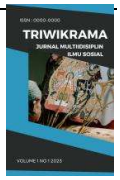
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 7, 2025
E-ISSN: 2988-1986
Open Access:



SERANGAN SIBER PADA ISIDEN *POWER GRID* TAHUN 2020 DAN DAMPAKNYA TERHADAP HUBUNGAN INDIA-TIONGKOK

Nadila Dinar Sadi[1], Imam Fadhil Nugraha [2]
[1,2] Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Makassar, Indonesia.

ARTICLE INFO

Article history:
Received Mei, 2025
Revised Mei, 2025
Accepted Mei, 2025
Available online Mei , 2025

nadiladinars@gmail.com,
Imamfadhil86@gmail.com

A B S T R A K

Tulisan ini bertujuan untuk menjelaskan tentang kasus serangan siber yang terjadi di Mumbai pada tahun 2020 serta dampaknya terhadap dinamika hubungan bilateral antara India dan Tiongkok. Serangan diduga melibatkan aktor siber yang berafiliasi dengan negara asing menunjukkan kerentanan infrastruktur kritis India dan menandai eskalasi bentuk konflik non-tradisional di kawasan Asia Selatan. India sebagai salah satu negara dengan sistem digital yang berkembang pesat juga merupakan salah satu negara di Asia Selatan yang paling sering menjadi target serangan siber dengan motif politik, ekonomi, maupun strategis. Di sisi lain, Tiongkok sering dikaitkan sebagai aktor negara dengan kemampuan siber yang canggih dan strategi proyeksi kekuasaan melalui dominasi digital. Ketegangan geopolitik yang sudah ada antara kedua negara terkait sengketa perbatasan dan rivalitas regional semakin diperumit oleh dimensi siber yang kian menonjol. Melalui pendekatan analitis terhadap insiden Mumbai dan konteks strategis kawasan tulisan ini berupaya memahami bagaimana serangan siber telah menjadi alat baru dalam kontestasi kekuasaan antara India dan Tiongkok.

Kata Kunci: Serangan Siber; India; Tiongkok; Infrastruktur Kritis; Rivalitas Regional.

A B S T R A C T

This paper aims to explain the case of cyberattacks that occurred in Mumbai in 2020 and their impact on the dynamics of bilateral relations between India and China. The attack allegedly involving foreign-affiliated cyber actors demonstrated the vulnerability of India's critical infrastructure and marked an escalation of non-traditional forms of conflict in the South Asian region. India, as one of the countries with a rapidly growing digital system, is also one of the countries in South Asia most frequently targeted by cyberattacks with political, economic, or strategic motives. On the other hand, China is often associated as a state actor with sophisticated cyber capabilities and a strategy of power projection through digital domination. The already existing geopolitical tensions between the two countries over border disputes and regional rivalries are further complicated by the increasingly prominent cyber dimension. Through an analytical approach to the Mumbai incident and the regional strategic context this paper seeks to understand how cyberattacks have become a new tool in the contestation of power between India and China.

***Keywords**: Cyber Attack; India; China; Critical Infrastructure; Regional Rivalry.*

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 7, 2025
E-ISSN: 2988-1986
Open Access:

1. PENDAHULUAN

Memasuki abad ke-21 yang identik dengan revolusi Industri 4.0 membuat kehadiran komputer dan internet telah memberikan dampak besar bagi kehidupan manusia. Teknologi digital memungkinkan berbagai aktivitas dilakukan dengan lebih cepat dan efisien, mulai dari komunikasi, pekerjaan, hingga pengelolaan bisnis. Ketergantungan terhadap sistem digital pun semakin meningkat di sektor publik maupun swasta menjadikannya bagian tak terpisahkan dari kehidupan modern. Namun, di balik kemudahan yang ditawarkan penggunaan teknologi di ruang digital juga menghadirkan risiko baru dalam hal keamanan siber. Ancaman siber kini berkembang semakin kompleks dan sering terjadi, dengan berbagai bentuk serangan seperti *malware, ransomware, phishing*, hingga *Distributed Denial of Service* (DDoS) yang telah melanda banyak negara (Khristiawan, 2024). Negara-negara di seluruh dunia tidak hanya dihadapkan pada tantangan fisik dan militer tetapi juga pada ancaman yang muncul dari sistem digital yang semakin kompleks. Transformasi digital telah membawa perubahan besar dalam cara negara mengelola data, menjalankan pemerintahan, dan melindungi infrastruktur penting. Fenomena ini menempatkan dunia siber sebagai salah satu medan baru dalam kontestasi kekuatan antarnegara. Di era globalisasi yang marak akan digital membuat ancaman terhadap keamanan nasional tidak lagi terbatas pada serangan militer konvensional. Bentuk-bentuk ancaman non-tradisional seperti serangan siber terhadap infrastruktur vital juga bisa saja terjadi. Fenomena ini menandai pergeseran paradigma dalam studi hubungan internasional dan keamanan di mana dunia maya (*cyberspace*) menjadi arena baru dalam rivalitas geopolitik antarnegara. Serangan siber terus berkembang dengan cara mencari celah dalam sistem keamanan untuk mencuri informasi, mengganggu layanan, atau bahkan meminta tebusan. Negara yang belum siap menghadapi ancaman ini akan mengalami kerugian besar secara finansial, reputasi, maupun operasional.

Saat ini banyak infrastruktur vital seperti listrik, perbankan, transportasi, dan layanan kesehatan sangat bergantung pada sistem digital. Hal ini membuat layanan-layanan penting tersebut rentan terhadap gangguan (Khristiawan, 2024). Maka, Jika sistem digital ini diserang dampaknya bisa meluas dan menyebabkan gangguan terhadap kehidupan sehari-hari masyarakat. Dua negara di Kawasan Asia yang tengah menjadi sorotan karena dikenal sebagai pusat pertumbuhan ekonomi serta inovasinya di bidang teknologi yaitu India dan Tiongkok yang memiliki sejarah panjang dan kerap diwarnai persaingan. Walaupun terdapat kerja sama dalam berbagai sektor, ketegangan diantara keduanya tetap terasa khususnya dalam isu-isu strategis dan keamanan. Rivalitas ini tidak lagi terbatas pada konflik teritorial atau ekonomi tetapi telah meluas ke domain digital. Setelah empat bulan ketegangan antara India dan Tiongkok terjadi di perbatasan Ladakh Himalaya, India kembali mengalami serangan siber di Mumbai pada 12 Oktober 2020 yang berdampak pada berbagai sektor vital. Serangan ini membuat seluruh Mumbai dalam keadaan pemadaman listrik total yang mengakibatkan hilangnya kekuatan sumber listrik selama dua jam. Insiden ini menyebabkan 20 juta penduduk Mumbai mengalami hambatan dalam beraktivitas akibat jaringan kereta berhenti, tutupnya pasar saham, dan rumah sakit hanya dapat mengandalkan daya generator untuk menjaga ventilator tetap berjalan (Fahrisa, 2023, p. 141).

Berdasarkan analisis yang dilakukan oleh peneliti siber di *Recorded Future* menyebutkan bahwa insiden tersebut kemungkinan merupakan hasil dari serangan siber yang telah direncanakan dan berasal dari kelompok *RedEcho* yang diduga memiliki afiliasi dengan negara Tiongkok (nikhil, 2021). Hal ini menunjukkan bagaimana konflik di dunia maya menjadi kelanjutan dari ketegangan geopolitik yang sebelumnya terjadi secara fisik di perbatasan. Maka, dapat dikatakan bahwa atribusi serangan tersebut merunjuk ke Tiongkok yang secara historis juga terlibat konflik perbatasan dengan India memperkuat asumsi bahwa serangan

tersebut merupakan bagian dari strategi kekuasaaan non-tradisional dalam konflik asimetris ini. Dalam konteks rivalitas strategi antara India-Tiongkok menjadikan serangan siber sebagai instrumen baru untuk menekan dan menguji kapasitas lawan tanpa harus terlibat langsung menggunakan militer dan kekerasan. Hal ini menimbulkan pertanyaan mendasar tentang bagaimana negara-negara merespon ancaman seperti ini, sedangkan ancaman ini merupakan ancaman yang muncul tidak dengan bertatapan muka tetapi menggunakan teknologi. Selain itu dengan adanya ancaman tersebut bagaimana dinamika yang ada dapat mempengaruhi hubungan diplomatik dan kebijakan luar negeri suatu negara.

Hingga sekarang banyak studi akademik yang membahas mengenai insiden Mumbai 2020 masih terfokus pada aspek teknis serangan siber yang dilakukan. Belum banyak kajian yang secara mendalam membahas mengenai keterkaitan insiden siber dengan dinamika hubungan antara India-Tiongkok serta bagaimana respon pemerintah India terhadap insiden ini. Oleh karena itu, tulisan ini penting karena serangan siber bukan hanya persoalan teknis, tetapi juga berdampak terhadap stabilitas politik, hubungan diplomatik dan kedaulatan negara. Serangan siber kini menjadi bentuk konflik modern yang mampu melumpuhkan negara tanpa senjata konvensional. Dengan adanya insiden *power grid* mumbai 2020 membuktikan bahwa satu serangan saja bisa mengganggu kehidupan sosial, ekonomi, dan kepercayaan publik. Selain skala nasional hal ini juga dapat berdampak pada skala internasional. Melihat bahwa India dan Tiongkok adalah dua kekuatan besar Asia dengan hubungan bilateral yang penuh ketegangan membuat India mulai melakukan strategi *cyber security* di skala internasional, khususnya di Kawasan Indo-pasific. Maka tulisan ini akan menjelaskan lebih dalam mengenai bagaimana insiden *power grid mumbai* 2020 berpengaruh terhadap hubungan antara Tiongkok dan India pada bidang *cyber Security*.

2. TINJAUAN PUSTAKA

Tulisan ini menggunakan **teori konstruktivisme** dan pendekatan keamanan siber (cyber security) sebagai landasan konseptual dalam menganalisis dinamika hubungan antara India dan Tiongkok pasca insiden serangan siber terhadap jaringan listrik di Mumbai pada tahun 2020. Dalam kerangka konstruktivisme, hubungan internasional tidak semata-mata ditentukan oleh kekuatan material atau struktur anarki sistem internasional sebagaimana ditekankan dalam realisme atau liberalisme, melainkan dibentuk oleh struktur sosial yang terdiri atas norma, identitas, dan persepsi bersama (Wendt, 1992). Dalam artian negara dalam sistem internasional tidak berperilaku berdasarkan kepentingan yang objektif dan tetap. Jadi apa yang dianggap sebagai ancaman atau kepentingan sangat dipengaruhi oleh bagaimana aktor-aktor negara melihat dan memaknai situasi serta aktor lain di sekitarnya. Dalam hal ini, keamanan tidak lagi hanya soal perang atau serangan fisik, tetapi juga menyangkut ancaman di dunia maya. Serangan siber yang terjadi pada sistem kelistrikan Mumbai bukan hanya masalah teknis. Serangan semacam ini bisa dianggap sebagai bentuk tekanan politik atau pesan tersembunyi yang punya makna tertentu bagi negara yang mengalaminya. Karena itu India tidak hanya melihat peristiwa ini sebagai gangguan sistem, tetapi juga mengaitkannya dengan meningkatnya ketegangan dengan Tiongkok di wilayah perbatasan.

Melalui kacamata konstruktivisme, respons India terhadap insiden ini juga tidak dapat dilepaskan dari identitas nasional dan persepsi historis terhadap Tiongkok sebagai pesaing strategis di kawasan Asia. Sejak konflik perbatasan tahun 1962 hingga persaingan ekonomi dan militer kontemporer, Tiongkok telah dikonstruksi dalam narasi politik India sebagai "*the Other*" aktor yang selalu diposisikan secara berlawanan dalam dikotomi kepentingan dan

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

keamanan India. Akibatnya serangan ini menjadi bagian dari ketegangan yang menyangkut identitas nasional, keamanan, dan hubungan luar negeri. Maka penggunaan teori konstruktivisme dalam kajian ini memungkinkan analisis yang lebih mendalam atas makna politis serangan siber, termasuk bagaimana ia membentuk persepsi, memperkuat narasi musuh (*enemy image*), serta memengaruhi konfigurasi kebijakan luar negeri dan keamanan nasional. Dalam studi ini, serangan siber terhadap *power grid* Mumbai bukan hanya dilihat sebagai sebuah insiden teknis tetapi sebagai bagian dari narasi strategis yang memperdalam ketegangan bilateral dan memperkuat konstruksi identitas masing-masing negara dalam sistem internasional yang kompleks dan saling tergantung.

3. METODE

Tulisan ini akan menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus untuk menganalisis insiden pemadaman listrik di Mumbai pada tahun 2020 yang diduga sebagai bentuk serangan siber dari Tiongkok serta implikasinya terhadap hubungan bilateral antara India dan Tiongkok. Pendekatan ini dipilih karena memungkinkan peneliti untuk menggambarkan dan memahami fenomena secara mendalam melalui data kualitatif yang bersifat kontekstual dan interpretatif. Tulisan ini menggunakan teori konstruktivisme dan *cyber security* sebagai landasan konseptual dalam kajian hubungan internasional. Konstruktivisme menekankan peran penting konstruksi sosial, identitas, dan persepsi dalam membentuk interaksi antarnegara. Melalui perspektif ini keamanan tidak lagi hanya dilihat dari ancaman militer konvensional tetapi juga dari ancaman dunia maya (*cyber threats*) yang bisa bersifat politik, ekonomi, bahkan ideologis. Serangan siber dipahami tidak semata sebagai tindakan teknis, tetapi sebagai bagian dari narasi yang membentuk identitas dan persepsi ancaman antar aktor negara, dalam hal ini India dan Tiongkok.

Studi kasus ini berfokus pada tiga aspek utama: bentuk dugaan serangan siber yang dilakukan, respon kebijakan pemerintah India, dan pengaruhnya terhadap dinamika hubungan bilateral India–Tiongkok. Teknik analisis data dalam tulisan ini adalah analisis isi tematik. Teknik ini memungkinkan peneliti untuk mengidentifikasi tema-tema utama dari berbagai dokumen yang relevan. Data diperoleh melalui studi pustaka dan analisis dokumen yang mencakup laporan resmi pemerintah, artikel berita nasional dan internasional, laporan lembaga kajian strategis, serta jurnal dan artikel ilmiah yang membahas insiden dan hubungan kedua negara. Analisis dilakukan dengan menelaah konten secara sistematis untuk mengungkap pola-pola makna yang mencerminkan persepsi, kebijakan, dan dinamika hubungan bilateral pasca-insiden. Dengan pendekatan ini diharapkan dapat memberikan pemahaman mendalam mengenai bagaimana serangan siber sebagai bentuk ancaman non-konvensional dapat memengaruhi hubungan internasional antara India-Tiongkok.

4. HASIL DAN PEMBAHASAN

Pembahasan ini disusun secara sistematis dalam beberapa sub bagian yang saling berkaitan Untuk memahami makna strategis dari insiden pemadaman listrik di Mumbai pada tahun 2020 yang diduga sebagai hasil dari serangan siber oleh aktor negara asing. Setiap bagian bertujuan untuk menjelaskan secara menyeluruh mengenai konteks, bentuk serta implikasi dari insiden tersebut terhadap hubungan bilateral antara India dan Tiongkok, khususnya dalam konteks keamanan digital dan politik luar negeri. Di awali dengan analisis mengenai rivalitas strategis India–Tiongkok dalam dinamika regional dan siber. Pada poin ini akan dijelaskan bagaimana persaingan antara kedua negara telah berkembang dari konflik teritorial di kawasan perbatasan Himalaya menjadi kompetisi yang lebih kompleks di ranah digital. Selanjutnya, akan dijelaskan bagaimana insiden pemadaman listrik di Mumbai sebagai instrumen kekuasaan

non-tradisional dalam strategi asimetris. Pembahasan dilanjutkan dengan mengevaluasi respons dan diplomasi siber India dalam forum internasional pasca insiden. Terakhir, akan dibahas persepsi dan penilaian strategis Tiongkok terhadap kebijakan keamanan digital India.

4.1 Rivalitas Strategis India-Tiongkok dalam Dinamika Regional dan Siber

Pada abad ke-21 Asia mengalami fase kebangkitan signifikan yang ditandai dengan pergeseran kekuatan global dari negara-negara Barat menuju Kawasan Asia. Dalam konteks ini, Tiongkok dan India muncul sebagai dua kekuatan dominan yang tengah melonjak secara geopolitik dan geostrategis. Hubungan antara kedua negara yang sama-sama memiliki senjata nuklir sangat berpotensi akan kerja sama. Namun jika melihat kedua negara ini telah dibayangi oleh ketegangan struktural yang bersumber dari faktor historis, geopolitik, ekonomi, dan kepentingan strategis. Baik Tiongkok maupun India memiliki warisan peradaban yang panjang dan menjadikan kebanggaan terhadap sejarah tersebut sebagai bagian penting dalam identitas nasional mereka. Setelah India memproklamasikan kemerdekaannya pada tahun 1947 dan Tiongkok membentuk Republik Rakyat pada tahun 1949, hubungan awal antara kedua negara sempat bersifat harmonis dengan semboyan "India dan Tiongkok adalah saudara". Namun, hubungan ini rusak secara permanen akibat meletusnya perang tahun 1962. Konflik bersenjata tersebut dipicu oleh perselisihan wilayah di Aksai Chin dan Arunachal Pradesh dan berakhir dengan kekalahan besar di pihak India. Perang ini menjadi titik awal ketidakpastian dan ketegangan geopolitik yang masih berlangsung hingga kini. Meskipun berbagai upaya normalisasi telah dilakukan sejak tahun 1980-an dan 1990-an, status garis perbatasan yang dikenal sebagai *Line of Actual Control* (LAC) masih belum disepakati secara tuntas oleh kedua belah pihak. (Beyaz, 2025). Rivalitas keduanya telah berlangsung selama beberapa dekade dan diperparah oleh konflik-konflik yang belum terselesaikan, baik di darat maupun laut.

Hingga akhirnya muncul dimensi baru dari rivalitas yang sedang terjadi. Puncak dari bentrokan dikarenakan adanya persaingan militer yang tidak ada habisnya membuat persaingan antara India-Tiongkok tidak hanya berlangsung di darat dan laut tetapi juga merambat ke ruang siber. Persaingan strategis antara keduanya tercermin dari cara mereka saling memposisikan dalam aspek politik, militer, ekonomi, serta bidang teknologi dan keamanan digital. Sebelum terjadinya insiden pemadaman listrik di Mumbai pada Oktober 2020 kondisi keamanan siber antara India dan Tiongkok menunjukkan ketimpangan yang mencolok dari segi kapabilitas teknis, kesiapan strategis, maupun pendekatan kelembagaan terhadap ancaman dunia maya. Tiongkok yang merupakan salah satu kekuatan global yang telah lama memprioritaskan keamanan siber sebagai bagian integral dari strategi nasionalnya telah mengembangkan ekosistem siber yang terstruktur, terpusat, dan ofensif. Dalam berbagai dokumen pertahanan seperti *China's National Defense White Paper* yang menegaskan pentingnya "informatisasi" dalam perang modern termasuk penggunaan ruang siber sebagai wahana untuk memperoleh keunggulan strategis (Xinhua, 2019). Tiongkok mengembangkan unit-unit militer khusus seperti *Unit 61398* serta mendukung kelompok-kelompok peretas yang dikenal secara internasional seperti *APT10, APT41*, dan *RedEcho* yang diduga kuat memiliki keterkaitan dengan militer atau badan intelijen negara. Kelompok-kelompok ini aktif melakukan serangan siber bertarget tinggi terhadap berbagai negara, khususnya untuk tujuan spionase ekonomi, pencurian data teknologi, hingga sabotase terhadap infrastruktur vital (Clarke & et.al,

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

2023, pp. 47-48). Aktivitas siber ofensif yang dilakukan oleh kelompok-kelompok ini mencerminkan pendekatan strategis Tiongkok yang tidak hanya defensive tetapi juga proaktif dalam mengekspansi pengaruhnya di ranah digital global.

Tiongkok juga berhasil membangun integrasi antara strategi keamanan siber dan ekspansi teknologi globalnya. Perusahaan-perusahaan besar seperti Huawei dan ZTE bukan hanya menjadi pemain utama di industri telekomunikasi dunia, tetapi juga dianggap sebagai alat strategis untuk menyebarkan pengaruh teknologi Tiongkok dan mengumpulkan intelijen secara tidak langsung (3GIMBALS, 2025). Selain itu, infrastruktur digital domestik Tiongkok dikelola dengan sistem kontrol yang sangat ketat seperti yang terlihat dari keberadaan *Great Firewall* yang memungkinkan negara mengawasi, menyensor, sekaligus melindungi jaringan dalam negeri dari gangguan eksternal (Gent, 2024). Pendekatan sentralistik dan koersif ini menjadikan Tiongkok sangat unggul dalam melaksanakan operasi siber ofensif maupun dalam memperkuat pertahanan jaringan nasionalnya. Sebaliknya, India masih berada dalam tahap membangun ekosistem keamanan siber nasional sebelum insiden Mumbai 2020. Meskipun pertumbuhan sektor digital di India tergolong pesat, penguatan aspek keamanannya masih belum seimbang. Menurut laporan dari *The Security Company*, hampir setengah dari anggota dewan perusahaan di India masih kurang paham tentang bahaya dan risiko yang ada di dunia keamanan siber. Selain itu, meskipun pasar keamanan siber di India berkembang dengan pesat, jumlah ahli yang benar-benar terampil di bidang ini masih sangat kurang. Sophos melakukan survei tentang 'Masa Depan Keamanan Siber di Asia Pasifik dan Jepang'. Hasil surveinya menunjukkan bahwa sebanyak 93% perusahaan di India mengaku bahwa kesadaran keamanan siber di antara karyawan, termasuk para eksekutif tingkat dewan masih sangat kurang (Ali, 2023).

India memang memiliki lembaga-lembaga seperti *CERT-In* (*Computer Emergency Response Team India*) dan NCIIPC (*National Critical Information Infrastructure Protection Centre*) namun koordinasi antarinstansi masih sering dianggap kurang efisien dan belum terintegrasi dalam satu kerangka komando strategi nasional (Yadav, 2025, pp. 4-5). Selain itu, rancangan *National Cyber Security Strategy* sudah disusun sejak 2019 tetapi hingga 2020 belum juga difinalisasi dan diterapkan secara menyeluruh. Hal ini mencerminkan lemahnya kesiapan kebijakan strategis dalam menghadapi ancaman digital yang terus berkembang. Dalam konteks ini menjadikan semacam ketimpangan di mana India cenderung bersikap defensive sedangkan Tiongkok sudah jauh lebih agresif dan proaktif di dunia siber. Serangan terhadap infrastruktur digital seperti jaringan listrik, komunikasi, dan sistem informasi strategis menjadi bentuk baru dari konflik asimetris. Insiden pemadaman listrik besar-besaran di Mumbai tahun 2020 menjadi titik balik untuk India lebih memikirkan keamanan siber negaranya. Serangan siber dapat menimbulkan gangguan luas tanpa melibatkan konfrontasi fisik secara langsung serta seringkali sulit diatribusi secara hukum. Hal ini menjadikan siber sebagai instrumen strategis yang efektif untuk menekan lawan secara diam-diam namun berdampak nyata terhadap stabilitas nasional dan hubungan internasional.

Dengan adanya insiden pemadaman listrik di Mumbai pada tahun 2020 menjadikan rivalitas India-Tiongkok semakin luas. Persaingan antara India dan Tiongkok dalam ranah siber mencerminkan perubahan lanskap geopolitik yang kini tidak hanya mempertaruhkan kekuatan fisik tetapi juga kemampuan teknologi dan keamanan digital. Dengan adanya persepsi yang berbeda antara kedua negara mengenai strategi keamanan, menegaskan bahwa di era modern seperti sekarang keamanan siber sangat mempengaruhi stabilitas nasional dan hubungan internasional setiap negara mengenai bagaimana mereka akan

mengelola dan mengamankan ruang siber mereka. Rivalitas ini tidak hanya berdampak terhadap hubungan bilateral tetapi juga terhadap arsitektur keamanan digital regional dan global. Dengan respon yang akan diberikan India terhadap insiden ini membuat negara- negara lain di kawasan menjadi terdorong untuk mengambil posisi strategis untuk membuat pertahanan keamanaan yang memadai. Oleh karena itu, analisis terhadap insiden ini sangat relevan untuk memahami bagaimana siber digunakan sebagai alat geopolitik serta bagaimana negara-negara seperti India membangun respons diplomatik serta teknis yang strategis dalam menghadapi ancaman di ruang digital.

4.2 Insiden *Power Grid* Mumbai 2020 sebagai Instrumen Kekuasaan Non-Tradisional dalam Strategi Asimetris.

Insiden pemadaman listrik di Mumbai pada 12 Oktober 2020 bukanlah gangguan listrik biasa. Kota Mumbai yang merupakan jantung keuangan India dan salah satu kota metropolitan tersibuk di dunia mengalami pemadaman total selama beberapa jam bukanlah hal yang biasa. Aktivitas penting seperti operasional rumah sakit, layanan perbankan, dan sistem transportasi publik lumpuh secara mendadak (Fahrisa, 2023, p. 141). Pada awalnya pemerintah India menyebutkan bahwa gangguan ini disebabkan oleh kegagalan teknis dalam sistem transmisi listrik. Namun investigasi lanjutan menunjukkan adanya kemungkinan elemen siber yang terlibat dalam insiden ini. Laporan dari perusahaan keamanan siber *Recorded Future* mengindikasikan adanya aktivitas digital mencurigakan dari kelompok *RedEcho* yang diduga berafiliasi dengan negara Tiongkok. Dalam laporan tersebut dikatakan bahwa Tiongkok telah menanamkan *malware* ke dalam *Industrial Control System* (ICS) dan *Supervisory Control and Data Acquisition* (SCADA) cari kepanjangan dari ini. milik operator energi utama India (INSIKT GROUP, 2022). Aktivitas ini dilakukan tidak hanya sebelum insiden melainkan berlangsung beberapa minggu setelahnya. Hal ini menunjukkan adanya infiltrasi yang sistematis bukan serangan dadakan atau spontan. Insiden ini berbeda dengan agresi militer konvensional yang bersifat terbuka dan langsung, kali ini serangan yang dilakukan **melalui cara bekerja yang tersembunyi dan berlapis** seperti manipulasi informasi, sabotase siber, spionase digital dan serangan terhadap infrastruktur kritis.

Tindakan seperti ini merupakan bagian dari kekuasaan non-tradisional dalam kerangka teori hubungan internasional dan keamanan. India dan Tiongkok memiliki kekuatan militer dan ekonomi yang relatif setara namun perbedaan dalam keamanan siber menjadikan celah yang dapat dimanfaatkan oleh Tiongkok. Dalam kondisi tersebut **serangan siber terhadap sektor energi menjadi alat tekanan politik dan psikologis** yang efektif untuk melemahkan kepercayaan publik dan menguji respons pemerintah India. Faktanya insiden pemadaman Mumbai terjadi tidak lama setelah **bentrokan militer di perbatasan Ladakh** antara pasukan India dan Tiongkok yang menyebabkan korban jiwa di kedua belah pihak. Ketegangan ini memunculkan dugaan kuat bahwa serangan siber tersebut dilakukan dalam rangka membalas atau memberi tekanan terhadap India dalam domain yang berbeda yakni ruang siber (Sanger & Schmall, 2021). Mumbai dipilih karena merupakan jantung keuangan India dan metropolitan tersibuk, dengan menjadikan Mumbai sebagai target serangan akan menciptakan dampak efek psikologis maksimal dengan melumpuhkan rumah sakit, perbankan, dan transportasi publik. Ini adalah strategi yang sengaja dirancang untuk menciptakan ketidakpastian dan melemahkan kepercayaan publik terhadap kapasitas negara dalam melindungi warganya. Dalam teori kekuasaan non-tradisional keberhasilan

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

bukan diukur dari seberapa besar kerusakan fisik tetapi dari seberapa dalam dampak yang ditinggalkan terhadap stabilitas politik dan persepsi publik (Rid, 2013, pp. 3,5). Dengan memilih target seperti Mumbai yang memiliki nilai simbolik, ekonomi, dan politik tinggi penyerang menunjukkan pemahaman strategis bahwa satu gangguan yang dapat menghasilkan efek dominasi yang lebih besar dibanding konfrontasi militer terbuka. Jika dugaan tersebut benar maka Tiongkok sedang menyampaikan sinyal strategis kepada India bahwa mereka dapat mengganggu kota besar di India tanpa perlu memulai konflik militer.

Sehingga kita dapat menyimpulkan bahwa ruang siber bukan hanya pelengkap perang tetapi telah menjad alat tekanan politik yang nyata. Serangan terhadap infrastruktur energi seperti jaringan listrik memiliki dampak yang luas namun tidak mudah dilacak secara langsung ke pelakunya. Kompleksitas teknis dalam melakukan atribusi serangan siber memberikan keuntungan signifikan bagi penyerang, karena pembuktian keterlibatan suatu negara memerlukan analisis forensik mendalam. Dari perspektif Tiongkok, pendekatan ini juga bisa menjadi cara untuk menghindari sanksi internasional atau reaksi terbuka karena atribusi dalam serangan siber sangat sulit dibuktikan secara cepat dan pasti. Seperti yang dilakukan Tiongkok dengan mengelak adanya kontribusi dalam serangan yang terjadi di India dan menyerahkan beban pembuktian kepada negara korban. Selain itu, insiden seperti ini juga dapat digunakan untuk **mengumpulkan intelijen teknis**, mengukur kapasitas respons dan pemulihan sistem target, serta menciptakan ketakutan atau kekhawatiran di kalangan masyarakat dan investor. Semua ini dilakukan untuk memperlemah posisi strategis India secara tidak langsung baik di bidang ekonomi, politik, maupun keamanan nasional. Keuntungan strategis ini menjadikan serangan siber sebagai bagian dari **arsenal kekuasaan yang efisien dan berbiaya rendah.**

Sedangkan bagi India, insiden ini menjadi titik balik penting dalam memandang ancaman keamanan nasional. Jika sebelumnya fokus lebih besar diberikan pada pertahanan militer konvensional kini muncul kesadaran bahwa investasi pada pertahanan siber, kolaborasi intelijen dan diplomasi digital merupakan keharusan strategis. Dibandingkan dengan konflik konvensional yang memerlukan mobilisasi militer besar-besaran, operasi siber dapat dilakukan dengan sumber daya terbatas namun menghasilkan gangguan maksimal terhadap fungsi vital negara target. Meskipun belum ada bukti publik yang mengonfirmasi keterlibatan Tiongkok secara langsung, insiden Mumbai telah memicu **perubahan signifikan dalam kebijakan keamanan digital India.** Pemerintah mulai melakukan Langkah-langkah strategis untuk memperkuat keamanan siber dan merancang perencanaan jangka Panjang agar insiden tersebut tidak terulang lagi. Hal ini menunjukkan bahwa efek strategis dari insiden tersebut bukan hanya bersifat sementara tetapi **menciptakan pergeseran kebijakan jangka panjang** yang memengaruhi arah hubungan India–Tiongkok. Secara keseluruhan, insiden *Power Grid* Mumbai menunjukkan bagaimana infrastruktur sipil dapat dimanfaatkan sebagai **target strategis dalam konflik antarnegara modern** dan bagaimana ruang siber telah menjadi medan pertempuran yang tak kalah pentingnya dari darat dan laut. Analisis terhadap peristiwa ini membuat rekontruksi pemahaman yang lebih luas tentang bentuk-bentuk kekuasaan baru dalam politik internasional serta menyoroti urgensi untuk memperkuat tata kelola keamanan siber sebagai bagian dari strategi pertahanan nasional menjadi lebih meningkat.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 7 2025
E-ISSN: 2988-1986
Open Access:

4.3 Diplomasi Siber India dalam Forum Internasional Pasca Insiden dan Penilaian Strategis Tiongkok terhadap Kebijakan Keamanan Digital India

Meskipun otoritas India tidak secara terbuka menyebutkan Tiongkok sebagai pelaku investigasi independent tetapi fakta bahwa laporan dari perusahaan keamanan siber global seperti *Recorded Future* menyampaikan indikasi kuat bahwa kelompok peretas yang terafiliasi dengan negara Tiongkok kemungkinan terlibat dalam infiltrasi terhadap sistem kelistrikan India (INSIKT GROUP, 2021). Untuk merespon hal ini, India tidak dapat langsung membalas dengan cara langsung melakukan serangan balik kepada Tiongkok karena jika India melakukan hal tersebut Tiongkok akan mengetahui batas maksimum dan kapabilitas daya serang yang India miliki. Maka hal yang dilakukan India adalah memblokir lebih dari 59 aplikasi asal Tiongkok sejak pertengahan 2020 dengan alasan keamanan nasional berdasarkan Pasal 69A Undang-Undang Teknologi Informasi 2000 (Delhi, 2020). Beberapa bulan kemudian pada September 2020 MeitY kembali menambah daftar tersebut dengan memblokir 118 aplikasi lainnya termasuk aplikasi yang sangat populer seperti *TikTok, WeChat*, dan *PUBG Mobile*. Maka, secara keseluruhan sepanjang tahun 2020 India telah melarang total 220 aplikasi asal Tiongkok untuk beroperasi di wilayahnya (Febrianti & dkk, 2022, p. 293). Dengan langkah yang diambil India juga berusaha memberikan solusi untuk Keputusan ini dengan mulai mengembangkan ekosistem teknologi dalam negeri melalui program Atmanirbhar Bharat yang salah satu fokusnya adalah mengurangi ketergantungan terhadap teknologi asing, terutama dalam bidang perangkat keras dan jaringan komunikasi.

India menyadari bahwa dominasi aplikasi Tiongkok dalam ekosistem digital India dapat menciptakan kerentanan struktural, di mana data pengguna dan pola perilaku masyarakat India dapat dimanfaatkan untuk kepentingan intelijen atau manipulasi informasi. Pemerintah mulai mendorong pengembangan industri *cybersecurity* lokal dan investasi dalam penelitian keamanan digital. Selain itu, pendidikan dan pelatihan di bidang keamanan siber ditingkatkan, baik di institusi pemerintah maupun lembaga pendidikan tinggi. Sembari melakukan pemblokiran aplikasi, India mengambil langkah utama untuk mempercepat perumusan dan implementasi *National Cyber Security Strategy* (NCSS) yang sebelumnya sempat tertunda. Dengan melakukan audit keamanan digital pada beberapa fasilitas penting termasuk pembangkit listrik dan sistem kontrol industri. Strategi ini dirancang untuk memberikan kerangka kerja nasional dalam mengelola keamanan siber secara terkoordinasi, mulai dari pencegahan, deteksi, hingga respons terhadap serangan siber. Fokus utama dalam strategi ini mencakup perlindungan terhadap infrastruktur kritis, pengembangan kapasitas sumber daya manusia di bidang keamanan siber, peningkatan kerja sama internasional, serta pelibatan sektor swasta dalam sistem pertahanan digital nasional untuk mengidentifikasi celah yang dapat dimanfaatkan oleh pihak luar sebagai respons awal India dalam meningkatan sistem pengawasan terhadap infrastruktur penting dengan bekerja sama antar instansi khususnya antara *CERT-In* (*Computer Emergency Response Team* – India) dan organisasi sektor energi *(Devanny & Laudrain, 2025)*.

Namun respon India tidak hanya hanya bersifat internal tetapi secara paralel, India mulai mendorong agenda keamanan siber dalam diplomasi luar negerinya baik secara bilateral maupun multilateral. Salah satu langkah penting yang dilakukan India adalah mengadopsi pendekatan diplomasi siber yang proaktif dengan berpartisipasi dalam berbagai forum internasional. *Quadrilateral Security Dialogue* (Quad) yang melibatkan India, Amerika Serikat, Jepang, dan Australia, India mendorong pembentukan norma-

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

norma perilaku negara di ruang siber dan peningkatan kapasitas keamanan siber di kawasan Indo-Pasifik *(Devanny & Laudrain, 2025)*. Langkah ini menandai pergeseran India dari pendekatan isolatif ke pendekatan kooperatif dalam menghadapi ancaman siber lintas negara. India juga secara aktif mengusulkan pembentukan standar internasional dalam tata kelola ruang siber dan mendorong pembagian intelijen siber antaranggota. Upaya ini juga mencerminkan kesadaran India bahwa keamanan digital tidak bisa hanya ditangani secara nasional tetapi membutuhkan sinergi regional dan global. Dalam forum PBB dan G20 India mengangkat pentingnya norma perilaku negara di ruang siber termasuk tanggung jawab negara dalam mencegah aktivitas siber yang merusak terhadap infrastruktur kritikal negara lain. India juga mendukung pembentukan mekanisme multilateral yang dapat membantu mengatribusi dan merespons serangan siber lintas negara dengan lebih transparan dan adil. Selain itu, India mendorong penyusunan kerangka hukum internasional yang mengatur tentang penggunaan kekuatan di dunia maya dan perlindungan infrastruktur sipil dari ancaman digital *(Saxena & Mahan, 2023, pp. 3,13)*.

India juga menggunakan kasus Mumbai sebagai contoh untuk menunjukkan bagaimana serangan siber dapat memiliki dampak nyata terhadap keamanan dan kesejahteraan masyarakat sehingga perlu ada kesepakatan global mengenai batas-batas perilaku negara di dunia digital. Perlu dicatat bahwa respons diplomatik India juga dilakukan secara hati-hati. Meskipun banyak pihak di dalam negeri menekan pemerintah untuk lebih keras terhadap Tiongkok, India memilih untuk tidak langsung menuduh Tiongkok secara resmi. Strategi ini sejalan dengan pendekatan "*strategic restraint*" yang selama ini menjadi ciri khas diplomasi India dalam menghadapi konflik regional sekaligus untuk menjaga ruang negosiasi terbuka di tengah meningkatnya ketegangan geopolitik di Asia. Secara keseluruhan insiden Mumbai menjadi titik balik dalam cara India memandang ancaman siber sebagai hal yang krusial. Serangan ini mendorong transformasi dari pendekatan yang bersifat defensif menjadi lebih proaktif dalam berbagai asepek, tidak hanya dalam aspek teknis tetapi juga dalam diplomasi digital dan pembentukan arsitektur keamanan siber yang inklusif di tingkat internasional. Langkah ini dilakukan untuk menegaskan bahwa dunia maya kini telah menjadi arena penting dalam hubungan internasional dan respons terhadapnya tidak cukup hanya dengan teknologi tetapi juga strategi dan kerja sama politik global.

Dari sudut pandang Tiongkok, sistem keamanan siber India dinilai masih berkembang dan belum sepenuhnya mampu menghadapi ancaman canggih. Hal ini membuka peluang bagi Tiongkok untuk memproyeksikan kekuatan dalam bentuk tekanan non-militer termasuk melalui serangan siber skala kecil yang bersifat uji coba atau sebagai bentuk *gray-zone operations* yang berada di ambang perdamaian dan konflik terbuka. Dari perspektif strategis Tiongkok, *gray-zone operations* memberikan *return on investment* yang sangat tinggi. Dengan biaya operasional yang relatif rendah. Tiongkok dapat menciptakan ketidakstabilan signifikan dalam infrastruktur kritis India dengan menguji kapasitas respons sistem pertahanan India dan memperoleh intelijen berharga tentang kerentanan teknis tanpa memicu sanksi internasional yang serius. Namun sejak 2020 India mulai menunjukkan peningkatan signifikan dalam kapasitas pertahanan sibernya termasuk dalam hal perlindungan infrastruktur informasi penting, pengembangan kapasitas, kemitraan publik-swasta, dan kerja sama internasional (RSM, 2025). Hal ini menunjukkan bahwa India tidak lagi dapat diremehkan sebagai aktor pasif dalam domain digital. Dengan demikian strategi Tiongkok terhadap India juga mulai bergeser dari dominasi teknologi ke arah pengelolaan konflik siber secara berhati-hati untuk menghindari eskalasi terbuka.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 7 2025
E-ISSN: 2988-1986
Open Access:

Menanggapi tuduhan India terkait insiden yang terjadi di Mumbai pada tahun 2020 Tiongkok secara konsisten membantah keterlibatan negara dalam aktivitas tersebut (RISING, 2022). Tiongkok mengklaim bahwa mereka juga menjadi korban serangan siber yang berasal dari India dengan laporan dari perusahaan keamanan siber Tiongkok yang menyoroti serangkaian serangan yang menargetkan Tiongkok dan Pakistan. Sejak adanya kebijakan yang dibuat India terhadap pemblokiran 59 aplikasi asal Tiongkok termasuk TikTok dan WeChat dengan alasan keamanan nasional (Delhi, 2020). Tiongkok mengecam langkah ini sebagai diskriminatif dan melanggar prinsip-prinsip Organisasi Perdagangan Dunia (WTO). Kementerian Perdagangan Tiongkok menyatakan keprihatinan serius dan berharap India memperlakukan semua investor asing secara adil dan tidak diskriminatif (International Asian News, 2021). Selain itu, Tiongkok juga memanfaatkan operasi informasi sebagai instrument strategis untuk memperoleh keunggulan atas India dalam ranah politik. Mereka semakin aktif dalam melancarkan kampanye disinformasi terhadap India dengan tujuan merusak reputasi internasional India dan memperkuat klaim territorial di wilayah sengketa seperti Landhak dan isu Kashmir (Hasija, 2025). Kampanye disinformasi Tiongkok terhadap India tidak hanya bertujuan merusak citra dan menurunkan moral militer tetapi juga menciptakan *cognitive confusion* dalam pengambilan keputusan strategis India. Dengan menyebarkan narasi yang kontradiktif Tiongkok berusaha mencegah India untuk fokus pada perencanaan strategis jangka panjang.

Namun sebaliknya, India telah melakukan banyak perkembangan terhadap kebijakan siber negaranya, yang dimana hal ini turut memengaruhi cara Tiongkok memandang India sebagai tantangan sekunder dibandingkan dengan fokus utamanya di kawasan Pasifik dan persaingan dengan AS. Kebangkitan hubungan India-AS terutama melalui Strategi Indo-Pasifik telah meningkatkan kekhawatiran Tiongkok terhadap kemungkinan terbentuknya aliansi yang dapat mengancam kepentingannya di Asia Selatan dan Samudra Hindia (Beyaz, 2025). Maka, dalam beberapa tahun terakhir Tiongkok mulai aktif mempromosikan konsep "*Cyber Sovereignty*" gagasan bahwa negara berhak penuh atas regulasi internet di dalam perbatasannya untuk menandingi narasi kebebasan digital yang diusung oleh negara-negara Barat (Associated Press, 2023). Dalam konteks ini Tiongkok melihat peluang dan risiko sekaligus. Di satu sisi India masih menjadi pasar digital besar yang strategis sementara di sisi lain jika India semakin dekat dengan aliansi digital Barat hal ini akan memperkecil ruang pengaruh Tiongkok di kawasan. Karena itu Tiongkok cenderung menjaga pendekatan yang ambigu terhadap India dengan tetap bersikap keras terhadap tuduhan siber namun tetap berusaha membuka saluran kerja sama teknologi pada isu-isu netral seperti AI, big data atau *e-commerce* lintas batas. Dalam hal ini Tiongkok menggunakan pendekatan multi-layer yang menggabungkan operasi siber, *warfare* informasi, diplomasi ekonomi, dan *narrative control* untuk mempertahankan pengaruh strategisnya sambil mengelola risiko eskalasi dengan India yang semakin menguat dalam domain siber.

5. KESIMPULAN

Dengan adanya historis rivalitas antara kedua negara telah menunjukkan bahwa banyaknya ketidaksamaan antara India dan Tiongkok. Dimana India memandang dirinya sebagai negara demokratis yang berkomitmen pada keterbukaan dan transparansi digital sementara Tiongkok menekankan stabilitas dan kontrol dalam ruang sibernya. Perbedaan identitas ini mempengaruhi persepsi masing-masing terhadap tindakan satu sama lain. Dengan India

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

melihat Tiongkok sebagai ancaman terhadap kedaulatan digitalnya dan Tiongkok melihat kebijakan India sebagai upaya untuk membendung pengaruh Tiongkok. Kedua negara memiliki norma dan nilai yang berbeda terkait tata kelola internet. India cenderung mendukung internet yang bebas dan terbuka sementara Tiongkok mendorong konsep kedaulatan siber. Perbedaan ini menciptakan ketegangan dalam forum internasional dan mempengaruhi kebijakan masing-masing negara dalam merespons isu-isu siber. Interaksi berulang antara India dan Tiongkok dalam isu-isu siber membentuk dinamika sosial yang kompleks. Tindakan satu pihak sering kali dipersepsikan sebagai ancaman oleh pihak lain yang kemudian memicu respons defensif atau ofensif dan menciptakan siklus ketegangan yang berkelanjutan. Meskipun hubungan India-Tiongkok kerap diwarnai rivalitas, kedua negara tetap dapat menjalin kerja sama dalam membentuk norma atau etika bersama terkait keamanan siber.

Forum seperti ASEAN, *Shanghai Cooperation Organization* (SCO) dan BRICS dapat menjadi wadah dialog untuk menghindari serangan terhadap infrastruktur publik yang bisa merugikan kedua pihak. Upaya ini dapat mengurangi risiko konflik yang lebih besar dan mendorong stabilitas regional. Respon Tiongkok terhadap kebijakan keamanan digital India mencerminkan dinamika kompleks yang dipengaruhi oleh identitas nasional, norma, dan persepsi bersama. Dengan kata lain hubungan India–Tiongkok saat ini mencerminkan bentuk "kompetisi yang dikelola", di mana konfrontasi terbuka dihindari namun kompetisi strategis tetap berlangsung di berbagai bidang siber, ekonomi, dan militer. Persaingan ini kemungkinan akan terus membentuk arsitektur keamanan dan geopolitik Asia dalam beberapa dekade ke depan. Melalui lensa konstruktivisme kita dapat memahami bahwa tindakan dan reaksi kedua negara tidak hanya didasarkan pada kepentingan material tetapi juga pada konstruksi sosial atas realitas dan kepentingan mereka. Pendekatan ini dapat memberikan pembaca wawasan yang lebih dalam mengenai bagaimana konflik dan kerja sama suatu negara di ranah siber dapat berkembang di masa depan.

6. SARAN

Berdasarkan hasil analisis yang dilakukan, terdapat beberapa saran yang bisa di pertimbangkan. Dalam sektor-sektor vital seperti energi, transportasi, dan layanan publik lainnya India perlu meningkatkan sistem keamanan siber secara menyeluruh. Sistem ini tidak cukup hanya dikelola oleh institusi militer atau intelijen tetapi juga perlu melibatkan lembaga pemerintah sipil, sektor swasta, dan masyarakat. Peningkatan ini mencakup pembaruan regulasi, penguatan kapasitas sumber daya manusia, dan pemantauan sistem digital secara berkala. Penting bagi India untuk membangun respons diplomatik yang transparan dan berbasis bukti dalam menanggapi dugaan serangan siber. Pendekatan ini dapat memperkuat posisi India dalam forum internasional dengan membangun kepercayaan global dan menghindari eskalasi konflik yang tidak perlu. Selain itu diperlukan dorongan kolaborasi antara perguruan tinggi, lembaga riset, dan peneliti dari negara atau bahkan secara internasional. Melalui kerja sama akademik banyak aspek keamanan siber yang bisa dikaji lebih dalam sekaligus membangun diplomasi jalur alternatif melalui ilmu pengetahuan dan teknologi. Hal ini dapat membuka ruang dialog yang lebih netral di tengah ketegangan politik.

7. DAFTAR PUSTAKA

3GIMBALS. (2023, March 15). *Chinese telecom infrastructure in the U.S.: National security risks and supply chain threats*. 3GIMBALS. https://3gimbals.com/insights/chinese-telecom-infrastructure-in-the-u-s-national-security-risks-and-supply-chain-threats/

Associated Press. (2023, November 8). *China's Xi urges countries unite in tackling AI challenges but makes no mention of internet controls*. AP News: https://apnews.com/article/china-internet-cyberspace-d6504b721034e7107d4ae09de516886c

Banks, J. A. (2007). *Educating citizens in a multicultural society* (2nd ed.). New York: Teachers College Press.

Beyaz, F. (2025, 19 May). *Threat perception, competition and the quest for hegemony in China-India relations*. E-International Relations. https://www.e-ir.info/2025/05/19/threat-perception-competition-and-the-quest-for-hegemony-in-china-india-relations/

Clarke, R., & et al. (2023). *The evolution of Chinese cyber offensive operations and Association of Southeast Asian Nations* (ASEAN). *JSTOR*, 47-48.

Devanny , J., & Laudrain, A. P. B. (2025). *Interpreting India's Cyber Statecraft*. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft

Delhi, P. (2020, June 29). *Government bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order*. *Press Information Bureau*. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1635206

Fahrisa, T. R. (2023). *The Indian Government's cybersecurity strategy from Kautilya's perspective: Mumbai cyber attacks* 2020. *Indonesian Journal of International Relations*, 141.

Febrianti, R., & dkk. (2022). PERSAINGAN KEKUASAAN ANTARA INDIA DAN CINA:. *Intermestic*, 293. Intermestic.

Gent, E. (2024, October 23). *China extends the "Great Firewall" into space. Retrieved from* https://industrialcyber.co/critical-infrastructure/us-fcc-launches-probes-into-ccp-linked-entities-amid-national-security-concerns/

Hasija, N. (2025, May 11). *China launched a misinformation campaign following the Pahalgam attack. Retrieved from* https://sundayguardianlive.com/investigation/china-launched-a-misinformation-campaign-following-the-pahalgam-attack

International Asian News. (2021, January 27). *China opposes India's desicion to continue Chinese apps ban, says it violates WTO rules*. *The times of India*: https://timesofindia.indiatimes.com/india/china-opposes-indias-decision-to-continue-chinese-apps-ban-says-it-violates-wto-rules/articleshow/80480454.cms

INSIKT GROUP. (2021, February 28). *China-linked group RedEcho targets the Indian power sector amid heightened border tensions*. *Recorded Future*. https://www.recordedfuture.com/research/redecho-targeting-indian-power-sector

INSIKT GROUP. (2022, April 6). *Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group*. *Recorded Future*: https://www.recordedfuture.com/research/continued-targeting-of-indian-power-grid-assets

Industrial Cyber. (2023, October 26). *US FCC launches probes into CCP-linked entities amid national security concerns*. *Industrial Cyber*. https://industrialcyber.co/critical-infrastructure/us-fcc-launches-probes-into-ccp-linked-entities-amid-national-security-concerns/

*Corresponding author
E-mail addresses: nadiladinars@gmail.com

Joshi, S., & Singh, D. (2020, November 20). *Mega Mumbai power outage may be result of cyber attack, final report awaited. India Today*. https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20

Khristiawan, D. (2024, June 15). Keamanan siber dan kebutuhan sistem digital di dunia maya. *Kementerian Pertahanan Republik Indonesia*. https://www.kemhan.go.id/pothan/2024/07/15/Keamanan%20Siber%20dan%20Kebutuhan%20Sistem%20Digital%20Di%20Dunia%20Mayaeamanan-siber-dan-kebutuhan-sistem-digital-di-dunia-maya.html?cv=1

Nikhil, p. (2021, Feb 28). *Chinese cyberattack that caused the 2020 Mumbai blackout was a 'warning shot': Report*. wionews: https://www.wionews.com/india-news/chinese-cyberattack-that-caused-the-2020-mumbai-blackout-was-a-warning-shot-report-367125

Priya, S., & Naresh, N. (2020). *A case study on Mumbai power outage. i-Manager's Journal on Power Systems Engineering, 8*(3), 34–38. https://doi.org/10.26634/jps.8.3.17795

Rising, D. (2022, April 7). *Chinese hackers reportedly target India's power grid. AP News*. https://apnews.com/article/technology-business-china-india-b9e32f0d36843b2ac2764d0b4ae2c7e6

RSM. (2025, January 10). *Understanding India's Cybersecurity Policy Frameworks: IT Act, National Cybersecurity Policy, and Strategy*. RSM Global: https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks

Rid, T. (2013). *Cyber War Will Not Take Place*. Dalam T. Rid, *Cyber War Will Not Take Place* (hal. 3,5). *United Kingdom: Oxford University Press*.

Strategic Study India. (2021). *Chinese cyber exploitation in India's power grid – Is there a linkage to Mumbai power outage? Strategic Study India*. https://strategicstudyindia.com/chinese-cyber-exploitation-india-power-grid-mumbai-outage

Sanger, D., & Schmall, E. (2021, September 27). *China appears to warn India: Push too hard and the lights could go out. The New York Times*. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

Saxena, S., & Mahan, K. (2023). *Establishing global norms to protect critical information infrastructure. ThinkTwenty*, 3, 13.

The State Council Information Office of the People's Republic of China. (2019, July 24). *China's national defense in the new era* [White paper]. *The State Council of the People's Republic of China*. https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

Wendt, A. (1992). *Anarchyis whatstatesmake ofit: the*, 391–425. International Organization.

Xinhua. (2019, July 24). *China issues white paper on national defense in new era*. english.gov.cn: https://english.www.gov.cn/statecouncil/ministries/201907/24/content_WS5d37ca73c6d00d362f668c58.html

Yadav, D. P. (2025). *National Security of India with a Special Focus on Cybersecurity. amoghvarta*, 4-5.