

The Great Firewall: Analisis Mendalam tentang Sensor dan Pengawasan Internet di China Era Masa Kini

Eunike Octavia Nababan¹, Farhanah Basri², Zaqi Amanda Lubis³, Lia Wulandari⁴

IlmuKomputer^{1,2,3}, Ilmu Politik⁴, Universitas Pembangunan Nasional "Veteran" Jakarta Email:

2210512004@mahasiswa.upnvj.ac.id



INFO ARTIKEL

ABSTRAK

Research Article

Kata Kunci:

Great Firewall of China,
Sensor Internet,
Pengawasan Siber,
Geopolitik Global

Article History

Dikirim : 20 Juni 2024

Diterima: 01 Juli 2024

Dipublikasi: 30 Juli 2024

Great Firewall of China (GFW), sebagai bagian dari Golden Shield Project, merupakan sistem pengawasan dan pengendalian internet yang dirancang oleh pemerintah Tiongkok untuk menyaring, membatasi, dan mengontrol akses informasi demi menjaga stabilitas politik, keamanan nasional, dan kedaulatan siber. Penelitian ini menganalisis mekanisme sensor internet yang diterapkan GFW dan dampaknya terhadap masyarakat, ekonomi digital, serta geopolitik global. Dengan pendekatan deskriptif kualitatif berbasis studi literatur, ditemukan bahwa GFW menggunakan teknologi canggih seperti pemfilteran URL, peracunan DNS, dan kecerdasan buatan untuk menyensor konten yang dianggap sensitif. Dampaknya meliputi pembatasan kebebasan berekspresi, hambatan inovasi teknologi, dan pengaruh signifikan terhadap hubungan internasional Tiongkok. Kesimpulannya, GFW efektif sebagai alat kontrol informasi, tetapi menimbulkan tantangan dalam transparansi dan kebebasan digital. Penelitian lanjutan dapat mengeksplorasi dampaknya terhadap inovasi teknologi, perdagangan, dan respons masyarakat terhadap keterbatasan akses informasi.

ABSTRACT

The Great Firewall of China (GFW), as part of the Golden Shield Project, is an internet surveillance and control system designed by the Chinese government to filter, limit, and control access to information in order to maintain political stability, national security, and cyber sovereignty. This research analyzes the internet censorship mechanism implemented by GFW and its impact on society, the digital economy, and global geopolitics. Using a descriptive qualitative approach based on a literature study, it is found that GFW uses advanced technologies such as URL filtering, DNS poisoning, and artificial intelligence to censor content that is considered sensitive. The impacts include restrictions on freedom of expression, barriers to technological innovation, and significant influence on China's international relations. In conclusion, GFW is effective as an information control tool, but poses challenges in transparency and digital freedom. Further research could explore its impact on technological innovation, trade, and societal responses to limited access to information.

1. Pendahuluan

Dalam era globalisasi seperti saat ini, setiap negara dituntut untuk dapat beradaptasi dengan perkembangan di segala bidang, terlebih lagi di bidang teknologi yang perubahan serta inovasinya sangat masif salah satunya adalah internet. Internet telah menjadi salah satu sarana utama untuk berbagi

informasi dan berkomunikasi secara global. Hal tersebut menyebabkan dibutuhkannya peningkatan keamanan nasional mengingat masifnya perkembangan yang disebabkan oleh internet.

Sadar dengan kondisi tersebut, membuat banyak negara maju dan negara berkembang yang berusaha menjadikan internet sebagai suatu hal yang perlu dikuasai, dijelajahi, dikontrol, dan dijaga. Sehingga, tidak semua negara memberikan kebebasan akses yang sama terhadap akses informasi menggunakan internet ini. China, sebagai salah satu negara dengan jumlah pengguna internet terbesar di dunia, menerapkan sistem sensor yang dikenal sebagai *Great Firewall* yang merupakan bagian dari mekanisme yang lebih besar yang disebut dengan Golden Shield Project (Quan, 2020). Sistem ini dirancang untuk mengontrol dan membatasi akses informasi dari luar negeri, dengan tujuan menjaga stabilitas sosial dan keamanan nasional. Melalui *Great Firewall*, pemerintah China dapat memblokir akses ke berbagai situs *web* asing, media sosial, dan konten yang dianggap mengancam.

Internet muncul di China pada 20 April 1994 dengan sekitar 10.000 pengguna aktif kemudian mengalami lonjakan yang sangat signifikan, hingga 6 tahun setelahnya yaitu pada 1998 pemerintah China mulai mengimplementasikan proyek *Golden Shield*, yang kemudian dikenal sebagai *Great Firewall of China* (GFW) (Zulfikar, 2023). Sejak saat itu, pertumbuhan pengguna internet di China terus meningkat pesat, dengan laporan dari *China Internet Network Information Center* (CINIC) menunjukkan bahwa jumlah pengguna internet mencapai lebih dari 900 juta pada tahun 2023 (Xinhua, 2024). Peningkatan ini tidak hanya mencerminkan adopsi teknologi yang cepat tetapi juga memicu kekhawatiran pemerintah mengenai potensi penyebaran informasi yang tidak terkontrol.

Dalam upaya untuk mengatasi kekhawatiran tersebut, pemerintah mulai menerapkan kebijakan sensor yang lebih ketat, termasuk pembatasan akses terhadap situs-situs yang dianggap berpotensi mengancam stabilitas politik dan sosial. Penelitian terbaru menunjukkan bahwa GFW kini menggunakan teknologi canggih seperti kecerdasan buatan untuk memantau dan menyensor konten secara *real-time*, menciptakan tantangan baru bagi pengguna yang ingin mengakses informasi bebas (USCC, 2024).

Penelitian ini bertujuan untuk melakukan analisis mendalam tentang *Great Firewall*, dengan fokus pada mekanisme sensor dan pengawasan internet yang diterapkan di China era masa kini untuk

memberikan wawasan mendalam mengenai tantangan yang dihadapi oleh pengguna internet di China serta dampak dari kebijakan sensor terhadap interaksi sosial dan perkembangan ekonomi digital. Penelitian ini juga bertujuan untuk memberikan kontribusi penting bagi pemahaman tentang kontrol informasi dalam konteks global.

2. Tinjauan Pustaka

Fenomena kontrol informasi di Tiongkok melalui "*The Great Firewall*" mencerminkan strategi kompleks yang menggabungkan sensor, propaganda, dan pengawasan. Langkah-langkah ini dilakukan untuk menjaga kestabilan dalam negeri sekaligus mendukung kebijakan luar negeri. Penelitianpenelitian sebelumnya menunjukkan bahwa "*The Great Firewall*" bukan hanya sekedar alat teknis untuk menyensor konten internet, tetapi juga berfungsi sebagai sarana ideologis yang mengarahkan narasi nasional sesuai dengan kepentingan pemerintah. Sebagai contoh, penelitian yang dalam artikelnya berjudul "Pembatasan Akses Internet sebagai Upaya China Menjaga Keamanan Nasional: *The Great Firewall of China*" oleh Faisal Mufti Zulfikar (2023) menggarisbawahi bahwa kontrol informasi di era digital Tiongkok dilakukan melalui penyaringan ketat terhadap konten yang bertentangan dengan narasi pemerintah, termasuk membungkam kritik domestik dan memperkuat legitimasi politik melalui propaganda yang efektif.

Di sisi lain, pembahasan mengenai peran keamanan siber dalam membangun kekuatan siber Tiongkok melalui "*The Great Firewall*" yang pada artikelnya berjudul "*China's Great Firewall: Cybersecurity as Strategy for Building World Cyberpower*" oleh Harvardry Gerald Abraham Wowor, Arfin Sudirman, Arfin Sudirman (2023), menunjukkan bahwa pengawasan internet di Tiongkok melibatkan pendekatan yang lebih dinamis, seperti mengelola interaksi pengguna dengan *platform* digital yang diawasi. Langkah ini memperlihatkan bagaimana pemerintah mampu tidak hanya membatasi akses informasi tetapi juga membentuk opini publik melalui algoritma yang diarahkan untuk memperkuat nasionalisme. Hal ini relevan dengan kajian analisis yang dilakukan pada artikel berjudul

"Implikasi Ruang Siber Terhadap Geopolitik Negara" oleh Iqbal Ramadhan (2021), yang menjelaskan bagaimana narasi nasionalisme siber muncul di bawah pengaruh kebijakan digital Tiongkok.

Nasionalisme ini, yang sering kali terfasilitasi oleh "*The Great Firewall*" digunakan untuk memperkuat solidaritas domestik sekaligus membangun citra positif Tiongkok di mata internasional, meskipun seringkali mendapatkan kritik dari negara Barat.

Penelitian lainnya mengenai fenomena "*wolf warrior diplomacy*," yang dibahas dalam "*China's Wolf Warrior Diplomacy: The Interaction of Formal Diplomacy and Cyber-Nationalism*" oleh Jonathan Sullivan dan Weixiang Wang (2023) juga merupakan contoh konkret dari bagaimana nasionalisme siber yang dihasilkan oleh "*The Great Firewall*" mampu mempengaruhi diplomasi formal Tiongkok. Fenomena ini menggambarkan perubahan kebijakan luar negeri Tiongkok yang menjadi lebih agresif sekaligus merespons aspirasi nasionalisme masyarakatnya. Dalam konteks ini, "*wolf warrior diplomacy*" digunakan untuk menghadapi kritik internasional sambil memenuhi kebanggaan patriotik di dalam negeri. Seperti dijelaskan, diplomasi ini bukan hanya tentang menyensor internet, tetapi juga memanfaatkan internet sebagai alat strategis untuk membentuk narasi nasional di tingkat global dan domestik (Sullivan dan Wang, 2023).

Selain itu, penelitian serupa berjudul "*China's Economic Cyber Strategy In Facing Economic Cyber Threats 2020-2023*" oleh Sylvia Octa Putri, Hanna Tri Indah Farras S, Dio Fathul Rachman, Intan Fauzi Septiana, Jerry Yeremiah Sihombing (2023), juga menjadi tambahan bukti bahwa keberhasilan "*The Great Firewall*" sebagai alat pengawasan tidak terlepas dari kemampuan pemerintah Tiongkok untuk berinovasi dalam menciptakan mekanisme kontrol yang semakin adaptif. Dalam hal ini, penggunaan kecerdasan buatan untuk mendeteksi dan menyensor konten bermuatan politis menjadi salah satu contoh konkret. Di sisi lain, langkah ini sering dikritik oleh organisasi internasional karena dianggap melanggar hak asasi manusia dan kebebasan berekspresi (Putri dkk., 2023).

Selain dari beberapa penelitian yang sudah disebutkan sebelum terdapat beberapa penelitian lainnya mengenai penyensoran konten internet di Tiongkok. Namun, penelitian-penelitian tersebut cenderung lebih berfokus pada aspek teknis dari *Great Firewall*, seperti bagaimana algoritma dan

teknologi kecerdasan buatan digunakan untuk menyaring konten, serta bagaimana pengguna internet di Tiongkok mencoba mengatasi pembatasan ini melalui penggunaan VPN atau teknologi lainnya. Penelitian-penelitian tersebut juga membahas dampak dari kebijakan sensor terhadap kebebasan berekspresi, inovasi teknologi, dan hubungan internasional Tiongkok. Karena itu, penelitian ini akan membahas tidak hanya terkait mekanisme teknis dari *Great Firewall*, tetapi juga dampaknya terhadap masyarakat, ekonomi digital, dan geopolitik global.

3. Metode

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi literatur untuk menyelidiki mekanisme sensor dan pengawasan internet yang diterapkan melalui *Great Firewall* di China. Fokus utama penelitian ini adalah menganalisis berbagai sumber literatur yang relevan, termasuk artikel akademik, jurnal, dan publikasi media yang membahas kebijakan internet dan dampaknya terhadap masyarakat China. Pengumpulan data dilakukan melalui pencarian sistematis terhadap literatur yang berkaitan dengan *Great Firewall*, termasuk sejarah implementasinya, teknik-teknik sensor yang digunakan, serta dampak sosial dan ekonomi dari kebijakan ini. Sumber-sumber yang dianalisis terutama berasal dari jurnal-jurnal ilmiah dan publikasi akademis yang telah kredibel, sehingga menjamin validitas dan keandalan informasi.

Analisis dokumen bertujuan untuk mendapatkan wawasan mendalam mengenai kebijakan resmi pemerintah terkait *Great Firewall* serta implikasinya terhadap akses informasi dan kebebasan berekspresi di China. Dengan pendekatan ini, penelitian ini diharapkan mampu memberikan gambaran tentang pengaruh *Great Firewall* terhadap dinamika sosial dan ekonomi digital.

Hasil dari penelitian ini diharapkan dapat memberikan wawasan mendalam mengenai tantangan yang dihadapi oleh pengguna internet di China serta dampak dari kebijakan sensor terhadap interaksi sosial dan perkembangan ekonomi digital. Penelitian ini juga bertujuan untuk memberikan kontribusi penting bagi pemahaman tentang kontrol informasi dalam konteks global.

4. Hasil dan Pembahasan

4.1 Mekanisme Sensor dan Pengawasan Internet pada *Great Firewall*

Mekanisme sensor dan pengawasan internet di bawah sistem *Great Firewall of China* (GFW) merupakan salah satu kebijakan paling signifikan dalam menjaga stabilitas politik, keamanan negara, dan kedaulatan siber Tiongkok. GFW adalah bagian dari proyek Golden Shield Project (GSP), yang menjadi instrumen penting dalam mengontrol informasi yang terakses oleh masyarakat Tiongkok. Mekanisme ini didasarkan pada kombinasi teknologi penyensoran yang canggih, regulasi ketat, dan pengawasan manual, yang semuanya bekerja secara harmonis di bawah arahan berbagai lembaga pemerintah, termasuk Administrasi Ruang Siber Tiongkok dan Komisi Urusan Siber Pusat.

Sistem GFW bekerja dengan menggunakan beberapa metode utama, seperti pemfilteran URL, peracunan DNS, pemblokiran VPN ilegal, serangan *man-in-the-middle*, dan probing aktif. Pemfilteran URL dilakukan dengan mendeteksi kata kunci tertentu di *website* yang dianggap sensitif terhadap stabilitas politik atau keamanan nasional. Situs-situs yang mengandung kata kunci seperti "Tiananmen" atau "kemerdekaan Tibet" langsung diblokir. Peracunan DNS adalah teknik di mana pengguna yang mencoba mengakses situs *web* tertentu diarahkan ke alamat IP palsu, sehingga mereka tidak dapat mengakses konten tersebut. Selain itu, pemerintah Tiongkok juga memblokir penggunaan VPN yang tidak terdaftar secara resmi. VPN yang sah harus menyerahkan data pengguna kepada pemerintah dan mengikuti kebijakan sensor yang berlaku.

Selain teknologi penyaringan otomatis, *manual enforcement* juga memainkan peran penting. Pemerintah mempekerjakan ratusan ribu pekerja sipil untuk memantau konten daring dan melaporkan pelanggaran. Mereka, dibantu oleh teknologi kecerdasan buatan (AI), melakukan kontrol terhadap media sosial lokal seperti WeChat, Sina Weibo, dan QQ, memastikan bahwa konten yang dapat mengancam stabilitas domestik tidak menyebar luas. Pendekatan ini menunjukkan bahwa GFW tidak hanya bertujuan untuk mengendalikan teknologi informasi, tetapi juga untuk menekan segala bentuk kebebasan berekspresi yang dianggap berlawanan dengan ideologi Partai Komunis Tiongkok.

Dalam implementasinya, GFW tidak hanya mengandalkan teknologi domestik seperti Huawei dan Sugon, tetapi juga menggunakan perangkat keras dan perangkat lunak dari perusahaan asing seperti Cisco dan Nortel. Ironisnya, meskipun negara-negara Barat sering mengkritik kebijakan GFW, mereka secara tidak langsung telah berkontribusi pada pengembangannya melalui teknologi yang dijual ke Tiongkok. Salah satu studi kasus lain yang relevan adalah dengan adanya pemblokiran Google di Tiongkok. Pada tahun 2002, Google mulai mengalami gangguan akses akibat kebijakan penyensoran. Pada tahun 2006, Google meluncurkan domain Google.cn untuk memenuhi persyaratan pemerintah Tiongkok, termasuk menyensor konten yang dianggap sensitif. Namun, pada 2010, Google memutuskan untuk memindahkan operasinya ke Hong Kong karena tidak ingin terus-menerus tunduk pada kebijakan sensor. Langkah ini mengakibatkan hilangnya layanan Google di Tiongkok, yang kemudian digantikan oleh mesin pencari lokal, Baidu.

Kasus Google ini mencerminkan bagaimana GFW tidak hanya menjadi alat pengawasan, tetapi juga instrumen geopolitik untuk melindungi pasar domestik dari pengaruh asing. Dengan memblokir konten asing yang tidak sesuai dengan ideologi pemerintah, GFW juga memberi ruang bagi perusahaan lokal untuk berkembang tanpa persaingan langsung. Hal ini mengukuhkan peran GFW sebagai alat proteksionisme ekonomi, di mana kontrol teknologi digunakan untuk mendukung perusahaan lokal seperti Alibaba, Tencent, dan Baidu. Secara umum, mekanisme GFW menggambarkan pendekatan holistik Tiongkok dalam mengontrol ruang siber, di mana teknologi, regulasi, dan pengawasan manual bersatu untuk menciptakan sistem sensor internet yang paling canggih dan ketat di dunia.

4.2 Dampak Kebijakan Sensor terhadap Masyarakat dan Kebebasan Berekspreasi

Kebijakan sensor internet melalui *Great Firewall of China* (GFW) membawa dampak signifikan pada kehidupan masyarakat Tiongkok, terutama terkait dengan kebebasan berekspreasi dan akses terhadap informasi. Di satu sisi, kebijakan ini berhasil menciptakan stabilitas politik dan melindungi kedaulatan nasional. Namun, disisi lain, langkah-langkah pengendalian yang ketat ini telah mengorbankan kebebasan individu dan transparansi informasi.

Dampak paling mencolok adalah terbatasnya kebebasan berekspresi. Internet, yang menjadi ruang untuk berbagi ide dan pendapat, di Tiongkok justru menjadi alat kontrol negara. Pemerintah Tiongkok mengatur penggunaan internet melalui undang-undang yang kabur dan ambigu, seperti Undang-Undang Keamanan Siber dan peraturan terkait rahasia negara. Ketidakjelasan definisi "rahasia negara" memungkinkan pemerintah untuk menindak siapa saja yang dianggap melanggar kebijakan, bahkan jika pelanggaran tersebut tidak jelas. Contoh kasus adalah penangkapan Shi Tao, seorang jurnalis yang dijatuhi hukuman penjara sepuluh tahun karena mengirimkan email yang dianggap membocorkan rahasia negara.

Kebijakan ini juga telah menciptakan rasa takut di kalangan masyarakat. Penggunaan teknologi pengawasan yang canggih, seperti keharusan menggunakan identitas asli dalam aktivitas daring, membuat masyarakat enggan untuk menyuarakan pendapat yang berlawanan dengan pemerintah. Pada tahun 2021, Facebook, Twitter, dan WhatsApp tetap diblokir, bahkan selama pandemi COVID-19 ketika aplikasi ini menjadi saluran utama komunikasi global. Sebagai gantinya, aplikasi lokal seperti WeChat dan QQ diberdayakan. Namun, pemerintah memanfaatkan ekosistem ini untuk memantau percakapan publik dan menyensor konten yang dianggap bertentangan dengan pemerintah. Namun, pembatasan ini tidak sepenuhnya diterima oleh masyarakat. Penggunaan VPN merupakan bentuk perlawanan terhadap kebijakan GFW. Banyak masyarakat Tiongkok menggunakan VPN untuk mengakses situs-situs asing yang diblokir, meskipun tindakan ini berisiko terkena sanksi hukum. Protes terhadap kebijakan sensor juga semakin meningkat, terutama di kalangan generasi muda yang lebih terpapar pada nilai-nilai global.

Di sisi lain, GFW juga membawa dampak positif bagi masyarakat Tiongkok. Dengan memblokir perusahaan teknologi asing, pemerintah memberikan ruang bagi perusahaan lokal untuk berkembang tanpa persaingan dari luar. Hal ini memungkinkan munculnya raksasa teknologi seperti Alibaba, Tencent, dan Baidu, yang kini menjadi tulang punggung ekonomi digital Tiongkok. Selain itu, stabilitas politik yang dihasilkan dari pengendalian informasi memungkinkan pemerintah untuk fokus pada pembangunan ekonomi dan pengentasan kemiskinan.

Namun demikian, dampak negatif dari kebijakan sensor ini, seperti pelanggaran hak asasi manusia, pembatasan kebebasan berekspresi, dan isolasi dari komunitas global, tetap menjadi isu yang sangat kontroversial. Dari perspektif teori Hak Asasi Manusia, kebijakan penyensoran yang ketat melanggar prinsip-prinsip kebebasan berekspresi sebagaimana diatur dalam Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR). Meskipun Tiongkok telah menandatangani konvensi ini, implementasi kebijakannya bertentangan dengan nilai-nilai universal yang diatur dalam perjanjian tersebut.

4.3 Implikasi Ekonomi Digital dan Geopolitik Global

Kebijakan *Great Firewall of China* (GFW) tidak hanya berdampak pada masyarakat domestik, tetapi juga memiliki implikasi besar terhadap ekonomi digital Tiongkok dan geopolitik global. Melalui kontrol ketat terhadap akses internet, Tiongkok telah berhasil menciptakan ekosistem digital yang mandiri dan berdaya saing, sekaligus memperkuat posisi geopolitiknya di kancah internasional.

Dalam konteks ekonomi digital, *Great Firewall of China* (GFW) bertindak sebagai bentuk proteksionisme ekonomi. Dengan membatasi akses ke layanan internet asing, Tiongkok mendorong munculnya alternatif lokal seperti Baidu (pengganti Google), Youku (pengganti YouTube), dan WeChat (pengganti WhatsApp). Model ini memungkinkan perusahaan-perusahaan Tiongkok untuk berkembang tanpa persaingan langsung dari raksasa teknologi Barat. Akibatnya, perusahaan seperti Alibaba, Tencent, dan Huawei telah menjadi pemimpin global di sektor teknologi, tidak hanya di pasar domestik tetapi juga di pasar internasional.

Selain itu, kebijakan *Great Firewall of China* (GFW) juga membantu menciptakan ketahanan ekonomi digital. Dengan mengandalkan teknologi dan layanan buatan lokal, Tiongkok berhasil mengurangi ketergantungan pada produk dan layanan asing. Hal ini memberikan Tiongkok keuntungan strategis dalam menghadapi potensi konflik dagang atau sanksi ekonomi dari negaranegara Barat. Contohnya, dalam konflik perdagangan dengan Amerika Serikat, Tiongkok mampu bertahan karena memiliki infrastruktur digital yang mandiri.

Dari sudut pandang geopolitik, *Great Firewall of China* (GFW) mencerminkan upaya Tiongkok untuk mempromosikan konsep kedaulatan siber. Melalui diplomasi siber, Tiongkok berusaha untuk mengubah paradigma global tentang internet, dari yang sebelumnya bersifat bebas dan terbuka menjadi lebih terkontrol dan terorganisir (Segal, 2020). Tiongkok secara aktif mempromosikan konsep ini di forum internasional seperti ICANN dan W3C, serta melalui inisiatif seperti Jalur Sutra Digital dalam proyek OBOR (*One Belt One Road*) (Das, 2017). Dengan ekspansi teknologi Tiongkok ke negara-negara berkembang, seperti pemasangan jaringan 5G oleh Huawei di Afrika dan Asia, Tiongkok memperluas pengaruhnya sekaligus mengeksport model kontrol internetnya ke negara lain.

Pendekatan tersebut tetap menuai kritik dari negara-negara Barat, terutama Amerika Serikat, yang menganggap *Great Firewall of China* (GFW) sebagai ancaman terhadap nilai-nilai demokrasi dan kebebasan informasi. Selain itu, banyak perusahaan Barat mengalami kesulitan beroperasi di Tiongkok karena harus mematuhi aturan sensor yang ketat. Kondisi ini memicu ketegangan dalam hubungan ekonomi dan geopolitik antara Tiongkok dan negara-negara Barat. Salah satu studi kasus lain yaitu pada pengembangan TikTok dan Douyin, yang dimiliki oleh ByteDance, menjadi contoh bagaimana perusahaan Tiongkok berhasil menavigasi regulasi domestik dan internasional. Douyin, sebagai versi domestik TikTok, beroperasi di bawah pengawasan ketat pemerintah Tiongkok, sementara TikTok dirancang untuk pasar internasional dengan penyesuaian terhadap regulasi di luar Tiongkok. Strategi ini mencerminkan bagaimana perusahaan Tiongkok mampu beradaptasi dengan regulasi yang berbeda di pasar global, sekaligus memanfaatkan kebijakan domestik yang mendukung mereka.

Kasus TikTok dan Douyin menunjukkan bagaimana *Great Firewall of China* (GFW) membantu perusahaan Tiongkok berkembang dengan melindungi mereka dari persaingan asing di pasar domestik. Hal ini menciptakan ekosistem digital yang kompetitif di tingkat global. Sementara itu, inisiatif Jalur Sutra Digital mencerminkan bagaimana Tiongkok menggunakan teknologi sebagai alat diplomasi untuk memperluas pengaruh geopolitiknya. Namun, strategi ini juga memicu kekhawatiran di negara-negara Barat, terutama terkait potensi penyalahgunaan teknologi untuk pengawasan dan pelanggaran privasi.

Hal ini menciptakan ketegangan dalam hubungan geopolitik antara Tiongkok dan negara-negara Barat, terutama Amerika Serikat.

Secara keseluruhan, *Great Firewall of China* (GFW) telah menjadi alat strategis yang memungkinkan Tiongkok mengkonsolidasikan kekuatan ekonomi digitalnya sekaligus memperkuat posisinya dalam geopolitik global. Namun, pendekatan ini juga meningkatkan risiko fragmentasi internet global (splinternet), di mana dunia terpecah menjadi blok-blok digital yang berbeda dengan nilai dan aturan yang saling bertentangan. Contohnya, Tiongkok mempromosikan konsep kedaulatan siber yang menekankan kontrol negara atas internet di dalam perbatasannya, berbeda dengan nilai-nilai Barat yang mendukung internet yang bebas dan terbuka. Dalam forum internasional seperti ICANN dan W3C, Tiongkok mendorong aturan yang lebih terorganisir dan terkontrol, sementara negara-negara Barat cenderung mempertahankan prinsip kebebasan informasi dan netralitas internet.

5. Kesimpulan

Penelitian ini mengungkap bahwa *Great Firewall of China* (GFW) merupakan mekanisme sensor internet yang kompleks dan strategis, yang jauh melampaui sekadar teknologi pembatasan. GFW berfungsi sebagai instrumen multidimensional pemerintah Tiongkok untuk mengontrol informasi, menjaga stabilitas politik, melindungi ekonomi digital, dan memperkuat posisi geopolitik global. Melalui teknologi canggih dan pendekatan pengawasan yang komprehensif, GFW berhasil membatasi akses informasi, membentuk narasi nasional, dan menciptakan ekosistem digital mandiri yang melindungi perusahaan lokal dari persaingan asing. Namun, keberhasilan ini datang dengan biaya yang signifikan terhadap kebebasan berekspresi dan hak asasi manusia, menciptakan ketegangan antara kebutuhan kontrol pemerintah dan nilai-nilai demokrasi global. Penelitian ini menyoroti bagaimana teknologi internet dapat dimanfaatkan sebagai alat kekuasaan yang *powerful*, sekaligus memunculkan pertanyaan mendalam tentang masa depan kebebasan informasi di era digital.

Mengingat kompleksitas *Great Firewall of China*, penelitian selanjutnya disarankan untuk mengeksplorasi strategi masyarakat dalam mengatasi pembatasan internet, mengkaji dampak jangka

panjang terhadap inovasi teknologi, dan menganalisis evolusi model sensor internet dengan berkembangnya kecerdasan buatan. Penelitian mendatang perlu melakukan studi komparatif tentang kontrol internet di berbagai negara serta memperdalam analisis implikasi geopolitik dari model kontrol digital Tiongkok, guna memberikan pemahaman komprehensif tentang dinamika kebebasan informasi di era digital.

6. Referensi

- AKDUMAN, B. (2023). From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance. *Uluslararası Sosyal Bilimler Dergisi*, 7(28), 442-469.
- Bandur, H. E., Louisa, C., & Gibran, H. M. (2024). Pengaruh Sistem Kebijakan Social Credit Dalam Aspek Hukum Pada Etika Dan Budaya Masyarakat China. *Nusantara: Jurnal Pendidikan, Seni, Sains dan Sosial Humaniora*, 2(01).
- Das, S. B. (2017). OBOR's digital connectivity offers both benefits and risks.
- Englehart, N. (2021). The Great Firewall of China: The implementations and impact of internet censorship. *The Synapse: Intercollegiate Science Magazine*, 28(1), 8.
- FOLEY, J. J. (2023). China's Authoritarian Grip: How China Reinforces Social Control, Cultivates a Climate of Fear, and Minimizes Dissent. *Journal of Indo-Pacific Affairs*, 6(8).
- Han, R. (2023). Debating China beyond the great firewall: digital disenchantment and authoritarian resilience. *Journal of Chinese Political Science*, 28(1), 85-103.
- Hoang, N. P., Dalek, J., Crete-Nishihata, M., Christin, N., Yegneswaran, V., Polychronakis, M., & Feamster, N. (2024). {GFWeb}: Measuring the Great Firewall's Web Censorship at Scale. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 2617-2633).
- Kaye, D. B. V., Chen, X., & Zeng, J. (2021). The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok. *Mobile Media & Communication*, 9(2), 229-253. <https://doi.org/10.1177/2050157920952120>
- Niaki, A. A., Hoang, N. P., Gill, P., & Houmansadr, A. (2020). Triplet Censors: Demystifying Great

{Firewall's} {DNS} Censorship Behavior. In 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20).

- Putri, S. O., Farras S, H. T. I., Rachman, D. F., Septiana, I. F., & Sihombing, J. Y. (2024). CHINA'S ECONOMIC CYBER STRATEGY IN FACING ECONOMIC CYBER THREATS 2020 - 2023. Proceeding of International Conference on Business, Economics, Social Sciences, and Humanities, 7, 517-527. <https://doi.org/10.34010/icobest.v7i.563>
- Prasetyo, D. (2021). Subyektifitas dan Kehidupan Sosial dalam Dunia Digital di China (Memahami Hubungan Antar Negara dan Masyarakat pada Era Media Digital). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(2), 134-144.
- Quan, E. (2022). Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping. *Sigma: Journal of Political and International Studies*, 39(1), 4.
- Ramadhan, I. (2021). Implikasi Ruang Siber Terhadap Geopolitik Negara The Implication of Cyberspace Towards State Geopolitics.
- Segal, A. (2020). China's vision for cyber sovereignty and the global governance of cyberspace. *NBR Special Report*, (87), 85-100.
- Sullivan, J., & Wang, W. (2023). China's "wolf warrior diplomacy": The interaction of formal diplomacy and cyber-nationalism. *Journal of Current Chinese Affairs*, 52(1), 68-88.
- Setiawan, M. C. A., et al. The Relationship Between Identity Politics and Trade Protectionism Under Donald Trump's Administration. *Journal of Political Issues*, vol. 2, no. 1, 2020, pp. 58-68, doi:10.33019/jpi.v2i1.32.
- Taylor, M. (2022). Building Digital Authoritarianism: From the Great Firewall to the New IP. In *China's Digital Authoritarianism: A Governance Perspective* (pp. 1-24). Cham: Springer International Publishing.
- USCC. (2024). *Censorship practices of the People's Republic of China*. Retrieved from https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf
- Wowor, H. G. A., Sudirman, A., & Hakiki, F. (2023). China's Great Firewall: Cybersecurity as Strategy for Building World Cyberpower. *JISPO Jurnal Ilmu Sosial dan Ilmu Politik*, 13(2), 193-232.
- Xinhua. (2024). Pengguna internet di China tembus 1,09 miliar pada 2023. Antara News.

<https://www.antaranews.com/berita/4024998/pengguna-internet-di-china-tembus-109-miliar-pada-2023>

Yahya, F. A., & Mutia, R. T. N. The Great Firewall of China: Praktik Kebijakan Sensor Internet Pada Era Xi Jinping. *Historia: Jurnal Pendidik dan Peneliti Sejarah*, 6(1), 13-24.

Zulfikar, F. M. (2023). Pembatasan akses internet sebagai upaya China menjaga keamanan nasional: The Great Firewall of China. *Bhavana: Jurnal Studi Global*, 1(1), 26–38. <https://doi.org/10.59408/bjgs.v1i1.54>