokasi dana NATO (Schmidt 2007, 7). Dengan memanfaatkan reputasi Estonia sebagai negara digital terdepan dan dukungan koalisi Baltik, Ilves berhasil mempengaruhi persepsi negara-negara sponsor, memperkuat argumen

Estonia bahwa CCDCOE akan meningkatkan kesiapan kolektif NATO menghadapi ancaman siber (NATO 2008, 16).

5. Interaksi antar aktor dan negosiasi lintas jalur

Proses pengambilan keputusan CCDCOE melibatkan interaksi kompleks antara aktor domestik, regional, dan internasional (Ottis 2008, 15). Misalnya, Ansip berkomunikasi secara simultan dengan kementerian, parlemen, dan tim teknis untuk menyiapkan dokumen resmi yang dapat digunakan Ilves dalam pertemuan NATO (Laasme 2011, 63). Interaksi ini bersifat dua arah: informasi teknis dari Tallinn University dan Kementerian Pertahanan digunakan untuk mendukung negosiasi internasional, sementara feedback dari negara sponsor NATO digunakan untuk menyesuaikan kebijakan domestik dan alokasi anggaran (Tikk, Kaska, dan Vihul 2010, 22).

Pertemuan formal di Tallinn dengan delegasi NATO melibatkan diskusi mendalam mengenai mandat CCDCOE, komposisi staf, pendanaan, dan prosedur operasional (Schmidt 2007, 8). Ilves memimpin diplomasi formal, Ansip memastikan dukungan internal dan kepatuhan birokrasi (Ottis 2008, 18), sementara negara Baltik berperan sebagai koalisi penekan yang menegaskan kepentingan kawasan (Rõigas 2014, 57). Debat intens terjadi mengenai definisi tugas pusat, lingkup yurisdiksi, dan standar keamanan, di mana setiap pemain berusaha memaksimalkan posisi bargaining mereka (NATO 2008, 18).

6. Dinamika bargaining: konflik dan kompromi

Negosiasi menghadapi beberapa titik kritis. Negara sponsor yang ragu seperti Prancis dan Italia mengajukan pertanyaan tentang relevansi tambahan pusat cyber, potensi tumpang tindih dengan NATO CIS, dan alokasi anggaran (Schmidt

2007, 9). Ilves dan koalisi Baltik menjawab dengan argumentasi teknis dan strategis, menekankan bahwa CCDCOE akan menjadi pusat inovasi, latihan, dan koordinasi, bukan duplikasi fungsi (NATO 2008, 20). Ansip menekankan kesiapan administratif Estonia, transparansi penggunaan anggaran, dan pengawasan legislatif, sehingga pihak yang awalnya skeptis akhirnya memberikan persetujuan konseptual (Ottis 2008, 21).

Selain itu, interaksi domestik menuntut manuver politik. Ansip harus mempertahankan dukungan parlemen meski ada tekanan oposisi (Sarwidaningrum 2024, 250). Ia menggunakan kombinasi argumen rasional, kompromi anggaran, dan mekanisme konsultasi reguler untuk menjaga konsensus. Pada titik ini, permainan politik bersifat simultan: Ansip memainkan jalur internal, Ilves memainkan jalur internasional, sementara negara sponsor dan koalisi Baltik menegosiasikan persetujuan kolektif (Allison & Zelikow 1999, 37).

7. Implementasi keputusan hingga garis finis

Keberhasilan pendirian CCDCOE ditandai oleh penandatanganan dokumen pendirian resmi oleh NATO dan Estonia pada tahun 2008 (Pressman & Wildavsky 1973, 45). Proses ini menandai garis finis permainan politik: pemerintah Estonia berhasil memobilisasi dukungan internal, lobi internasional, dan koordinasi multilateral untuk mendirikan pusat, sementara pihak oposisi tetap memantau implementasi dan pelaporan anggaran (Allison & Zelikow 1999, 40). Jalannya permainan menunjukkan kompleksitas pengambilan keputusan modern: keputusan formal hanyalah stasiun di sepanjang jalan, sementara manuver politik, tekanan, dan koordinasi antar pemain menentukan hasil akhir (Pressman & Wildavsky 1973, 47).

Keseluruhan proses, dari Estonia Shutdown 2007 hingga pendirian CCDCOE, menampilkan karakteristik game politik: pemain dengan kepentingan berbeda berinteraksi di berbagai level, menggunakan posisi, informasi, reputasi, koalisi, dan strategi negosiasi untuk mencapai tujuan (Allison & Zelikow 1999, 42). Keberhasilan pendirian CCDCOE mencerminkan kemampuan Estonia memanfaatkan kombinasi faktor domestik dan internasional secara optimal, serta menegaskan bahwa dalam pengambilan keputusan keamanan siber multinasional, politik internal dan diplomasi global berjalan beriringan (Pressman & Wildavsky 1973, 50).

Tabel 1. Aktor-aktor Estonia dalam Rapat Pendirian CCDCOE

Aktor	Peran / Wewenang	Posisi / Stance dalam Rapat	Keterangan / Strategi
Kementerian Pertahanan	Mengatur kebijakan pertahanan nasional, memimpin aspek keamanan militer-siber, dan menjadi penghubung utama dengan NATO	**Pro** terhadap pembentukan CCDCOE	Menekankan bahwa CCDCOE memperkuat kapasitas nasional, bukan mengurangi kedaulatan; akses teknologi, pelatihan, intelijen NATO dianggap keuntungan strategis (Tikk et al. 2010).
Presiden Toomas Hendrik Ilves	Kepala negara, otoritas diplomasi luar negeri, pengangkat isu Estonia di forum internasional	Pro	Menggunakan retorika diplomatik: mengubah narasi dari “korban pasif” menjadi “pelopor solusi global”; meyakinkan parlemen & bisnis melalui keuntungan reputasional (Schmidt 2013).
Perdana Menteri Andrus Ansip	Koordinator kebijakan domestik, kepala pemerintahan, penghubung antar	Pro-Kompromi	Menawarkan jalan tengah: sebagian pendanaan CCDCOE dialokasikan ke pelatihan teknis bank, swasta, dan akademisi;

	lembaga		menyatukan pro-kontra melalui distribusi manfaat (Laasme 2011).
Kementerian Ekonomi dan Komunikasi	Menangani sektor digital & telekomunikasi nasional, infrastruktur domestik	Kritis awalnya, lalu menerima setelah ada jaminan	Khawatir fokus pada NATO akan mengurangi prioritas domestik; akhirnya setuju setelah dijanjikan paket kebijakan terpisah untuk infrastruktur nasional.
Sektor Perbankan dan Bisnis	Penyedia layanan keuangan & ekonomi digital, terdampak langsung serangan siber	Skeptis awalnya, lalu mendukung setelah kompromi	Khawatir ketergantungan pada NATO; akhirnya mendukung setelah dilibatkan dalam agenda pelatihan & perlindungan infrastruktur keuangan.
Akademisi atau Universitas	Riset & inovasi teknologi, sumber daya manusia siber	Netral-Pro	Awalnya hanya sebagai pengamat; kemudian dilibatkan dalam penelitian & publikasi internasional di bawah CCDCOE.
Media Nasional	Pengawas publik, penyampai opini ke masyarakat	Kritis	Mengangkat perdebatan publik terkait kedaulatan & ketergantungan pada NATO; namun juga memberi legitimasi ketika narasi pro-CCDCOE berhasil dibentuk (Rõigas 2014).

Sumber: Diolah oleh Penulis

BAB 4

PENUTUP

4.1. Kesimpulan

Analisis pengambilan keputusan pemerintah Estonia dalam pendirian NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) pada 2007–2008 menunjukkan bahwa respons Estonia terhadap serangan siber besar-besaran yang menimpa negara tersebut merupakan hasil dari interaksi politik yang kompleks, baik di tingkat domestik maupun internasional (Allison 1971). Dengan menggunakan **Governmental Politics Model**, penelitian ini menekankan bahwa keputusan pendirian CCDCOE bukanlah hasil pertimbangan satu otoritas tunggal, melainkan produk dari negosiasi, bargaining, dan kompromi di antara berbagai aktor dengan kepentingan, preferensi, dan kemampuan berbeda (Ottis 2008). Model ini memungkinkan pemahaman bahwa kebijakan nasional adalah arena "permainan politik" di mana aktor domestik seperti Presiden, kementerian, dan badan keamanan saling mempengaruhi proses pengambilan keputusan melalui lobbying, penyusunan agenda, dan aliansi strategis (Allison 1971).

Presiden Toomas Hendrik Ilves muncul sebagai aktor sentral yang memanfaatkan posisi Estonia sebagai salah satu negara digital paling maju untuk memperkuat legitimasi internasional dari inisiatif ini (NATO 2008a). Ilves secara aktif mengkonsolidasikan dukungan domestik, menekankan urgensi keamanan siber, dan mempromosikan persepsi Estonia sebagai negara yang mampu menjadi pionir pertahanan siber. Kementerian luar negeri dan lembaga pertahanan juga memainkan peran strategis dalam merumuskan diplomasi proaktif, memfasilitasi

komunikasi dengan NATO, serta memastikan bahwa dampak nyata dari Estonia Shutdown 2007 tersampaikan secara meyakinkan kepada para pemangku kepentingan internasional (Ottis 2008). Model analisis ini menyoroti bagaimana kepentingan, kapasitas, dan persepsi masing-masing aktor saling bertabrakan dan berkompromi sehingga menghasilkan kebijakan akhir (Allison 1971).

Selain itu, penelitian menunjukkan bahwa faktor domestik seperti kapasitas teknis Estonia, pengalaman e-government, dan stabilitas politik memperkuat posisi tawar negara ini di forum internasional (E-Estonia 2018). Di sisi lain, dinamika internasional, termasuk persepsi NATO terhadap meningkatnya ancaman siber, mendorong aliansi untuk mendukung pendirian CCDCOE di Tallinn. Negara-negara seperti Finlandia, Swedia, dan Amerika Serikat memberikan dukungan logistik, teknis, dan politis, memperlihatkan bagaimana interaksi antara aktor domestik dan internasional menghasilkan kebijakan yang efektif (NATO 2008b). Penggunaan **Governmental Politics Model** secara eksplisit memperlihatkan bahwa pendirian CCDCOE bukan semata keputusan rasional tunggal, tetapi hasil dari pergeseran kekuasaan, pengaruh politik, dan kalkulasi strategis berbagai aktor yang terlibat (Allison 1971).

Dengan demikian, pendirian CCDCOE dapat dipahami sebagai konsekuensi dari permainan politik yang kompleks di mana aktor domestik dan internasional bekerja secara simultan. Model ini membuktikan efektivitasnya dalam menjelaskan bagaimana kepentingan individu dan kelompok, tekanan politik, serta strategi lobbying membentuk kebijakan keamanan siber yang memiliki implikasi global (Allison 1971; NATO 2008a; Ottis 2008). Keberhasilan Estonia dalam meyakinkan NATO untuk mendirikan pusat pertahanan siber di Tallinn

mencerminkan sinergi antara kapasitas domestik, diplomasi cerdas, dan pemahaman politik internasional yang matang.

4.2 Rekomendasi

Penelitian selanjutnya dapat memperluas analisis dengan menyoroti bagaimana keberadaan NATO CCDCOE telah memengaruhi keamanan siber regional dan kebijakan pertahanan digital negara-negara anggota NATO setelah 2008. Studi longitudinal juga dapat dilakukan untuk menilai efektivitas strategi diplomasi Estonia dalam memelihara posisi Tallinn sebagai pusat rujukan pertahanan siber, termasuk dalam konteks perkembangan ancaman siber yang semakin canggih. Selain itu, penelitian berikutnya dapat mengintegrasikan perspektif multi-level governance, menelaah bagaimana interaksi antara aktor domestik, aliansi internasional, dan industri teknologi mempengaruhi pengambilan kebijakan keamanan siber secara berkelanjutan. Analisis komparatif dengan negara lain yang menghadapi ancaman siber serupa juga akan membantu memperluas pemahaman mengenai faktor-faktor kunci yang menentukan keberhasilan negosiasi internasional dan pembentukan pusat pertahanan siber di tingkat global.

DAFTAR PUSTAKA

Pamment,. J., Sazonov, V., Granelli, F., Aday, S., Adzans, M., Cerenkova, U. B., Gravelines, J. P., Hils, M., Holmstrom, M., Klus, A., Sanchez, I. M., Mattiisen, M., Molder, H., Morakabati, Y., Sari, A., Simons, G., & Terra, J. (2019). *Hybrid threats: 2007 cyber attacks on Estonia*. StratCom. Diakses dari: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Army University Press. 2024. *NATO's Cyber Era (1999–2024): Implications for Multidomain Operations*. Accessed October 5, 2025. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA/.

Efthymiopoulos, M. 2019. "Cyber-defense put to the test: the Estonian case of 2007 in 2019." *Journal of Innovation and Entrepreneurship*. https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z.

Studia Securitatis. 2023. "NATO's Mechanisms for the Governance of Cybersecurity." Accessed October 5, 2025. https://magazines.ulbsibiu.ro/studiasecuritatis/natos-mechanisms-for-the-governance-of-cybersecurity/.

ArXiv. 2023. "A Comparative Study of National Cyber Security Strategies of Ten Nations." Accessed October 5, 2025. https://arxiv.org/abs/2303.13938.

Creswell, John W. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. Thousand Oaks, CA: SAGE Publications.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: SAGE Publications.

Allison, G. T. (1971). *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company.

Allison, Graham T., and Philip Zelikow. 1999. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York: Longman.

Czosseck, Christian, Rain Ottis, and Anna-Maria Taliharm. 2011. "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." *International Journal of Cyber Warfare and Terrorism* 1 (1): 24–39.

Crandall, Matthew, and Collin Allan. 2015. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Foreign Policy Analysis* 11 (1): 109–126.

Neustadt, Richard E. 1960. *Presidential Power and the Modern Presidents: The Politics of Leadership from Roosevelt to Reagan*. New York: Wiley.

Pamment, James, Christopher Paul, Linda Robinson, and Janis Sarts. 2019. *Strategic Communication in International Relations: Practical Lessons from NATO and the EU*. Riga: NATO Strategic Communications Centre of Excellence.

Sarwidaningrum,. I. (2024, July 13). *Apa yang Dilakukan Usai Serangan Siber? Pelajaran Penting dari Estonia, Australia, dan Polandia*. Kompas. Diakses dari:

https://www.kompas.id/baca/internasional/2024/07/13/apa-yang-dilakukan-usai-serangan-siber-pelajaran-penting-dari-estonia-australia-dan-polandia
Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2019). *Weaponized narratives: The new battlespace*. Brookings Institution Press.
BBC News. (2007, May 17). *Estonia hit by "Moscow cyber war"*. BBC. Diakses dari:
https://news.bbc.co.uk/2/hi/europe/6665145.stm
Crandall, J. R., & Allan, T. (2015). On cyberattack attribution and the potential role of international law. *Journal of International Affairs, 68*(1), 123–137.
Gross, M. (2017). Cyber attacks in Estonia: Lessons learned. *Journal of Strategic Security, 10*(1), 45–62. https://doi.org/10.5038/1944-0472.10.1.1544
Kalvet, T. (2007). *The Estonian information society developments since the 1990s*. PRAXIS Center for Policy Studies.
Kash, W. (2008). Cyber war: Estonia attacked from Russia. *Technology Review*. Diakses dari:
https://www.technologyreview.com/2008/09/25/128122/cyber-war-estonia-attacked-from-russia/
McGuinness, D. (2017, May 27). How a cyber attack transformed Estonia. *BBC News*. Diakses dari:
https://www.bbc.com/news/39655415
NATO CCDCOE. (2022). *About us: NATO Cooperative Cyber Defence Centre of Excellence*. Diakses dari:
https://ccdcoe.org/about-us/
Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163–190). IOS Press.
Rõigas, H. (2014). Cyber security and NATO's collective defence. *NATO CCDCOE Publications*.
Sarwindaningrum, D. (2024). Dinamika konflik identitas dan serangan siber Estonia 2007. *Jurnal Hubungan Internasional, 12*(1), 55–74.
Schmidt, N. (2007). NATO and Estonia: The alliance's role in cyber defence. *NATO Review*. Diakses dari:
https://www.nato.int/docu/review/2007/issue2/english/analysis.html
Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.
Blank, S. (2008). Russia and the cyber threat to Estonia. *International Journal of Intelligence and CounterIntelligence, 21*(3), 427–447. https://doi.org/10.1080/08850600701854681
CCDCOE. (2020). *Locked Shields cyber defence exercise*. NATO Cooperative Cyber Defence Centre of Excellence. Diakses dari:
https://ccdcoe.org
Czosseck, C., & Tikk, E. (2011). Learning from the "Cyberattacks against Estonia" – 2007. In C. Czosseck, E. Tyugu, & T. Wingfield (Eds.), *Proceedings of the 3rd International Conference on Cyber Conflict* (pp. 1–18). CCDCOE Publications.
Dunn Cavelty, M. (2010). Cyber-terror – Looming threat or phantom menace? The

framing of the US cyber-threat debate. *Journal of Information Technology & Politics, 7*(1), 19–36. https://doi.org/10.1080/19331680903041845
Ehin, P., & Berg, E. (2009). Incompatible identities? Baltic-Russian relations and the EU as an arena for identity conflict. In P. Ehin & E. Berg (Eds.), *Identity and foreign policy: Baltic-Russian relations and European integration* (pp. 1–15). Ashgate.
Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49–60.
https://doi.org/10.5038/1944-0472.4.2.3
Hommik, M. (2007, November 27). President Ilves speaks out on cyber security. *Postimees*.
Kaska, K. (2010). Cooperative cyber defence: The case of Estonia. In C. Czosseck & K. Geers (Eds.), *The virtual battlefield: Perspectives on cyber warfare* (pp. 111–130). IOS Press.
Kaska, K., Beckvard, H., & Minárik, T. (2019). *National cyber security organisation: Estonia*. NATO CCDCOE Publications.
Kasekamp, A. (2010). *A history of the Baltic states*. Palgrave Macmillan.
Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government, an International Journal, 9*(2), 142–157. https://doi.org/10.1504/EG.2012.046419
Laasme, T. (2011). Cyber defence in small states: The case of Estonia. *Baltic Security & Defence Review, 13*(2), 57–83.
Matthews, R. (2014). Defence industry cooperation in small states: The case of Estonia. *Defence Studies, 14*(3), 282–302. https://doi.org/10.1080/14702436.2014.922222
Ministry of Defence Estonia. (2018). *National defence development plan 2017–2026*. Ministry of Defence.Diakses dari:
https://kaitseministeerium.ee
NATO. (2008). *Centres of Excellence*. North Atlantic Treaty Organization. Diakses dari:
https://www.nato.int/cps/en/natolive/topics_68372.htm
Riigikogu. (2010). *Rules of procedure and internal rules act*. Riigikogu. Diakses dari:
https://www.riigikogu.ee
Schmidt, N. (2013). NATO and cyber defence: Mission accomplished? *NATO Review*. Diakses dari:
https://www.nato.int/docu/review/2013/cyber/EN
Shackelford, S. J. (2009). From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law, 27*(1), 192–251.
State Budget Act. (2010). *State budget law of Estonia*. Riigi Teataja. Diakses dari:
https://www.riigiteataja.ee
Kaska, K., Beckvard, H., & Minárik, T. (2019). *National cyber security organisation: Estonia*. NATO CCDCOE Publications.
Laasme, T. (2011). Cyber defence in small states: The case of Estonia. *Baltic Security & Defence Review, 13*(2), 57–83. Schmidt, N. (2007). The 2007 Estonian cyberattacks. *Journal of Baltic Security, 3*(1), 123–136.

Deutsche Welle (DW). 2023. “How Estonia Outpaced the Rest of Europe at Digitalization.” November 23, 2023. https://www.dw.com/en/how-estonia-outpaced-the-rest-of-europe-at-digitalization/a-73098771.

Frost & Sullivan Institute. 2023. *Why Estonia Is Europe’s Digital Powerhouse: A Study in E-Governance Transformation*. Frost & Sullivan Institute. https://frostandsullivaninstitute.org/why-estonia-is-europes-digital-powerhouse-a-study-in-e-governance-transformation.

Government of Estonia. 2024. *E-Residency: Estonia’s Trustworthy Business Environment for Entrepreneurs*. Government of Estonia. https://www.e-resident.gov.ee/blog/posts/trustworthy-business-environment-for-entrepreneurs/.

Kütt, Andres. 2020. “Estonia Is a ‘Digital Republic’ – What That Means and Why It May Be Everyone’s Future.” *The Conversation*, September 29, 2020. https://theconversation.com/estonia-is-a-digital-republic-what-that-means-and-why-it-may-be-everyones-future-145485.

Vinkel, Priit, and Tarvi Martens. 2004. “Electronic Voting in Estonia.” In *Electronic Voting and Democracy: A Comparative Analysis*, edited by N. Kersting and H. Baldersheim, 105–120. New York: Palgrave Macmillan.

E-Estonia. (2018). “Digital Estonia: The foundation of e-government and cybersecurity.” Diakses dari: https://e-estonia.com

NATO. (2008a). “Centres of Excellence: Cyber Defence Initiatives.” North Atlantic Treaty Organization. Diakses dari: https://www.nato.int/cps/en/natolive/topics_68372.htm

NATO. (2008b). “Cyber Defence Policy and Support to Member States.” North Atlantic Treaty Organization. Diakses dari: https://www.nato.int/cps/en/natolive/topics_78170.htm

GudangSSL. 2019. “Apa Itu DDoS dan Cara Mengatasinya.” Diakses Oktober 5, 2025. https://gudangssl.id/blog/apa-itu-ddos-dan-cara-mengatasinya/.