BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Konsep studi keamanan internasional telah mengalami transformasi signifikan sejak berakhirnya era Perang Dingin. Pada era Perang Dingin, konsep keamanan dalam studi HI selalu dihubungkan dengan hal militer. Keamanan selalu dikaitkan dengan konsep ancaman militer dan konflik antar negara, dengan kata lain studi keamanan internasional merupakan studi tentang ancaman, penggunaan dan pengendalian kekuatan militer. Setelah era Perang Dingin, konsep keamanan mengalami perluasan yang signifikan dari fokus militer menjadi mencakup isu-isu non-tradisional seperti keamanan siber, energi, lingkungan, dan kesehatan global. Internet sebagai infrastruktur utama dalam kehidupan modern turut menjadi titik rawan dalam lanskap keamanan kontemporer, khususnya dalam menghadapi ancaman digital lintas negara (Keinonen, 2023).

Pertanyaan siapa yang mengendalikan informasi, bagaimana data dikendalikan, dan siapa yang memiliki kekuasaan dalam ruang digital menjadi isu strategis dalam hubungan antarnegara. Ancaman-ancaman ini sering kali melibatkan aktor-aktor non-negara. Kemajuan teknologi dan dinamika geopolitik telah mendorong negara-negara untuk menyesuaikan kebijakan pertahanannya melalui pendekatan keamanan komprehensif yang mencakup pencegahan serangan siber dan perlindungan infrastruktur digital dari ancaman asimetris. Kemajuan teknologi informasi dan meningkatnya ancaman non-tradisional telah mendorong negara untuk mengadopsi kebijakan pertahanan yang adaptif, termasuk integrasi teknologi digital dan respons terhadap serangan siber serta aktor non-negara. Perkembangan ini mencerminkan pelebaran studi keamanan internasional pasca-Perang Dingin, yang kini tidak lagi terbatas pada isu militer, melainkan juga mencakup keamanan data, ekonomi, dan infrastruktur digital (Keinonen, 2023). Interaksi antara aktor negara dan non-negara semakin intens dan menentukan dinamika keamanan

global, di era keamanan digital. Negara harus mengelola hubungan kompleks dengan perusahaan teknologi multinasional dan kelompok non-negara lain yang memiliki pengaruh besar dalam ruang siber, menjadikan keamanan digital sebagai arena negosiasi kekuasaan yang melampaui batas tradisional (Nye, 2010).

Perkembangan dunia internasional menunjukkan bahwa konflik antarnegara kini juga terjadi di dunia maya (cyberspace). Perkembangan dunia siber internasional merupakan fenomena yang berkembang pesat sejak munculnya teknologi internet pada akhir abad ke-20. Transformasi digital global yang dipicu oleh konektivitas internet tidak hanya mengubah cara manusia berkomunikasi dan bekerja, tetapi juga menciptakan domain baru dalam politik dan keamanan internasional. Internet yang awalnya dirancang sebagai sarana pertukaran informasi ilmiah kini telah menjadi infrastruktur vital yang menopang berbagai sektor kehidupan: ekonomi, pendidikan, pertahanan, hingga diplomasi. Era digital menciptakan ketergantungan negara terhadap sistem digital dan data, yang kemudian membuka peluang sekaligus kerentanan baru terhadap berbagai bentuk ancaman yang bersifat transnasional dan tidak konvensional. Serangan siber, spionase digital, pembajakan data, hingga kontrol terhadap informasi global menjadi bagian dari strategi nasional berbagai negara, (Nye, 2010).

Fenomena ini menandai bahwa internet tidak lagi netral, melainkan menjadi medan kontestasi kekuatan negara. Sebagai hasil dari perkembangan ini, dunia siber bukan hanya isu teknis atau privat, melainkan telah menjadi isu keamanan internasional utama. Negara yang gagal mengamankan ruang sibernya dapat menjadi korban serangan dari negara lain atau kelompok non-negara. Dalam konteks keamanan siber, salah satu isu utamanya adalah pembatasan akses internet (internet censorship). Negara seperti Tiongkok memanfaatkan alat-alat digital untuk membatasi warganya mengakses informasi dari luar, terutama informasi yang bertentangan dengan kepentingan politik domestik. Model sensor ini bukan hanya bersifat defensif, tapi juga

refleksi dari ketakutan terhadap pengaruh budaya, politik, dan ideologi luar, terutama dari negara-negara liberal seperti Amerika Serikat, (Creemers, 2017).

Amerika Serikat, sebagai negara pelopor dalam pengembangan teknologi digital, memegang peranan dominan dalam politik digital karena keberadaan perusahaan teknologi raksasa yang berperan sebagai infrastruktur utama dalam arsitektur internet global. Perusahaan-perusahaan seperti Google, Facebook, Amazon, dan Microsoft tidak hanya menguasai pasar teknologi global tetapi juga menjadi alat strategis dalam menyebarkan nilai-nilai demokrasi dan liberalisme Amerika melalui kontrol mereka atas platform komunikasi dan data global. Dominasi ini didukung oleh investasi besar dalam riset dan pengembangan teknologi serta ekosistem inovasi yang kuat, yang memungkinkan AS mempertahankan keunggulan kompetitif dalam ruang digital sekaligus memperkuat kekuatan lunaknya di tingkat internasional, (Segal, 2016).

Tiongkok memandang dominasi digital Amerika Serikat sebagai ancaman terhadap kedaulatan nasionalnya. Sebagai negara yang mengedepankan prinsip non-intervensi dan stabilitas domestik, Tiongkok menanggapi hal tersebut dengan memperkuat infrastruktur dan regulasi digital dalam negerinya. Bentuk dari respons ini adalah pembentukan Cyberspace Administration of China (CAC) pada tahun 2014. China membentuk CAC sebagai badan utama pengendali ruang digital nasional. CAC diberi wewenang untuk menyensor, menghapus konten, serta mengatur kerja sama digital, termasuk terhadap perusahaan asing seperti Apple, Microsoft, dan Amazon. CAC secara aktif mengawasi platform digital asal AS dan memberlakukan peraturan yang membuat mereka harus tunduk pada sensor lokal, yang secara efektif membatasi operasi bebas mereka, (Creemers, 2017).

Cyberspace Administration of China (CAC), yang secara resmi dibentuk pada tahun 2014, merupakan institusi yang lahir dari kebutuhan strategis Partai Komunis Tiongkok (PKT) untuk mengkonsolidasikan kontrol atas ruang digital yang semakin berkembang pesat dan kompleks. Sebelum pembentukannya, kebijakan terkait internet di Tiongkok dikelola secara terfragmentasi oleh

berbagai kementerian, sehingga tidak efisien dan kurang terkoordinasi. Dengan dibentuknya CAC, Tiongkok mengintegrasikan fungsi-fungsi pengawasan internet, penyensoran konten, dan pengelolaan data di bawah satu badan pusat yang berada langsung di bawah Dewan Negara serta struktur partai. CAC juga bertugas menyusun peraturan-peraturan strategis seperti Cybersecurity Law (2017) dan Data Security Law (2021), yang secara eksplisit mewajibkan perusahaan baik domestik maupun asing untuk mematuhi kontrol data negara dan tunduk pada sensor politik, (Wang & Luo, 2021).

Cara kerja CAC melibatkan kombinasi antara pengawasan algoritmik, kontrol manusia, dan pemanfaatan teknologi kecerdasan buatan untuk menyaring konten yang dianggap "berbahaya", "mengganggu stabilitas sosial", atau "melawan nilai-nilai sosialisme dengan karakteristik Tiongkok". CAC memiliki kekuasaan luas untuk menghapus konten, membatasi distribusi informasi, menjatuhkan sanksi pada perusahaan digital, serta mengatur kerja sama transnasional di bidang teknologi informasi. Dalam konteks hubungan internasional, CAC digunakan sebagai alat strategis untuk menghalangi dominasi platform Barat seperti Google, Facebook, dan Twitter, yang dianggap menyebarkan nilai-nilai liberal, seperti kebebasan berekspresi, hak individu, dan pluralisme politik, nilai yang dipandang bertentangan dengan prinsip stabilitas politik dan otoritas negara yang dipegang teguh oleh Tiongkok, (Chen, 2025).

Secara ideologis, CAC merupakan bagian dari agenda informatization dan cyber sovereignty yang dicanangkan oleh Presiden Xi Jinping, yang menekankan bahwa "tidak ada kedaulatan nasional tanpa kedaulatan jaringan", (Segal, 2018). Dengan retorika tersebut, Tiongkok membingkai pengendalian internet bukan sebagai represi, melainkan sebagai bentuk perlindungan terhadap integritas nasional dari infiltrasi budaya dan politik asing, khususnya dari Amerika Serikat. Dengan kemampuan CAC untuk mengatur siapa yang boleh beroperasi di internet Tiongkok dan bagaimana mereka harus berperilaku, badan ini tidak hanya berperan sebagai regulator domestik, tetapi juga sebagai perisai negara dalam menghadapi pengaruh teknologi Barat yang dianggap

mengancam legitimasi rezim dan stabilitas sosial-politik dalam negeri, (Creemers, 2017).

Sejak dibentuknya Cyberspace Administration of China (CAC) pada tahun 2014, Pemerintah Tiongkok secara bertahap meningkatkan kontrol terhadap perusahaan teknologi Amerika Serikat. Salah satu langkah awal yang signifikan adalah pemblokiran penuh terhadap Google, termasuk layanan Gmail dan Google Search, yang terjadi pada 26 Juni 2014 menjelang peringatan tragedi Tiananmen. Meskipun Facebook telah diblokir sejak 2009, tekanan terhadap platform milik Meta lainnya seperti WhatsApp meningkat hingga akhirnya diblokir total pada September 2017. Pada tahun 2018, CAC juga mulai menekan Apple dengan mewajibkan pemindahan data iCloud pengguna Tiongkok ke perusahaan lokal, yakni Guizhou-Cloud Big Data (GCBD). Ketegangan antara Tiongkok dan Amerika Serikat memuncak pada periode 2020 - 2021, ketika CAC memperketat regulasi terhadap perusahaan seperti Microsoft melalui penutupan LinkedIn di Tiongkok pada Oktober 2021. Puncak dari ketegangan ini terjadi pada tahun 2021 - 2022, saat CAC menjatuhkan sanksi terhadap perusahaan ride-hailing Didi Chuxing hanya beberapa hari setelah perusahaan tersebut melakukan penawaran saham perdana (IPO) di New York pada 30 Juni 2021, dengan dalih pelanggaran keamanan data. Kebijakan-kebijakan tersebut menunjukkan bagaimana CAC memainkan peran sentral dalam menegakkan kedaulatan digital dan membatasi pengaruh perusahaan teknologi Amerika Serikat di ruang digital Tiongkok (Creemers, 2018).

Berdasarkan uraian di atas, peneliti tertarik untuk mengkaji fenomena ini melalui perspektif politik cyber internasional. Penulis melihat bahwa pembentukan Cyberspace Administration of China (CAC) tidak semata-mata sebagai langkah administratif, melainkan mencerminkan motif strategis Tiongkok untuk mempertahankan kedaulatan digital dan membatasi pengaruh asing, khususnya dari Amerika Serikat. Melalui pendekatan teori Cyberpower yang dikembangkan oleh Joseph Nye, penelitian ini bertujuan untuk memahami bagaimana kekuatan siber digunakan sebagai alat pengaruh dan kontrol dalam tatanan global. Penekanan utama penelitian ini terletak pada analisis

mengapa Tiongkok menggunakan CAC sebagai instrumen untuk membangun kekuatan sibernya demi mencapai kepentingan nasional dan menjaga stabilitas politik domestik dari pengaruh Barat.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dari penelitian ini adalah: bagaimana Cyberspace Administration of China digunakan sebagai instrumen untuk membatasi pengaruh perusahaan teknologi Amerika Serikat?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis bagaimana peningkatan pembatasan internet yang dilakukan oleh pemerintah Tiongkok terhadap perusahaan asing Amerika Serikat melalui dinamika kebijakan digital Tiongkok melalui pembentukan Cyberspace Administration of China (CAC). Secara khusus, penelitian ini bertujuan untuk:

1. Menjelaskan latar belakang dan tujuan pembentukan Cyberspace Administration of China (CAC) tahun 2014 sebagai respons terhadap dinamika global di ruang siber, khususnya terhadap dominasi Amerika Serikat dalam infrastruktur digital.
2. Menganalisis secara mendalam bagaimana kebijakan pembatasan konten dan regulasi digital yang diterapkan oleh Cyberspace Administration of China (CAC) terhadap perusahaan asing Amerika Serikat merefleksikan upaya perlindungan data, kontrol informasi, dan keamanan nasional Tiongkok.
3. Mengkaji pembentukan dan kebijakan CAC melalui perspektif teori Cyberpower (Joseph Nye) untuk melihat bagaimana Tiongkok menggunakan kekuatan digital sebagai alat strategis dalam hubungan internasional.

4. Menginterpretasikan kebijakan CAC sebagai bentuk implementasi kedulatan digital sebagai upaya tingkok dalam mempertahankan kontrol atas ruang siber nasional dan membatasi pengaruh asing.
5. Mengidentifikasi implikasi kebijakan CAC terhadap hubungan Tiongkok dengan Amerika Serikat dalam bidang teknologi, ekonomi digital, dan keamanan siber.

1.4 Manfaat Penelitian

A. Manfaat Teoritis

1. Penelitian ini dapat memberikan kontribusi sebagai sumber akademik awal yang membahas hubungan antara kebijakan digital Tiongkok dan teori keamanan internasional secara lebih sistematis.
2. Penelitian ini diharapkan dapat bekontribusi untuk menjadi referensi studi dalam memahami bagaimana konsep kedaulatan digital dioperasikan oleh negara dalam konteks kebijakan dunia maya.
3. Penelitian ini mampu menawarkan celah teoritis yang dapat memperluas kajian mengenai kedaulatan digital dalam konteks hubungan internasional kontemporer.

B. Manfaat Praktis

1. Secara praktis, penelitian ini dapat menjadi sumber informasi awal bagi masyarakat akademik mengenai dinamika pembatasan ruang digital yang dilakukan oleh negara besar seperti Tiongkok.
2. Dapat menjadi pola pengetahuan masyarakat dalam memahami isu-isu kontemporer terkait kontrol informasi, sensor digital, serta implikasinya terhadap tatanan global.
3. Memberikan dasar bagi peneliti selanjutnya yang ingin mengkaji topik serupa dengan pendekatan yang lebih mendalam.