JIMR: Journal Of International Multidisciplinary Research

http://azramedia-indonesia.azramediaindonesia.com/index.php/JIMR/index
DOI : https://doi.org/10.62668/jimr.v4i01.934
Email : info@azramediaindonesia.com

Open Access

APLIKASI DOMESTIK SEBAGAI INSTRUMEN KEDAULATAN DIGITAL DAN KEAMANAN NASIONAL: STUDI STRATEGIS ATAS PENDEKATAN TIONGKOK

Andi Anggun Ainul Khaliq Asbullah*[1], Imam Fadhil Nugraha[2]
Universitas Hasanuddin, Indonesia
*Corresponding Author: andianggun53@gmail.com

Info Article
Received :
03 April 2025
Revised :
03 May 2025
Accepted :
02 June 2025
Publication :
30 June 2025

Keywords:
Digital Sovereignty, National Security, Domestic Applications
Kata Kunci:
Kedaulatan Digital, Keamanan Nasional, Aplikasi Domestik

Abstract: *The development of information and communication technology has encouraged countries to build new defense strategies to deal with non-traditional threats, including threats to digital sovereignty. China is one country that actively develops and utilizes domestic digital apps as a strategic instrument to protect national security and limit foreign influence in cyberspace. This research aims to analyze how China's strategy of using domestic applications functions as a digital defense fortress and an instrument of sovereignty in the face of global cyber geopolitical dynamics. This research uses a qualitative approach with a descriptive narrative method and literature review. The results show that banning foreign platforms, developing domestic applications, and digital payment systems are part of China's overall strategy in controlling domestic data and information flows. The conclusion of this research confirms that China is not only building technological independence, but also creating a closed and controlled cyberspace as an effort to maintain digital sovereignty and prevent external intervention in national stability China's domestic apps.*

Abstrak: Perkembangan teknologi informasi dan komunikasi telah mendorong negara-negara untuk membangun strategi pertahanan baru dalam menghadapi ancaman non-tradisional, termasuk di dalamnya ancaman terhadap kedaulatan digital. Tiongkok merupakan salah satu negara yang secara aktif mengembangkan dan memanfaatkan aplikasi digital domestik sebagai instrumen strategis untuk melindungi keamanan nasional dan membatasi pengaruh asing dalam ruang siber. Penelitian ini bertujuan untuk menganalisis bagaimana strategi penggunaan aplikasi domestik oleh Tiongkok difungsikan sebagai benteng pertahanan digital serta instrumen kedaulatan dalam mengha dapi dinamika geopolitik siber global. Metode penelitian dengan pendekatan kualitatif, metode deskriptif naratif dan analisis kajian literatur. Hasil penelitian menunjukkan bahwa pelarangan platform asing, pengembangan aplikasi domestik, dan sistem pembayaran digital merupakan bagian dari strategi menyeluruh Tiongkok dalam mengendalikan arus data dan informasi domestik. Kesimpulan dari penelitian ini menegaskan bahwa Tiongkok tidak hanya membangun kemandirian teknologi, tetapi juga menciptakan ruang siber yang tertutup dan terkendali sebagai upaya mempertahankan kedaulatan digital serta mencegah intervensi eksternal terhadap stabilitas nasional.

INTRODUCTION

Di era transformasi digital yang semakin pesat, teknologi informasi dan komunikasi telah berkembang dan menjadi pondasi utama dalam berbagai aspek kehidupan berbangsa dan bernegara, mulai dari sektor ekonomi, politik, sosial, hingga pertahanan dan keamanan. Kemajuan dalam teknologi digital khususnya internet, telah membuka peluang yang besar bagi negara-negara untuk memperluas jangkauan diplomasi dan pengaruhnya di dunia internasional. Namun, di sisi lain perkembangan ini juga membawa tantangan yang kompleks terhadap keamanan nasional suatu negara. Perang tidak lagi semata-mata terjadi dalam bentuk militer, melainkan telah bergeser ke ranah baru yang dikenal dengan ruang siber (*cyberspace*) (Sharma, 2025). Dalam ruang ini, aktor-aktor negara dan non-negara saling berkompetisi untuk memperoleh dominasi informasi dan pengaruh strategis yang kemudian menimbulkan ancaman baru terhadap kedaulatan dan stabilitas suatu negara.

Keamanan siber kini menjadi bagian tak terpisahkan dalam kerangka keamanan nasional di berbagai negara. Perkembangan teknologi digital yang begitu cepat telah menciptakan dimensi ancaman baru yang tidak lagi bersifat konvensional. Ancaman seperti peretasan data, penyebaran disinformasi, hingga manipulasi opini publik melalui platform digital berpotensi melemahkan stabilitas politik, ekonomi, dan sosial suatu negara. Ruang siber tidak lagi dipandang sebagai sekadar media komunikasi, melainkan telah bertranformasi menjadi arena strategis tempat berlangsungnya kompetisi kekuasaan dan pengaruh antara berbagai aktor negara dan non-negara. Hal ini menuntut negara tidak lagi hanya bertanggung jawab menjaga perbatasan fisik, tetapi juga dituntut untuk mengamankan perbatasan digitalnya.

Salah satu isu dalam keamanan siber global adalah dominasi platform digital yang berasal dari perusahaan teknologi asing. Sejumlah perusahaan teknologi besar asal Amerika Serikat seperti *Google, Apple, Meta* (yang mencakup *Facebook*, *Instagram*, Whatsapp) *Amazon*, dan *Microsoft* telah menguasai sebagian besar infrastruktur digital dan aplikasi yang digunakan masyarakat global (Cronin, 2023). Ketergantungan negara-negara terhadap platform-platform ini menciptakan ketidakseimbangan dalam kontrol atas data, privasi pengguna, serta informasi lintas batas negara. Situasi ini memunculkan kekhawatiran terkait kedaulatan digital, di mana negara-negara kehilangan kendali atas data warganya dan menjadi rentan terhadap intervensi ekternal. Dalam hal ini, dominasi platform digital asing bukan hanya persoalan ekonomi digital

global, melainkan juga merupakan tantangan strategis yang berkaitan erat dengan keamanan nasional dan independensi kebijakan suatu negara dalam ranah siber.

Melihat dinamika tersebut, muncul berbagai respons dari negara-negara yang berupaya mengurangi ketergantungan terhadap platform digital asing sebagai bagian dari strategi mempertahankan kedaulatan digital nasional. Tiongkok merupakan salah satu negara yang secara aktif mengembangkan alternatif terhadap dominasi ekosistem digital global yang didominasi oleh perusahaan teknologi asing (Fitzgerald, Wu, & Sandel, 2022, p. 1). Berbeda dengan banyak negara lain yang membiarkan platform asing secara luas, Tiongkok memilih pendekatan yang lebih proaktif terhadap ruang digital domestiknya dengan membatasi dan bahkan melarang sejumlah platform asing. Sebagai gantinya, Tiongkok mendorong pertumbuhan teknologi domestiknya dengan mengembangkan platform-platform seperti *Wechat, Aliplay, Douyin* (*TikTok* Tiongkok), *Baidu*, dan berbagai platform lain yang beroperasi dalam sistem regulasi yang dikontrol ketat oleh negara.

Langkah yang dilakukan Tiongkok ini tidak hanya dilihat sebagai upaya mempertahankan kontrol politik, tetapi juga sebagai strategi dalam menjaga keamanan nasional di era digital. Dengan mengembangkan aplikasi dometiknya sendiri, Tiongkok berusaha memastikan bahwa data warganya dikelola dan disimpan dalam yurisdiksi nasional, sehingga terhindar dari potensi eksploitasi atau intervensi oleh aktor asing. Dalam kerangka studi keamanan non-tradisional, pendekatan Tiongkok ini mencerminkan perluasan konsep keamanan yang tidak lagi terbatas pada ancaman militer, tetapi mencakup dimensi teknologi digital. Hal ini juga menunjukkan bagaimana negara memosisiskan diri sebagai aktor utama dalam mengatur dan mengamankan ruang siber. Pendekatan seperti ini juga menyoroti bagaimana cara pandang Tiongkok dalam memahami ancaman dan bagaimana teknologi digital dapat digunakan sebagai instrumen kedaulatan.

Pemanfaatan aplikasi domestik oleh Tiongkok sebagai instrumen dalam menjaga kedaulatan dan keamanan nasional merupakan bagian dari respon terhadap tantangan dunia digital yang semakin kompleks. Dalam menghadapi risiko yang muncul dari ketergantungan terhadap teknologi asing dan ancaman terhadap keamanan nasional, Tiongkok mengembangkan pendekatan dalam mengelola ruang siber. Untuk memahami lebih dalam mengenai bagaimana Tiongkok memanfaatkan aplikasi domestik menjadi bagian dalam menjaga kedaulatan digital dan membentuk sistem

keamanan nasional yang responsif terhadap ancaman ruang siber yang kompleks, penulis menemukan berbagai literatur yang membahas isu ini.

Literatur pertama yaitu penelitian yang dilakukan oleh Rogier Creemers yang berjudul ”*The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy*”. Dalam tulisannya, Creemers menjelaskan bagaimana konsep *cybersecurity* di Tiongkok berkembang secara konseptual, institusional, dan regulatif, dimana konsep ini sangat berbeda dengan pendekatan negara-negara barat. Penelitian ini menganalisis bagaimana para pemimpin Tiongkok sejak tahun 1990-an telah membentuk kerangka keamanan digital yang berorientasi pada kebutuhan untuk menjaga stabilitas rezim dan kedaulatan nasional di tengah kemajuan teknologi yang pesat (Creemers, 2023, p. 175). Hal ini menunjukkan bahwa pendekatan Tiongkok terhadap keamanan digital tidak hanya bersifat teknis, tetapi juga dengan pertimbangan politik dan ideologis yang menekankan sentralisasi kekuasaan negara dalam merespons dinamika dunia digital.

Penelitian tersebut juga mengungkapkan bahwa dalam perspektif Tiongkok, *cybersecurity* tidak hanya dipahami sebagai perlindungan terhadap peretasan atau gangguan teknis, melainkan mencakup aspek ideologis, sosial, poltik, dan ekonomi. Pemerintah Tiongkok memandang dunia digital sebagai ruang strategis yang rentan terhadap intervensi asing hingga ancaman terhadap legitimasi Partai Komunis Tiongkok (PKT) (Creemers, 2023, pp. 175-176). Oleh karena itu, kebijakan keamanan siber di Tiongkok diarahkan untuk membangun kedaulatan digital melalui penguatan terhadap infrastuktur nasional, regulasi ketaat terhadap data, dan pengawasan ketata terhadap konsten serta aktivitas digital. Dengan pendekatan ini, kebijakan keamanan siber Tiongkok berfungsi sebagai benteng kedaulatan digital nasional, di mana mekanisme pengawasan dan regulasi ketat yang melindungi ruang digital dari campur tangan asing dan menjaga legitimasi rezim.

Literatur kedua yaitu penelitian yang dilakukan oleh Tai Ming Cheung yang berjudul “*The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities*”. Penelitian ini mengkaji bagaimana Tiongkok membangun industri keamanan sibernya dengan menyeimbangkan antara kepentingan keamanan nasional, pertimbangan geopolitik, dan tujuan pembangunan teknologi dan ekonomi. Cheung menyoroti bahwa strategi keamanan siber Tiongkok sangat dipengaruhi oleh pendekatan *techno-nationalism*, yaitu pandangan bahwa penguasaan teknologi harus menjadi alat untuk memperkuat kekuatan dan keamanan

nasional (Cheung, 2018, pp. 4-5). Dalam hal ini, pemerintah mengambil peran dominan sebagai regulator, investor, dan pengguna, sembari mengkoordinasikan hubungan dengan aktor-aktor lainnya seperti militer, lembaga keamanan negara, serta perusahaan teknologi nasional.

Cheung menunjukkan bahwa sejak awal 2000-an, Tiongkok secara aktif mengembangkan strategi keamanan siber yang tidak hanya berfokus pada perlindungan teknis, tetapi juga menekankan kedaulatan digital dan kontrol informasi dalam negeri sebagai bagian dari agenda politik nasional (Cheung, 2018, p. 10). Dalam hal ini, Tiongkok melihat internet bukan sekedar alat komunikasi atau ekonomi, tetapi sebagai arena pertarungan ideologis dan geopolitik yang menuntu kehadiran negara sevara aktif dalam mengatur dan mengawasi aktifitas digital. Oleh sebab itu, kebijakan siber Tiongkok dirancang untuk memperkuat kendali negara terhadap informasi domestic melalui pengembangan *firewall* nasional, pembatasan platform asing, serta promosi aplikasi domestic seperti WeChat, Alibaba, dan Tiktok versi lokal (Douyin) yang beroperasi sesuai dengan regulasi pemerintah.

Literatur ketiga berjudul *The Rise and Influence of Weibo (Microblogs) in China* oleh Eric Harwit. Penelitian ini membahas perkembangan pesan dan pengaruh platform microblog seperti Weibo di Tiongkok, terutama dalam aspek politik, sosial, dan komersial. Harwit menjelaskan meskipun berada dalam ruang digital yang diawasi ketat oleh negara, Weibo tetap menjadi wadah ekspresi publik dan alat komunikasi efektif antar warga dan pemerintah (Harwit, 2014, p. 1085). Meskipun terdapat ruang untuk kebebasan berekspresi di ruang digital, kebebasan tersebut tetap berada dalam pengawasan ketat pemerintah. Keberadaan Weibo menunjukkan adanya dinamika antara kebutuhan negara untuk mengontrol informasi dan tekanan dari masyarakat untuk memperoleh ruang diskusi daring. Oleh karena itu, Tiongkok menjalankan sistem pengawasan ruang digital yang ketat sebagai instrument untuk mempertahankan kontrol negara atas informasi, membatasi potensi ancaman, dan melindungi keamanan nasional dari pengaruh eksternal.

Literatur sebelumnya menunjukkan bahwa pemanfaatan aplikasi-aplikasi domestik Tiongkok tidak hanya dilatarbelakangi oleh pertimbangan teknis semata, melainkan juga oleh kepentingan politik, ideologis, dan keamanan negara. Pada penelitian pertama, Rogier Creemers menyoroti pentingnya kerangka konseptual, institusional, dan regulatif untuk menjaga stabilitas rezim dan kedaulatan nasional melalui pengawasan dan regulasi digital. Di samping itu, penelitian kedua oleh Tai

Ming Cheung menjelaskan bagaimana *techno-nastionalism* menggerakkan pemerintah Tiongkok untuk mengembangkan industri keamanan siber nasional, dengan memposisikan negara sebagai regulator, investor, dan pengguna teknologi domestik. Sementara itu, pada literatur ketiga oleh Eric Harwit menggambarkan dinamika interaksi antara kontrol negara dan ruang ekspresi publik melalui platform domestik Tiongkok sep (Weibo).

Berdasarkan ketiga literatur tersebut, terlihat keterkaitan dalam memahami pemanfaatan aplikasi domestik Tiongkok sebagai instrumen kedaulatan digital dan keamanan nasional negara, yang bisa dilihat pada kesatuan kerangka konseptual dan regulative yang menjelaskan sentralisasi kontrol negara atas ruang siber, strategi *techno-nationalism* yang menjadikan penguasaan teknologi domestik sebagai pilar kekuatan nasional, serta praktik pengawasan konten dan ekspresi publik yang dipadu dalam platform seperti Weibo. Sehingga ketiga penelitian ini memberikan pijakan yang kuat dalam mengkaji lebih dalam mengenai bagaimana aplikasi-aplikasi domestik berperan sebagai instrumen kedaulatan digital dalam mengintegrasikan kebijakan keamanan nasional perlu diteliti lebih lanjut.

Kajian ini semakin penting untuk memahami sejauh mana aplikasi domestik benar-benar berfungsi sebagai instrument kedaulatan digital dan keamanan nasional. Oleh karena itu, penelitian ini akan membahas bagaimana Tiongkok menggunakan aplikasi domestik sebagai instrument dalam menjaga kedaulatan digital dan keamanan nasional, strstrategi apa yang digunakan dan bagaimana aplikasi-aplikasi tersebut diintegrasikan ke dalam kerangka kebijakan nasional yang lebih luas. Pemahaman yang mendalam terhadap pendekatan ini tidak hanya penting secara teoritis, tetapi juga relevan bagi negara-negara lain dalam mengelola ruang digital yang berdaulat. Dengan demikian, penelitian ini diharapkan mampu memberikan analisis kritis terhadap cara Tiongkok menghadirkan kembali peran sentralnya dalam ruang digital sebagai bentuk perlindungan atas kepentingan nasionalnya.

METHOD

Penelitian ini menggunakan metode *narrative descriptive* dalam pendekatan kualitatif dengan kajian literatur (*literature review*) untuk memahami strategi Tiongkok dalam memanfaatkan aplikasi digital domestik sebagai instrumen dalam upaya menjaga kedaulatan digital dan memperkuat keamanan nasional. Melalui metode ini, penulis berupaya menyusun narasi analitis yang menggambarkan dinamika Tiongkok dalam

menghadapi tantangan dominasi platform digital asing serta upaya negara tersebut dalam menciptakan ekosistem digital yang berdaulat. Penelitian ini memanfatkan berbagai sumber literatur seperti buku, artikel ilmiah, jurnal akademik, laporan penelitian, serta publikasi yang kredibel dan relevan. Data yang dikumpulkan akan dianalisis untuk mengidentifikasi pola-pola kebijakan dan s trategi yang digunakan Tiongkok dalam konteks keamanan digital.

Dengan menggunakan pendekatan *narrative descriptive*, penulis dapat menarasikan bagaimana strategi digital Tiongkok terbentuk sebagai respon terhadap ancaman keamanan siber, serta bagaimana negara tersebut memanfaatkan regulasi, kontrol data, dan inovasi teknologi sebagai alat untuk mempertahankan kedaulatan nasional di era digital. Kajian terhadap kebijakan digital ini dilakukan dengan menyoroti kebijakan pelarangan platform asing, pengembangan infrastruktur digital lokal, serta pembentukan kerangka hukum yang ketat dalam pengelolaan ruang siber. Selain itu, penelitian ini juga akan menelaah peran negara sebagai aktor pertama dalam mengatur interaksi digital warganya, serta bagaimana kontrol negara terhadap data domestik menjadi bagian dari strategi geopolitik digital Tiongkok. Dengan demikian, analisis yang dihasilkan diharapkan mampu memberikan pemahaman yang komprehensif mengenai bagaimana aplikasi domestik menjadi bagian dalam menjaga kedaulatan digital dan membentuk sistem keamanan nasional yang responsif terhadap ancaman ruang siber yang kompleks.

RESULTS AND DISCUSSION

Results

Dalam beberapa dekade terakhir, perkembangan teknologi komunikasi telah mengubah cara negara-negara memandang keamanan nasional. Ruang digital yang sebelumnya hanya dianggap sebagai media pertukaran informasi, kini menjadi dimensi baru dalam geostrategi dan pertahanan nasional. Negara-negara tidak lagi hanya menghadapi ancaman fisik dari luar batas wilayahnya, tetapi juga tantangan digital yang tak kasat mata. Perkembangan teknologi informasi dan komunikasi menjadikan data sebagai alat strategis baru dalam geopolitik global. Serangan siber, pencurian data, dan manipulasi digital kini menjadi senjata baru dalam konflik antarnegara. Negara yang tidak siap secara digital bisa menjadi korban serangan tanpa menyadarinya secara lansung. Hal ini menunjukkan adanya reorientasi ancaman yang menuntut negara untuk memperkuat kapasitas pertahanan sibernya.

Reorientasi Keamanan Nasional di Era Digital

Di masa depan, keamanan nasional akan semakin ditentukan oleh kecakapan digital suatu negara, karena ancaman kini tidak lagi terbatas pada invasi fisik atau konflik konvensional. Ancaman digital kini menjadi senjata baru dalam era digital, di mana negara-negara saling menguji ketahanan satu sama lain tanpa harus menyebrangi perbatasan fisik (Kaloudis, 2024, p. 5) . Ancaman digital tidak bisa ditanggulangi hanya dengan pendekatan defensif, tetapi juga harus proaktif dengan mengembangkan teknologi dalam negeri dan membentuk kerangka hukum digital yang kuat. Perbatasan digital harus diperkuat, bukan hanya untuk membatasi akses asing yang dapat membahayakan tetapi juga untuk melindungi kedaulatan dan keamanan nasional suatu negara. Tanpa penguatan perbatasan digital, suatu negara akan retan menjadi objek dominasi teknologi dari aktor asing, yang pada akhirnya akan melemahkan posisi geopolitiknya.

Negara-negara perlu memahami bahwa infrastrukur digital seperti pusat data, server, dan kabel bawah laut adalah aset yang perlu dilindungi. Serangan terhadap infrastruktur tersebut dapat menimbulkan kekacauan di bidang ekonomi, politik, hingga layanan publik. Ketika pusat data dirusak atau diretas, jutaan data penting dapat hilang, dicuri, atau bahkan dimanipulasi untuk kepentingan tertentu. Dengan meningkatnya intensitas ancaman di ruang siber, negara perlu memperkuat kapasitas mereka dalam memitigasi risiko-risiko ancaman yang muncul (Safitr, Lubis, & Fakhrurroja, 2023, p. 9). Langkah ini tidak hanya penting untuk melindungi kedaulatan digital, tetapi juga untuk menjaga stabilitas nasional secara menyeluruh. Negara yang gagal membangun sistem perlindungian digital akan lebih rentan terhadap serangan yang dapat merusak tatanan sosial dan politik. Dalam era di mana batas-batas negara tidak hanya bersifat geografis tetapi juga digital, perlindungan terhadap infrastruktur digital bukanlah pilihan, melainkan keharusan.

Aplikasi Domestik Sebagai Alat Pertahanan Digital

Di tengah ketergantungan tinggi terhadap teknologi, banyak negara menghadapi dilema besar. Di satu sisi, mereka membutuhkan platform digital untuk memodernisasi sistem komunikasi, pelayanan publik, pendidikan, hingga sistem keamanan nasional. Namun di sisi lain, sebagian besar platform yang dominan di dunia digital berasal dari negara besar yang memiliki kekuatan ekonomi, teknologi, dan politik global. Ketidakseimbangan ini mengarah pada situasi di mana negara-negara berkembang dan

bahkan negara maju kehilangan kendali penuh atas infrasturktur informasinya sendiri. Platform seperti *Google, Facebook, Instagram, TikTok, WhatsApp,* hingga *Amazon* dan *Microsoft* telah menjadi tulang punggung kehidupan digital global. Dominasi teknologi ini menciptakan ketergantungan baru, di mana negara-negara pengguna berada dalam posisi pasif dan rentan terhadap kebijakan perusahaan maupun negara asal platform tersebut. Dalam kondisi seperti ini, kedaulatan digital menjadi semakin relevan, negara tidak hanya dituntut untuk melindungi warganya dari ancaman digital, tetapi juga perlu membangun kapasitas teknologi domestik yang mampu bersaing dan mandiri.

Dalam kerangka keamanan non-tradisional, negara bukan lagi satu-satunya aktor yang berperan dalam pertahanan. Dibutuhkan kerja sama yang lebih erat antara pemerintah, sektor industri teknologi, perusahaan keamanan digital, hingga masyarakat sipil untuk mengahadapi ancaman digital (Amoo, Atadoga, Abrahams, & et.al, 2024, p. 214). Melalui pertukaran informasi, pemanfaatan sumber daya bersama, serta penerapan strategi yang efektif, keempat aktor tersebut dapat membangun sistem pertahanan digital yang kuat terhadap ancaman yang terus berkembang. Kerja sama ini memungkinkan respon yang lebih cepat dan terkoordinasi terhadap berbagai bentuk serangan siber. Masing-masing aktor memiliki peran yang saling melengkapi dalam menciptakan sistem pertahanan digital.

Kerja sama antar aktor-aktor dalam mengembangkan teknologi digital sangat dibutuhkan untuk membangun ekosistem digital nasional yang mandiri dan berdaulat. Kerja sama ini penting dalam menciptakan infrastruktur digital yang kuat, aman, dan sesuai dengan kepentingan nasional. Salah satu langkah yang dapat dilakukan adalah dengan mengembangkan aplikasi domestik yang memungkinkan negara untuk mengontrol arus data dan informasi tanpa campur tangan pihak asing. Dengan demikian, negara tidak hanya mengurangi ketergantungan pada platform digital asing yang berpotensi menjadi alat intervensi, tetapi juga memperkuat kemampuan dalam mengelola data secara mandiri. Aplikasi domestik yang dikembangkan dengan standar keamanan tinggi dan berdasarkan regulasi nasional dapat menjadi instrumen dalam menjaga integritas informasi, mencegah kebocoran data, serta memperkuat kepercayaan publik terhadap sistem digital nasional.

Strategi Digital Tiongkok dan Dampaknya Terhadap Keamanan Nasional

Pendekatan melalui pengembangan aplikasi digital ini menjadi bagian dari strategi Tiongkok dalam membangun kedaulatan digitalnya yang berkaitan langsung

dengan sistem keamanan nasional Tiongkok. Sebagai langkah konkretnya, pemerintah Tiongkok menjalin kerja sama erat dengan perusahaan-perusahaan teknologi besar dalam negeri seperti *Huawei, Tencent, Alibaba,* dan perusahaan teknologi lainnya. Kerja sama ini bertujuan untuk mempercepat inovasi dalam mengembangkan aplikasi domestik, mengelola data berskala besar (*big data*), dan dalam bidang jaringan internet 5G (Melnik, 2019, pp. 28-33). Melalui kerja sama ini, Tiongkok berupaya mengurangi ketergantungan pada teknologi asing, dan membangun sistem digital yang sepenuhnya dikendalikan negara. Perusahaan-perusahaan tersebut tidak hanya berperan sebagai pengembang teknologi, tetapi juga sebagai mitra dalam menjalankan kebijakan pemerintah di ruang digital. Kerja sama ini membantu pemerintah dalam menciptakan eksosistem digital yang tertutup namun kuat, dengan fokus utama pada perlindungan data, pengawasan informasi, dan pebguatan sistem keamanan siber.

Dalam perpektif Tiongkok, konsep *cyber sovereignty* merujuk pada hak eksklusif suatu negara untuk mengatur, mengawasi, dan mengendalikan internet dalam batas wilayahnya, termasuk mengendalikan infrastruktur digital, mengatur konten, dan menetapkan regulasi data lintas batas. Bagi Tiongkok, ruang digital merupakan perpanjangan dari kedaulatan negara yang sah, sama halnya dengan wilayah daratan, laut, dan udara. Pendekatan ini berbeda dengan prinsip *digital openness* yang dianut oleh negara-negara barat seperti Amerika Serikat yang lebih menekankan pada keterbukaan dan kebebasan informasi. Dalam pandangan negara-negara barat, internet dipandang sebagai ruang terbuka yang bersifat transnasional dan tidak boleh dibatasi oleh otoritas negara secara sewenang-wenang.

Tiongkok menjadi salah satu negara yang secara aktif membentuk dan mengembangkan ekosistem digital sendiri sesuai dengan kepentingan nasional. Dalam menghadapi tantangan global di ruang digital, Tiongkok memosisikan dirinya sebagai negara yang memiliki pendekatan paling berani. Pemerintah Tiongkok memilih jalur kemandirian teknologi dengan mengembangkan ekosistem digital nasional yang tertutup. Langkah ini berakar pada pemahaman bahwa ruang digital adalah bagian dari kedaulatan negara yang harus dikontrol secara ketat demi stabilitas nasional (Drinhausen & Lee, 2021). Salah satu ciri utama strategi digital Tiongkok adalah pembatasan terhadap platform asing dan promosi besar-besaran terhadap aplikasi domestik. Platform asing seperti *Google, Facebook, Instagram,* dan *Twitter* diblokir di Tiongkok, sementara masyarakat diarahkan untuk menggunakan aplikasi domestik seperti *WeChat, Douyin, Baidu, Weibo, Alipay*, dan aplikasi domestik lainnya.

Aplikasi-aplikasi ini bukan hanya alat komunikasi atau transaksi, tetapi juga instrumen negara untuk memantau, mengelola, dan mengarahkan dinamika sosial digital sesuai dengan kebijakan nasional.

Beberapa aplikasi dometik yang dimiliki Tiongkok memiliki peran masing-masing dalam menjaga kedaulatan digital dan memperkuat keamanan nasional melalui kontrol menyeluruh terhadap aktivitas daring masyarakat. *WeChat* sebagai pengganti WhatApp, yang merupakan sarana komunikasi utama masyarakat Tiongkok. Melalui aplikasi ini, masyarakat dapat bertukar pesan, melakukan penggilan suara dan video, yang memiliki fitur yang hampir sama dengan WhatsApp. Sementara itu, Douyin berperan sebagai pengganti TikTok versi internasional dan menjadi platform video pendek yang sangat popular di kalangan generasi muda Tiongkok. Selanjutnya, Baidu sebagai pengganti Google yang berperan menjadi mesin pencari dan menyediakan akses informasi yang sesuai dengan kebijakan sensor negara. Adapun Weibo sebagai pengganti Twitter yang merupakan platform mikroblog utama Tiongkok dan berfungsi sebagai ruang diskusi publik daring. Kemudian Alipay, sebagai salah satu platform pembayaran digital Tiongkok, yang berfungsi sebagal alat transaksi dan pusat pengumpulan data keuangan Tiongkok. Seluruh aplikasi domestik yang dimiliki Tiongkok ini, berada dibawah pengawasan ketat pemerintah Tiongkok dengan sistem penyaringan konten, pengendalian algoritma, dan pengawasan ekonomi digital.

Strategi digital Tiongkok yang mengutamakan aplikasi domestik tidak hanya berdampak pada aspek teknologi dan informasi, tetapi juga memiliki implikasi luas terhadap keamanan nasional dan posisi geopolitik negara tersebut. Dengan mengembangkan dan memprioritaskan penggunaan aplikasi digital buatan dalam negeri, pemerintah Tiongkok mampu membentuk sistem kontrol informasi yang terpusat. Pendekatan ini tidak semata-mata bertujuan untuk kemandirian teknologi, tetapi juga untuk memperkuat peran negara dalam mengelola arus informasi yang beredar di masyarakat. Dalam konteks tersebut, pemerintah Tiongkok meluncurkan kebijakan *Cybersecurity Law* yang memperkuat kontrol negara data dan jaringan digital. Kebijakan ini dirancang untuk memastikan bahwa setiap informasi yang bergerak dalam sistem digital nasional tetap berada dalam cakupan pengawasan negara (Creemers, 2023, p. 132). Dengan kebijakan ini, strategi digital Tiongkok bukan hanya soal teknologi, tapi juga tentang menjaga kedaulatan negara dan keamanan digital nasional.

Sebagai bagian dari implementasinya, Tiongkok membangun dan memperkuat sistem *Great Firewall,* yaitu sistem penyaringan internet nasional yang berfungsi memblokir akses terhadap situs-situs dan platform asing yang dianggap tidak sejalan dengan kebijakan negara (Great Wall China Education Consultant, n.d.). Melalui sistem ini pemerintah memiliki kendali penuh dalam mengatur lalu lintas informasi, membatasi konten yang dinilai berbahaya, serta mencegah masuknya ideologi asing yang berpotensi menganggu stabilitas politik dalam negeri. Platform-platform besar asal Amerika Serikat yang berada di bawah naungan perusahaan tekonologi seperti *META,* merupakan contoh platform yang diblokir sebagai upaya menjaga digital domestik dari pengaruh luar. Tiongkok menyadari bahwa peperangan di era modern tidak lagi selalu berlangsung di medan tempur fisik, melainkan ruang digital yang merupakan tempat informasi dapat digunakan sebagai senjata yang mempengaruhi opini publik dan keamanan nasional. Dalam hal ini, Tiongkok berupaya untuk menguasai infrastruktur digital dan menetapkan batas-batas agar tidak bergantung pada teknologi asing.

Lebih jauh lagi, Tiongkok tidak hanya berupaya menjaga data domestik tetap berada dalam yurisdiksi nasional, tetapi juga berusaha mengekspor model dan teknologinya ke luar negeri melalui inisiatif seperti *Digital Silk Road* yang menjadi bagian dari program *Belt and Road Initiative* (BRI). Melalui kerangka kerja ini, Tiongkok menawarkan berbagai bentuk infrasturktur digital kepada negara-negara mitra mulai dari jaringan internet generasi kelima (5G) hingga pengelolaan penyimpanan data. Dengan menyebarkan teknologinya ke negara lain, Tiongkok secara tidak langsung memperkenalkan prinsip-prinsip kedaulatan digital yang berpihak pada negara, di mana pemerintah memiliki kontrol yang kuat atas data dan aktiivitas digital di wilayahnya (Abdurrohim & Tayibnapis, 2022, pp. 212-213). Tentu pendekatan ini menimbulkan kekhawatiran di beberapa negara, terutama yang mengutamakan prinsip keterbukaan, transparansi, dan perlindungan privasi.

Meskipun strategi digital Tiongkok telah berhasil membangun sistem yang kuat dan mandiri melalui pengembangan aplikasi buatan dalam negeri serta pembatasan akses terhadap platform asing, pendekatan ini juga menimbulkan kekhawatiran serius, terutama dalam hal etika dan hak asasi manusia. Salah satu dampak yang paling nyata semakin terbatasnya ruang untuk kebebasan berekspresi. Internet yang seharusnya menjadi ruang terbuka bagi masyarakar untuk berbagi ide, menyuarakan pendapat, dan mendorong diskusi publik, justru berubah menjadi alat kontrol negara (Nababan, Basri,

Lubis, & dkk, 2024, p. 139). Kondisi ini menciptakan suasna di mana warga merasa perlu berhati-hati dalam menyampaikan pandangan, bahkan dalam percakapan daring yang bersifat pribadi. Pada akhirnya, kebijakan ini dinilai efektif dalam menjaga kedaulatan digital dan keamanan nasional namun kurangnya penghormatan terhadap hak-hak fundamental individu.

Hal ini menimbulkan kekhawatiran dalam hak asasi manusia dan prinsip etika digital. Sistem pengawasan yang ketat, penyaringan konten, dan pembatasan akses terhadap informasi global membatasi ruang kebebasan berekspresi dan menghalangi akses masyarakat terhadap perspetif yang beragam. Dalam banyak kasus, individu yang menyuarakan kritik terhadap pemerintah melalui platform digital domestik menghadapi risiko sensor, pemantauan, dan bahkan represi. Media sosial dan aplikasi yang dikelola oleh perusahaan domestik beroperasi dalam ekosistem yang sangat dikontrol negara, di mana algoritma secara aktif menyaring kata kunci tertentu, menutup akun pengguna yang dianggap menyebarkan konten sensitif, serta memfasilitasi pelacakan identitas pengguna yang dianggap melanggar narasi resmi.

Fenomena ini menunjukkan dilema antara kebutuhan akan keamanan dan perlindungan negara dengan prinsip-prinsip kebabasan sipil dalam pembangunan ruang digital. Ketika negara terlalu dominan dalam ruang digital, maka risiko pelanggaran hak-hak sipil akan semakin besar terlebih jika tidak diimbangi dengan mekanisme pengawasan yang transparan. Teknologi digital yang awalnya dipandang sebagai alat pemberdayaan individu justru dibalik fungsinya menjadi instrumen unruk membatasi kebebasan berekspresi dan mengontrol opini publik. Tidak adanya kebebasan pers, ruang partisipasi publik yang terbatas dalam merumuskan kebijakan digital, serta kriminalisasi terhadap wacana kritis membuat ruang digital kehilangan fungsinya sebagai ruang partisipasi publik yang aman.

CONCLUSION

Perkembangan teknologi digital menjadi ranah perebutan kekuasaan antar negara dengan memperluas pengaruh diplomasi nya untuk penguatan eksistensi dalam lingkup internasional. Ancaman global yang bersifat non-konvensional ini menuntut negara-negara untuk tidak hanya meningkatkan perbatasan fiisknya namun juga perbatasan digitalnya. Dedikasi negara dalam mendominasi dunia digital mengarahkan pada ketergantungan terhadap aplikasi-aplikasi digital internasional yang membuat negara rentan terhadap eskposur intervensi asing dan pelemahan kontrol atas data

masyarakat. Merespon hal ini, negara juga berupaya untuk melakukan pengurangan ketergantungan terhadap aplikasi asing. Tiongkok dalam hal ini membentuk sebuah dinding digital untuk mengurangi keterikatan terhadap aplikasi digital asing dan mendorong pertumbuhan kekuatan digital domestiknya.

Tiongkok melakukan inovasi dengan melakukan kerja sama dengan perusahaan-perushaan digital besar untuk mengembangkan aplikasi digital serta pengelolaan data dan jaringan internet skala besar. Strategi ini juga ditujukan untuk menjaga kedaulatan nasional Tiongkok dan tetap memegang kontrol penuh atas ruang digitalnya. Tiongkok juga membentuk regulasi yang menjadi dasar dalam penanganan jaringan internet agar berada di bawah pengawasan penuh pemerintah. Pembentukan sistem penyaringan internet juga dilakukan oleh Tiongkok untuk memilah informasi dan konten yang akan masuk ke dalam kedaulatan Tiongkok. Berbeda dari negara-negara lain, Tiongkok menyuarakan kemampuan pengaruh kekuatan besarnya melalui kerja sama digital dengan negara mitra yang secara tidak langsung mendorong negara tersebut untuk bergantung pada Tiongkok.

Dengan mengangkat fenomena penggunaan aplikasi domestik sebagai representasi dari pemanfaatan teknologi untuk memperkuat nasionalisme digital dalam sistem politik yang terpusat dan represif, studi ini melengkapi kekosongan dalam literatur tentang hubungan antara teknologi digital dan nasionalisme otoriter. Penelitian ini dapat memperkaya wacana studi keamanan non-tradisional dan kedaulatan digital, khususnya dalam konteks negara-negara yang menganut pendekatan kontrol sentralistik seperti Tiongkok. Pendekatan Tiongkok menunjukkan bahwa dominasi negara atas ruang digital yang tidak hanya berfungsi untuk perlindungan terhadap ancaman luar, tetapi juga sebagai sarana untuk memperkuat legitimasi politik domestik. Dengan demikian, fenomena ini juga menceminkan bagaimana kekuasaan digital dapat dikonstruksikan sebagai bagian dari strategi geopolitik yang lebih luas.

REFERENCES

Abdurrohim, M., & Tayibnapis, R. G. (2022). CHINA DIGITAL SILK ROAD AND INDONESIA DIGITAL TRANSFORMATION. *MANDALA: Jurnal Ilmu Hubungan Internasional*, 212-213.

Amoo, O. O., Atadoga, A., Abrahams, T. O., & et.al. (2024). THE LEGAL LANDSCAPE OF CYBERCRIME: A REVIEW OF CONTEMPORARY

ISSUES IN THE CRIMINAL JUSTICE SYSTEM. *World Journal of Advanced Research and Reviews*, 214.

Cheung, T. M. (2018). THE RISE OF CHINA AS A CYBERSECURITY INDUSTRIAL POWER: BALANCING NATIONAL SECURITY, GEOPOLITICAL, AND DEVELOPMENT PRIORITIES. *Journal of Cyber Policy*, 5-11.

Creemers, R. (2023). CYBERSECURITY LAW AND REGULATION IN CHINA: SECURING THE SMART STATE. *China Law and Society Review*, 132.

Creemers, R. (2023). The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. *Journal of Contemporary China*, 175-176.

Cronin, A. K. (2023). *HOW PRIVATE TECH COMPANIES ARE RESHAPING GREAT POWER COMPETITION.* The Kissinger Center Papers.

Drinhausen, K., & Lee, J. (2021, June 15). *THE CCP IN 2021: SMART GOVERNANCE, CYBER SOVEREIGNTY AND TECH SUPREMACY*. Retrieved from MERICS (Mercator Institute for China Studies)

Fitzgerald, R., Wu, X., & Sandel, a. T. (2022). CHINESE SOCIAL MEDIA: TECHNOLOGY, CULTURE, AND CREATIVITY. *Discourse, Context & Media*, 1.

Great Wall China Education Consultant. (2022). *THE STORY OF CHINA'S GREAT FIREWALL, THE WORLD'S MOST SOPHISTICATED CENSORSHIP SYSTEM*. Retrieved June 9, 2025, from Great Wall China Education Consultant.

Harwit, E. (2014). THE RISE AND INFLUENCE OF WEIBO (MICROBLOGS) IN CHINA. *Asian Survey*, 1085.

Kaloudis, M. (2024). DIGITAL SOVEREIGNTY AS A WEAPON OF DIPLOMACY IN CYBER WARFARE IN DEMOCRACIES. In *National Security in the Digital and Information Age* (p. 5). London: IntechOpen.

Melnik, J. (2019). CHINA'S "NATIONAL CHAMPIONS": ALIBABA, TENCENT, AND HUAWEI. *Education About Asia, Association for Asian Studies.*, 28-33.

Nababan, E. O., Basri, F., Lubis, Z. A., & dkk. (2024). THE GREAT FIREWALL: ANALISIS MENDALAM TENTANG SENSOR DAN PENGAWASAN INTERNET DI CHINA ERA MASA KINI. *Journal of Politics and Democracy Studies (JPDS)*, 139.

Safitr, M. F., Lubis, M., & Fakhrurroja, d. H. (2023). COUNTERATTACKING CYBER THREATS: A FRAMEWORK FOR THE FUTURE OF CYBERSECURITY. *Sustainability*, 9.

Sharma, A. (2025). *CYBER WARS: A PARADIGM SHIFT FROM MEANS TO ENDS.* Retrieved from NATO Cooperative Cyber Defence Centre of Excellence : https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf