CONVERGENCE: JOURNAL OF GLOBAL DYNAMICS

Program Studi Hubungan Internasional, UIN Alauddin Makassar
ISSN: 3109 – 4228 (Print) | e-ISSN: 3109 – 4198 (Online)

TELAAH KEBIJAKAN SIBER TIONGKOK DAN PENGARUHNYA TERHADAP PERUSAHAAN TEKNOLOGI AMERIKA SERIKAT

Siti Alifiyah Safitri[1], Aditya Maulana Hasymi[2]
Universitas Amikom Yogyakarta, Indonesia. Email: sitialifiyah@students.amikom.ac.id
Universitas Amikom Yogyakarta, Indonesia. Email: adityahasymi@amikom.ac.id

Abstract

This research explores the establishment of the Cyberspace Administration of China (CAC) as a strategic response by the Chinese government to counter the influence of American technology companies in the digital sphere. Employing a descriptive qualitative method and grounded in Digital Sovereignty and Cyberpower theories, this study analyzes the role of CAC as a central instrument in managing digital governance and national information control. Findings reveal that CAC serves not only as an administrative authority but also as a political apparatus designed to ensure ideological conformity, protect national data, and promote digital independence. Through strict regulations and censorship, CAC imposes operational limitations on U.S.-based tech firms like Google, Facebook, Apple, and Microsoft. These actions align with China's broader ambition to establish cyber sovereignty, safeguard national security, and ensure domestic political stability. By analyzing CAC's institutional design and policy implementation, this research contributes to understanding how authoritarian states leverage digital governance to challenge Western technological dominance and reshape global internet governance norms.

Keywords: Cyberspace Administration of China; Digital Sovereignty; U.S. Technology Companies; Cyberpower; Political Stability.

Abstrak

Penelitian ini membahas pembentukan Cyberspace Administration of China (CAC) sebagai respons strategis pemerintah Tiongkok dalam menghadapi pengaruh perusahaan teknologi Amerika Serikat di ruang digital. Dengan metode kualitatif deskriptif dan berlandaskan teori Kedaulatan Digital serta Cyberpower, penelitian ini menganalisis peran CAC sebagai instrumen utama dalam tata kelola digital dan kontrol informasi nasional. Hasil penelitian menunjukkan

bahwa CAC tidak hanya berfungsi sebagai lembaga administratif, tetapi juga sebagai alat politik untuk menjaga keseragaman ideologis, melindungi data nasional, dan mendorong kemandirian digital. Melalui regulasi ketat dan sensor, CAC membatasi operasional perusahaan teknologi asal AS seperti Google, Facebook, Apple, dan Microsoft. Kebijakan ini mencerminkan ambisi lebih luas Tiongkok untuk menegakkan kedaulatan dunia maya, menjaga keamanan nasional, dan menjamin stabilitas politik domestik. Dengan menganalisis struktur kelembagaan dan kebijakan CAC, penelitian ini memberi kontribusi dalam memahami bagaimana negara otoriter memanfaatkan tata kelola digital untuk menantang dominasi teknologi Barat dan membentuk ulang norma global dalam tata kelola internet.

Kata Kunci: Cyberspace Administration of China; Kedaulatan Digital; Perusahaan Teknologi Amerika Serikat; Cyberpower; Stabilitas Politik.

PENDAHULUAN

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. Namun, setelah era Perang Dingin berakhir, makna konsep keamanan diperluas mencakup isu-isu non-militer, dengan mencakup berbagai isu yang tidak bersifat militer, seperti keamanan siber, energi, lingkungan, hingga kesehatan global. Internet, sebagai infrastruktur komunikasi global, menjadi salah satu titik rawan dalam lanskap keamanan kontemporer (Deibert, 2013).

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. Pergeseran dari pendekatan keamanan tradisional ke non-tradisional memiliki implikasi signifikan terhadap kebijakan dan strategi keamanan nasional (Buzan, 1991). Kemajuan teknologi dan dinamika geopolitik mendorong transformasi dalam kebijakan pertahanan, termasuk integrasi teknologi baru dan penyesuaian terhadap ancaman asimetris. Studi keamanan internasional pasca Perang Dingin telah mengalami proses pelebaran atau perluasan dalam hal subjek yang dikaji, (Hough, 2008). 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). China, dan negara-negara besar lainnya aktif dalam membangun kapabilitas siber ofensif dan defensive, yang bertujuan untuk melindungi infrastruktur digital mereka dari ancaman luar (Deibert, 2013).

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).

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).

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. Fokus utama penelitian ini terletak pada analisis mengapa kebijakan Tiongkok melalui Cyberspace Administration of China terarah pada pada pembatasan pengaruh perusahaan teknologi Amerika Serikat dalam konteks rivalitas siber global?

TINJAUAN PUSTAKA

Seiring meningkatnya relevansi isu keamanan digital dalam studi hubungan internasional, berbagai penelitian telah membahas dinamika antara negara, teknologi, dan kekuasaan di ruang siber. Joseph Nye dalam konsep Cyberpower, menjelaskan bagaimana negara dapat menggunakan ruang siber untuk memperoleh kekuatan politik, keamanan, dan ekonomi melalui tiga dimensi utama: koersif, produktif, dan persuasif. Dalam konteks Tiongkok, pendekatan ini menjadi relevan dalam menjelaskan bagaimana kebijakan digital diarahkan untuk membangun kekuatan negara di dunia maya (Nye, 2010).

Sementara itu, dalam bukunya Networks and States Mueller memperkenalkan konsep Digital Sovereignty, yaitu hak negara untuk mengatur arus informasi, data, dan infrastruktur digital di wilayahnya. Konsep ini menjadi penting ketika negara-negara seperti Tiongkok berusaha membatasi pengaruh asing yang datang melalui perusahaan teknologi raksasa dari Amerika Serikat, (Mueller, 2010). Rogier Creemers juga menjelaskan bahwa pembentukan CAC adalah bagian dari strategi Partai Komunis Tiongkok untuk memperkuat kontrol sosial dan ideologis melalui dunia digital (Creemers, 2017).

Aynne Kokas dalam Trafficking Data menyoroti bagaimana Tiongkok secara sistematis

menggunakan regulasi data dan kebijakan keamanan digital untuk memperkuat kedaulatan nasional sekaligus menekan perusahaan asing (Kokas, 2022). Selain itu, Adam Segal menegaskan bahwa CAC memainkan peran strategis tidak hanya dalam pengaturan domestik tetapi juga sebagai alat kebijakan luar negeri untuk menantang dominasi teknologi Barat (Segal, 2016). Penelitian oleh Zeng, Stevens, dan Chen (2017) memperkuat temuan ini dengan menjelaskan bagaimana wacana kedaulatan dunia maya digunakan oleh Beijing untuk membentuk norma alternatif dalam tata kelola internet global.

Penelitian dari Clementi (2023) menyoroti dimensi yuridis dan historis dari CAC sebagai bagian dari transisi Tiongkok menuju negara cerdas yang menggunakan sistem pengawasan berbasis AI. Li (2023) juga menegaskan bahwa CAC berperan besar dalam restrukturisasi kebijakan sosial dan pengelolaan opini publik digital di bawah prinsip stabilitas sosial. Temuan dari Hong dan Goodnight (2022), serta Deibert (2020), juga menggambarkan bagaimana CAC adalah bagian dari strategi negara untuk membingkai internet sebagai ruang berdaulat, bukan ruang terbuka.

Penelitian oleh Zhang & Gilli (2021) menambahkan bahwa model regulasi digital Tiongkok telah mulai diadopsi oleh negara-negara lain dengan rezim otoriter, menciptakan efek demonstratif dalam tata kelola digital global. Mereka menyebut CAC sebagai contoh utama dari bagaimana kebijakan domestik dapat menjadi model ekspor normatif. Di sisi lain, penelitian dari Feldstein (2019) menunjukkan bahwa kemampuan CAC dalam mengontrol arus informasi menjadi dasar bagi lahirnya apa yang disebut sebagai “authoritarian digitalism.”. Sementara itu, karya Kendra Schaefer (2021) menekankan bahwa keberhasilan CAC tidak dapat dilepaskan dari sinergi antara birokrasi partai dan kemajuan teknologi domestik Tiongkok, terutama dalam pengembangan platform-platform nasional seperti WeChat dan Baidu. Dalam analisisnya, CAC bukan sekadar alat kontrol, melainkan aktor yang aktif dalam proses inovasi digital yang diarahkan oleh negara. Chertoff & Simon (2021) juga memperlihatkan bagaimana kebijakan CAC membentuk ulang norma global terkait privasi, hak digital, dan pengawasan siber, terutama melalui keterlibatan Tiongkok dalam forum multilateral seperti ITU dan BRICS.

Sebagian besar penelitian yang telah ada cenderung fokus pada aspek teknis, hukum, atau implikasi ekonomi dari pembentukan Cyberspace Administration of China (CAC). Namun, masih sedikit kajian yang secara eksplisit menganalisis CAC sebagai instrumen cyberpower dan digital sovereignty dalam konteks hubungan internasional serta dampaknya terhadap perusahaan teknologi asing, khususnya Amerika Serikat. Selain itu, masih minim kajian yang menyandingkan

pembentukan CAC dengan teori kekuatan siber dalam melihat bagaimana kebijakan digital dijadikan instrumen politik luar negeri dan stabilisasi dalam negeri oleh pemerintah Tiongkok. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan mengkaji secara komprehensif peran CAC sebagai aktor strategis dalam persaingan kekuatan siber global.

Kerangka Teoritis

1. Kedaulatan Digital (Digital Sovereignty)

Kedaulatan digital (digital sovereignty) merupakan konsep yang berkembang pesat dalam dekade terakhir sebagai respons terhadap dominasi teknologi global oleh segelintir aktor terutama perusahaan teknologi besar dari Amerika Serikat. Istilah ini merujuk pada hak dan kapasitas suatu negara untuk mengatur, mengelola, dan melindungi ruang digitalnya sendiri termasuk data, konten, infrastruktur, serta aktivitas digital dalam batas teritorialnya dari intervensi pihak asing sesuai dengan kepentingan nasionalnya. Konsep ini muncul akibat meningkatnya kekhawatiran bahwa internet global telah dikendalikan oleh perusahaan-perusahaan teknologi raksasa yang sebagian besar berbasis di Amerika Serikat (seperti Google, Facebook, Amazon, dan Apple), sehingga membuat negara-negara lain berada dalam posisi pasif atau bergantung. Milton Mueller (2010), dalam bukunya "Networks and States", menjadi salah satu tokoh awal yang mengangkat perdebatan ini dalam konteks tata kelola internet global. Ia melihat bahwa negara-negara non-Barat mulai memperjuangkan hak untuk mengatur informasi dan teknologi digital di dalam negeri sebagai bentuk perpanjangan kedaulatan negara modern.

Menurut Mueller, seorang akademisi terkemuka dalam kajian tata kelola internet global, kedaulatan digital adalah bentuk kontestasi atas struktur kekuasaan dalam ruang siber, di mana negara-negara menuntut kontrol yang lebih besar atas arus informasi, platform digital, dan data warganya. Ia menyatakan bahwa dominasi perusahaan teknologi global telah menciptakan ketimpangan dan kerentanan yang membahayakan kedaulatan negara- negara lain. Dalam konteks ini, kedaulatan digital muncul sebagai bentuk resistensi terhadap sistem internet terbuka yang dikendalikan oleh nilai-nilai liberal dan mekanisme pasar bebas (Mueller, 2010).

Deibert dalam bukunya berjudul "Reset: Reclaiming the Internet for Civil Society", menyatakan bahwa terdapat lima elemen atau pilar kedaulatan digital, (1) Kontrol atas infrastruktur digital, negara memiliki kendali atas jaringan, server, dan puast data dalam wilayah yuridiksinya. (2) Pengaturan konten dan Platform, negara memliki hak untuk menentukan konten

apa yang dapat diakses atau diblokir dalam ruang digital nasional. (3) Perlindungan dan pengelolaan data, negara menetapkan aturan terkait pengumpulan, penyimpanan, dan aliran data pibadi warga negaranya. (4) Pengembangan teknologi lokal, upaya untuk mengurangi ketergantungan terhadap teknologi asing dengan memproduksi solusi digital domestic. (5) Regulasi terhadap aktor asing, negara dapat membatasi atau mengatur aktivitas perusahaan asing yang dianggap mengancam stabilitas atau kedaulatan negaranya (Deibert, 2020).

Berdasarkan uraian di atas, teori kedaulatan digital sangat tepat digunakan dalam penelitian ini sebagai kerangka konseptual untuk menjelaskan tindakan dan kebijakan Tiongkok melalui CAC. Teori ini mampu menjawab alasan strategis, ekonomi, politik, dan ideologis di balik pembatasan terhadap perusahaan asing asal AS. Di sisi lain, penggunaan teori ini juga membantu menunjukkan bahwa kontrol digital bukan semata-mata represif, tetapi juga merupakan bagian dari strategi negara dalam merespons struktur kekuasaan global yang timpang dalam ekosistem teknologi informasi.

2. Cyberpower oleh Joseph Nye (2010)

Konsep Cyberpower yang dikembangkan oleh Joseph S. Nye Jr. dalam tulisannya "Cyber Power" (2010) merupakan salah satu pendekatan paling relevan dalam memahami dinamika kekuatan negara dalam ruang siber. Teori ini mengadaptasi konsep kekuasaan dalam hubungan internasional ke dalam konteks digital, dengan menyoroti bagaimana actor negara dan non-negara menggunakan teknologi informasi untuk mencapai kepentingan strategis mereka. Menurut Nye, cyberpower adalah "kemampuan untuk menggunakan ruang siber untuk menciptakan manfaat dan mempengaruhi orang lain dalam cara-cara yang sejalan dengan tujuan nasional". Dalam kerangka ini, kekuasaan dalam dunia maya tidak hanya bersifat koersif (menghancurkan atau menyerang), tetapi juga dapat bersifat persuasif (memengaruhi dan menarik), selaras dengan konsep kekuatan keras (hard power) dan kekuatan lunak (soft power) yang selama ini dikenal dalam teori hubungan internasional.

Nye membagi cyberpower menjadi tiga dimensi utama, (1) Cyberpower sebagai sarana untuk menyerang dan bertahan. Berkaitan dengan aspek militer dan keamanan, termasuk serangan siber, pertahanan jaringan, dan spionase digital. (2) Cyberpower sebagai alat ekonomi dan industry. Mengacu pada kemampuan negara untuk memanfaatkan ruang siber guna memperkuat keunggulan ekonomi, teknologi, dan infrastruktur digital. (3) Cyberpower sebagai kekuatan normative dan ideologis, di mana negara menggunakan internet untuk menyebarkan nilai-nilai,

membentuk opini public global, atau melindungi budaya dan identitas nasional dari pengaruh asing (Nye, 2010).

Menurut Nye (2010), cyberpower adalah kemampuan suatu aktor untuk menggunakan ruang siber untuk mencapai tujuan yang diinginkan melalui, (1) kekuatan koersif (coercion), misalnya serangan siber untuk melemahkan lawan, (2) kekuatan produktif (production), kemampuan menciptakan atau mengendalikan infrastruktur digital, (3) Kekuatan persuasive (attraction), penggunaan daya tarik dan legitimasi narasi di internet. Nye juga membagi sumber kekuasaan dalam ruang siber menjadi dua kategori utama, (1) Kekuatan keras (hard cyberpower), yang termasuk di dalamnya adalah tindakan siber ofensif seperti spionase, sabotase, sabotase digital, hingga pengendalian infrastruktur informasi. (2) Kekuatan lunak (soft cyberpower), misalnya pengaruh budaya digital, pengaturan narasi digital, dan penyebaran nilai-nilai ideologis melalui platform digital. Dalam teori ini, aktor negara dan non-negara sama-sama memiliki kapasitas untuk membentuk dan mempengaruhi struktur kekuasaan global melalui penggunaan internet dan teknologi informasi.

Dalam teori cyberpower yang dikembangkan oleh Joseph nye (2010), juga dijelaskan tiga alasan utama mengapa negara membangun kekuatan ruang siber (cyberpower). (1) Keamanan nasional (national security), negara membangun cyerpower untuk melindungi infrastruktur vital dan kedaulatan digitalnya dari ancaman siber, seperti serangan dari negara lain (cyberwarfare), spionase digital, dan gangguan terhadap sistem militer, energi, keuangan, dan pemerintahan. (2) Keuntungan ekonomi dan daya saing teknologi (economic competitiveness), cyberpower dibangun untuk melindungi dan memajukan industry digital dalam negeri, termasuk perlindungan terhadap inovasi dan hak kekayaan intelektual, dukungan terhadap perusahaan teknologi nasional, serta pembatasan competitor asing agar industry lokal dapat tumuh dan berkembang. (3) Pengaruh global dan soft power (global influence and soft power), negara membangun cyberpower untuk menyebarkan pengaruh ideologi dan nilai-nilai melalui raung digital. Seperti mengontrol narasi internasional, menghadirkan alternatif terhadap dominasi informasi barat, dan membangun kekuatan lunak melalui media dan teknoligi. Ketiga alasan ini menjelaskan motivasi strategis suatu negara untuk mengembangkan kapasitasnya dalam dunia digital.

Konsep cyberpower sangat relevan untuk menganalisis pembentukan dan kebijakan Cyberspace Administration of China (CAC), karena lembaga ini merupakan wujud konkret dari upaya negara Tiongkok untuk membentuk dan memonopoli kekuasaan di ruang digital nasional

maupun internasional. Setelah kebocoran informasi oleh Edward Snowden pada tahun 2013, yang menunjukkan bahwa Amerika Serikat melakukan pengawasan global melalui jaringan internet, Tiongkok merasa hal tersebut menjadi ancaman terhadap kedaulatan digital dan keamanan nasionalnya. Dalam konteks inilah, pembentukan CAC pada tahun 2014 dapat dilihat sebagai strategi untuk mengurangi ketergantungan terhadap infrastruktur digital Barat, khususnya dari perusahaan-perusahaan teknologi AS seperti Google, Facebook, dan Microsoft.

METODE PENELITIAN

Pada penelitian ini penulis menggunakan pendekatan kualitatif, dengan pendekatan deskriptif-kualitatif. Metode ini dipilih karena sesuai untuk menjawab pertanyaan penelitian yang berfokus pada pemahaman secara mendalam mengenai kebijakan pembentukan Cyberspace Administration of China (CAC) dan bagaimana lembaga tersebut digunakan sebagai instrument oleh pemerintah Tiongkok untuk membatasi pengaruh perusahaan teknologi asing, khususnya dari Amerika Serikat. Metode ini memungkinkan peneliti untuk menganalisis dokumen kebijakan, pernyataan resmi pemerintah, serta literatur akademik guna menginterpretasikan motif dan implikasi dari kebijakan yang diterapkan oleh CAC pada kurun waktu 2020 hingga 2022 karena tahun tersebut merupakan puncak ketegangan antara Tiongkok dan Amerika Serikat. sejak tahun 2020 CAC mulai menerapkan tindakan langsung terhadap perusahaan teknologi Amerika Serikat melalui kasus Didi Chuxing, dan pada 2022 mulai diberlakukan secara penuh Personal Information Protection Law (PIPL) dan Data Security Law yang memperkuat pembatasan terhadap pengaruh asing di ruang digital, seperti yang telah dijelaskan pada bab pendahuluan.

Teknik pengumpulan data dalam penelitian ini dilakukan melalui metode studi pustaka (library research), yang merupakan bagian integral dari pendekatan kualitatif dalam penelitian ilmu sosial dan hubungan internasional. Sumber data sekunder diperoleh melalui berbagai sumber tertulis yang relevan. Sumber utama dalam penelitian ini meliputi sejumlah dokumen resmi seperti Cybersecurity Law of the People's Republic of China (2017), Data Security Law (2021), serta kebijakan-kebijakan teknis dan ideologis yang dikeluarkan oleh CAC dan lembaga pemerintahan Tiongkok lainnya yang berkaitan dengan tata kelola internet dan data. Penelitian ini juga mengacu pada sumber landasan hukum resmi dari Office of the Central Cyberspace Affairs Commission yang mengatur secara langsung fungsi dan kebijakan Cyberspace Administration of China. Selain itu, laporan dan indeks global dari organisasi seperti Freedom House, Human Rights Watch, Reporters Without Borders, Access Now, dan Citizen Lab digunakan untuk memperoleh data

empirik terkait praktik sensor, pengawasan digital, serta pembatasan perusahaan teknologi asing di Tiongkok. Laporan-laporan ini juga membantu memetakan bagaimana kebijakan digital Tiongkok dipersepsikan dalam tatanan global, serta bagaimana negara-negara lain merespons ekspansi model kontrol digital Tiongkok.

HASIL DAN PEMBAHASAN

Bab ini akan menguraikan dan menganalisis Cyberspace administration of China digunakan sebagai instrumen untuk membatasi pengarh perusahan teknolgi Amerika Serikat. Analisis diawali dengan membuktikan dengan melihat dari struktur kelembagaan dan fungsi CAC dalam kerangka pemerintahan Tiongkok, termasuk posisi strategisnya di bawah Dewan Negara sebagai lembaga yang mengoordinasikan agenda keamanan siber nasional. Selanjutnya, pada bagian ini juga mengkaji secara spesifik kebijakan-kebijakan yang dikeluarkan oleh CAC terhadap perusahaan-perusahaan teknologi Amerika Serikat sebagai bentuk respon terhadap ancaman terhadap kedaulatan digital Tiongkok.

Proses ini akan dikaitkan dengan implementasi prinsip-prinsip kedaulatan siber sebagai bagian dari strategi pertahanan informasi nasional Tiongkok. Sebagai upaya untuk membuktikan argumen bahwa CAC merupakan instrumen cyberpower Tiongkok, maka akan dilakukan analisis lebih lanjut dengan menggunakan kerangka teori kekuatan siber (cyberpower) yang dikembangkan oleh Joseph S. Nye, kemudian Teori Kedaulatan Digital digunakan untuk menjelaskan bagaimana pembentukan dan kebijakan CAC mencerminkan upaya negara dalam mengontrol dan melindungi ruang digital domestik.

Struktur dan Fungsi Cyberspace Administration of China dalam Kontrol Digital Nasional

CAC beroperasi langsung di bawah Dewan Negara dan sekaligus berfungsi sebagai Kantor Informasi Internet Pusat yang berada dalam koordinasi dengan Partai Komunis Tiongkok (PKT). Lembaga ini memiliki mandat luas yang mencakup perumusan kebijakan siber nasional, pengawasan aktivitas digital, pengendalian arus informasi, serta regulasi terhadap perusahaan teknologi—baik domestik maupun asing. Dengan kedudukan tersebut, CAC menjadi tulang punggung dalam inisiatif Tiongkok untuk membangun dan mempertahankan kedaulatan digitalnya (Creemers, 2017).

Dalam praktiknya, CAC menjalankan fungsi pengaturan infrastruktur digital nasional melalui sejumlah kebijakan yang dirancang untuk memperkuat kendali negara atas jaringan dan data. Hal ini mencakup pembentukan standar teknis untuk jaringan, kewajiban audit keamanan data, serta penegakan

kebijakan registrasi identitas asli bagi pengguna internet. Kebijakan ini, yang dikenal sebagai real-name registration system, mewajibkan semua pengguna internet untuk mendaftarkan identitas asli mereka sebagai bagian dari upaya pelacakan dan pembatasan aktivitas daring yang tidak sesuai dengan garis politik negara (Creemers, 2017). Selain itu, CAC juga mengendalikan arus informasi digital lintas batas, termasuk membatasi akses dan lalu lintas data dari dan ke luar negeri melalui regulasi terhadap pusat data, layanan cloud, dan jaringan internet internasional (Creemers, 2017).

Salah satu instrumen utama yang digunakan CAC adalah penerapan real-name registration system, di mana semua pengguna internet diwajibkan menggunakan identitas resmi mereka untuk mengakses layanan digital. Sistem ini tidak hanya memudahkan pelacakan aktivitas pengguna, tetapi juga berfungsi sebagai alat pencegah bagi penyebaran konten yang dianggap melawan ideologi negara. Selain itu, CAC juga mengatur lalu lintas data lintas batas melalui kebijakan pembatasan ekspor data sensitif, serta pengawasan terhadap lokasi fisik pusat data agar tetap berada di dalam yurisdiksi Tiongkok (Creemers, 2017). CAC memastikan bahwa seluruh arsitektur jaringan dan infrastruktur informasi tidak hanya berada dalam kendali teknis, tetapi juga dalam otoritas politik negara.

Di luar pengaturan struktural, CAC juga mengembangkan mekanisme pengawasan dan sensor digital yang sangat kompleks dan terintegrasi. Pengawasan ini dijalankan melalui sistem algoritma dan kecerdasan buatan yang secara otomatis memantau, mengidentifikasi, dan menyensor konten yang dianggap berpotensi mengganggu stabilitas politik dan sosial. Sistem ini bekerja dalam kerangka yang dikenal luas sebagai Great Firewall of China, yakni sistem penyaringan internet yang memblokir akses ke situs-situs asing serta membatasi informasi global yang dianggap bertentangan dengan nilai-nilai Partai Komunis Tiongkok. Sensor tidak hanya dilakukan secara pasif, tetapi aktif dan adaptif terhadap perkembangan bahasa serta simbol dalam dunia maya. Bahkan konten humor, sindiran, atau simbol non- verbal yang membawa pesan politik dapat ditangkap oleh sistem sensor otomatis ini (Roberts, 2018). Lebih dari itu, CAC tidak bekerja sendirian, mereka membangun kolaborasi langsung dengan perusahaan teknologi lokal, yang diwajibkan untuk menerapkan sensor internal sesuai dengan pedoman pemerintah.

Sensor dan pengawasan juga diiringi oleh penegakan hukum digital yang represif. CAC sering kali bekerja bersama lembaga keamanan publik untuk memproses pelanggaran hukum daring, baik yang dilakukan oleh individu maupun oleh entitas swasta asing. Melalui regulasi seperti Cybersecurity Law 2017, CAC diberi legitimasi untuk melakukan audit, penyelidikan, hingga penutupan akun dan aplikasi yang melanggar ketentuan sensor. Kondisi ini adalah sebagai bagian dari tren global menuju "fragmentasi digital", di mana negara-negara otoriter seperti Tiongkok menggunakan perangkat teknis,

hukum, dan ideologis untuk menciptakan ekosistem internet tertutup dan dikontrol secara ketat oleh negara (Deibert, 2020). Maka dari itu, peran CAC dalam mekanisme pengawasan tidak hanya bersifat administratif, tetapi juga ideologis dan politis yakni memastikan bahwa internet di Tiongkok menjadi ruang yang aman secara politik dan terkendali secara sosial oleh negara.

Jika dilihat melalui kerangka teori kekuatan digital, maka CAC dapat diposisikan sebagai alat sentral negara untuk memproyeksikan, mempertahankan, dan mengontrol kekuasaan dalam ruang siber. Teori ini memandang bahwa kekuatan digital tidak hanya mencakup infrastruktur teknologi, tetapi juga kemampuan negara dalam mengatur informasi, membentuk opini publik, dan menegakkan otoritas melalui media digital. Dalam konteks Tiongkok, CAC menjadi instrumen institusional utama dalam penguasaan informational power, yaitu kekuatan yang timbul dari kemampuan negara untuk mengendalikan arus data dan narasi digital yang beredar dalam masyarakat (Qiang, 2019). Negara menggunakan teknologi spekulatif dan sistem data yang bersifat prediktif bukan hanya untuk mengetahui, tetapi juga untuk mengendalikan kemungkinan dengan kata lain, teknologi digunakan sebagai alat antisipasi dan intervensi politik terhadap masyarakat, (Hong, 2020). Melalui CAC, Tiongkok tidak sekadar mempertahankan kontrol atas infrastruktur digital domestik, tetapi juga memperluas kapasitas negara untuk melakukan pembentukan sosial (social shaping) terhadap ruang digital.

Kebijakan Cyberspace Administration of China terhadap Perusahaan Teknologi Amerika Serikat

Sebagai institusi yang bertanggung jawab langsung terhadap kontrol digital nasional, Cyberspace Administration of China (CAC) berperan aktif dalam menerapkan berbagai kebijakan yang membatasi kehadiran perusahaan teknologi asing, khususnya dari Amerika Serikat, di dalam ekosistem digital Tiongkok. Pembatasan tersebut dilakukan melalui kombinasi regulasi konten, keharusan penyimpanan data lokal, penyensoran ketat, serta tekanan politis dan administratif terhadap operasi bisnis perusahaan-perusahaan tersebut.

Salah satu bentuk konkret kebijakan ini dapat dilihat dalam pemblokiran Google pada tahun 2010, setelah perusahaan tersebut menolak untuk terus mematuhi aturan sensor internet yang ditetapkan oleh pemerintah Tiongkok. Google secara resmi memindahkan server pencariannya ke Hong Kong sebagai bentuk perlawanan, namun pemerintah Tiongkok tetap memblokir layanannya sepenuhnya dari daratan utama (Roberts, 2018). Kasus serupa terjadi pada LinkedIn, yang awalnya diberikan izin terbatas beroperasi di Tiongkok dengan syarat mematuhi sensor, tetapi pada tahun 2021, Microsoft

selaku pemilik platform tersebut akhirnya menutup operasi LinkedIn di Tiongkok dengan alasan "lingkungan operasional yang semakin menantang" serta kesulitan untuk menyeimbangkan antara tuntutan pemerintah Tiongkok dan nilai-nilai korporat asal AS (Deibert, 2020).

Apple, sebagai satu-satunya perusahaan teknologi besar AS yang masih dapat bertahan dalam sistem digital Tiongkok, juga harus melakukan penyesuaian besar untuk tetap beroperasi. Sejak tahun 2017, Apple dipaksa untuk menghapus ratusan aplikasi dari App Store Tiongkok, termasuk aplikasi berita asing, VPN, dan layanan komunikasi terenkripsi, sebagai bagian dari kepatuhan terhadap arahan CAC. Salah satu contoh yang menonjol terjadi pada tahun 2017, ketika Apple menghapus lebih dari 600 aplikasi VPN dari App Store atas permintaan pemerintah Tiongkok. Kemudian, pada tahun 2019 dan 2020, Apple juga menghapus aplikasi media seperti The New York Times serta aplikasi yang mendukung gerakan pro-demokrasi Hong Kong. Selain itu, Apple diwajikan menyimpan data pengguna Tiongkok di server lokal yang dikelola oleh perusahaan milik negara, Guizhou-Cloud Big Data, yang berada di bawah pengawasan langsung otoritas pemerintah China. Langkah ini secara langsung menimbulkan kekhawatiran terhadap privasi pengguna dan risiko akses negara terhadap data pribadi tersebut (Qiang, 2019). Hal ini memperlihatkan bahwa CAC bukan hanya melakukan sensor konten, tetapi juga menuntut kedaulatan penuh atas data digital warga negaranya, sekalipun harus menekan perusahaan global yang sebelumnya dominan di Tiongkok.

Kebijakan tersebut sejalan jika dilihat melalui kacamata teori Kedaulatan Digital, yang menegaskan bahwa setiap negara memiliki hak penuh untuk mengatur dan melindungi ruang digitalnya, termasuk dalam hal pengelolaan data, sensor informasi, dan kontrol terhadap aktor asing yang beroperasi dalam batas wilayah sibernya. Dalam konteks ini, tindakan CAC mencerminkan upaya aktif negara dalam mempertahankan otonomi digital dan melindungi infrastruktur informasinya dari pengaruh eksternal, sebagaimana yang dikedepankan dalam prinsip-prinsip dasar kedaulatan negara di era digital.

Respon dari perusahaan-perusahaan teknologi AS terhadap kebijakan CAC sangat bervariasi, tergantung pada posisi bisnis dan prinsip masing-masing perusahaan. Google memilih mundur penuh dan mengkritik keras sistem sensor Tiongkok, yang dinilai bertentangan dengan prinsip keterbukaan informasi. LinkedIn, awalnya mencoba mencari jalan tengah dengan menyensor konten tertentu, namun pada akhirnya tidak mampu mempertahankan posisi di tengah tekanan politis dan publik. Sementara Apple, meskipun tetap bertahan, dikritik karena terlalu patuh terhadap regulasi sensor dan dianggap mengorbankan prinsip-prinsip kebebasan berekspresi demi akses pasar (Roberts, 2018). Dalam konteks ini, CAC berhasil menekan perusahaan-perusahaan besar teknologi AS untuk memilih antara patuh

terhadap aturan negara atau kehilangan akses pasar Tiongkok. Kebijakan ini merefleksikan pendekatan Tiongkok yang memosisikan kedaulatan digital sebagai alat utama dalam menghadapi dominasi perusahaan asing, dengan CAC sebagai eksekutor regulasi dan kontrol. Kebijakan ini sebagai bagian dari strategi data nationalism, yakni di mana negara berupaya merebut kembali kendali atas infrastruktur, data, dan ruang digital dari aktor transnasional (Deibert, 2020).

Cyberspace Administration of China sebagai Instrumen Cyberpower dalam Persaingan Politik Cyber Global

Merujuk pada konsep Joseph Nye, kekuatan dalam ruang siber tidak hanya bersifat destruktif atau koersif (seperti serangan siber), tetapi juga mencakup aspek produktif dan persuasif, yakni menciptakan dan mengelola infrastruktur digital serta menyebarkan pengaruh ideologis dan narasi strategis. Nye menjelaskan bahwa cyberpower adalah "kemampuan untuk menggunakan ruang siber untuk menciptakan manfaat dan mempengaruhi orang lain dalam cara yang sejalan dengan tujuan nasional" (Nye, 2010). Dalam kerangka ini, CAC merupakan perwujudan konkret dari penggunaan ketiga bentuk kekuasaan tersebut dalam konteks digital Tiongkok. Dengan demikian, CAC dapat dipahami sebagai alat negara yang dirancang untuk mencapai berbagai kepentingan strategis melalui kontrol terhadap ruang digital.

Pertama, dalam dimensi keamanan nasional (national security), CAC bertugas sebagai garda depan negara dalam menjaga ruang digital domestik dari infiltrasi pengaruh asing, serangan siber, dan penyebaran informasi yang dianggap mengganggu stabilitas politik dan sosial. Sejak skandal Edward Snowden tahun 2013 yang mengungkap pengawasan digital global oleh Amerika Serikat, Tiongkok memandang infrastruktur digital global yang didominasi oleh perusahaan-perusahaan AS sebagai ancaman langsung terhadap kedaulatan digitalnya. Dalam konteks ini, CAC bertindak sebagai alat kekuatan koersif (coercive cyberpower). Hal tersebut dilakukan melalui pemblokiran dan pembatasan terhadap platform-platform teknologi asing seperti Google (yang diblokir sejak 2010), Facebook dan Twitter (yang diblokir sejak 2009), serta LinkedIn (ditutup operasionalnya pada tahun 2021). Tidak hanya memblokir, CAC juga mewajibkan perusahaan asing yang masih beroperasi, seperti Apple, untuk mematuhi regulasi ketat, termasuk penghapusan aplikasi yang bertentangan dengan regulasi sensor dan penyimpanan data di server lokal yang dikendalikan oleh perusahaan milik negara. Tindakan ini menggambarkan bentuk kekuatan koersif negara dalam mengontrol dan memaksa aktor asing untuk tunduk pada aturan main yang ditetapkan dalam ruang digital nasional.

Kedua, CAC juga menjalankan fungsi sebagai instrumen cyberpower dalam dimensi ekonomi

dan industri, yaitu bagaimana negara menggunakan kebijakan digital untuk mendukung perkembangan teknologi nasional dan menghambat dominasi asing. Menurut Nye, cyberpower dalam aspek ini mencakup kemampuan untuk menciptakan dan mengendalikan infrastruktur digital yang menjadi fondasi kekuatan ekonomi dan daya saing teknologi negara, (Nye, 2010). CAC berperan dalam mengatur seluruh aspek infrastruktur digital domestik, termasuk sertifikasi perangkat lunak, standar keamanan jaringan, kebijakan e-commerce, dan perlindungan data. Salah satu contohnya adalah penguatan perusahaan dalam negeri seperti Huawei, Alibaba, Baidu, dan Tencent yang mendapat dukungan struktural dan proteksi melalui kebijakan CAC. Dengan membatasi masuknya pesaing asing dan mendikte aturan main teknologi, CAC secara aktif mendorong decoupling digital dari Barat, terutama Amerika Serikat. Hal ini menunjukkan perwujudan nyata dari kekuatan produktif (productive power) sebagaimana dimaksud Nye, di mana negara memiliki kapasitas untuk menciptakan struktur teknologi yang berpihak pada tujuan nasional jangka panjang.

Ketiga, CAC memainkan peran sentral dalam membentuk pengaruh global Tiongkok melalui ruang digital, atau dalam istilah Nye disebut sebagai kekuatan persuasif (persuasive cyberpower). Dalam dimensi ini, kekuasaan digital digunakan untuk mengatur narasi, menyebarkan nilai-nilai nasional, serta melindungi identitas budaya dari dominasi ideologi asing. Tiongkok, melalui CAC, mengembangkan wacana alternatif terhadap model internet Barat yang menekankan keterbukaan dan kebebasan informasi. Sebaliknya, konsep cyberspace sovereignty atau kedaulatan dunia maya, yang menjadi pijakan kebijakan CAC, mengedepankan hak negara untuk mengatur arus informasi, data, dan infrastruktur sesuai konteks nasional masing-masing. Melalui forum seperti World Internet Conference di Wuzhen, Tiongkok berupaya melegitimasi model pengaturan internet yang bersifat tertutup, terpusat, dan dikendalikan oleh negara sebagai bentuk sah dari praktik kedaulatan digital. Nye menekankan bahwa cyberpower bukan hanya tentang kemampuan memaksa, tetapi juga "kemampuan untuk menarik dan menetapkan agenda" (Nye, 2010). Dalam hal ini, CAC menjadi alat utama Tiongkok dalam menciptakan norm entrepreneurship digital yang menantang dominasi narasi liberal global.

Dalam praktiknya, ketiga bentuk kekuatan ini koersif, produktif, dan persuasif tidak berjalan secara terpisah. CAC mengintegrasikan ketiganya dalam satu kerangka kebijakan nasional yang solid. Sebagai contoh, saat CAC memaksa Apple untuk menghapus aplikasi VPN dan menyimpan data di server dalam negeri, tindakan tersebut tidak hanya memiliki dampak keamanan (koersif) dan ekonomi (produktif), tetapi juga mengandung dimensi ideologis, yakni menunjukkan bahwa perusahaan asing pun harus tunduk pada nilai dan sistem Tiongkok jika ingin bertahan. Hal ini menegaskan bahwa CAC adalah instrumen strategis dalam menggabungkan hard dan soft cyberpower, sebagaimana digambarkan

Nye sebagai ciri khas dari kekuatan digital modern.

Dengan demikian, dalam kacamata teori cyberpower Joseph Nye (2010), CAC bukan hanya representasi dari kebijakan domestik, tetapi sekaligus simbol dari transformasi kekuatan negara di abad ke-21. CAC menjelma menjadi alat negara untuk memperkuat kedaulatan digital, mempertahankan keamanan nasional, membangun daya saing industri teknologi, serta menanamkan pengaruh ideologis di tataran global. Dengan menguasai ruang siber melalui kebijakan, regulasi, dan kontrol infrastruktur digital, Tiongkok melalui CAC telah memperlihatkan bagaimana sebuah negara dapat secara efektif menggunakan cyberpower sebagai alat utama dalam persaingan politik global di era digital.

KESIMPULAN

Penelitian ini menunjukkan bahwa pembentukan Cyberspace Administration of China (CAC) oleh Pemerintah Tiongkok bukan semata-mata langkah administratif, melainkan bagian dari strategi besar untuk mempertahankan kedaulatan digital dan mengurangi dominasi perusahaan teknologi asing, khususnya yang berasal dari Amerika Serikat. CAC berperan sebagai instrumen utama negara dalam mengatur, mengawasi, dan membatasi ruang digital domestik, sekaligus menjadi alat politik dalam menghadapi tekanan ideologis dan teknologi dari Barat.

Secara kelembagaan, CAC didirikan pada tahun 2014 di bawah koordinasi langsung Partai Komunis Tiongkok (PKT) dan Dewan Negara dengan tujuan mengonsolidasikan kontrol atas infrastruktur digital, pengawasan konten, dan pengelolaan data yang sebelumnya tersebar di berbagai lembaga. Secara fungsional, CAC menerapkan kebijakan seperti sensor digital, sistem identitas nyata (real-name registration), serta pembatasan arus data lintas batas sebagai bentuk perlindungan terhadap stabilitas politik dan keamanan nasional, sekaligus sebagai upaya membatasi pengaruh perusahaan asing seperti Google, Facebook, LinkedIn, dan Apple. Dalam kerangka teori Kedaulatan Digital, tindakan CAC dapat dipahami sebagai upaya strategis negara untuk merebut kembali otoritas atas ruang digitalnya dan menolak dominasi teknologi serta nilai-nilai liberal dari luar. Sementara itu, melalui teori Cyberpower Joseph Nye, CAC dilihat sebagai alat kekuasaan digital yang menggabungkan elemen koersif, produktif, dan persuasif untuk membentuk lanskap informasi domestik sesuai dengan kepentingan nasional.

Kebijakan-kebijakan ini tidak hanya berdampak pada situasi domestik Tiongkok, tetapi juga menciptakan ketegangan baru dalam hubungan dengan Amerika Serikat, khususnya dalam isu teknologi dan hak digital global. Dengan demikian, pembentukan CAC merepresentasikan upaya strategis Tiongkok dalam mengonsolidasikan kekuasaan negara di ruang siber melalui

institusi yang terpusat, dengan landasan pada narasi kedaulatan digital dan perlindungan terhadap keamanan nasional. Pembentukan dan peran CAC menunjukkan bagaimana Tiongkok memanfaatkan kebijakan digital sebagai alat untuk memperkuat kontrol negara atas ruang siber, mempertahankan stabilitas politik domestik, serta merespons tantangan dari dominasi teknologi asing, khususnya Amerika Serikat. Hal ini mencerminkan transformasi pendekatan keamanan digital Tiongkok yang bersifat defensif sekaligus proaktif dalam menghadapi dominasi teknologi asing dalam lanskap digital global.

DAFTAR PUSTAKA

Allison, G. (2018). *The Great Tech Rivalry: China vs the U.S*. Harvard Kennedy School Belfer Centre.

Attrill, N., & Fritz, A. (2021). *China's Cyber Vision: How the Cyberspace Administration of China is Building a New Consensus on Global Internet Governance*. Australian Strategic Policy Institute.

Brady, A. M. (2009). *Marketing dictatorship: Propaganda and thought work in contemporary China*. Rowman & Littlefield Publishers.

Buzan, B. (1983). *People, States and Fear: The National Security Problem in International Relations*. Brighton: Wheatsheaf Books.

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (2nd ed.). London: Harvester Wheatsheaf.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge University Press.

Chander, A., & Sun, H. (Eds.). (2023). *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.

Chen, Y. (2025). The Accuracy and Biases of AI-Based Internet Censorship in China. *Journal of Research in Social Science and Humanities*, 4(2), 27–36.

Chertoff, M., & Simon, T. (2021). *The Impact of Chinese Cyber Policies on Global Norms*. Council on Foreign Relations.

Clementi, D. (2024). Between Digital Surveillance and Individual Protection: A Juridical and Comparative History of the Cyberspace Administration of China. *Rivista di Digital Politics*, 4(2), 343–370.

Clementi, E. (2023). China’s Digital Leviathan: Surveillance, Sovereignty, and the Cyberspace Administration of China. *Journal of East Asian Studies*, 25(2), 133–157.

Creemers, R. (2017). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 26(103), 85-100.

Creemers, R. (2018). China’s Social Credit System: An Evolving Practice of Control. *SSRN*

Electronic Journal.

Creemers, R. (2020). China's Conception of Cyber Sovereignty. In *Governing Cyberspace: Behaviour, Power and Diplomacy* (pp. 107-145).

Creemers, R. (2022). China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), tyac011.

Deibert, R.J. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal Books.

Deibert, R.J. (2020). *Reset: Reclaiming the Internet for Civil Society*. Toronto: House of Anansi Press.

Fang, B. (2018). Digital Sovereignty: The Role of the Cyberspace Administration of China in Internet Regulation and Control. *International Journal of Cyber Policy and Governance*, 5(1), 1–16.

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace.

Feldstein, S. (2021). *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. Oxford University Press.

Gao, X. (2022). An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator*, 57(3), 15–30.

Hong, S. H. (2020). Technologies of Speculation: The Limits of Knowledge in a Data-Driven Society. In *Technologies of Speculation*. New York University Press.

Hong, Y., & Goodnight, G. T. (2022). How to Think About Cyber Sovereignty: The Case of China. In *China's Globalizing Internet* (pp. 7-25). Routledge.

Hong, Y., & Goodnight, G.T. (2022). Authoritarian Information Order: The Digital Construction of Cyber Sovereignty in China. *Communication and the Public*, 7(1), 23–39.

Hough, P. (2008). *Understanding Global Security*. London: Routledge.

Jia, M. (2024). Authoritarian Privacy. *The University of Chicago Law Review*, 91(3), 733–810.

Jiang, Y. (2012). *Cyber-Nationalism in China: Challenging Western Media Portrayals of Internet Censorship in China*. University of Adelaide Press.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*, 111(3), 484–501.

Kokas, A. (2022). *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*.

Kokas, A. (2023). *Trafficking Data: How China is Winning the Battle for Digital Sovereignty*. Oxford University Press.

Lamont, C. (2021). *Research Methods in International Relations*.

Li, X. (2023). Data Politics in China: The Role of CAC in Managing Digital Society. *Asian Journal of Communication*, 33(1), 43–60.

Li, Y. (2023). Cyberspace and Social Governance: The Role of the Cyberspace Administration

Office. In *Handbook on Local Governance in China* (pp. 224-243). Edward Elgar Publishing.

MacKinnon, R. (2009). China's Censorship 2.0: How Companies Censor Bloggers. *First Monday*.

Miao, W., & Lei, W. (2016). Policy Review: The Cyberspace Administration of China. *Global Media and Communication*, 12(3), 337-340.

Miao, W., Zhu, H., & Chen, Z. (2018). Who's in Charge of Regulating the Internet in China: The History and Evolution of China's Internet Regulatory Agencies. *China Media Research*, 14(3).

Moore, G. J. (2023). Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies. *Journal of Chinese Political Science*, 28(1), 151-167.

Mozur, P., & Zhong, R. (2021). Apple Bows to Beijing's Rules, and iCloud Data Is Now Controlled by China. *The New York Times*.

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Nye, J. S. (2010). *Cyberpower*. Cambridge, MA: Harvard University Belfer Center for Science and International Affairs.

Portrait, A. (2023). The Cyberspace Administration of China. In *The Emergence of China's Smart State* (pp. 9).

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's Cybersecurity Law. *Computer Law & Security Review*, 34(6), 1342–1354.

Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*, 30(1), 53–67.

Roberts, M. (2018). *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton University Press.

Schaefer, K. (2021). *China's Techno-Authoritarianism: How the CAC Shapes the Future of Data Governance*. Trivium China Briefing Report.

Schia, N. N., & Gjesvik, L. (2022). *China's Cyber Sovereignty*. Norwegian Institute for International Affairs (NUPI).

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Hachette UK.

Segal, A. (2018). When China Rules the Web: Technology in Service of the State. *Foreign Affairs*, 97(5), 10–18.

Segal, A. (2020). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *Current History*, 119(816), 9–14.

Wang, A. (2020). Cyber Sovereignty at Its Boldest: A Chinese Perspective. *Ohio St. Tech. LJ*, 16, 395.

Wang, Q., & Luo, X. (2021). China's Cyberspace Administration and the New Era of Internet Governance. *Journal of Contemporary Asia*, 51(4), 567–583.

Xu, B., & Albert, E. (2014). Media Censorship in China. *Council on Foreign Relations*, 25(1), 243–249.

Yang, G. (2009). *The Power of the Internet in China: Citizen Activism Online*. Columbia University Press.

Zeng, J., Stevens, S., & Chen, X. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics & Policy*, 45(3), 432–464.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of Internet Sovereignty. *Politics & Policy*, 45(3), 432–464.

Zhang, A., & Gilli, A. (2021). Digital Authoritarianism Goes Global: China's Cyber Sovereignty Doctrine and Its International Influence. *Strategic Studies Quarterly*, 15(2), 40–63.

Zhang, Y., & Gilley, B. (2021). Authoritarian Resilience in the Digital Era: Surveillance, Propaganda, and the Chinese Communist Party. *Journal of Democracy*, 32(2), 59–73.

Zhao, Y. (2008). *Communication in China: Political Economy, Power, and Conflict*. Lanham, MD: Rowman & Littlefield Publishers.

Zheng, Y. (2007). *Technological Empowerment: The Internet, State, and Society in China*. Stanford University Press.