

**SEKURITISASI RUANG SIBER OLEH PEMERINTAH TIONGGOK:  
ANALISIS KEBIJAKAN *GREAT FIREWALL* (2013-2025) MELALUI  
PERSPEKTIF BARRY BUZAN  
SKRIPSI**



**UNIVERSITAS  
ISLAM  
INDONESIA**

Oleh:

**OCTAVIANI GUSTINAWATI**

22323096

**PROGRAM STUDI HUBUNGAN INTERNASIONAL  
FAKULTAS ILMU SOSIAL DAN BUDAYA  
UNIVERSITAS ISLAM INDONESIA**

**2025**

**SEKURITISASI RUANG SIBER OLEH PEMERINTAH TIONGKOK:  
ANALISIS KEBIJAKAN *GREAT FIREWALL* (2013-2025) MELALUI  
PERSPEKTIF BARRY BUZAN**

**SKRIPSI**

Diajukan kepada Program Studi Hubungan Internasional  
Fakultas Ilmu Sosial dan Budaya  
Universitas Islam Indonesia  
Untuk memenuhi sebagian dari syarat guna memperoleh  
Derajat Sarjana S1 Hubungan Internasional



Oleh:

**OCTAVIANI GUSTINAWATI**

22323096

**PROGRAM STUDI HUBUNGAN INTERNASIONAL  
FAKULTAS ILMU SOSIAL BUDAYA DAN BUDAYA  
UNIVERSITAS ISLAM INDONESIA**

**2025**

**HALAMAN PENGESAHAN**

**Sekuritisasi Ruang Siber Oleh Pemerintah Tiongkok: Analisis Kebijakan  
Great Firewall (2013-2025) Melalui Perspektif Sekuritisasi Barry Buzan**

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

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



Mengesahkan

Program Studi Hubungan Internasional  
Fakultas Ilmu Sosial dan Budaya

Universitas Islam Indonesia

Ketua Program Studi



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

Dewan Penguji

Tanda Tangan

1 Ayu Heryati Naqsabandiyah, S.IP., M.A.

2 Mohammad Rezky Utama, S.IP., M.Si.

3 Alfredha Shinta Putri, S.IP., M.H.I.

## PERNYATAAN INTEGRITAS AKADEMIK

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

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

Memberikan pernyataan yang tidak benar dianggap sebagai pelanggaran integritas akademik.

21 Januari 2026,



---

*Octaviani Gustinawati*

## DAFTAR ISI

<b>SKRIPSI</b>	i
<b>HALAMAN PENGESAHAN</b>	Error! Bookmark not defined.
<b>PERNYATAAN INTEGRITAS AKADEMIK</b>	Error! Bookmark not defined.
<b>DAFTAR ISI</b>	v
<b>DAFTAR GAMBAR</b>	vii
<b>DAFTAR TABEL</b>	viii
<b>ABSTRAK</b>	ix
<b>BAB 1 PENDAHULUAN</b>	1
<b>1.1 Latar Belakang</b>	1
<b>1.2 Rumusan Masalah</b>	6
<b>1.3 Tujuan Penelitian</b>	6
<b>1.4 Cakupan Penelitian</b>	6
<b>1.5 Tinjauan Pustaka</b>	7
<b>1.6 Kerangka Pemikiran</b>	10
<b>1.8 Metode Penelitian</b>	14
1.8.1 <i>Jenis Penelitian</i>	14
1.8.2 <i>Subjek dan Objek Penelitian</i>	14
1.8.3 <i>Metode Pengumpulan Data</i>	14
1.8.4 <i>Proses Penelitian</i>	15
<b>1.9 Sistematika Pembahasan</b>	15
<b>BAB 2</b>	17
<b>2.1 Dinamika Kebijakan <i>Great Firewall of China</i></b>	17
<b>2.2 Kebijakan <i>The Great Firewall of China</i> Era Kepemimpinan Xi Jinping</b>	22
<b>BAB 3</b>	34
<b>3.1 <i>Speech Act</i> sebagai Instrumen <i>Securitizing Actor</i> dalam Membingkai Ancaman Keamanan Siber Digital Tiongkok terhadap Audiens</b>	34
3.1.1 <i>Aktor Sekuritisasi</i>	34
3.1.2 <i>Speech Act</i>	37
3.1.3 <i>Functional Actor</i>	44
3.1.4 <i>Audiens</i>	46
<b>3.2 <i>Existential Threat</i> Keamanan Siber sebagai Ancaman Nyata terhadap <i>Referent Object</i> Nasional Tiongkok</b>	48
<b>3.3 Analisis <i>Emergency Act</i> dalam Kebijakan <i>The Great Firewall of China</i></b>	55

<b>BAB 4</b>	60
<b>4.1 Kesimpulan</b>	60
<b>4.2 Rekomendasi</b>	62
<b>DAFTAR PUSTAKA</b>	63

## DAFTAR GAMBAR

<b>Gambar 3. 1</b> Dampak <i>Lockdown</i> COVID-19 terhadap Rasio Pengikut Baru Twitter di Tiongkok Daratan dibandingkan Hong Kong .....	52
--	----

## DAFTAR TABEL

**Tabel 2. 1** Perbandingan Kebijakan GFW Sebelum dan Pada Era Xi Jinping..... 31

## ABSTRAK

Pada era kepemimpinan Xi Jinping, pemerintah Tiongkok memperkuat kebijakan *The Great Firewall of China* sebagai respons terhadap arus informasi digital yang semakin pesat. Penelitian ini bertujuan untuk menganalisis kebijakan *The Great Firewall of China* pada periode 2013-2025 dengan menggunakan pendekatan teori sekuritisasi yang dikembangkan oleh Barry Buzan, Ole Waever, dan Jaap de Wilde (1998). Metode penelitian yang digunakan adalah studi literatur dengan pendekatan kualitatif dan analisis teori sekuritisasi sebagai alat analisis utama dalam menjawab rumusan masalah. Dalam studi kasus ini, pemerintah Tiongkok khususnya Xi Jinping diposisikan sebagai *securitizing actor* yang membingkai isu ancaman internet sebagai *existential threat* kepada audiens. Isu ini dinyatakan sebagai ancaman yang mengganggu *referent object* yang merupakan kedaulatan negara, stabilitas politik, identitas nasional, legitimasi pemerintah, dan keamanan nasional. Maka dari itu pemerintah Tiongkok merespons isu ini dengan menerapkan *emergency act* melalui penguatan kebijakan *The Great Firewall of China* atau pengawasan dan pemblokiran situs asing. Sehingga pembatasan sensor internet yang diterapkan merupakan bentuk *emergency act* yang telah dilegitimasi dengan mengsekuritisasi ruang digital, meskipun hal ini bertentangan dengan hak asasi manusia atau kebebasan berekspresi.

**Kata-kata kunci:** *Great Firewall of China*, Keamanan Siber, Sekuritisasi, Tiongkok, Xi Jinping.

## ABSTRACT

*During the leadership of Xi Jinping, the Chinese government strengthened The Great Firewall of China policy in response to the increasingly rapid flow of digital information, This study aims to analyze The Great Firewall Of China policy during the period 2013-2025 using the securitization theory developed by Barry Buzan, Ole Waever, and Jaap de Wilde(1998). The research employs a qualitative approach through literature review, with securitization theory serving as the main analytical framework to address the research problem. In this case study, the Chinese government, particularly Xi Jinping, is positioned as the securing actor who frame =s the issue of the internet as an existential threat to the audience. This issue is constructed as a threat to the referent objects, namely state sovereignty, political stability, national identity, government legitimacy, and national security. Consequently, the Chinese government responds to this perceived threat by implementing emergency acts through The Great Firewall of China, including increased surveillance and the blocking of foreign websites. Therefore, the restrictions and censorship of the internet that have been implemented constitute a form of emergency act that has been legitimized through the securitization of the digital space, despite the fact that these measures contradict human rights and freedom of expression.*

**Keywords:** *China, Cybersecurity, Great Firewall of China, Securitization, Xi Jinping.*

# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang

Pergeseran sistem politik abad ke-21 membuka babak baru dalam persaingan antar negara yang kini semakin menonjol dalam perebutan pengaruh pada skala regional, global, hingga internasional. Di sisi lain, derasnya arus globalisasi juga mendorong perubahan dalam dinamika dunia politik sekaligus memperluas cara pandang terhadap isu keamanan nasional maupun internasional. Pesatnya kemajuan teknologi informasi dan komunikasi turut membuka kemungkinan bagi suatu negara untuk membatasi atau memblokir akses internet di wilayahnya. Tindakan ini umumnya didorong oleh tiga alasan utama. Pertama, untuk mempertahankan stabilitas politik di dalam negeri. kedua, sebagai upaya menjaga keamanan nasional. ketiga, untuk melindungi nilai-nilai tradisi sosial maupun dari pengaruh intervensi asing.

Dalam konteks perkembangan teknologi dalam skala global, Tiongkok menunjukkan dinamika yang signifikan. Meskipun internet pada fase awal perkembangannya merupakan hasil inisiatif Amerika Serikat, pemerintah Tiongkok mampu memanfaatkan teknologi tersebut untuk memperkuat peran negara dalam penyediaan layanan digital dan membangun kekuatan perangkat lunaknya. Pada tahap awal, Tiongkok mengalami keterlambatan dalam mengadopsi teknologi sebagai instrumen untuk memperkuat posisinya di ranah Internasional. Namun, keterlambatan tersebut justru mendorong Tiongkok untuk aktif mengejar ketertinggalan melalui pemanfaatan peluang dalam bidang Sains, Teknologi, Teknik, dan Matematika (STEM) sebagai sarana untuk mencapai keunggulan.

Sejak tahun 1975, STEM ditetapkan sebagai salah satu dari empat pilar utama modernisasi sebagaimana dikemukakan oleh Deng Xiaoping, yang kemudian mendorong Tiongkok muncul sebagai salah satu aktor global dalam bidang pengembangan dan penguasaan teknologi (Quan 2022, 20).

Sejak internet mulai berkembang di Tiongkok tepatnya pada tahun 1995, pemerintah Tiongkok mulai mempersiapkan rencana dalam mengatur dan mengendalikan akses internet. Pemerintah Tiongkok merumuskan kebijakan pengaturan arus media dan informasi dengan beranjak dari pernyataan Deng Xiaoping pada tahun 1980-an yang menyatakan, “Jika kamu membuka jendela, udara segar dan lalat akan masuk.” Pernyataan tersebut kemudian dijadikan landasan filosofis oleh pemerintah Tiongkok dalam menyusun kebijakan yang bertujuan untuk membatasi masuknya pengaruh asing yang dianalogikan sebagai “lalat”, sekaligus mencegah masuknya informasi dan nilai-nilai yang dianggap bertentangan dengan kepentingan negara serta nilai-nilai sosial yang berlaku (Wowor, Sudirman, and Hakiki 2023, 197).

Pada era globalisasi saat ini, bukan hanya Tiongkok yang merasakan semakin terbukanya arus informasi, yang bahkan telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan manusia. Negara-negara lain juga menghadapi tuntutan untuk terus berinovasi dan beradaptasi dalam dunia digital lintas batas negara. Kondisi tersebut mendorong pemerintah Tiongkok untuk mengambil langkah pengendalian yang ketat terhadap arus informasi dan aktivitas digital. Hal ini tercermin dari kebijakan “*The Great Firewall of China*”, yang mulai dikembangkan sejak tahun 1990-an pada masa pemerintahan PRC (*People’s Republic of China*) di bawah kepemimpinan Partai Komunis.

*The Great Firewall of China*, tidak merujuk pada satu kebijakan tunggal, akan tetapi merupakan gabungan antara perangkat hukum dan sistem teknologi yang secara kolektif digunakan untuk mengatur dan mengendalikan internet di Tiongkok. Sejak disahkannya undang-undang CL97 pada tahun 1997 sebagai regulasi pertama yang mengkriminalisasi kejahatan siber, serta adanya peluncuran *Golden Shield Project* yang bertujuan membatasi akses data asing ke dalam wilayah Tiongkok (Koty 2017). Kebijakan awal ini yang menjadi fondasi bagi pembentukan kerangka regulasi internet yang didukung oleh sistem penyensoran daring, yang secara resmi dikenal dengan nama Proyek Perisai Emas dan diura Tiongkok dikenal dengan nama *The Great Firewall of China*.

Memasuki era kepemimpinan Xi Jinping, ruang siber mulai dipandang sebagai sumber ancaman non-tradisional yang memiliki pengaruh cukup signifikan terhadap keamanan nasional Tiongkok. Ancaman siber tidak hanya berkaitan dengan penyebaran informasi tetapi juga termasuk disinformasi. Selain itu, adanya peningkatan serangan siber, pencurian data, dan pemanfaatan teknologi digital oleh pihak luar negeri yang dianggap oleh Tiongkok dapat memengaruhi, mengganggu, atau mengancam kedaulatan nasional serta stabilitas politik Tiongkok. Fase awal pengembangan GFW secara teknis diselesaikan pada tahun 2006, dan penerapannya terbatas pada wilayah Tiongkok daratan dan tidak secara langsung mencakup Hong Kong maupun Makau sebagai wilayah administratif khusus (Crawford 2023). Sehingga pengendalian informasi dari kebijakan ini membentuk ekosistem internet yang tertutup dengan jumlah pengguna yang besar, dan menciptakan internet di dalam internet yang memperkuat dominasi digital nasional.

Pada masa kepemimpinan presiden Xi Jinping tepatnya pada tahun 2013, semakin diperketatnya internet dengan dipekerjakannya sekitar dua juta orang untuk melakukan analisis opini publik dengan menyensor secara manual dan melakukan pemantauan terhadap aktivitas situs daring. Selain itu adanya tim yang dibentuk untuk melakukan penyuntingan komentar dan unggahan yang patriotik, kebanyakan narasi yang muncul terkait dengan dukungan terhadap Partai Komunis Tiongkok (PKT). Pada masa jabatan Xi juga, penyaringan informasi bukan hanya sebatas media sosial, tetapi mencakup perusahaan internet Tiongkok yang diharuskan menandatangani perjanjian “Ikrar Publik terkait Pengaturan Diri dan Etika Profesional untuk Industri Internet Tiongkok” dan menegaskan agar media mengikuti garis ideologi partai demi menjaga keamanan, otoritas, dan kesatuan partai (Quan 2022, 21).

Dalam implementasinya, kebijakan *The Great Firewall of China* mencakup beberapa kategori utama pemblokiran situs web dalam penerapannya, seperti situs yang mengandung konten pornografi, permainan video, situs berbagi informasi (*slideshare* dan *thepiratebay*), media berita internasional (*nytimes*, *bloomberg*, dan *rfa*), situs yang berkaitan dengan Falun Gong atau praktik spiritual (*epochtimes*, *aboluowang*, dan *ntdv*). Tiongkok juga melakukan pemblokiran terhadap beberapa aplikasi yang cukup terkenal dikalangan masyarakat global, seperti *youtube*, *facebook*, *twitter*, *blogspot*, dan *wordpress*. Selain itu, Tiongkok juga mulai memperketat terkait dengan regulasi siaran televisi, terutama pelarangan terhadap promosi konten yang dianggap tidak sesuai dengan ketentuan usia, berupa pelecehan seksual, konten yang dapat memicu perang antar etnis, serta yang menjurus kepada LGBTQ (Zulfikar 2023, 28).

Internet yang dapat diakses oleh siapa saja dan dimana saja juga berpotensi memunculkan ancaman berupa ekstrimisme politik dan ideologi, melalui penyebaran berbagai jenis pesan yang bersifat sensitif. Saat ini, internet bahkan digunakan sebagai salah satu alat dalam strategi militer, karena kemampuan internet lebih mudah dalam menjangkau serta melakukan perekrutan pada orang-orang yang mungkin memiliki tujuan serupa, atau ingin melakukan penyerangan terhadap suatu negara maupun lembaga lainnya yang dianggap sebagai musuh mereka. Maka dari itu, Tiongkok memandang internet sebagai medan baru dalam pertempuran yang memiliki keterkaitan erat dengan isu keamanan nasional. Hal ini terutama terkait dengan kejahatan siber yang mencakup serangan dengan mengincar *social networking* atau pembocoran data, pemalsuan data, penyebaran hoaks, pemalsuan identitas, sampai dengan perang informasi (Zulfikar 2023, 28).

Dalam konteks ini, dapat dilihat bahwa kebijakan *The Great Firewall of China* yang diterapkan oleh Tiongkok dapat menjadi bahan pertimbangan yang cukup penting. Melihat bagaimana negara-negara di seluruh dunia sedang berupaya menghadapi tantangan dalam penyebaran informasi yang tidak terkendali, yang berpotensi mengancam keamanan nasional, hingga adanya pengikisan budaya yang terjadi akibat dari arus globalisasi. Setiap negara juga dituntut untuk mampu dalam menyeimbangkan antara perlindungan keamanan nasional dan keterbukaan informasi. Kebijakan *The Great Firewall of China* yang mendapatkan pro kontra masyarakat internasional dapat menjadi kajian yang menarik dalam dinamika saat ini.

Berdasarkan uraian yang telah dipaparkan oleh penulis di atas, maka dapat dilihat latar belakang dari kajian ilmiah ini adalah bagaimana kebijakan *The Great*

*Firewall of China* melalui perspektif sekuritisasi Barry Buzan dalam dunia digital oleh pemerintah Tiongkok. Apakah kebijakan ini hanya sebagai bentuk kontrol informasi oleh pemerintah, atau kebijakan ini telah dirancang serta dipersiapkan sebagai strategi jangka panjang dalam menghadapi dinamika globalisasi dan perkembangan teknologi informasi yang semakin meluas.

## **1.2 Rumusan Masalah**

Berdasarkan penjelasan latar belakang penelitian yang telah disampaikan, maka fokus utama dari riset ini adalah: Bagaimana Tiongkok melakukan sekuritisasi melalui kebijakan *Great Firewall of China* (2013-2025) dalam menjaga keamanan ruang siber Tiongkok?

## **1.3 Tujuan Penelitian**

Riset ini memiliki tujuan sebagai berikut:

1. Untuk menganalisis langkah-langkah yang telah dilakukan oleh Tiongkok dalam pembatasan akses internet demi menjaga keamanan nasional seperti penggunaan AI, big data, dan juga sistem penyaringan untuk melakukan pengawasan terhadap masyarakat sipil Tiongkok.
2. Untuk menjelaskan upaya kebijakan *Great Firewall Of China* dalam menunjukkan komitmen pemerintah Tiongkok untuk mengamankan dan mengendalikan ruang digital sebagai isu penting nasional, dengan melihat pengawasan dan kontrol negara terhadap aktivitas siber selama periode 2013-2025.

## **1.4 Cakupan Penelitian**

Penelitian ini akan menganalisis bagaimana kebijakan *Great Firewall of China* berperan dalam sektor keamanan nasional Tiongkok, dengan menggunakan

teori sekuritisasi yang dikemukakan oleh Barry Buzan. Rentang waktu yang diambil, yaitu dari tahun 2013 hingga 2025 karena sejak masa pemerintahan Xi Jinping, fokus pemerintah bukan hanya isu tradisional tetapi mulai fokus terhadap penegasan isu keamanan non-tradisional atau akses informasi digital yang menjadi salah satu prioritas hingga saat ini.

*Great Firewall of China* tidak hanya berfokus pada pembatasan akses maupun pemblokiran informasi digital dari luar Tiongkok, tetapi juga bertujuan untuk melindungi masyarakatnya dari pengaruh westernisasi dan propaganda yang dianggap dapat mengganggu kestabilan nasional Tiongkok. Kebijakan ini dianggap relevan dengan era digital saat ini, hal ini dikarenakan kontrol akan narasi publik dipandang penting untuk menjaga kestabilan politik dan kedaulatan nasional Tiongkok.

## **1.5 Tinjauan Pustaka**

Tinjauan pertama saya berasal dari jurnal yang berjudul “*China’s Great Firewall: Cybersecurity as Strategy for Building World Cyberpower*” yang ditulis oleh Harvardry Gerald Abraham Wowor, Arfin Sudirman, dan Falhan Hakiki (Wowor, Sudirman, and Hakiki 2023). Para penulis berpendapat bahwa penerapan *Great Firewall of China* tidak hanya bertujuan untuk menjaga keamanan digital, tetapi juga dapat menjadi alat dalam mempertahankan otoritarianisme Tiongkok. Para penulis menggunakan *cyberpower* dan *cybersecurity* sebagai kerangka analisis, yang menekankan bahwa *Great Firewall* tidak hanya memfilter atau membatasi informasi, wacana publik, maupun pembatasan akses terhadap narasi-narasi alternatif yang dapat memperkuat legitimasi dari Partai Komunis. Tetapi adanya *Great Firewall* juga dapat menjadi langkah strategis bagi Tiongkok untuk

membangun kekuatan digital nasional. Melalui pendekatan kualitatif, para penulis juga menyimpulkan bahwa *Great Firewall* bukan hanya terkait keamanan digital, tetapi bagaimana pemerintah berusaha untuk tidak bergantung pada produk luar negeri, melakukan inovasi, menjaga kestabilan dan keamanan negara terutama dari ancaman politik.

Tinjauan kedua berasal dari jurnal yang berjudul “*The Great Firewall of China: Praktik Kebijakan Sensor Internet pada Era Xi Jinping (2014-2021)*” yang ditulis oleh Faqih Albiruni Yahya, R, dan Tuty Nur Mutia (Yahya, R and Mutia 2023). Melalui pendekatan kualitatif, para penulis berpendapat bahwa kebijakan *Great Firewall of China* yang dibuat oleh Xi Jinping bukan hanya sekedar kebijakan yang berfungsi untuk menjaga keamanan, tetapi ingin membatasi pengaruh ideologi asing, mempertahankan legitimasi Partai Komunis, dan menjadikan Tiongkok sebagai kekuatan siber global. Selain itu, penulis juga menjelaskan bagaimana kebijakan *Great Firewall of China* semakin diperkuat dengan adanya regulasi seperti undang-undang keamanan siber, dan adanya pembentukan lembaga pengawasan khusus yang mengatur arus informasi di Tiongkok. Namun di sisi lain, penulis juga menyoroti dampak negatif dari kebijakan ini terhadap hak atas kebebasan berekspresi, serta banyak masyarakat merasa terkekang dan mencari berbagai cara untuk mendapatkan akses internet lebih, salah satunya dengan menggunakan VPN.

Tinjauan ketiga berasal dari jurnal yang berjudul “*Pembatasan Akses Internet Sebagai Upaya China Menjaga Keamanan Nasional: The Great Firewall of China*” yang ditulis oleh Faisal Mufti Zulfikar (Zulfikar 2023). Melalui pendekatan teori neorealisme, penulis menjelaskan bagaimana internet yang

seharusnya memberikan dampak positif karena membawa arus informasi lintas batas dan mendorong keterbukaan bagi seluruh lapisan masyarakat, justru dipandang oleh Tiongkok sebagai potensi ancaman yang perlu dikendalikan. Penulis menyoroti bahwa *The Great Firewall* merupakan bagian dari upaya pemerintah Tiongkok untuk menjaga stabilitas dan ideologi negara. Selain itu, penulis juga memaparkan bagaimana pembatasan internet tidak hanya berdampak secara domestik, tetapi juga terhadap perusahaan multinasional yang beroperasi di Tiongkok. Hal ini sejalan dengan konsep kedaulatan siber yang dikedepankan oleh Tiongkok dalam melegitimasi penyensoran hingga ke ranah internasional.

Tinjauan keempat berasal dari jurnal yang berjudul "*From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance*" yang ditulis oleh Birol Akduman (Akduman 2023). Penulis menjelaskan pengawasan Tiongkok bermula dari tembok besar yang berfungsi sebagai peringatan dan pertahanan. Hingga berevolusi menjadi *Great Firewall* yang berfokus pada keamanan siber dan dunia digital. Dapat dikatakan bahwa pengawasan telah menjadi elemen penting yang telah dilakukan oleh Tiongkok terutama untuk memperkuat legitimasi negara. *Great Firewall* juga dianggap sebagai kebijakan yang strategis untuk menghadapi dinamika global dan ancaman siber luar negeri. Namun disisi lain, kebijakan ini masih memunculkan perdebatan seputar keseimbangan keamanan nasional dan privasi individu.

Literatur-literatur diatas telah membahas kebijakan *The Great Firewall of China*. Berbagai literatur ini akan menjadi dasar untuk penelitian mengenai kebijakan Tiongkok dalam mengelola keamanan digital. Penelitian ini akan berbeda dengan literatur-literatur yang telah ada, karena lebih fokus terhadap analisis

sekuritisasi dunia digital yang dilakukan oleh pemerintah Tiongkok melalui kebijakan *Great Firewall*, dengan menggunakan perspektif Barry Buzan. Melalui perspektif sekuritisasi, penelitian ini bertujuan untuk menganalisis faktor-faktor yang mempengaruhi Tiongkok dalam mengimplementasikan kebijakan tersebut untuk menjaga kedaulatan dan stabilitas nasional antara tahun 2013 hingga 2025.

## 1.6 Kerangka Pemikiran

Dalam penelitian ini penulis menggunakan pendekatan sekuritisasi sebagaimana yang dirumuskan oleh Barry Buzan, Ole Waever, dan Jaap de Wilde dalam bukunya yang berjudul *Security: A New Framework for Analysis* yang diterbitkan pada tahun 1998. Barry Buzan memberikan pandangan baru terkait isu keamanan yang pada saat ini tidak hanya sebatas ancaman militer tetapi juga dapat berupa non-militer. Sehingga dalam hal ini negara juga memiliki wewenang atau hak untuk melakukan tindakan dalam menjaga keamanan negaranya, baik secara militer maupun non-militer.

Menurut Barry Buzan, sekuritisasi biasanya dimulai dengan tindakan ujaran (*speech act*). *Speech act* merupakan proses untuk membangun pemahaman bersama dalam mempertimbangkan serta merespon secara kolektif suatu ancaman, yang dimana akan memunculkan tindakan prioritas yang dilakukan untuk menjaga keberlangsungan hidup demi menghindari dampak buruk pada masa mendatang (Buzan, Wæver, and Wilde 1998, 26).

Dalam teori sekuritisasi terdapat beberapa elemen yang berperan penting, yaitu aktor sekuritisasi, audiens, *existential threat*, *referent object*, dan *emergency act*. Aktor sekuritisasi biasanya adalah individu atau kelompok, dapat berupa elit politik, pemimpin negara, maupun oposisi. Dalam hal ini, suatu isu dapat

dikategorikan sebagai masalah keamanan apabila terdapat pernyataan dari aktor tertentu dan diterima oleh masyarakat (Buzan, Wæver, and Wilde 1998, 40). Dalam hal ini juga terdapat *functional aktor* yang dimana ini merupakan pihak-pihak yang berperan dalam sektor tertentu dan memberikan pengaruh besar terhadap proses atau keputusan yang diambil mengenai isu keamanan untuk melindungi *referent object* (Buzan, Wæver, and Wilde 1998, 36). Sementara itu, audiens dapat didefinisikan sebagai individu maupun kelompok yang memiliki kapabilitas dalam menyetujui maupun menolak isu ancaman keamanan yang disampaikan oleh aktor sekuritisasi (Buzan, Wæver, and Wilde 1998, 31).

Ancaman keamanan pada saat ini bersifat *existential*, yaitu mengancam keberadaan maupun kelangsungan hidup suatu entitas tertentu. *Existential threat* tidak selalu berkaitan dengan standar universal sebagaimana yang telah ditetapkan dalam beberapa hal yang dianggap mengancam kehidupan individu, tetapi dapat dipahami dengan menspesifikkan karakter dari objek (*Referent object*) yang menjadi rujukan khusus seperti militer, politik, ekonomi, sektor masyarakat, dan lingkungan. Dalam konteks militer hal ini dapat merujuk terhadap negara maupun kelangsungan hidup angkatan bersenjata. Sementara dalam konteks politik, merujuk pada ancaman eksistensial terhadap kedaulatan maupun ideologi negara (Buzan, Wæver, and Wilde 1998, 21).

*Referent object* dapat dipahami sebagai sesuatu yang dianggap penting untuk dilindungi karena adanya ancaman, dengan objek yang dipertahankan berdasar pada kelangsungan hidup yang dapat berupa negara, bangsa, individu, dan identitas. Dari sini, dapat memunculkan *emergency act*, yaitu kebijakan yang dibuat secara khusus oleh aktor sekuritisasi sebagai respons terhadap keadaan darurat yang

harus segera diselesaikan, meskipun dilakukan secara terpaksa dan sepihak, serta berada di luar batas prosedur politik selama tujuannya untuk keberlangsungan objek yang dilindungi.

Berdasarkan penjelasan teori sekuritisasi yang dikembangkan oleh Barry Buzan, penulis menganalisis bahwa kebijakan *The Great Firewall of China* telah memenuhi kriteria sekuritisasi. Tujuan utama sekuritisasi dalam konteks ini adalah memperoleh legitimasi politik bagi negara untuk mengambil tindakan luar biasa terhadap isu yang sebelumnya berada di luar kategori keamanan. Informasi digital yang pada awalnya dipandang sebagai bagian dari proses modernisasi kemudian dibingkai oleh pemerintah Tiongkok sebagai isu keamanan melalui proses politik dan wacana sekuritisasi, sehingga diposisikan sebagai *existential threat* terhadap stabilitas nasional, kedaulatan negara, dan kontrol ideologis. Proses tersebut menjelaskan perubahan status informasi digital dari isu non-keamanan menjadi persoalan keamanan, yang kemudian mendorong negara untuk mengambil tindakan di luar mekanisme kebijakan umum. Dalam konteks ini, *emergency act* tidak muncul secara tiba-tiba, melainkan merupakan hasil dari keberhasilan proses sekuritisasi, ketika pemerintah Tiongkok sebagai aktor sekuritisasi berhasil meyakinkan audiens dengan menyatakan arus informasi digital sebagai ancaman yang mendesak dan memerlukan penanganan khusus demi menjaga keberlangsungan *referent object*. Oleh karena itu, Tiongkok memperoleh legitimasi untuk menerapkan kebijakan khusus diluar dari kebijakan konvensional (Stepka 2022, 18-19).

## 1.7 Argumen Sementara

Kebijakan *The Great Firewall of China* dalam penelitian ini dianalisis melalui perspektif Barry Buzan sebagai respons negara terhadap *existential threat* dalam ranah digital. Ancaman tersebut dipahami sebagai arus informasi asing, khususnya yang berasal dari Barat, karena dinilai berpotensi mengganggu stabilitas politik, identitas nasional, dan keamanan siber Tiongkok. Pemerintah Tiongkok melalui pernyataan resminya melakukan *speech act* dengan membingkai pembatasan akses internet sebagai langkah untuk melindungi nilai-nilai nasional dari pengaruh eksternal (Buzan, Wæver, and Wilde 1998, 26). Presiden Xi Jinping sebagai *securitizing actor* bersama dengan Cyberspace Administration of China (CAC) berperan sebagai *functional actor*, secara aktif membingkai arus informasi asing sebagai ancaman terhadap kedaulatan negara dan membantu dalam perumusan serta implementasi kebijakan keamanan siber (Buzan, Wæver, and Wilde 1998, 36-40).

Audiens dalam proses sekuritisasi ini adalah masyarakat dan elite politik yang diharapkan menerima narasi terkait ancaman tersebut sebagai isu nyata dan mendesak. Ancaman yang dibingkai kemudian diarahkan pada *referent object* yang dianggap perlu untuk dilindungi, karena berkaitan dengan kedaulatan negara, nilai-nilai budaya Tiongkok, serta legitimasi politik pemerintah (Buzan, Wæver, and Wilde 1998, 36). Atas dasar ini, negara mengambil *emergency acts* berupa pemblokiran situs asing, pengawasan dan pembatasan konten informasi, serta penguatan regulasi siber. Dengan demikian, kebijakan *The Great Firewall of China* diposisikan bukan sekadar sebagai instrumen pembatasan kebebasan digital,

melainkan sebagai tindakan luar biasa yang dilegitimasi untuk melindungi objek vital negara dari ancaman eksistensial.

## **1.8 Metode Penelitian**

### *1.8.1 Jenis Penelitian*

Penelitian ini menggunakan metode kualitatif. Pendekatan ini lebih tepat untuk memahami secara mendalam dinamika sosial dalam ranah Internasional yang kompleks. Metode ini mengandalkan teks dan narasi serta berorientasi pada pemaknaan dari berbagai sudut pandang partisipan. Dalam penelitian kualitatif, peneliti berperan sebagai instrumen utama yang memungkinkan pengumpulan data secara deskriptif, kontekstual, dan fleksibel dalam menangkap perkembangan dinamika sosial (Nurrisa, Hermina, and Norlaila 2025, 794). Maka daripada itu, metode ini akan digunakan sebagai alat untuk menyelesaikan topik sekuritisasi dunia digital oleh pemerintah Tiongkok melalui kebijakan *The Great Firewall of China* tahun 2013-2025.

### *1.8.2 Subjek dan Objek Penelitian*

Subjek dalam penelitian ini adalah Tiongkok. Sedangkan objek dalam penelitian ini adalah kebijakan sekuritisasi dunia digital pemerintah Tiongkok melalui kebijakan *The Great Firewall of China* yang ditinjau dari perspektif sekuritisasi Barry Buzan.

### *1.8.3 Metode Pengumpulan Data*

Penelitian ini berfokus pada analisis yang menggunakan data sekunder yang diperoleh dari berbagai sumber seperti artikel ilmiah, buku, jurnal, laporan, serta berita yang telah terverifikasi kredibilitasnya.

#### 1.8.4 Proses Penelitian

Penelitian ini memanfaatkan internet sebagai pengumpulan data dengan cara mengunduh dan membaca artikel ilmiah, jurnal, buku, dan laporan yang berkaitan dengan sekuritisasi Tiongkok. Setelah pengumpulan data, penulis akan melakukan proses reduksi dengan mengelompokkan informasi, membuang data yang tidak relevan, serta menyaring informasi yang lebih spesifik dan sesuai dengan fokus penelitian. Data yang telah dipilih akan disajikan dalam bentuk narasi pada bab dan sub-bab yang relevan (Purnia and Alawiyah 2020, 7). Tahap akhir dari penelitian ini adalah penyusunan argumen sementara berdasarkan data yang tersedia, yang nantinya akan diperkuat dengan temuan data selanjutnya.

#### 1.9 Sistematika Pembahasan

Secara sistematis, penelitian ini akan diuraikan menjadi empat bab utama:

- Bab pertama menjelaskan terkait dengan latar belakang, rumusan masalah, cakupan penelitian, tujuan penelitian, kerangka pemikiran, kajian pustaka, argumen sementara, dan metode penelitian.
- Bab kedua akan menjelaskan mengenai tindakan sekuritisasi yang dilakukan oleh Tiongkok terhadap dunia digital melalui kebijakan *The Great Firewall of China*. Pada bab ini menjadi pijakan awal sebelum masuk ke tahap analisis teori yang akan dibahas pada bab selanjutnya di bab 3, pengantar tersebut diuraikan melalui identifikasi permasalahan dan dinamika yang muncul dari kebijakan *The Great Firewall of China*.
- Bab ketiga, penulis mengaplikasikan teori sekuritisasi Barry Buzan terhadap studi kasus yang telah diangkat, dengan membuat pembagian sub bab-topik utama yaitu melalui analisis faktor internal dan eksternal.

- Pada bagian terakhir, penulis menyusun kesimpulan dan saran yang bertujuan untuk merangkum keseluruhan penelitian yang telah dilakukan, sekaligus memberikan rekomendasi yang dapat menjadi rujukan bagi penelitian di masa mendatang.

## BAB 2

### DINAMIKA KEBIJAKAN THE GREAT FIREWALL OF CHINA DALAM KONTEKS SEKURITISASI RUANG DIGITAL

Bab ini membahas dinamika kebijakan *Great firewall of China* sebagai bagian dari upaya pemerintah Tiongkok dalam mengelola dan mengendalikan ruang digital Tiongkok. Bab ini juga akan mengfokuskan pada perkembangan dan perbedaan kebijakan sejak fase awal hingga penguatannya pada era kepemimpinan Xi Jinping, dengan melihat latar belakang kemunculan kebijakan, tujuan pengendalian arus informasi, serta peran negara dalam menjaga stabilitas politik dan keamanan siber. Bab ini menjadi landasan empiris untuk memahami konteks kebijakan sebelum dianalisis menggunakan perspektif teori sekuritisasi.

#### 2.1 Dinamika Kebijakan *Great Firewall of China*

Pada subbab ini akan menganalisis dinamika kebijakan *The Great Firewall of China* yang dilatarbelakangi dari perkembangan teknologi digital Tiongkok. Pembahasan ini akan berfokus pada beberapa faktor kemunculan kebijakan, termasuk peningkatan penggunaan internet dan kekhawatiran negara terhadap arus informasi global. Subbab ini akan menjelaskan kebijakan *The Great Firewall of China* sebagai sebuah instrumen penting dalam pengendalian ruang digital nasional Tiongkok.

Setelah kematian Mao Zedong tepatnya pada tahun 1976, Tiongkok di bawah kepemimpinan Deng Xiaoping mulai mengalami masa reformasi. Pada masa ini muncul kebijakan *Open Door Policy* yang mengubah arah pembangunan Tiongkok. Kebijakan ini merupakan awal mula Tiongkok membuka diri terhadap negara lain dengan melakukan kerjasama, saling bertukar ilmu pengetahuan,

inovasi dan teknologi (Pradana 2022, 4). Dari kebijakan ini, Tiongkok mulai mengembangkan perangkat sistem pengawasan negara berbasis teknologi yang merupakan bentuk nyata dari adanya modernisasi dan juga penguatan terhadap kontrol sosial masyarakat Tiongkok.

Dalam perkembangannya, Tiongkok merupakan salah satu negara yang telah menunjukkan kemajuan yang pesat dalam bidang teknologi dan komunikasi. Perkembangan ini tidak hanya mencerminkan terkait dengan kemajuan ekonomi maupun inovasi teknologi Tiongkok, tetapi juga memperlihatkan bagaimana perkembangan teknologi telah menjadi bagian dari kehidupan masyarakat Tiongkok. Sejak tahun 1999, pengguna internet di Tiongkok telah mencapai sekitar 9 juta jiwa, yang dimana ini menandakan tingginya interkoneksi antar masyarakat Tiongkok (Yusrizal 2014, 5).

Dalam hal ini keamanan siber menjadi salah satu aspek penting yang tidak dapat diabaikan. Keamanan siber dapat diartikan sebagai kekuatan suatu negara untuk melindungi diri dan juga instansi yang berada didalamnya dari berbagai ancaman digital yang ada, seperti spionase, sabotase, kejahatan daring, penipuan, pencurian identitas, dan interaksi siber lainnya yang berpotensi untuk merusak sistem pemerintahan (Guo 2018, 139). Hal ini dikarenakan adanya akses yang tidak terbatas terhadap ruang siber yang dapat menyampaikan pesan maupun informasi secara bebas, maka negara perlu untuk memberikan batasan yang dapat menghindari ancaman dunia digital yang bersifat kompleks.

Sebagai respon terhadap pesatnya arus internet yang masuk ke Tiongkok, membuat pemerintah Tiongkok melahirkan sebuah kebijakan yang dikenal dengan nama *The Great Firewall of China*. *The Great Firewall of China* merupakan

kebijakan yang telah dikembangkan pada tahun 1990-an. Kebijakan ini dianggap memiliki peran penting bagi keberlangsungan Partai Komunis Tiongkok. Salah satu tujuan utama dari adanya kebijakan ini adalah bagaimana mempertahankan posisi dari partai komunis dengan mengendalikan arus informasi ruang digital (Yahya, R and Mutia 2023, 22). Kebijakan ini dilatarbelakangi karena adanya kekhawatiran potensi transformatif dari tindakan komunikatif yang dianggap dapat mengganggu ideologi partai melalui kemunculan ide dan gagasan yang tidak selaras dengan nilai dan budaya yang dijunjung oleh negara Tiongkok.

Selain terkait dengan menjaga ideologi partai, kebijakan ini dianggap penting karena sistem penyensoran dan pemblokiran dilakukan terhadap konten yang dianggap dapat menyebarkan ujaran kebencian, serta informasi palsu yang dapat memicu terjadinya perselisihan, perjudian, kekerasan, pembunuhan, hingga konten yang dianggap dapat mengganggu stabilitas keamanan jaringan Tiongkok (Zulfikar 2023, 29). Pemerintah Tiongkok melihat bahwa dengan adanya arus informasi maupun komunikasi yang tidak segera dikendalikan baik dari sektor pendidikan, hiburan, dan bisnis maka dapat memberikan dampak buruk yang berpotensi memunculkan ketegangan sosial serta politik. Kebijakan ini sebagai salah satu upaya yang dilakukan oleh Tiongkok untuk mengendalikan dan menjaga stabilitas nasional siber Tiongkok dengan menyentuh seluruh lapisan masyarakat, dan dapat membuat perlindungan secara menyeluruh, terutama terhadap ruang digital dengan efektif.

Tiongkok sebagai salah satu negara yang telah menetapkan batasan akses informasi dan komunikasi, dengan melibatkan ratusan masyarakat sipil dengan sistem penyensoran yang telah diresmikan, terperinci, dan memadai. Memasuki

awal tahun 2002, Google pernah diblokir oleh Tiongkok tetapi tidak berselang lama pemblokiran dicabut tetapi tetap dengan adanya batasan pencarian. Tiongkok juga membuat berbagai macam perjanjian serta persetujuan yang harus ditandatangani oleh pihak Google. Pada tahun 2010, Tiongkok pernah menerbitkan *White Paper* terkait dengan “*The Internet in China*” yang didalamnya menegaskan terkait dengan pentingnya internet sebagai sebuah sarana utama dalam meningkatkan ekonomi, politik, budaya, dan kehidupan sosial Tiongkok. Internet juga ditempatkan sebagai sebuah bagian dari adanya strategi nasional dengan mengutamakan infrastruktur digital, dan pengembangan riset. *White paper* menegaskan adanya prinsip *cyber sovereignty*, regulasi pemerintah, keamanan daring anak dibawah umur, pengawasan publik dan pendidikan hukum serta etika. Hal ini akan membuka akses layanan dan hak warga dalam kerangka hukum. Perlu diketahui jika *White Paper* berbeda dengan *The Great Firewall of China*, *White Paper* menekankan regulasi, pengembang internet dan *cyber sovereignty*. Sedangkan *The Great Firewall of China* menekan pada pemblokiran dan penyensoran konten internet. Hingga tercatat internet memainkan peran penting dalam perkembangan anak dibawah umur, sementara itu informasi internet justru ada yang bersifat pornografi, ilegal, dan berbahaya dengan memasuki tahap merusak kesehatan fisik dan psikologis kaum muda. Maka dari itu, hal ini diakui sebagai sebuah isu penting yang menjadi perhatian pemerintah (USC US-China Institute 2010).

Hingga pada tahun 2012 terdapat beberapa konten daring yang telah dilakukan pemblokiran karena dianggap dapat mengancam stabilitas Tiongkok, yaitu website bertukar informasi (*thepiratebay.se*, *slideshare.net*); media berita luar

negeri (*nytimes.com*, *Bloomberg.com*, *rfa.org*); media aplikasi luar negeri (*youtube*, *facebook*, *twitter*, *wordpress*, *blogspot*); website Falun Gong atau gerakan spiritual serta latihan meditasi (*epochtimes*, *aboluowang*, [www.ntdv.com](http://www.ntdv.com)), dan memasuki tahun 2015 hingga 2016 kebijakan sensor tidak hanya terkait dengan isu politik tetapi memasuki fase moral dan sosial seperti situs porno, serta konten yang mengandung unsur LGBT (Zulfikar 2023, 27).

Namun semakin pesatnya arus globalisasi tentunya membuat pertumbuhan internet di Tiongkok terus mengalami lonjakan yang cukup signifikan. Hal ini dapat dilihat pada tahun 2024, dimana jumlah pengguna internet di Tiongkok mencapai 1,099 miliar jiwa, besaran lonjakan yang terjadi sekitar 7,42 juta pengguna jika dibandingkan pada tahun-tahun sebelumnya. Jumlah ini tentunya menempatkan Tiongkok sebagai negara dengan pengguna internet terbesar di dunia. Dari total keseluruhan, penggunaan internet di wilayah perkotaan mencapai 795 juta pengguna atau sekitar 72,3% dari total keseluruhan populasi masyarakat perkotaan Tiongkok. Sedangkan di pedesaan terdapat sekitar 304 juta jiwa pengguna internet atau sekitar 27,7% dari total populasi pedesaan Tiongkok (China Internet Network Information Center (CNNIC) 2024).

Meskipun kebijakan ini juga dinilai efektif dalam menjaga keamanan siber digital dan kedaulatan keamanan nasional Tiongkok, akan tetapi disisi lain dalam penerapannya juga menimbulkan hambatan dalam berbagai aktivitas, seperti komunikasi dan urusan bisnis. Adanya pembatasan akses terhadap sejumlah situs dan media sosial menimbulkan interaksi antar individu maupun kelompok menjadi terbatas. Akibatnya, banyak pengguna internet di Tiongkok melakukan berbagai cara untuk melewati sistem penyensoran dengan tujuan dapat mengakses berbagai

situs serta memperoleh kebebasan dalam berekspresi dan berkomunikasi yang lebih luas dalam dunia maya (Yahya, R and Mutia 2023, 21).

Dengan demikian, kebebasan internet dipandang sebagai ancaman yang dapat mengganggu stabilitas kekuasaan. Maka dari itu sistem penyensoran di Tiongkok ditingkatkan statusnya menjadi kebijakan keamanan nasional, meskipun menuai kritik karena dinilai membatasi kebebasan berekspresi dan berpendapat.

## **2.2 Kebijakan *The Great Firewall of China* Era Kepemimpinan Xi Jinping**

Pada sub bab ini akan membahas terkait dengan kebijakan *The Great Firewall of China* pada era Xi Jinping, khususnya pada periode tahun 2013-2025, dengan fokus pada pembatasan akses internet, pengendalian informasi, pemblokiran konten, dan peningkatan keamanan siber yang semakin diperketat dengan tujuan menjaga stabilitas dan ideologi negara.

Ideologi merupakan sebuah bentuk sistem pemikiran yang terdiri dari sekumpulan gagasan, ide, keyakinan, dan kepercayaan yang berfungsi sebagai sebuah landasan dalam mengatur kehidupan sosial secara menyeluruh dan terstruktur. Ideologi mencakup beberapa aspek kehidupan dalam masyarakat yang menjadikannya sebagai sebuah pedoman untuk mencapai tujuan serta menegakkan nilai-nilai dasar kehidupan dalam berbangsa dan bernegara (Mohtar and Dewantara 2021, 466).

Tiongkok merupakan salah satu negara yang memandang ideologi sebagai unsur penting yang tidak hanya berperan sebagai sebuah dasar pemikiran, tetapi juga sebuah pedoman dalam melegitimasi kebijakan dan memperkuat kekuasaan negara. Dalam upayanya menyebarluaskan ideologi, Tiongkok menggunakan

berbagai macam cara, diantaranya memanfaatkan berbagai macam institusi dan membentuk kelompok yang diberi wewenang oleh negara. Terlihat sejak era Mao Zedong hingga Hu jintao, penyebaran ideologi dilakukan melalui berbagai macam sarana seperti pendidikan, agama, hingga media dan pers yang berfungsi sebagai alat untuk memperkuat penyebaran ideologi (Pashya et al. 2021, 3).

Pada 14 Maret 2013, Kongres Nasional Tiongkok secara resmi menetapkan Xi Jinping sebagai Presiden Republik Rakyat Tiongkok. Xi Jinping memandang ideologi sebagai elemen kunci penting yang tidak hanya berperan sebagai sebuah dasar pemikiran, tetapi juga sebagai pedoman dalam melakukan legitimasi kebijakan dan mempertahankan stabilitas politik. Xi Jinping juga memperoleh legitimasi politik yang kuat, termasuk penghapusan batas masa jabatan presiden yang sebelumnya dibatasi hanya dua periode. Xi Jinping juga mulai menekankan pentingnya supremasi hukum dan profesionalisme dalam sistem peradilan yang bertujuan sebagai upaya Tiongkok dalam memperkuat posisi sosialisme dengan karakteristik Tiongkok, hal ini sekaligus melemahkan faksi politik yang dianggap berpotensi dalam menyaingi kekuasaannya. Lebih jauh, Xi Jinping juga membuat sebuah visi jangka panjang yang dapat menempatkan Tiongkok sebagai sebuah kekuatan utama dunia pada tahun 2050, terutama dalam bidang politik, militer, teknologi, dan pembangunan ekonomi nasional (Albeit F. 2025, 887).

Pada tahun 2013 dalam pidatonya di *National Propaganda and Ideology Work Conference*, Xi Jinping menegaskan bahwa media memang memiliki peran yang strategis dalam mempertahankan citra dan reputasi suatu negara. Xi Jinping juga menekankan bahwa Tiongkok perlu dalam *enhancing international communication capacity* atau memperkuat cara dan kemampuan Tiongkok dalam

menyampaikan pesan maupun membentuk citra negara dalam ranah internasional. Selain itu juga *innovating foreign propaganda methods* atau bagaimana Tiongkok menyebarkan pesan politik dan ideologi yang digunakan kepada dunia luar. Yang terakhir *strengthening the national discourse system* atau membangun sebuah narasi nasional yang kuat dan sesuai dengan nilai maupun sudut pandang Tiongkok (Klimeš and Maurizio 2018, 315-318).

Melalui strategi ini, Tiongkok berupaya membangun konsep dan narasi baru yang berfungsi sebagai jembatan komunikasi antara Tiongkok dan dunia internasional. Narasi tersebut dirancang untuk menyampaikan citra positif terkait Tiongkok, dengan menekankan pada pentingnya “*China Story*” atau “menceritakan kisah Tiongkok dengan baik” sebagai sebuah inti dari diplomasi komunikasi yang ingin untuk dikembangkan (Klimeš and Maurizio 2018, 318).

Xi Jinping memanfaatkan peran media dalam menyebarluaskan kebijakan pemerintah melalui berbagai saluran media seperti televisi, surat kabar, radio, dan *platform* digital (Pashya et al. 2021, 7). Media dan pers mendapatkan perhatian khusus sejak dibawah kepemimpinan Xi Jinping. Dalam masa pemerintahannya, Xi Jinping juga menekankan pada perlunya menanamkan nilai-nilai yang menggambarkan karakteristik dari identitas nasional Tiongkok. Upaya ini dilakukan oleh Tiongkok untuk mencegah masuknya ideologi asing yang dapat mengganggu stabilitas politik dan budaya Tiongkok.

Hal ini merujuk pada tujuan pemerintah untuk menciptakan “*Chinese Spirit*” atau identitas yang kuat seperti taat kepada kebijakan, patriotisme, kerja keras, harmoni, integritas, dan kepercayaan terhadap Partai Komunis. Wacana politik juga disebarluaskan melalui media dengan tujuan dapat menembus seluruh

khalayak dan membentuk pola pikir masyarakat (Zhang 2022, 606). Dengan memandang media internet sebagai sebuah instrumen penting yang dapat membangun opini, maka pengendalian terhadap arus informasi dan ruang digital juga menjadi penting bagi Tiongkok. Hal ini yang membuat kebijakan *The Great Firewall of China* semakin diperketat dengan tujuan untuk menjaga arus informasi dan stabilitas nasional.

Pada Desember 2013, adanya peningkatan keamanan siber di Tiongkok yang dibuat oleh *Political Bureau of the Communist Party of China* (politburo) yang membentuk kelompok pimpinan pusat yang bernama *Zhongyang Wangluo He Xinxihua Lingdao Xiaozu* atau yang lebih dikenal dengan nama *Central Leading Group of Cybersecurity and Information*, yang dipimpin langsung oleh Presiden Xi Jinping dalam menyusun dan merumuskan strategi nasional, rencana pembangunan, serta kebijakan terkait dengan keamanan siber. Awalnya pemerintah mempekerjakan sekitar dua juta analisis opini publik untuk melakukan penyensoran manual dan juga melakukan pemantauan terhadap aktivitas pengguna internet. Disisi lain, selain memanfaatkan sumber daya manusia, pemerintah juga memanfaatkan permainan algoritma dengan membuat komentar serta unggahan yang pro partai untuk mendukung pemerintah dalam ruang digital (Quan 2022, 21).

Sebagai tindak lanjut, pada Februari 2014 terbentuklah kantor kelompok pimpinan pusat urusan dunia maya yang dikenal dengan nama *Cyberspace Administration of China* (CAC) (Yuen 2015, 54). Pada November 2014, pemerintah Tiongkok melakukan *World Internet Conference* atau konferensi internet dunia pertama kalinya sebagai sebuah sarana dalam mempromosikan visinya terhadap tata kelola internet global terutama dalam konsep kedaulatan siber.

Tiongkok juga menegaskan pentingnya hak setiap negara untuk mengendalikan konten dan arus internet yang masuk kedalam negara secara menyeluruh, dengan memperkuat otonomi dan kemandirian digital, sehingga tidak terpengaruh oleh kapitalisme, westernisasi, dan intervensi politik asing. Dalam hal ini secara langsung menegaskan jika posisi negara sebagai aktor yang memiliki otoritas tertinggi dalam ruang digital (Xu and Yu 2022, 2).

Selain dibentuknya *Cyberspace Administration of China (CAC)* dan *World Internet Conference*, pada periode ini juga negara mulai melakukan penyatuan lembaga-lembaga yang sebelumnya terfragmentasi, sehingga kendali dan pembuatan kebijakan dapat berjalan dengan efektif. Hingga dari sinilah mulai lahirnya kebijakan strategis seperti Undang-Undang Keamanan Siber yang mengatur segala aspek digital (Creemers 2021, 19). Pada tahun ini juga terdapat pengawasan dan penyensoran terhadap konten daring, baik konten individu maupun komersial. Pemerintah juga mulai menetapkan standar bagi para jurnalis media digital, mengatur akun publik WeChat, serta memperluas sistem penggunaan nama asli sebagai mekanisme dalam melakukan kontrol untuk membatasi tindakan yang dianggap tidak sesuai ketetapan atau dinilai merugikan Tiongkok dalam dunia digital (Creemers, n.d., 13).

Memasuki tahun 2015, arah dari kebijakan siber di Tiongkok menunjukkan peningkatan, hal ini dilihat dari pernyataan yang diberikan oleh Lu Wei selaku kepala CAC yang memperkenalkan konsep kedaulatan siber sebagai sebuah pondasi utama dalam mempertahankan posisi Tiongkok sebagai negara dengan tata kelola internet global. Adanya perbedaan antara model tata kelola ruang berbasis pada *multi-stakeholder* yang lebih mencerminkan kepentingan negara Barat, dan

tata kelola ruang multilateral yang memberikan negara kendali utama dalam menentukan arah dan aturan untuk ruang digitalnya sendiri. Hal ini semakin dipertegas oleh pernyataan Xi Jinping dalam pidatonya yang menyatakan bahwa setiap negara memiliki hak penuh untuk mengatur arus informasi dan stabilitas dunia digital sebagai bagian dari kedaulatan nasional (Schia and Gjesvik 2017, 2).

Di tahun 2015, Tiongkok mulai memperketat pemblokiran VPN (*Virtual Private Network*), layanan yang memungkinkan pengguna internet Tiongkok mengakses melalui koneksi terenkripsi dan tersembunyi. VPN dianggap sebagai sebuah ancaman karena dapat menembus *The Great Firewall of China* atau tembok api besar yang memberi akses ke *platform* asing, memungkinkan penyebaran kritik maupun informasi yang dapat mengganggu stabilitas sosial dan politik Tiongkok (Wu and Mai 2019, 5064). Pemerintah juga memperkuat kerangka hukum terkait dengan siber yang tertuang dalam Undang-Undang Keamanan Siber dan Undang-Undang Anti Terorisme, yang dimana ini mewajibkan perusahaan teknologi untuk menyimpan data nasional, melakukan sensor konten sensitif, dan bekerja sama dengan pihak berwenang dalam mengelola deskripsi data (Freedom House 2022).

Pada tahun 2016, pemerintah Tiongkok mulai melakukan pendorongan terhadap penyedia aplikasi untuk lebih terstruktur dalam melakukan pengelolaan data bagi para pengguna, serta melakukan registrasi terlebih dahulu, yang membuat penyimpanan data secara menyeluruh dan lengkap, membuat kebijakan *The Great Firewall of China* menjadi substansial (Freedom House 2016). Pada tahun 2017 Undang-Undang Keamanan Siber mulai diberlakukan secara efektif yang dengan khusus mengatur operator jaringan, terutama dari aspek infrastruktur informasi penting atau yang lebih dikenal dengan istilah CIIO (*Critical Information*

*Infrastructure Operators*) pihak yang bertugas dalam menjaga ketersediaan data serta kerahasiaannya untuk kepentingan keamanan negara Tiongkok (Smeenk et al. 2017). Hingga tepat pada 27 Juni 2017, disahkannya *National Intelligence Law* yang membahas terkait dengan kewajiban lembaga negara dan masyarakat yang saling mendukung dan bekerja sama dalam pengumpulan data untuk keamanan nasional.

Pada tahun 2018, implementasi dari Undang-Undang Keamanan Siber Tiongkok semakin diperkuat dengan adanya sejumlah peraturan turunan yang baru, dengan memperjelas kewajiban bagi para operator jaringan dan juga sektor infrastruktur informasi kritis. Ketentuan ini tidak hanya diberlakukan bagi para lembaga negara, tetapi juga meliputi beberapa sektor seperti transportasi, telekomunikasi, perbankan, asuransi, farmasi dan pelayanan kesehatan lainnya. Pada 15 September 2018, pemerintah Tiongkok mulai memberlakukan *Provisions on Internet Security Supervision and Inspection* yang memberikan akses atau kewenangan kepada otoritas keamanan publik dalam melakukan pengawasan maupun pemeriksaan langsung terhadap penyediaan internet tetapi berdasarkan pada kebutuhan dan tingkat resiko keamanan siber (HSF Kramer 2018).

Pada tahun 2019, *The Great Firewall of China* semakin diperketat bukan hanya pada pemblokiran akses tetapi diperluas hingga pengendalian ruang wacana domestik atau seluruh bentuk ruang komunikasi, percakapan, hingga pertukaran informasi. Pada tahun ini juga terdapat beberapa aturan baru yang dikeluarkan oleh *China Netcasting Service Association* terkait dengan pengawasan konten online yang didalamnya mencakup video pendek, *streaming*, dan standar editorial untuk *platform* internet Tiongkok baik yang mengandung unsur humor, satir politik, dan

bentuk ekspresi kreatif lainnya yang masuk kategori sindiran serta berpotensi menggiring opini (Freedom House 2019). Setiap platform diwajibkan untuk mempekerjakan minimal satu manusia untuk meninjau setiap 1000 video yang di unggah dalam sehari, serta peninjauan dilakukan secara otomatis dan manual.

Pada tahun 2020, saat pandemi COVID-19, pemerintah Tiongkok semakin memperketat kebijakan *The Great Firewall of China*. Pada masa ini dianggap internet sebagai sebuah ancaman, karena mempercepat digitalisasi dan ketergantungan pada dunia digital (Freedom House 2020). Pemerintah Tiongkok juga mulai menerapkan *Cybersecurity Review Measures* atau sebuah regulasi yang mewajibkan adanya peninjauan terhadap suatu produk atau layanan teknologi digital yang memungkinkan menimbulkan ancaman keamanan, terkhusus bagi para operator infrastruktur dan *platform* digital besar (China Law Translate 2020).

Pada tahun 2021, pemerintah Tiongkok melakukan kontrol dengan kampanye *Clear and Bright* atau sebuah kontrol terhadap konten digital yang mengganggu ideologis, seperti *fan culture*, *influencer*, dan media sosial yang membentuk opini publik secara negatif. Adanya penambahan regulasi yang dikenal *Data Security Law* dan *Personal Information Protection Law*, yang dimana ini memperkuat kontrol negara untuk menyimpan, memproses dan membatasi transfer data ke luar negeri (Simangunsong and Sijabat 2024, 326).

Pada tahun 2022, *Cybersecurity Review Measures* kembali direvisi dengan memperketat setiap perusahaan yang mengelola data pribadi lebih dari satu juta pengguna untuk menjalani pemeriksaan keamanan nasional sebelum melakukan kerja sama maupun penawaran saham dengan pihak luar. Pembaharuan ini menekankan upaya meminimalisir risiko kebocoran data, pengawasan

terhadap alur data strategis, serta pemantauan terhadap algoritma dan sistem rekomendasi atau saran konten maupun informasi tertentu (Creemers and Webster 2022).

Pada tahun 2023, pemerintah Tiongkok mulai berfokus pada AI Generatif dan Teknologi *Deep Synthesis*. Pemerintah Tiongkok mulai menekankan adanya risiko dalam keamanan informasi dan integritas konten yang dapat ditimbulkan dari AI, termasuk didalamnya potensi penyebaran informasi palsu yang diakibatkan oleh kebocoran privasi, integritas ideologis, dan bias informasi maupun diskriminatif. Terdapat juga regulasi *Deep Synthesis* yang menetapkan kewajiban bagi para penyedia AI untuk memastikan output yang dihasilkan mulai dari teks, gambar, audio, video, dan adegan virtual wajib untuk mematuhi pedoman hukum dan nilai ideologis yang dianut negara (Zou and Zhang 2024, 4).

Pada tahun 2024, adanya pengetatan regulasi pada sektor tata kelola konten digital yang semakin ditunjukkan sejak CAC menetapkan dua instrumen pada 14 September. Instrumen pertama, yaitu peningkatan *Measures for the Labelling of AI Generated Synthetic Content* yang menjadikan pengawasan semakin ketat terhadap penyedia layanan informasi internet dengan memberikan label pada konten yang dihasilkan oleh AI. Hal ini tidak hanya penetapan jenis label, tetapi termasuk waktu, mekanisme, dan verifikasi yang harus dilakukan sebelum konten disebar. Rancangan ini juga diwajibkan bagi setiap *platform* distribusi aplikasi untuk dapat memastikan bahwa aplikasi yang disediakan sesuai dengan aturan pelabelan konten AI. Instrumen kedua, terkait dengan *Cybersecurity Technology Labelling Method for Content Generated by AI* yang mengatur ketentuan teknis yang lebih rinci

sebagai sebuah standar wajib melalui konsultasi ekstensif dengan para ahli industri maupun perusahaan (Zou and Zhang 2024, 10).

Pada tahun 2025 belum terdapat kebijakan resmi terkait *The Great Firewall of China*. Akan tetapi pada tahun ini Tiongkok mengalami gangguan pada port TCP 443 yang merupakan jalur utama jalan HTTPS, sehingga berdampak pada kesulitan akses layanan internasional seperti iCloud dan Tesla. Beberapa analisis mengatakan bahwa itu merupakan *misconfiguration* dalam sistem, namun faktanya layanan digital domestik Tiongkok tetap berjalan lancar, yang membuat gangguan ini terlihat sistematis. Disisi lain adanya temuan teknis terkait dengan *fingerprint* yang melewati port 443 tidak sesuai dengan pola perangkat *The Great Firewall* yang sebelumnya (Wu 2025). Banyak analisis yang beranggapan jika gangguan ini merupakan uji coba atau sebuah penerapan model baru pengetatan sensor *The Great Firewall of China 2025*, dikarenakan dalam beberapa tahun terakhir gangguan teknis muncul ketika *The Great Firewall* sedang diuji, diperbarui, atau diperketat.

**Tabel 2. 1 Perbandingan Kebijakan GFW Sebelum dan Pada Era Xi Jinping**

Periode	Fokus Konten yang Disensor	Instrumen Kebijakan	Bentuk Regulasi
Sebelum Era Xi Jinping (1990-2012)	<ul style="list-style-type: none"> <li>• Media berita internasional (<i>New York Times</i>, <i>Bloomberg</i>, <i>RFA</i>)</li> <li>• Situs berbagi informasi (<i>SlideShare</i>, <i>The Pirate Bay</i>)</li> <li>• Platform media sosial (<i>YouTube</i>, <i>Facebook</i>,</li> </ul>	<ul style="list-style-type: none"> <li>• Penutupan akses ke <i>platform</i> dan situs asing</li> <li>• Penyaringan kata kunci</li> <li>• Pembatasan fungsi dan jangkauan layanan asing</li> </ul>	<ul style="list-style-type: none"> <li>• Pengaturan teknis internet oleh berbagai lembaga</li> <li>• White paper “<i>The Internet in China</i>” (2010) terkait penegasan regulasi internet dan prinsip kedaulatan siber</li> </ul>

	<p><i>Twitter, Blogspot, WordPress)</i></p> <ul style="list-style-type: none"> <li>• Situs Falun Gong dan praktik spiritual</li> <li>• Konten pornografi dan ilegal</li> </ul>		
Era Xi Jinping (2013-2025)	<ul style="list-style-type: none"> <li>• Konten ideologi dan kritik politik</li> <li>• Opini publik dan wacana digital</li> <li>• Konten moral dan sosial (LGBT, <i>fan culture, influencer</i>)</li> <li>• Video pendek dan <i>live streaming</i></li> <li>• Satire politik</li> <li>• Data dan algoritma</li> <li>• Konten AI (AI generatif dan deep sythesis)</li> </ul>	<ul style="list-style-type: none"> <li>• Penyensoran manual dan algoritmatis</li> <li>• Pengawasan <i>platform</i> digital</li> <li>• Pemblokiran VPN</li> <li>• Penguatan narasi konten pro partai</li> </ul>	<ul style="list-style-type: none"> <li>• UU Keamanan Siber (2017) terkait pengaturan keamanan jaringan dan data</li> <li>• <i>National Intelligence Law</i> (2017) terkait kewajiban kerja sama untuk keamanan nasional</li> <li>• <i>Cybersecurity Review Measures</i> (pemeriksaan keamanan perusahaan data besar)</li> <li>• Regulasi CAC terkait pengawasan konten digital dan AI</li> <li>• <i>Data Security Law</i> dan PIPL (<i>Personal Information Protection Law of the People's Republic of China</i>) yang mengatur pengendalian data serta informasi pribadi</li> </ul>

Sumber: Data diolah penulis dari berbagai sumber (Freedom House 2019; Quan 2022; Creemers 2021; Zou and Zhang 2024).

Dengan demikian, tabel ini menunjukkan adanya pergeseran kebijakan *Great Firewall of China* dari pengelolaan teknis akses internet menjadi instrumen pengendalian ruang digital yang lebih terpusat pada era kepemimpinan Xi Jinping. Pergeseran ini terjadi karena adanya ancaman terhadap posisi Partai Komunis Tiongkok dari arus informasi global, media asing, dan *platform* digita internasional yang dianggap membawa pengaruh ideologi luar yang tidak sejalan, sehingga internet diposisikan sebagai objek yang perlu diamankan melalui kebijakan dan regulasi khusus.

Untuk menghadapi ancaman ini, Xi Jinping sebagai presiden sekaligus Sekretaris Jenderal Partai Komunis Tiongkok memegang peran sentral dalam perumusan kebijakan keamanan siber. Posisinya memberikan legitimasi politik yang kuat, sehingga dapat bertindak sebagai aktor sekuritisasi yang sah. Sejak awal kepemimpinannya, Xi Jinping telah membentuk *Central Leading Group of Cybersecurity and Informatization*, yang kemudian membentuk CAC sebagai lembaga utama pengelola dan pengawasan ruang digital. Sehingga hal ini menegaskan posisi Xi Jinping sebagai aktor dengan otoritas tertinggi.

Berdasarkan hal tersebut, kebijakan *Great Firewall* mengalami penguatan dan perluasan antara tahun 2013-2025, yang selanjutnya akan dianalisis menggunakan pendekatan sekuritisasi Barry Buzan, Ole Waever, dan Jaap de Wilde dalam *Security: A New Framework for Analysis*.

## BAB 3

### ANALISIS TEORI SEKURITISASI PADA KEBIJAKAN *THE GREAT FIREWALL OF CHINA*

Bab ini akan menganalisis kebijakan *The Great Firewall of China* menggunakan perspektif teori sekuritisasi yang dikemukakan oleh Barry Buzan, Ole Waever, dan Jaap de Wilde. Dengan fokus utama mengkaji bagaimana pemerintah Tiongkok bertindak sebagai aktor sekuritisasi melalui *speech act* dalam membingkai isu ancaman keamanan siber sebagai *existential threat*, serta bagaimana ancaman tersebut mengancam *referent object*. Selain itu, bab ini juga akan membahas penerapan *emergency act* sebagai bentuk legitimasi kebijakan Tiongkok terhadap pengelolaan ruang digital Tiongkok.

#### **3.1 *Speech Act* sebagai Instrumen *Securitizing Actor* dalam Membingkai Ancaman Keamanan Siber Digital Tiongkok terhadap Audiens**

##### *3.1.1 Aktor Sekuritisasi*

Barry Buzan, Ole Waever, dan Jaap de Wilde dalam bukunya yang berjudul *Security: A New Framework for Analysis*, menjelaskan bahwa proses sekuritisasi selalu melibatkan *securitizing actor* yang melakukan *speech act* dalam membingkai suatu isu sebagai sebuah ancaman. *Securitizing actor* dapat berasal dari berbagai pihak, termasuk pemerintah, partai politik, hingga kelompok kepentingan yang memiliki kapabilitas dan legitimasi untuk menentukan apakah sebuah isu layak dikatakan sebagai persoalan keamanan nasional (Buzan, Wæver, and Wilde 1998). Berbeda dengan aktor yang hanya melaksanakan kebijakan, *securitizing actor* adalah pihak yang menyatakan suatu obyek sebagai ancaman dan menetapkan

urgensinya. Secara umum, *securitizing actor* merupakan pihak yang memiliki otoritas untuk berbicara atas nama negara, sehingga mampu untuk mempengaruhi persepsi publik serta mendapatkan dukungan terhadap isu yang dibingkai.

Dalam konteks studi kasus ini, aktor sekuritisasi yang membingkai internet sebagai sebuah ancaman terhadap keamanan siber adalah Xi Jinping. Xi Jinping memegang tiga jabatan utama yaitu, Presiden Republik Rakyat Tiongkok, Sekretaris Jenderal Partai Komunis Tiongkok, dan Ketua Komisi Militer Pusat. Kombinasi jabatan ini menempatkan Xi Jinping sebagai pemimpin tertinggi di Tiongkok, dengan otoritas kekuasaan yang mencakup eksekutif, simbolik, dan militer. Masa jabatan Xi Jinping sebagai presiden dan Ketua Militer dimulainya sejak tahun 2013, menyusul penghapusan batas masa jabatan presiden pada 2018, yang semakin memperkuat posisinya dalam sistem politik di Tiongkok. Posisi Xi Jinping sebagai Sekretaris Jenderal Partai Komunis Tiongkok juga menegaskan dominasi partai dalam semua aspek pemerintahan, sedangkan jabatannya sebagai Ketua Komisi Militer Pusat memberikan kendali penuh terhadap kekuatan militer, menjadikannya seorang aktor yang mampu untuk mengintervensi kebijakan strategis negara dan membingkai isu keamanan dengan legitimasi yang dimiliki (Wulandari et al. 2024, 305).

Hal ini dikarenakan Partai Komunis Tiongkok merupakan satu-satunya partai yang berkuasa di Tiongkok dan menjadi pilar utama sistem politik negara. Partai ini memiliki struktur administrasi yang terpusat, sehingga memungkinkan pengendalian penuh atas seluruh lembaga negara, termasuk Kongres Rakyat Nasional sebagai lembaga legislatif tertinggi, dan lembaga-lembaga pemerintahan lainnya yang menjalankan fungsi eksekutif dan administratif. Legitimasi politik

partai diperkuat sejak era Deng Xiaoping dalam praktik sosialisme pasarnya yang diterapkan Partai Komunis Tiongkok dalam mendorong pertumbuhan ekonomi. Konstitusi Republik Rakyat Tiongkok juga menegaskan adanya kepemimpinan Partai Komunis Tiongkok dalam seluruh aspek pemerintahan, termasuk didalamnya hak atas pekerjaan, pendidikan, dan kehidupan, dengan tetap memprioritaskan kepentingan partai dalam stabilitas politik dan keamanan sosial (Wulandari et al. 2024, 298).

Meskipun perannya lebih simbolik sebagai Presiden Republik Rakyat Tiongkok dalam kegiatan sehari-hari, tetapi tetap memiliki wewenang signifikan dalam situasi tertentu, terutama menyangkut kebijakan yang berkaitan dengan keamanan nasional (Wulandari et al. 2024, 299). Dengan adanya beberapa jabatan yang dimiliki oleh Xi Jinping, maka hal ini menjelaskan Xi Jinping sebagai aktor sekuritisasi dominan, karena dapat menetapkan internet dan informasi digital sebagai sebuah isu yang mengancam keamanan siber, serta membingkai narasi tersebut untuk mendapatkan dukungan dari masyarakat.

Dengan kekuasaan dan legitimasi politik yang dimiliki, Xi Jinping dapat mengatur kebijakan keamanan siber, membuat serta mengarahkan lembaga terkait untuk memastikan bahwa isu keamanan siber dapat diterima oleh publik, dan lembaga negara sebagai isu penting. Hal ini menunjukkan bahwa struktur politik Tiongkok yang terpusat dibawah Partai Komunis Tiongkok memberikan Xi Jinping kemampuan untuk bertindak sebagai aktor sekuritisasi. Proses ini akan dijelaskan lebih lanjut melalui *speech act* yang dilakukan oleh Xi Jinping dalam membingkai isu keamanan siber pada sub bab berikutnya.

### 3.1.2 *Speech Act*

Dengan adanya legitimasi yang dimiliki oleh *securitizing actor*, maka hal ini akan mempermudah dalam melakukan *speech act* atau dapat dipahami sebagai upaya yang dilakukan untuk membingkai ancaman melalui pernyataan atau narasi tertentu yang ditujukan kepada audiens. Melalui *speech act*, sebuah isu yang sebelumnya dianggap tidak mengancam dapat berubah sebagai sebuah isu yang mengancam, karena sifatnya yang jadi mengancam keamanan nasional dan memerlukan kebijakan baru atau darurat (Buzan, Wæver, and Wilde 1998, 26-34). *Speech act* menjadi penting karena *securitizing actor* dapat mempengaruhi cara audiens dalam memahami suatu ancaman apakah isu tersebut dianggap berbahaya atau tidak, atau mendesak atau tidak. Dengan kata lain, efektivitas dari sekuritisasi serta pembentukan kebijakan dapat diterima, dengan bergantung pada keberhasilan *speech act* dalam membentuk persepsi audiens.

Maka *speech act* dalam praktiknya tidak hanya berbentuk ujaran atau pernyataan langsung. Mengacu pada pandangan Balzacq, dalam proses *speech act* dapat diperkuat dengan adanya unsur non linguistik seperti penggunaan metafora, emosi, stereotip, gestur, dan kebohongan. Semua ini dilakukan untuk memperkuat framing terkait dengan isu ancaman keamanan nasional yang diharapkan dapat diterima oleh audiens (BAELE and THOMSON 2017, 652).

Sejak awal masa pemerintahan Xi Jinping pada tahun 2013 mulai terlihat adanya fokus terhadap ruang digital sebagai salah satu aspek yang menentukan keamanan nasional Tiongkok. Hal ini terlihat sejak Agustus 2013, bocornya pidato internal Xi Jinping yang menyatakan “*The Internet has become the main battlefield for the public opinion struggle,*” (Economy 2018, 72).

Narasi ini kemudian diperkuat pada tahun 2014, ketika Xi Jinping memberikan pernyataan “ *cybersecurity and informatization are two wings of one body, and two wheels of one engine*” dalam pertemuan pertama *Central Leading Group of Cybersecurity and Informatization*. Hal ini menegaskan bahwa pembangunan digital dan keamanan siber dianggap harus berjalan beriringan sebagai sebuah pondasi dari modernisasi nasional. Jika keamanan siber rapuh maka seluruh sistem keamanan digital, stabilitas politik dan sosial negara akan terganggu (Gao 2023, 769).

Pada tahun 2015, konsistensi penekanan terhadap isu keamanan semakin terlihat ketika Xi Jinping menyampaikan pidato dalam *World Internet Conference* di Wuzhen. Dalam kesempatan tersebut, Xi Jinping menyatakan

*“In order to promote reforms in global cyberspace governance, we should insist on the following principles: first, respect internet sovereignty. The principle of sovereign equality enshrined in the charter of the United Nations is one of the basic norms in contemporary cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace on an equal footing,”* (Zeng, Stevens, and Chen 2017, 1).

Tiongkok membuat pengakuan atas kedaulatan siber digital nasionalnya dengan menempatkan internet sebagai ruang bebas tanpa batas. Internet dipandang sebagai domain yang tetap memerlukan pemantauan otoritas negara, serta adanya batasan yang dianggap perlu untuk menjaga stabilitas nasional.

Dalam pidato yang dilakukan oleh Xi Jinping pada 16 Desember 2015, menyatakan

*“A secure, stable and prosperous cyberspace is of great significance to all countries and the world. In the real world, there are still lingering wars, shadows of terrorism and occurrences of crimes. Cyberspace should not become a battlefield for countries to wrestle with one another, still less*

*should it become a hotbed for crimes. Countries should work together to prevent and oppose the use of cyberspace for criminal activities such as terrorism, pornography, drug trafficking, money laundering and gambling. All cyber crimes, be they commercial cyber thefts or hacker attacks against government networks, should be firmly combated in accordance with relevant laws and international conventions. No double standards should be allowed in upholding cyber security. We cannot just have the security of one or some countries while leaving the rest insecure, still less should one seek the so-called absolute security of itself at the expense of the security of others.”*

Dengan demikian, keamanan siber dibingkai sebagai syarat utama dalam menjaga perdamaian dan keadilan dalam tata kelola internet global (Ministry of Foreign Affairs People's Republic of China 2015).

Dalam sebuah simposium yang diselenggarakan pada 2016, Xi Jinping memberikan pernyataan terkait dengan keamanan siber yang merupakan prasyarat utama bagi pembangunan digital Tiongkok. Dalam pertemuan ini, Xi Jinping menekankan perlunya mempertahankan dan memperkuat pertahanan siber, infrastruktur informasi, dan peningkatan teknologi domestik. Pada kesempatan lain di tahun yang sama, Xi Jinping memberikan pernyataan jika Tiongkok harus lebih dahulu memastikan teknologi aman dan berada dibawah kendali nasional. Hal ini juga dikaitkan dengan sistem teknologi informasi yang aman dan dapat dikendalikan oleh negara (Doshi et al. 2021, 12).

Xi Jinping juga mengatakan jika ambisi ini beranjak dari historis bangsa dan luka masa lalu terhadap kegagalan Tiongkok dalam ketertinggalan industrialisasi pada abad ke-20. Sehingga hal ini yang menjadikan Tiongkok merasa memiliki peluang dalam revolusi industri, dengan bertekad untuk memanfaatkan momentum revolusi informasi demi mengejar ketertinggalan. Hal ini juga ditegaskan dengan pernyataan Xi Jinping yaitu “pihak yang unggul akan memperoleh kemenangan

besar, sedangkan yang tertinggal akan mengalami kehancuran.” (Doshi et al. 2021, 6). Masih ditahun yang sama tepatnya pada 19 April 2016, Xi Jinping sebagai bagian dari *securitizing actor* meminta para pejabat untuk memanfaatkan internet dalam memahami opini publik. Xi Jinping juga mengatakan jika persaingan antarnegara besar dalam bidang keamanan internet tidak hanya bergantung pada aspek teknologi, tetapi masuk didalamnya gagasan dan opini publik. Dari hal ini, dapat disimpulkan jika opini publik memiliki peran yang penting dalam menentukan suatu kebijakan. Hal ini dikarenakan adanya pembentukan opini yang berfungsi sebagai bentuk dukungan maupun penolakan. Selain itu, Opini publik juga menjadi wadah strategis dalam membentuk persepsi, pemahaman, dan mempengaruhi sudut pandang masyarakat terhadap suatu isu.

Memasuki tahun 2018 tepatnya tanggal 20-21 April, Xi Jinping menyampaikan pidatonya dalam *National Cybersecurity and Informatization Work Conference* di Beijing. Dalam pidatonya, dikatakan bahwa internet tidak boleh menjadi sebuah *platform* yang dalam penyebaran informasinya merugikan atau menimbulkan permasalahan. Jika tidak adanya keamanan siber maka tidak adanya juga keamanan nasional, stabilitas ekonomi, dan kesulitan dalam kesejahteraan masyarakat. Keamanan siber juga telah menjadi fokus pemerintah Tiongkok, sehingga keamanan siber dianggap sebagai sebuah pilar dalam menjaga stabilitas nasional Tiongkok (Xinhua 2018).

Selain itu terdapat konferensi yang dilaksanakan di Wuzhen pada Oktober 2019, yang dimana pada konferensi tersebut membahas kembali isu keamanan siber yang semakin menjadi prioritas. Xi Jinping juga melakukan peningkatan kerjasama internasional dengan cara berdialog. Berdasarkan pernyataan yang diberikan oleh

Xi Jinping, hal ini perlu dilakukan karena adanya kompleksitas yang terus meningkat terutama terkait dengan internet yang dianggap dapat berimbas terhadap keamanan siber (Hongpei 2019). Maka dari itu pada konferensi ini, Tiongkok mempertahankan perannya sebagai negara yang bertanggung jawab dalam kontribusi dunia digital, keterbukaan ruang siber, dan juga menjaga keamanan data digital.

Namun pada tahun 2020, adanya pandemi COVID-19 membuat Tiongkok harus bekerja sama dengan negara lain secara *online* atau *daring*, hal ini dikarenakan adanya isolasi yang dilakukan di setiap negara. Dari pandemi ini juga yang menyebabkan adanya peralihan pendidikan yang menjadi *daring*, *telemedicine*, dan juga komunikasi yang mengandalkan digital atau internet. Sehingga pada pembukaan upacara *World Internet Conference ke-7* yang diselenggarakan di Wuzhen, Xi Jinping menyatakan akan melakukan revolusi informasi dan siap melakukan kerjasama dengan negara lain secara digital. Hal ini berguna untuk tetap menjaga stabilitas ekonomi, kolaborasi digital, dan percepatan perkembangan digital (Yu, Yuanyuan, and Zhenhuan 2020). Namun disisi lain, karena internet yang masih dianggap sebagai ancaman, maka Xi Jinping akan tetap membuat pola baru keamanan siber, dengan membentuk komunitas bersama digital yang bertujuan untuk menciptakan masa depan yang lebih baik.

Pada sesi studi kolektif ke-34 Politbiro ke-19 yang diselenggarakan pada tanggal 18 Oktober 2021, Xi Jinping menegaskan pentingnya pengembangan ekonomi digital dan keamanan digital sebagai sebuah pilar strategis bagi Tiongkok. Xi Jinping juga menyoroti dengan adanya percepatan perkembangan teknologi digital maka akan meningkatkan risiko terkait dengan keamanan, termasuk

didalamnya keamanan ekonomi. Sehingga diperlukannya regulasi dan pengawasan yang memadai, dengan cara memperkuat tata kelola digital, membangun sistem pengawasan, dan adanya perlindungan terhadap keamanan data serta inovasi teknologi digital (Creemers, Costigan, and Webstar 2022).

Pada pembukaan *World Internet Conference* 9 November 2022, yang diselenggarakan di Wuzhen, Tiongkok. Presiden Xi Jinping dalam suratnya menyatakan bahwa teknologi digital saat ini saling terhubung dalam seluruh bidang, dan membawa perubahan signifikan dalam ranah kehidupan saat ini. Xi Jinping juga mengajak komunitas internasional untuk bersama-sama membuat ruang siber yang lebih adil, terbuka, aman, dan dinamis. Xi Jinping juga menegaskan bahwa Tiongkok siap untuk bekerja sama dalam skala global untuk pembangunan digital, sumber daya, ekonomi digital, tata kelola efisien, budaya digital, dan kerja sama keamanan digital yang saling menguntungkan satu sama lain (Xinhua 2022).

Pada 8 November 2023, pada pembukaan *World Internet Conference* yang diselenggarakan di Wuzhen, Tiongkok. Presiden Xi Jinping kembali menyampaikan pidato melalui sebuah video, yang menyatakan bahwa internet saat ini telah menjadi kekuatan penting bagi pembangunan, keamanan, dan pertukaran antar peradaban. Hal ini tentunya membutuhkan pembangunan komunitas dunia maya untuk masa depan bersama. Xi Jinping juga menekankan perlunya ruang siber yang aman, stabil, makmur bagi semua negara, dan menghormati masing-masing kedaulatan siber tiap negara. Hal ini dapat dilakukan dengan cara memperkuat keamanan data, perlindungan informasi dari kejahatan siber, dan melakukan tata kelola digital dengan pengembangan AI. Xi Jinping juga mengatakan bahwa

internet dapat dinikmati secara adil, menjadi solusi untuk kesenjangan digital, dan mendukung inklusivitas budaya global (Embassy of the People's Republic of China in the Republic of Indonesia 2023).

Pada 8 November 2024, Presiden Xi Jinping menyampaikan ucapan selamat melalui video pada pembukaan *World Internet Conference Wuzhen Summit 2024*. Xi Jinping menyatakan bahwa perlu diberlakukannya peningkatan pengembangan digital dan AI yang aman, inovatif, dan inklusif dalam rangka membangun komunitas masa depan bersama dunia maya. Perlunya keamanan dan tata kelola yang kuat untuk memastikan teknologi digital dapat bermanfaat bagi seluruh kalangan serta berfungsi sebagai penjaga stabilitas sosial dan ekonomi. Xi Jinping juga menegaskan kembali perlu adanya revolusi yang merangkul tren pengembangan digital berbasis internet maupun kecerdasan buatan, serta siap untuk melakukan kerja sama dengan negara lain dan saling menghormati kedaulatan siber setiap negara (Weilan, Zishuai, and Jingjing 2024).

Pada 28 November 2025, Politbiro Komite Sentral Partai Komunis Tiongkok melakukan studi kolektif ke-23 dengan fokus pembahasan terkait penguatan tata kelola daring. Dalam sesi yang dilakukan, Xi Jinping mulai menegaskan jika tata kelola daring merupakan hal yang krusial dalam upaya menjadikan Tiongkok sebagai kekuatan siber. Xi Jinping juga mengatakan jika hal ini tidak hanya terkait dengan pembangunan nasional Tiongkok maupun keamanan negara, tetapi juga menyangkut kepentingan seluruh masyarakat. Hal ini memerlukan mekanisme jangka panjang yang dianggap dapat tepat sasaran, proaktif, sistematis dan kolaboratif, yang dapat menciptakan lingkungan yang bersih dan sehat. Kepemimpinan dari Komite Sentral Partai, tata kelola daring

komprehensif, dan upaya kolaboratif lintas departemen juga harus diperkuat. Xi Jinping mengatakan bahwa semua instansi diharapkan meningkatkan tanggung jawab politik dan kepemimpinannya dengan menyelesaikan isu yang memanfaatkan internet (Center for Security and Emerging Technology 2025).

Xi Jinping juga menyoroti pentingnya pengawasan *platform* daring, media independen, dan organisasi jaringan multi saluran untuk dapat menyebarkan hal positif. Hal ini dikarenakan adanya laporan keamanan siber 2025, yang menunjukkan peningkatan risiko terkait dengan AI serta serangan siber sekitar 29% dan pelanggaran data 26%. Menanggapi hal ini, Undang-Undang Keamanan Siber yang berlaku sejak 2017 dalam menjaga kedaulatan dunia maya mulai direvisi dengan menambahkan fokus tantangan dalam menghadapi AI (DESHENG 2025).

Sekuritisasi yang dilakukan terhadap kebijakan *The Great Firewall of China*, terkait keamanan siber Tiongkok yang dimulai dari tahun 2012-2025 memperlihatkan konsistensi *speech act* yang dilakukan oleh aktor sekuritisasi, yaitu Xi Jinping. Sejak awal masa kepemimpinannya, internet secara bertahap dan sistematis telah dibingkai sebagai isu keamanan yang berpotensi dalam mengancam stabilitas politik, serta nilai-nilai sosial Tiongkok.

### 3.1.3 *Functional Actor*

Dalam kerangka teori sekuritisasi Barry Buzan, Ole Wæver, dan Jaap de Wilde, selain *securitizing actor*, terdapat juga aktor lain yang disebut *functional actor*. *Functional actor* merupakan aktor yang tidak berasal dari sistem politik atau tidak berperan sebagai pembentuk wacana keamanan melalui *speech act*, tetapi hadirnya tetap diperhitungkan karena memiliki pengaruh, seperti perusahaan, serikat pekerja, dan organisasi tertentu (Buzan, Wæver, and Wilde 1998, 36).

Sejak masa kepemimpinan Xi Jinping terdapat perubahan dalam memandang internet yang tidak hanya sebatas informasi dan administrasi, tetapi sebagai sebuah ancaman terhadap keamanan nasional, stabilitas politik, dan kedaulatan negara. Dalam konteks pengetatan kebijakan keamanan siber di Tiongkok, *Cyberspace Administration of China* dapat diposisikan sebagai salah satu contoh *functional actor*. *Cyberspace Administration of China* awalnya dibentuk sebagai sebuah respon pemerintah Tiongkok untuk pengelolaan ruang siber. CAC berakar dari *State Internet Information Office*, yang sejak lama telah berada dibawah kendali PKT. Tujuan awal dari adanya pembentukan CAC bukan sekedar mengelola aspek teknis internet, melainkan memastikan ruang digital berada dalam kendali partai dan negara (Saulnier 2022).

CAC sebagai lembaga negara, berperan sebagai lembaga yang menjalankan dan mengoperasionalkan kebijakan keamanan siber melalui regulasi teknis, pengawasan konten daring, serta mengelola perizinan layanan internet (Creemers 2024, 183). Melalui fungsi ini, CAC memastikan bahwa kebijakan pengamanan ruang siber dijalankan secara efektif, secara tidak langsung juga memperkuat proses dari sekuritisasi di Tiongkok meskipun tanpa melakukan *speech act* secara langsung.

Selain itu, melalui *Personal Information Protection Law* (PIPL), CAC secara resmi ditempatkan sebagai otoritas utama dalam melakukan pengawasan, penegakan, dan pengendalian terkait pemrosesan data pribadi Tiongkok. Posisi ini menegaskan peran CAC bukan hanya sebagai regulator teknis, akan tetapi juga sebagai pengawas utama dalam tata kelola digital Tiongkok. Mengingat kedudukan CAC yang berada langsung dibawah presiden Xi Jinping, maka orientasi kebijakan

akan sangat menekankan pada pengendalian ketat oleh negara, sejalan dengan prioritas keamanan nasional, stabilitas politik, dan nilai-nilai yang diterapkan (Simangunsong and Sijabat 2024, 6).

Dalam praktiknya, CAC tidak berperan sebagai aktor yang membentuk atau membuat wacana politik terkait dengan keamanan siber. Akan tetapi, CAC berfungsi sebagai lembaga pelaksana yang menerjemahkan arahan politik dan kebijakan strategis yang telah ditetapkan oleh pemimpin partai dan negara ke dalam aturan hukum, standar teknis, serta mekanisme administratif. Melalui kewenangan ini, CAC bertugas untuk mengatur konten daring, mengelola sistem perizinan media dan *platform* digital, serta melakukan pengawasan terhadap aktivitas online yang dianggap berdampak pada stabilitas politik Tiongkok (Saulnier 2022).

Dengan adanya peran ini menempatkan CAC sebagai penghubung dengan Xi Jinping sebagai *securitizing actor* dalam praktik pengelolaan ruang siber. CAC juga memastikan bahwa wacana keamanan siber yang dibangun oleh pemimpin politik dapat diterapkan dalam pengelolaan ruang siber. Oleh karena itu, CAC tidak berperan dalam membentuk narasi keamanan, melainkan sebagai *functional actor* yang menghubungkan keputusan politik dengan pelaksanaan kebijakan keamanan siber di Tiongkok.

#### 3.1.4 *Audiens*

Audiens dapat didefinisikan sebagai individu maupun kelompok yang memiliki kapabilitas dalam menyetujui maupun menolak isu ancaman keamanan yang disampaikan oleh aktor sekuritisasi (Buzan, Wæver, and Wilde 1998, 31). Keberhasilan dari *speech act* juga tercermin dari adanya tingkat penerimaan

masyarakat Tiongkok terhadap peningkatan kebijakan *The Great Firewall of China*.

Dalam hal ini, *speech act* yang dilakukan oleh *securitizing actor* khususnya Xi Jinping, terkait dengan isu keamanan siber dalam rangka menjaga stabilitas nasional Tiongkok menunjukkan tingkat keberhasilan yang relatif signifikan. Hal ini tercermin dari respon masyarakat terhadap kebijakan sensor internet yang diukur dalam studi Wang dan Mark pada tahun 2015, yang menunjukkan sekitar 42,7% responden yang menyatakan mendukung kebijakan sensor internet, 30,4% menyatakan tidak mendukung kebijakan sensor, sementara 30% lainnya memilih untuk tidak menjawab (Wang and Mark 2015, 15). Dari penelitian yang dilakukan oleh Wang dan Mark maka dapat disimpulkan adanya indikasi dalam tingkat penerimaan masyarakat Tiongkok terhadap *kebijakan The Great Firewall of China*, meskipun tetap disertai dengan adanya sikap netral maupun penolakan pada sebagian kalangan masyarakat Tiongkok.

Hingga saat ini masih adanya aksi protes secara terbuka dalam menembus sensor kerja *Great Firewall of China*. Seperti penggunaan VPN yang dapat diartikan sebagai bentuk protes masyarakat secara tidak langsung terhadap kebijakan GFW. VPN menjadi pilihan bagi audiens untuk menolak pembatasan ruang digital yang dianggap melanggar hak asasi individu. Dari hal ini, penerimaan audiens terkait dengan peningkatan kebijakan GFW tidak sepenuhnya utuh. Hal ini ditandai dengan adanya peningkatan upaya masyarakat dalam menerobos sistem, meskipun negara berhasil dalam mempertahankan kebijakan ini dengan jangka waktu yang cukup lama (Erwin 2021).

### **3.2 *Existential Threat* Keamanan Siber sebagai Ancaman Nyata terhadap Referent Object Nasional Tiongkok**

Dalam kerangka teori sekuritisasi Barry Buzan, Ole Waever, dan Jaap De Wilde, *existential threat* dapat diklasifikasikan ke dalam lima sektor utama, yaitu militer, politik, ekonomi, masyarakat, dan lingkungan. Pada penelitian ini menempatkan isu keamanan siber nasional Tiongkok masuk ke dalam sektor politik, yang dimana pada sektor ini *existential threat* secara tradisional dapat diartikan dalam hal prinsip pembentukan kedaulatan, dan ideologi dari negara. Kedaulatan dapat terancam secara *existential* oleh apapun yang mempertanyakan pengakuan, legitimasi, atau otoritas dari pemerintah (Buzan, Wæver, and Wilde 1998, 21-22). Hal ini selaras dengan ancaman yang dibingkai oleh pemerintah Tiongkok terkait dengan kebijakan *The Great Firewall of China* yang berkaitan dengan stabilitas nasional Tiongkok, legitimasi kekuasaan partai politik, serta bagaimana negara mengontrol dan memblokir arus informasi yang masuk.

Dalam konteks ini, keamanan politik dapat dipahami sebagai upaya dalam mempertahankan stabilitas organisasional negara dari berbagai ancaman non militer yang berpotensi mengganggu kedaulatan dan tatanan politik yang ada. Barry Buzan, Ole Waever, dan Jaap De Wilde juga menekankan inti sektor politik terletak pada perlindungan terhadap legitimasi, pengakuan, serta otoritas negara sebagai unit politik. Ancaman dalam sektor politik juga tidak selalu dalam bentuk serangan fisik, tetapi dapat berupa pelemahan legitimasi ideologi, penurunan kepercayaan publik, maupun tantangan terhadap struktur dan institusi politik yang menopang kekuasaan. Isu yang berkaitan dengan pengendalian informasi, regulasi ruang publik, dan pembungkaman wacana politik menjadi elemen sentral dalam keamanan

politik, secara langsung berkaitan dengan kemampuan negara dalam mengatur dan juga mempertahankan tatanan sosial serta stabilitas politik nasionalnya (Buzan, Wæver, and Wilde 1998, 141-145).

Kebijakan *The Great Firewall of China* juga tidak dapat dilepaskan dari fakta adanya transformasi ruang siber yang disebabkan oleh pesatnya perkembangan arus informasi dan komunikasi. Internet mendorong terbentuknya *network society* yaitu suatu tatanan sosial dimana kekuasaan dijalankan melalui penguasaan atas arus informasi dan komunikasi. Dalam kerangka *network society*, kekuasaan tidak hanya sebatas beroperasi melalui institusi negara konvensional, tetapi juga melalui kemampuan aktor termasuk negara dalam mengontrol, memfilter, dan mengarahkan komunikasi dalam ranah ruang digital. Hal ini menjadikan ruang siber sebagai arena kekuasaan yang penuh dengan persaingan politik, dimana penguasaan atas informasi dan juga komunikasi menjadi faktor penting. Akibatnya norma dan aturan perilaku yang sebelumnya dianggap stabil di ranah digital semakin mudah untuk diperdebatkan dan dilanggar (Ramich and Piskunov 2022, 243-248).

Serangan siber tidak hanya dipahami sebagai persoalan teknis, tetapi juga sebagai sebuah potensi ancaman terhadap kedaulatan negara terutama ketika menimbulkan kerusakan atau korban jiwa. Hal ini meningkatkan upaya negara dalam memperkuat keamanan siber, baik melalui kemampuan ofensif dan defensif yang kemudian memunculkan dilema dunia maya. Ruang siber juga telah berkembang menjadi ruang politik yang semakin sentral dalam proses pembangunan sosial, ekonomi, dan teknologi digital. Ancaman ruang siber

mencakup serangan terhadap infrastruktur kritis, masuknya pengaruh asing dalam ranah digital nasional, dan adanya penyebaran informasi yang dapat mengganggu stabilitas politik. Saat ini ruang siber mulai diposisikan sebagai salah satu domain utama dalam keamanan nasional, serta mendorong negara untuk memperkuat kontrol atas ruang internet domestik, termasuk didalamnya pengawasan terhadap konten dan aktivitas media sosial. Hal ini dapat dilihat dari langkah yang diambil oleh Tiongkok dalam memperketat kebijakan *The Great Firewall of China* yang pada awalnya hanya penyensoran menjadi pemblokiran, karena melihat adanya ancaman yang dapat mengganggu kedaulatan, legitimasi politik, dan stabilitas nasional. Dalam kerangka sekuritisasi, ruang siber bukan hanya sebagai sebuah teknologi, tetapi termasuk didalamnya sumber ancaman nyata yang dapat mengganggu otoritas negara seperti yang dirasakan oleh Tiongkok (Ramich and Piskunov 2022, 245-251).

Sejalan dengan teori Barry Buzan, Ole Waever, dan Jaap De Wilde bahwa *existential threat* dapat diartikan sebagai sebuah ancaman nyata yang dinyatakan oleh *securitizing actor* terhadap audiens melalui *speech act* bahwa terdapat *referent object* yang terancam dan perlu untuk dilindungi. *Referent object* merujuk pada entitas yang tidak hanya sebatas negara, tetapi di dalamnya dapat meliputi legitimasi politik, stabilitas rezim, dan ideologi negara (Buzan, Wæver, and Wilde 1998, 21). Tiongkok melihat dengan masuknya internet ke dalam domestik, tentunya berpotensi membawa nilai-nilai liberal yang berasal dari Barat. Hal ini dikhawatirkan akan mengikis nilai-nilai nasional Tiongkok, maka kebijakan sensor dapat dipahami sebagai upaya untuk menolak pengaruh westernisasi. Hal ini dikarenakan kebebasan yang diberikan tanpa adanya batasan akan memicu resiko

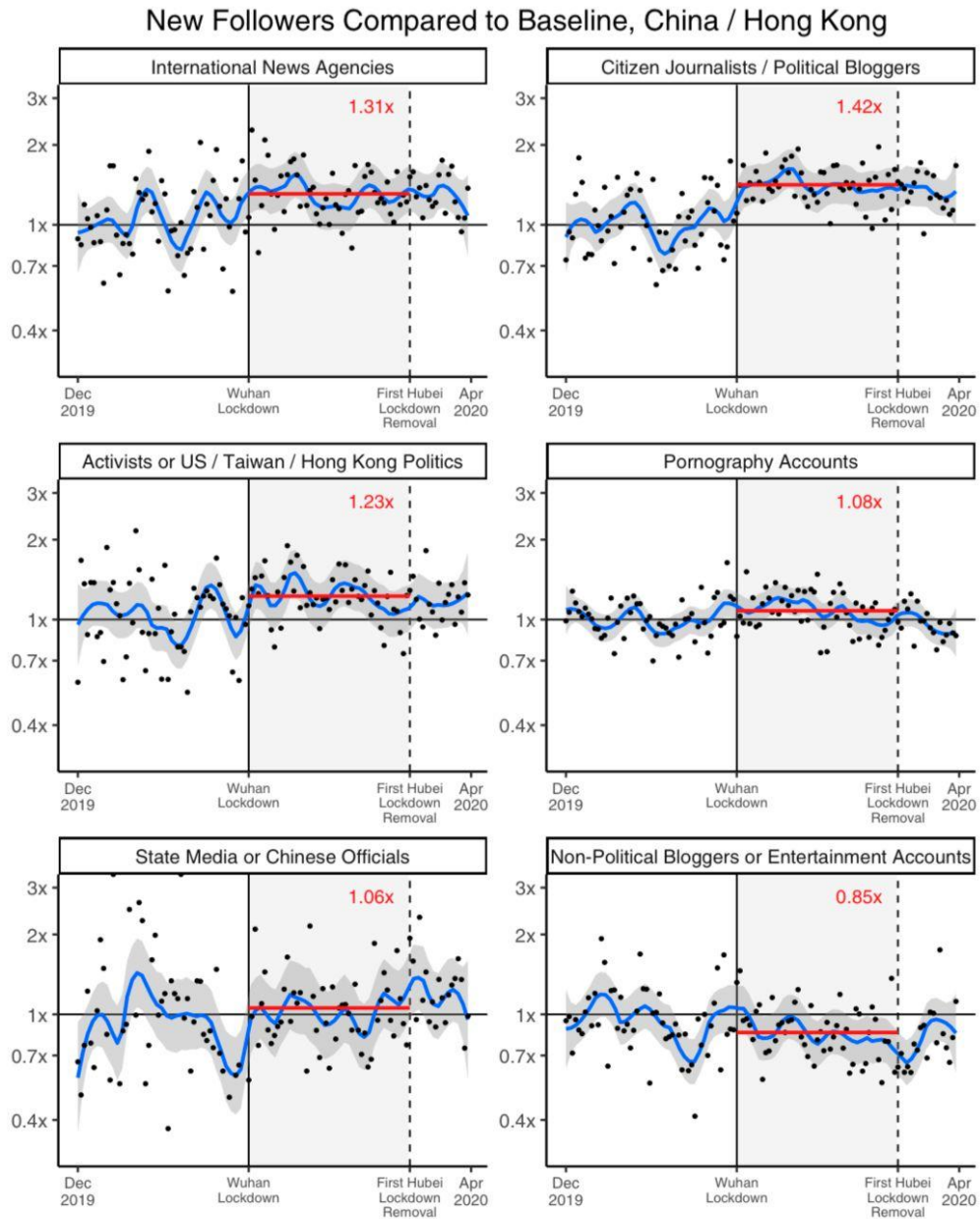
yang dapat membahayakan keamanan nasional, karena setiap tindakan yang dilakukan oleh masing-masing individu tidak dapat diprediksi (Zulfikar 2023, 21).

Dapat dilihat pada tahun 2014, umbrella movement menjadi sebuah simbol harapan bagi demokrasi dan juga kebebasan berekspresi ketika ribuan masyarakat menentang keputusan Tiongkok terkait dengan pembatasan mekanisme dalam pemilihan pemimpin Hong Kong. Hingga memasuki tahun 2019, harapan ini semakin memudar setelah adanya gelombang protes terhadap RUU ekstradisi dan pemberlakuan *National Security Law* oleh Beijing, yang secara tidak langsung mempersempit ruang berekspresi bagi aktivis pro-demokrasi (Li 2024). Hal ini dilakukan karena adanya peningkatan pengguna VPN, *platform* asing, dan juga jaringan lintas batas negara yang memungkinkan masyarakat menyebarluaskan protes terhadap pemerintah. Adanya praktik perlawanan yang dilakukan oleh masyarakat juga berupa penggunaan meme, simbol dan kode bahasa yang memiliki makna tersirat atau istilah samaran yang memungkinkan lolos dari sistem penyensoran, salah satu contohnya seperti penggunaan payung yang awalnya untuk melindungi diri tetapi menjadi hal ikonik bagi media lokal maupun internasional (Eckert 2024).

Hal ini juga terjadi pada saat diberlakukannya *lockdown* di Wuhan pada awal pandemi COVID-19. Sensor internet di Tiongkok semakin meningkat, terutama berkaitan dengan COVID-19, kebijakan pemerintah hingga kritik publik kepada pemerintah. Hal ini ditandai dengan adanya penghapusan konten dan penutupan akses diskusi dengan skala domestik hingga internasional. Beranjak dari hal ini banyak masyarakat yang mencoba untuk menerobos sensor dengan

penggunaan VPN, *platform* luar negeri terkhusus Twitter, hingga alat circumvention (Chang et al. 2021, 2-4).

**Gambar 3. 1 Dampak *Lockdown* COVID-19 terhadap Rasio Pengikut Baru Twitter di Tiongkok Daratan dibandingkan Hong Kong**



Sumber: (Chang et al. 2021)

Gambar di atas menunjukkan adanya peningkatan terhadap *platform* atau akun-akun Twitter yang membahas isu sensitif terkait dengan Tiongkok. Seperti

kantor berita internasional, jurnalis warga, aktivis politik, serta akun yang membahas kebijakan pemerintah mengalami lonjakan pengikut yang lebih besar. Twitter pada dasarnya tidak dapat diakses secara bebas di Tiongkok, namun dengan adanya lonjakan ini menjadi indikator bahwa semakin banyak pengguna internet yang berusaha untuk menerobos GFW, dan grafik yang ditunjukkan bersifat selektif terhadap konten politik dan kritik, bukan pada akun non-politik atau hiburan (Chang et al. 2021, 5). Penerobosan yang dilakukan selama masa COVID-19 dilakukan karena adanya kebutuhan mendesak akan informasi yang diakibatkan karena ketatnya sensor dan cepatnya penghapusan diskusi kritis terkait *lockdown* maupun kebijakan pemerintah, sehingga hal ini dilakukan sebagai alternatif dalam mencari informasi (Chang et al. 2021, 7).

Internet di Tiongkok dipandang sebagai *existential threat*, peningkatan penyensoran ini menggambarkan kecemasan yang dirasakan oleh pemerintah Tiongkok terhadap kemungkinan ketidakstabilan yang dapat ditimbulkan oleh arus informasi dan komunikasi yang tidak terkendali. Meskipun pemerintah Tiongkok memberikan kebebasan untuk berbicara serta kebebasan pers, akan tetapi tetap adanya ketidakjelasan dalam peraturan media termasuk didalamnya internet, pemberian ruang bagi para otoritas untuk membuat konten yang dianggap mengungkap rahasia negara (*guójiā mìmì*), dan membahayakan kepentingan negara (Creemers 2015, 3-6). Terdapat undang-undang dalam menjaga rahasia negara yang isinya meliputi penguatan kontrol atas arus informasi dengan mewajibkan perusahaan internet dan operator telekomunikasi untuk bekerjasama dalam menindak kebocoran rahasia negara, termasuk didalamnya bidang pertahanan,

urusan luar negeri, pembangunan nasional, ilmu pengetahuan dan teknologi, serta keamanan negara.

Tiongkok juga memiliki ambisi menjadi “kekuatan siber” untuk mendorong negara dalam menegakkan kontrol penuh atas internet domestik dan menolak gagasan bahwa internet adalah ruang bebas yang terbuka, tetapi justru memaknai internet sesuai dengan pandangan nilai-nilai nasional Tiongkok. Xi Jinping sebagai pemimpin negara juga menegaskan hal ini dalam pidatonya dengan mengatakan bahwa setiap negara memiliki hak untuk menentukan jalur pengembangan internet, model manajemen, kebijakan publik, dan juga partisipasi yang setara dalam tata kelola siber internasional, serta menegaskan larangan dalam melakukan intervensi urusan dalam negeri negara lain atau dukungan atas aktivitas siber yang dianggap membahayakan keamanan nasional negara.

Berdasarkan analisis diatas, internet yang hadir dipandang oleh Tiongkok sebagai *existential threat* karena membawa nilai-nilai asing atau pengaruh westernisasi yang berpotensi mengancam legitimasi, stabilitas, dan ideologi yang dianut oleh Tiongkok sebagai *referent object*. Peningkatan penyensoran merupakan respon yang dilakukan oleh Tiongkok untuk melindungi *referent object* dengan melakukan penyaringan maupun pemblokiran arus informasi komunikasi, penguatan sistem hukum, pertahanan kedaulatan politik nasional, dan menghindari potensi pengaruh eksternal.

### 3.3 Analisis *Emergency Act* dalam Kebijakan *The Great Firewall of China*

Ketika *securitizing actor* membingkai sebuah isu terkait dengan teknologi informasi dan komunikasi sebagai sebuah *existential threat* yang mengancam keamanan siber, stabilitas politik, kedaulatan negara, dan legitimasi politik Tiongkok. Kemudian isu tersebut mendapat dukungan dari masyarakat, maka ancaman atau isu tersebut akan dianggap sebagai sebuah *existential threat* yang harus segera diselesaikan dengan cara tindakan darurat di luar mekanisme politik (Buzan, Wæver, and Wilde 1998, 5).

Setelah isu tersebut dinyatakan sebagai sebuah isu darurat, maka negara mendapatkan legitimasi untuk membuat kebijakan diluar mekanisme, seperti pembatasan akses internet, penyensoran informasi dan komunikasi, serta penguatan pengawasan siber yang bertujuan untuk mencegah ancaman terus masuk dan berkembang sehingga menjadi sulit untuk dikendalikan (Buzan, Wæver, and Wilde 1998, 21).

Dalam konteks ini, legitimasi yang diambil oleh Xi Jinping terhadap pengetatan regulasi tidak muncul secara abstrak, melainkan diperoleh dari adanya kondisi yang direpresentasikan negara sebagai situasi darurat dalam ranah keamanan (Buzan, Wæver, and Wilde 1998, 5). Situasi yang dianggap darurat tidak selalu berkaitan dengan hal militer, tetapi dapat berupa ketidakstabilan politik yang diakibatkan oleh meningkatnya arus informasi lintas batas negara. Hal ini disebabkan oleh ruang digital yang dipandang sebagai sarana efektif dalam mempercepat penyebaran ideologi, sehingga memerlukan tindakan darurat.

Kondisi darurat dapat dilihat dari adanya peningkatan ketegangan politik yang terjadi pemerintah dan masyarakat, seperti gelombang protes pro demokrasi, meningkatnya penggunaan *platform* asing dan VPN. Kondisi seperti ini yang membuat pemerintah Tiongkok merasa perlu untuk memperketat pengawasan informasi, pemblokiran situs asing, dan meningkatkan kontrol terhadap ruang digital. Langkah ini dianggap efektif oleh negara untuk mencegah penyebaran disinformasi, menjaga ketertiban dan keamanan nasional (Freedom House 2021). Dalam kerangka teori sekuritisasi, kondisi-kondisi seperti ini berfungsi untuk memperkuat legitimasi *securitizing actor* dalam menerapkan kebijakan di luar mekanisme politik. Ketika suatu situasi dipresepsikan sebagai hal darurat, tindakan seperti pengetatan sensor konten, dan pembatasan akses internet tidak lagi dilihat sebagai kebijakan administratif, melainkan sebagai *emergency act* yang dianggap perlu dalam melindungi *referent object*, yaitu stabilitas politik, kedaulatan negara, dan legitimasi PKT.

Apabila melihat dari perspektif Barat, peningkatan penyensoran yang diterapkan di Tiongkok dianggap sebagai bentuk pembatasan terhadap hak asasi manusia, khususnya kebebasan dalam berekspresi. Meskipun Konstitusi Tiongkok menjamin kebebasan berbicara dan kebebasan menerbitkan, akan tetapi pelaksanaan hak-hak tersebut tetap terdapat kontrol dari Partai Komunis Tiongkok (PKT) sebagai bagian dari supremasi nasional. Konstitusi juga tidak menjadikan dasar hukum yang efektif dalam menuntut perlindungan hak di pengadilan, karena lembaga peradilan yang bersifat independen dan cenderung mengikuti arahan dari partai, terutama dalam kasus yang sejalan atau sensitif secara politik (Freedom House 2021).

Dalam ranah hukum terdapat berbagai peraturan yang secara eksplisit maupun implisit membatasi kebebasan berbicara secara daring. Ketentuan ini terkait dengan pencemaran nama baik, penciptaan gangguan ketertiban umum, kegiatan komersial ilegal, hingga pemerasan yang sering digunakan untuk menjerat ekspresi di ruang digital. Misalnya pencemaran nama baik yang diartikan secara luas hingga termasuk didalamnya rumor daring, informasi palsu, hingga konten yang merugikan masyarakat maupun negara. Adanya penafsiran terkait hukum yang luas membuat ruang bagi negara untuk melakukan berbagai tindakan terhadap bentuk kritik dan perbedaan pendapat di internet (Freedom House 2021).

Selain itu, dengan adanya penegakan hukum dari lembaga peradilan dan aparat penegak hukum tertinggi di Tiongkok yang mengeluarkan aturan penanganan tegas terhadap kejahatan yang dianggap dapat merusak otoritas PKT atau melemahkan negara dalam menjaga stabilitas. Hingga pada praktiknya, aturan ini berdampak pada meningkatnya risiko pemenjaraan masyarakat yang menyuarakan reformasi politik, aktivitas hak asasi manusia, hingga kelompok minoritas etnis dan agama yang menyampaikan kritik, sindiran, maupun ekspresi ketidaksetujuan terhadap PKT dan Xi Jinping. Dengan adanya pola penegakan hukum yang disertai dengan ancaman penangkapan, hal ini tidak hanya sebagai bentuk hukuman, tetapi termasuk membangun ketakutan dalam ranah ruang digital. Hukuman berupa penangkapan ini juga dianggap telah bertolak belakang dengan nilai dan hak asasi manusia dalam kebebasannya sebagai manusia sebagaimana yang tercantum dalam konvensi Internasionall terkait Hak Sipil dan Politik yang dimana ini juga telah ditandatangani oleh Tiongkok pada tahun 1998 (Yahya, R and Mutia 2023, 5).

Dengan meningkatkan penyensoran kebijakan *The Great Firewall of China*, yang merupakan seperangkat kebijakan untuk mengatur internet nasional Tiongkok, dengan melakukan pemblokiran di sejumlah situs asing, memperlambat lalu lintas internet lintas negara, serta melakukan penyensoran terhadap konten tertentu. Hal ini memicu masyarakat untuk melakukan *self censorship* hingga publik daring semakin menyempit dan kehilangan fungsi sebagai wadah untuk berekspresi dan bertukar ide secara bebas. Kebijakan ini sepenuhnya berfungsi untuk mengendalikan arus informasi dan komunikasi, kebijakan ini juga digunakan untuk memperkuat posisi partai komunis Tiongkok dan perusahaan domestik terutama layanan digital Tiongkok (Wowor, Sudirman, and Hakiki 2023, 197).

Hal ini selaras dengan keinginan Tiongkok terkait keamanan siber yang terus diperkuat sebagai upaya mempertahankan dominasi Partai Komunis Tiongkok dalam sistem politik nasional. Sebagai salah satu partai politik terbesar di dunia, PKT memiliki posisi yang dominan dalam sistem politik Tiongkok dengan kekuasaan politik berpusat pada satu partai yang mengarahkan jalannya pemerintahan. PKT tidak hanya sebagai partai politik tetapi juga berperan dalam peningkatan penyensoran kebijakan utama yang memastikan seluruh lembaga pemerintah baik ditingkat pusat dan provinsi untuk melaksanakan keputusan serta arahan dari partai secara konsisten. Dengan adanya proklamasi Xi Jinping mengenai “Era Baru Sosialisme dengan Karakteristik Tiongkok” pada Kongres Partai ke-19 tahun 2017, menjadi salah satu contoh yang menegaskan peran sentral dari PKT dalam menentukan arah pembangunan dan posisi Tiongkok dalam kancah global. Visi untuk menjadikan Tiongkok sebagai kekuatan global pada pertengahan

abad ke-21 dengan menempatkan stabilitas politik dan kontrol internet juga menjadi prasyarat utama (Albert 2025).

Namun, *The Great Firewall of China* juga memberikan dilema antara keamanan dan kebebasan, dimana negara memprioritaskan stabilitas dan keamanan siber sebagai bagian penting dalam kekuasaan dan legitimasi. Akan tetapi bagi pemerintah, ketidakstabilan politik yang dipicu oleh ancaman siber jauh lebih berbahaya dari pelanggaran HAM. Hal tersebut akhirnya memberikan konsekuensi yang serius terhadap hak asasi manusia dan kebebasan sipil dalam ruang digital. Akan tetapi, jika melihat ini dari sudut pandang Tiongkok, maka peningkatan sistem penyensoran dapat dipahami sebagai upaya untuk menjaga stabilitas politik, dan melindungi keamanan siber nasional Tiongkok. Meskipun kebijakan *The Great Firewall of China* terkesan keras dan juga restriktif bagi sebagian masyarakat Tiongkok dan masyarakat global, akan tetapi bagi pemerintah Tiongkok sendiri kebijakan ini sebagai penanganan yang efektif dan cerdas dalam menindaklanjuti hal-hal yang dianggap mengancam keamanan siber Tiongkok terutama di era politik digital saat ini.

Meskipun proses sekuritisasi yang dilakukan oleh Tiongkok mendapatkan kritik internasional karena dinilai melanggar kebebasan berekspresi dan hak asasi manusia. Akan tetapi Tiongkok tetap mempertahankan sistem penyensoran ini dengan alasan bahwa setiap negara memiliki hak kedaulatannya sendiri untuk mengatur ruang digital. Kebijakan terkait sistem penyensoran tidak sekedar kebijakan untuk mengendalikan informasi, tetapi diposisikan untuk menjaga stabilitas politik dan keamanan siber dari *existential threat* dalam ranah digital.

## **BAB 4**

### **PENUTUP**

#### **4.1 Kesimpulan**

Di era digital saat ini, arus informasi dan komunikasi berperan tidak hanya sebagai sarana pertukaran informasi, tetapi juga hal ini dapat dimanfaatkan untuk menyebarkan ideologi dengan cara pembentukan opini publik secara daring, hingga propaganda. Saat ini internet berperan sebagai ruang strategis yang penting dalam menjaga stabilitas politik, dan keamanan nasional. Bagi Tiongkok, keamanan siber dipandang sebagai instrumen penting atau *no cybersecurity no national security*, maka perlu berada dibawah kendali negara dengan tujuan untuk menjaga keamanan nasional dan kedaulatan negara.

Sejak masuknya internet ke Tiongkok, proses modernisasi terus mengalami percepatan seiring dengan meningkatnya jumlah pengguna internet sebagai dampak dari derasnya arus globalisasi. Kondisi ini yang kemudian memunculkan kekhawatiran pemerintah Tiongkok terhadap potensi ancaman yang dapat mengganggu stabilitas politik, legitimasi Partai Komunis Tiongkok, dan identitas nasional. Disisi lain, keterbukaan terhadap ruang digital juga menimbulkan kekhawatiran terhadap masuknya westernisasi dan narasi politik Barat yang dinilai berpotensi melemahkan otoritas nasional Tiongkok.

Pada era kepemimpinan Xi Jinping, kekhawatiran ini kemudian dipertegas dengan penguatan sistem penyensoran internet. Hal ini dikarenakan, internet tidak lagi dipandang sebagai sarana modernisasi, melainkan sebagai ancaman yang memerlukan langkah protektif untuk menjaga stabilitas. Xi Jinping sebagai aktor sekuritisasi juga secara aktif melakukan berbagai *speech act* kepada audiens atau

masyarakat Tiongkok, dengan membingkai ruang digital sebagai ancaman nyata. Melalui berbagai pidato resmi, kebijakan nasional, serta pembentukan *Cyberspace Administration of China* (CAC), pemerintah Tiongkok secara konsisten menegaskan jika keamanan siber merupakan hal utama dalam menjaga keamanan nasional.

Melalui berbagai *speech act* yang dilakukan oleh Xi Jinping, menegaskan adanya *existential threat* atau ancaman dari arus informasi dan komunikasi yang mengancam *referent object*, yang dimana ini merupakan negara, termasuk di dalamnya stabilitas politik, kedaulatan nasional, dan legitimasi partai. Sebagai respon dari berbagai ancaman yang dibawa oleh internet terhadap keamanan siber, maka pemerintah Tiongkok kemudian menerapkan *emergency act* atau tindakan darurat berupa penguatan kebijakan *The Great Firewall of China*. Kebijakan ini merupakan sistem yang melakukan penyensoran dan pemblokiran terhadap situs asing serta konten yang dianggap tidak sesuai dengan nilai-nilai yang dianut oleh Tiongkok. Pada akhirnya ruang digital tetap berada dalam kendali negara dan tidak dimanfaatkan untuk hal yang bertentangan dengan kepentingan negara.

Oleh karena itu, kebijakan *The Great Firewall of China* mencerminkan adanya dilema yang dirasakan oleh pemerintah dalam menjaga stabilitas nasional atau hak masyarakat sipil dalam mengakses ruang digital. Sekuritisasi yang dilakukan oleh pemerintah Tiongkok menunjukkan adanya prioritas utama terhadap keamanan nasional, tetapi disisi lain terdapat konsekuensi terhadap hak asasi manusia yang belum sepenuhnya diperhatikan dan dipertimbangkan.

## 4.2 Rekomendasi

Penelitian sangat menarik untuk diteliti lebih dalam dan dapat dikembangkan dengan menggunakan pendekatan teoritis yang berbeda. Penulis merekomendasikan agar penelitian selanjutnya dapat memperluas fokus kajian, misalnya dengan menganalisis kebijakan *The Great Firewall of China* dari periode kepemimpinan yang berbeda atau membandingkan kebijakan pengendalian internet Tiongkok dengan negara lain. Selain itu, penelitian selanjutnya juga dapat menggunakan teori lain dalam kajian keamanan non-tradisional, atau tetap menggunakan teori sekuritisasi untuk memperdalam analisa terkait pembungkaman ruang digital sebagai ancaman keamanan nasional.

## DAFTAR PUSTAKA

- Akduman, Birol. 2023. "From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance." *International Journal of Social Sciences (Uluslararası Sosyal Bilimler Dergisi)* 7, no. 28 (Mei): 442-469. <https://doi.org/10.52096/usbd.7.28.30>.
- Albert, Melissa. 2025. "Chinese Communist Party (CCP) | History & Party Structure." Britannica. <https://www.britannica.com/topic/Chinese-Communist-Party>.
- Albeit F., Reza. 2025. "DIPLOMACY AND GLOBAL SECURITY JOURNAL." *MODERNISASI DAN RESTRUKTURISASI MILITER TIONGKOK YANG BERKELAS DUNIA* 2, no. 2 (Oktober): 879-894. 10.36859/dgsj.v2i2.4607.
- BAELE, STE PHANE J., and CATARINA P. THOMSON. 2017. "ANALYTICAL ESSAY." *An Experimental Agenda for Securitization Theory* 19 (Desember): 646-666. <https://www.jstor.org/stable/48557272>.
- Buzan, Barry, Ole Wæver, and Jaap d. Wilde. 1998. *Security: a new framework for analysis*. Boulder, Colorado: Lynne Rienner Pub.
- Center for Security and Emerging Technology. 2025. At the 23rd Collective Study Session of the CCP Politburo, Xi Jinping Stressed: Strengthen the Long-Term Mechanism for Online Ecosystem Governance, Continue to Create a Clean and Correct Atmosphere in Cyberspace. <https://cset.georgetown.edu/publication/xi-jinping-politburo-study-session-online-governance/>.
- Chang, Keng C., William R. Hobbs, Margaret E. Roberts, and Zachary C. Threlkeld. 2021. "PNAS POLITICAL SCIENCES." *COVID-19 increased censorship circumvention and access to sensitive topics in China* 122, no. 52 (Januari): 1-9. <https://doi.org/10.1073/pnas.2102818119>.
- China Internet Network Information Center (CNNIC). 2024. "The 54th Statistical Report on China's Internet Development." Beijing, Beijing: CNNIC. <https://www.cnnic.com.cn/IDR/ReportDownloads/202411/P020241101318428715781.pdf>.
- China Law Translate. 2020. "community-supported, crowd-sourced Translation and Commentary." *Cybersecurity Review Measures* (22 ed.). [https://www.chinalawtranslate.com/en/cyber-security-review/?utm\\_source#gsc.tab=0](https://www.chinalawtranslate.com/en/cyber-security-review/?utm_source#gsc.tab=0).
- Creemers, Dr. Rogier. 2021. "LEIDEN ASIA CENTRE." *China's Cyber Governance Institutions*, 1-22.
- Creemers, Rogier. 2024. "JOURNAL OF CONTEMPORARY CHINA." *The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy* 33, no. 146 (Maret): 173-188. <https://doi.org/10.1080/10670564.2023.2196508>.
- Creemers, Rogier. 2015. *CYBER CHINA UPGRADING PROPAGANDA, PUBLIC OPINION WORK AND SOCIAL MANAGEMENT FOR THE 21ST CENTURY* 24 (93): 1-22. 10.1080/10670564.2014.962579.
- Creemers, Rogier, Johanna Costigan, and Graham Webstar. 2022. "Xi called for

- strong efforts toward development and national independence in digital technologies.” Translation: Xi Jinping’s Speech to the Politburo Study Session on the Digital Economy – Oct. 2021. <https://digichina.stanford.edu/work/translation-xi-jinpings-speech-to-the-politburo-study-session-on-the-digital-economy-oct-2021/>.
- Creemers, Rogier, and Graham Webster. 2022. “New review before foreign IPOs to be required for services with over 1 million users.” Translation: Cybersecurity Review Measures (Revised) – Effective Feb. 15, 2022. [https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/?utm\\_source](https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/?utm_source).
- Crawford, Douglas. 2023. “What is the Great Firewall of China and how does it work? - Proton VPN.” Proton VPN. <https://protonvpn.com/blog/great-firewall-china>.
- DESHENG, CAO. 2025. “Xi champions shared future in cyberspace - Chinadaily.com.cn.” China Daily. <https://www.chinadaily.com.cn/a/202511/06/WS690bd7efa310bfd27fc50ae.html>.
- Dinh, Trong H., and Phuong C. Nguyen. 2024. “Journal for Legal, Political and Social Theory and Philosophy.” *PROTECTING NATIONAL SOVEREIGNTY IN CYBERSPACE WITHIN THE CONTEXT OF DIGITAL GLOBALIZATION □ REGULATIONS OF SOME COUNTRIES AND PROPOSALS* 8, no. 1 (Juni): 5-29. 10.51204/IVRS\_24101A.
- Doshi, Rush, EMILY d. Bruyère, Nathan Picarsic, and John Ferguson. 2021. “Ringkasan eksekutif.” *Tiongkok sebagai “raksasa cyber” : Dua suara di Beijing terkait bidang telekomunikasi*, (Maret), 1-30. <https://share.google/LlyA72AxfyZmGFMfv>.
- Eckert, Paul. 2024. “Radio Free Asia.” EXPLAINED: How the umbrella became a Hong Kong protest symbol. <https://www.rfa.org/english/news/china/hong-kong-umbrella-protest-anniversary-china-occupy-central-09252024155635.html>.
- Economy, Elizabeth. 2018. *The Third Revolution: Xi Jinping and the New Chinese State*. New York: Oxford University Press.
- Embassy of the People's Republic of China in the Republic of Indonesia. 2023. “Embassy of the People's Republic of China in the Republic of Indonesia.” Xi Jinping Delivers a Video Speech at the Opening Ceremony of the 2023 World Internet Conference Wuzhen Summit. [https://id.china-embassy.gov.cn/eng/xwdt/202311/t20231127\\_11187680.htm?utm\\_source](https://id.china-embassy.gov.cn/eng/xwdt/202311/t20231127_11187680.htm?utm_source).
- Erwin, Samantha. 2021. “China's Conflicted Relationship With VPNs.” Dao Insights. <https://daoinsights.com/opinions/chinas-conflicted-relationship-with-vpns/>.
- Freedom House. 2016. “FREEDOM ON THE NET 2016.” FREEDOM ON THE NET 2016-CHINA. [https://freedomhouse.org/country/china/freedom-net/2016?utm\\_source](https://freedomhouse.org/country/china/freedom-net/2016?utm_source).
- Freedom House. 2019. “FREEDOM ON THE NET 2019.” FREEDOM ON THE

- NET 2019-China. <https://freedomhouse.org/country/china/freedom-net/2019>.
- Freedom House. 2020. "FREEDOM ON THE NET 2020." FREEDOM ON THE NET 2020-China. <https://freedomhouse.org/country/china/freedom-net/2020>.
- Freedom House. 2021. "FREEDOM ON THE NET 2021." FREEDOM ON THE NET 2021-China. <https://freedomhouse.org/country/china/freedom-net/2021>.
- Freedom House. 2022. "FREEDOM ON THE NET 2022." FREEDOM ON THE NET 2022-China. <https://freedomhouse.org/country/china/freedom-net/2022>.
- Gao, Raymond Y. 2023. "Chinese Journal of International Law." *A Battle of the Big Three?— Competing Conceptualizations of Personal Data Shaping Transnational Data Flows*, (November), 22-787. <https://doi.org/10.1093/chinesejil/jmad040>.
- Guo, Meirong. 2018. "International Journal of Critical Infrastructure Protection." *China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces* 22 (Juli): 139-149. <https://doi.org/10.1016/j.ijcip.2018.06.006>.
- Hongpei, Zhang. 2019. "globaltimes." Xi stresses common responsibility for internet governance. [https://www.globaltimes.cn/content/1167415.shtml?utm\\_source](https://www.globaltimes.cn/content/1167415.shtml?utm_source).
- HSF Kramer. 2018. "Herbert Smith Freehills Kramer." China Cybersecurity and Data Protection: A round up of recent developments - October 2018. <https://www.hsfkramer.com/insights/2018-11/china-cybersecurity-and-data-protection-a-round-up-of-recent-developments-october>.
- Klimeš, Ondřej, and Maurizio Maurizio. 2018. "Journal of Chinese Political Science." *Introduction: Ideology, Propaganda, and Political Discourse in the Xi Jinping Era* 23 (Juli): 313-322. <https://doi.org/10.1007/s11366-018-9566-3>.
- Koty, Alexander C. 2017. "China's Great Firewall: Business Implications." China Briefing. <https://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/>.
- Li, Yuchen. 2024. "Hong Kong protests: Little remains of Umbrella Movement – DW – 09/27/2024." DW. <https://www.dw.com/en/hong-kong-protests-little-remains-of-umbrella-movement/a-70343315>.
- Miao, Weishan, Min Jiang, and Yunxia Pang. 2021. "International Journal of Communication." *Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994–2017)* 15 (April): 1-24. <https://ijoc.org/index.php/ijoc/article/view/15944>.
- Ministry of Foreign Affairs People's Republic of China. 2015. Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference\_Ministry of Foreign Affairs of the People's Republic of China. [https://www.mfa.gov.cn/eng/xw/zyjh/202405/t20240530\\_11341037.html](https://www.mfa.gov.cn/eng/xw/zyjh/202405/t20240530_11341037.html).
- Mohtar, Tarmila, and Jagad A. Dewantara. 2021. "Jurnal Kewarganegaraan." *NEGARA: KEADAAN SUATU MASYARAKAT BERDASARKAN*

- IDEOLIGI YANG DIANUTNYA* 5 (Desember): 466-475.  
<https://share.google/SKcb9M88plruuhTJ6>.
- Nurrisa, Fahriana, Dina Hermina, and Norlaila. 2025. "Jurnal Teknologi Pendidikan Dan Pembelajaran (JTTPP)." *Pendekatan Kualitatif dalam Penelitian: Strategi, Tahapan, dan Analisis Data 2* (Januari-Maret): 793-800.  
<https://jurnal.kopusindo.com/index.php/jtpp/article/download/581/546/1655>.
- Pashya, Muhammad H., Nurul Faqiriah, Nani Septianie, Gufron Gozali, Elys Krisdiana, and Yeta Purnama. 2021. "Jurnal Khazanah." *PENERAPAN IDEOLOGI KOMUNIS OLEH XI JINPING SEBAGAI BENTUK INDOKTRINASI TERHADAP MASYARAKAT TIONGKOK MELALUI MODEL ALTHUSSERIAN* 13 (Agustus): 1-13. <https://share.google/8TnX3uGe0cOXbnTWP>.
- Pradana, Muhammad E. 2022. "Hasanuddin Journal of International Affairs." *Politik Luar Negeri Tiongkok Sejak Tahun 1978: Transisi, Rebalancing dan Aktivisme* 2, no. 1 (Februari): 1-14.  
<https://doi.org/10.31947/hjirs.v2i1.19839>.
- Quan, Emily. 2022. "Censorship Sensing: The Capabilities and Implications of China's." *Sigma: Journal of Political and International Studies* 39:19-31.  
<https://scholarsarchive.byu.edu/sigma/vol39/iss1/4>.
- Ramich, Mirzet S., and Danil A. Piskunov. 2022. "Vestnik RUDN. International Relations." *The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes* 22 (2): 238-255. 10.22363/2313-0660-2022-22-2-238-255.
- Schia, Niels, and Lars Gjesvik. 2017. "Norwegian Institute of International Affairs." *China's cyber sovereignty*, (April), 1-4. 10.13140/RG.2.2.30512.15360.
- Saulnier, Helen. 2022. "Behind the Facade of China's Cyber Super-Regulator." <https://tishberglaw.com/behind-the-facade-of-chinas-cyber-super-regulator.html>.
- Simangunsong, Edward Michael H., and Tama Amelia P. Sijabat. 2024. "Jurnal Hukum dan HAM Wara Sains." *Studi Komparatif China's Personal Information Protection Law Dengan Undang-Undang Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hak Privasi Masyarakat Indones* 3, no. 3 (Oktober): 323-329.  
<https://wnj.westscience-press.com/index.php/jhhws/index>.
- Smeenck, Gaby, James Wang, Axel Arnbak, and Dulijon Veldhoen. 2017. "Mondaq Legal 500 Intelligence." *China's New Cybersecurity Law Effective As Of 1 June 2017*.  
[https://www.mondaq.com/china/security/595440/chinas-new-cybersecurity-law-effective-as-of-1-june-2017?utm\\_source](https://www.mondaq.com/china/security/595440/chinas-new-cybersecurity-law-effective-as-of-1-june-2017?utm_source).
- Stępką, Maciej. 2022. "The Copenhagen School and Beyond. A Closer Look at Securitisation Theory." (Februari), 17-31. 10.1007/978-3-030-93035-6\_2.
- USC US-China Institute. 2010. "The Internet in China Information Office of the State Council of the People's Republic of China." PRC State

- Council, "The Internet in China," June 8, 2010. [https://china.usc.edu/node/20816?utm\\_source](https://china.usc.edu/node/20816?utm_source).
- Wang, Dakuo, and Gloria Mark. 2015. "ACM Transactions on Computer-Human Interaction." *Internet Censorship in China: Examining User Awareness and Attitudes* 22 (Oktober): 1-23. <http://dx.doi.org/10.1145/2818997>.
- Wulandari, Tri, M. R. Abdimas, Diva Miranda, Avin Octavia, and Afif Ramadhan. 2024. "ULIL ALBAB : Jurnal Ilmiah Multidisiplin." *Dari Revolusi ke Reformasi: Analisis Perbandingan Administrasi Publik dan Konstitusi di China dan Rusia* 3, no. 8 (Juli): 294-307. <https://doi.org/10.56799/jim.v3i8.4244>.
- Weilan, Zhang, Chen Zishuai, and Ma Jingjing. 2024. "Platform serves to building of a community with a shared future in cyberspace." Innovative, safe and inclusive growth in cyberspace urged as WIC opens. [https://www.globaltimes.cn/page/202411/1323476.shtml?utm\\_source](https://www.globaltimes.cn/page/202411/1323476.shtml?utm_source).
- Wowor, Harvardry Gerald A., Arfin Sudirman, and Falhan Hakiki. 2023. "China's Great Firewall: Cybersecurity as Strategy for Building World Cyberpower." *JISPO Jurnal Ilmu Sosial dan Ilmu Politik* 13 (2): 194-232. <https://journal.uinsgd.ac.id/index.php/jispo/article/download/27713/10587>.
- Wu, Mingshi. 2025. "Great Firewall Report." Analysis of the GFW's Unconditional Port 443 Block on August 20, 2025. [https://gfw.report/blog/gfw\\_unconditional\\_rst\\_20250820/en/](https://gfw.report/blog/gfw_unconditional_rst_20250820/en/).
- Wu, Shiwen, and Bo Mai. 2019. "International Journal of Communication." *Talking About and Beyond Censorship: Mapping Topic Clusters in the Chinese Twitter Sphere*, (Mei), 5057-5079. <http://ijoc.org>.
- Xinhua. 2018. "THE STATE COUNCIL THE PEOPLE'S REPUBLIC OF CHINA." Xi outlines blueprint to develop China's strength in cyberspace. [https://english.www.gov.cn/news/top\\_news/2018/04/22/content\\_281476120136986.htm](https://english.www.gov.cn/news/top_news/2018/04/22/content_281476120136986.htm).
- Xinhua. 2022. "THE STATE COUNCIL THE PEOPLE'S REPUBLIC OF CHINA." Xi sends congratulatory letter to 2022 World Internet Conference Wuzhen Summit. [https://english.www.gov.cn/news/topnews/202211/09/content\\_WS636b5a32c6d0a757729e2c8b.html?utm\\_source](https://english.www.gov.cn/news/topnews/202211/09/content_WS636b5a32c6d0a757729e2c8b.html?utm_source).
- Xu, Jian, and Haiqing Yu. 2022. "Media International Australia." *Regulating and governing China's internet and digital media in the Xi Jinping era*, (Juli), 1-6. 10.1177/1329878X221116402.
- Yahya, R, Faqih A., and Tuty N. Mutia. 2023. "THE GREAT FIREWALL OF CHINA: PRAKTIK KEBIJAKAN SENSOR INTERNET PADA ERA XI JINPING (2014-2021)." *Jurnal Pendidik dan Peneliti Sejarah* 6, no. 1 (Maret): 13-24. <https://doi.org/10.17509/historia.v6i1.50007>.
- Yu, Cheng, Hu Yuanyuan, and Ma Zhenhuan. 2020. "CHINADAILY." Xi: Create

- new paradigm for cybersecurity.  
[https://www.chinadailyhk.com/hk/article/186287?utm\\_source](https://www.chinadailyhk.com/hk/article/186287?utm_source).
- Yuen, Samson. 2015. "China Perspectives." *Becoming a Cyber Power China's cybersecurity upgrade and its consequences*, (Juni), 53-58. 10.4000/chinaperspectives.6731.
- Yusrizal, Muhammad. 2014. "Jom FISIP." *DAMPAK IMPLEMENTASI KEBIJAKAN THE GREAT FIREWALL OLEH PEMERINTAH CHINA TERHADAP AKTIVITAS GOOGLE INC DI CHINA (2006 ± 2012)* 1, no. 2 (Oktober): 1-14. <https://share.google/yVDSU1Uf30qbNKB0m>.
- Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "Politics & Policy." *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'* 3 (Juni): 432-464. 10.1111/polp.12202.
- Zhang, Junchen. 2022. "The "Chinese Dream" as a discursive symbol." *A corpus-assisted discourse study on political discursive construction and global media representations of the "Chinese Dream"* 18 (November): 605-631. <https://doi.org/10.1515/css-2022-2082>.
- Zou, Mimi, and Lu Zhang. 2024. "Cambridge Forum." *Navigating China's regulatory approach to generative artificial intelligence and large language models*, (Oktober), 1-16. 10.1017/cfl.2024.4.
- Zulfikar, Faisal M. 2023. "PEMBATASAN AKSES INTERNET SEBAGAI UPAYA CHINA MENJAGA KEAMANAN NASIONAL: THE GREAT FIREWALL OF CHINA." *Journal of Global Studies* 1, no. 1 (Maret): 27-38. <https://doi.org/10.59408/bjgs.v1i1.54>.