Triwikrama: Jurnal Ilmu Sosial
Volume 9 No.2 Tahun 2025
E-ISSN: 2988-1986
Open Access:

ANALISIS STRATEGI AMERIKA SERIKAT DAN TIONGKOK DALAM MENANGGULANGI *CYBER CRIME* PASCA-PANDEMI

Rania Nur Izzati[1], Atika Puspita Marzaman[2]
[1,2]*International Relations Department, Faculty of Social and Political Sciences, Hasanuddin University, Makassar, 90245.*

ARTICLEINFO

Article history:
Received : June 2025
Revised : June 2025
Accepted : June 2025
Available online

Korespondensi: Email:
[1]ranianurizzati01@gmail.com
[2]tika.marzaman@gmail.com

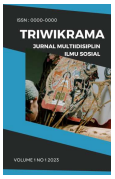
Abstrak

Pandemi COVID-19 telah mempercepat transformasi digital global beriringan dengan meningkatnya risiko kejahatan siber akibat melonjaknya ketergantungan digital. Sebagai dua negara besar global, Amerika Serikat dan Tiongkok menghadapi tantangan dan ancaman yang sama namun menanggulanginya dengan strategi yang berbeda. Jurnal ini menganalisis strategi kedua negara tersebut dalam menghadapi kejahatan siber khususnya pasca-pandemi, dengan mencakup kebijakan nasional utama, peran kelembagaan nasional, kerangka hukum, serta kerja sama internasional dari masing-masing negara. Amerika Serikat memajukan strategi berbasis dokumen strategisnya, yaitu *National Cybersecurity Strategy* 2023, yang menyoroti kerja sama internasional dan penguatan respons multilateral. Di sisi lain, Tiongkok menekankan strategi *state-centric* dengan menggunakan prinsip kedaulatan siber dan peninjauan ketat terhadap dinamika siber melalui *Cyberspace Administration of China* (CAC). Kedua negara ini memiliki persamaan dalam hal komitmen terhadap perlindungan infrastruktur, namun ideologi dan geopolitik masing-masing negara yang membentuk karakter masing-masing negara menjadi pembeda antar keduanya. Studi ini menunjukkan bahwa kejahatan siber pasca-pandemi telah menjadi ajang baru dalam kompetisi dominasi global, namun tetap menyediakan peluang kerja sama dalam isu-isu yang bersifat transnasional.

Kata kunci: Kejahatan Siber, Keamanan Siber, Strategi Nasional, Amerika Serikat, Tiongkok, Tata Kelola Digital.

Abstract

The COVID-19 pandemic has accelerated global digital transformation while increasing the risks associated with cybercrime due to growing digital dependence. As two of the world's major powers, the United States and China have faced similar cyber threats but have adopted notably different strategies in response. This study examines each country's post-pandemic cybersecurity approach, focusing on national policy frameworks, institutional roles, legal regulations, and international cooperation efforts. The United States has advanced a strategy guided by its 2023 National Cybersecurity Strategy, which emphasizes multilateral engagement and collaboration between the public and private sectors. In contrast, China has pursued a state-centric model rooted in the principle of cyber sovereignty, with strict regulatory oversight led by the Cyberspace Administration of China (CAC). While both nations share a commitment to protecting critical infrastructure and addressing cyber threats, their approaches are shaped by distinct political ideologies and geopolitical interests. The findings suggest that cybercrime in the post-pandemic era has become a strategic domain for global



power competition, highlighting the necessity for cross-border cooperation on transnational cyber issues.
***Keywords**: Cybercrime, Cyber Security, National Strategy, United States, China, Digital Governance.*

PENDAHULUAN

Di masa sekarang, kemampuan digital semakin maju dan teknologi informasi telah menjadi bagian yang selalu mendampingi manusia di kehidupan sehari-hari, mulai dari kegiatan-kegiatan individu hingga sistem yang mengatur skala besar seperti negara. Akan tetapi, adanya kemajuan teknologi ini juga disertai dengan timbulnya risiko kejahatan siber (*cybercrime*) yang semakin meningkat. Kejahatan siber memiliki bentuk yang bermacam-macam serangan seperti, pencurian data, peretasan sistem, penyebaran *malware*[1], hingga serangan *ransomware*[2] yang dimana macam-macam serangan ini semakin marak terjadi. Hal ini menyebabkan kondisi global sekarang diharuskan untuk menghadapi dan menanggulangi tantangan baru dalam bidang keamanan, yang dimana ancaman ini tidak lagi bersifat fisik seperti sebelum-sebelumnya, tetapi bersifat non-fisik, virtual, dan lintas negara.

Semenjak pandemi COVID-19 yang menimpa seluruh dunia pada tahun 2020, digitalisasi diberbagai sektor seperti pendidikan, pemerintahan, kesehatan, dan bisnis mengalami percepatan yang sangat signifikan. Masyarakat menjadi berketergantungan dengan teknologi digital yang memang sangat membantu untuk melakukan aktivitas-aktivitas sehari-hari di masa pandemi. Namun, dengan meningkatnya ketergantungan tersebut, para pelaku kejahatan siber memanfaatkan hal tersebut dengan memasuki celah keamanan pada teknologi digital ini. Berdasarkan laporan Interpol terdapat kenaikan yang signifikan dalam kasus kejahatan siber selama dan setelah masa pandemi. Terjadinya penyebaran COVID-19 yang sangat cepat membuat banyak sistem yang belum siap, termasuk rumah sakit, institusi pendidikan, dan perusahaan besar. Hal ini lah yang secara spesifik dimanfaatkan oleh para pelaku kejahatan siber. Bahkan, target serangan siber yang melonjak secara drastis selama pandemi pun turut berubah yang mulanya menargetkan individu menjadi infrastruktur penting dan lembaga pemerintahan yang tentunya sangat krusial. Mereka menyoroti bahwa kasus yang sering terjadi berada di bidang layanan kesehatan dan keuangan (INTERPOL, 2020). Selain itu, Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, juga turut mengamini hal ini dengan mencatat bahwa terdapat peningkatan lebih dari 1 miliar serangan siber disepanjang tahun 2021, yang cukup membuktikan bahwa ancaman digital di era pasca-pandemi sangat masif (BSSN, 2022). Fenomena ini menegaskan bahwa kejahatan siber termasuk bentuk ancaman non-tradisional yang harus diberikan perhatian khusus dari berbagai negara di seluruh dunia.

Jika dilihat dalam kajian hubungan internasional, kejahatan siber telah bertransformasi yang mulanya adalah kejahatan teknologi menjadi isu strategis lintas negara. Kejahatan siber tidak hanya menimbulkan dampak di sektor ekonomi infrastruktur, tetapi juga menjadi ancaman bagi stabilitas politik dan kepercayaan publik terhadap institusi suatu negara. Dalam hal ini, Amerika Serikat (AS) dan Tiongkok menjadi dua pihak penting yang sering kali mendapatkan perhatian lebih dalam isu keamanan siber global. Hal ini menjadikan landasan penelitian ini untuk memahami bagaimana dua negara berkekuatan besar tersebut menanggapi tantangan kejahatan siber terutama pasca-pandemi. Negara-negara adidaya seperti AS dan Tiongkok

[1] Malware atau malicious software merupakan sebuah perangkat lunak yang berbahaya untuk merusak, mengganggu, atau mendapatkan akses ke sistem computer, jaringan, atau data secara ilegal.
[2] Ransomware merupakan salah satu jenis malware yang berkerja untuk mengunci atau mengenkripsi data korban, kemudian melakukan pemaksaan penebusan kepada pemilik data agar data tersebut dapat diakses kembali.

berada di garis depan dalam menghadapi tantangan ini. Dalam hal ini, AS dan Tiongkok memiliki peran sebagai aktor, pembuat kebijakan, dan bahkan target. Strategi kedua negara dalam menanggulangi kejahatan siber tidak hanya menggambarkan kebijakan domestik, tetapi juga arah kebijakan luar negeri dan posisi mereka dalam tatanan global.

Amerika Serikat dipilih dalam penelitian ini karena perannya sebagai negara adidaya dan pemimpin dalam inovasi digital, dengan ketergantungan yang tinggi pada infrastruktur kritikal bersistem daring. Selain daripada itu, AS juga terkenal berperan aktif dalam mengedepankan tata kelola keamanan siber global, untuk mencegah adanya peningkatan kasus *cybercrime*. Salah satu kasus yang menunjukkan keseriusan respons AS terhadap *cybercrime* khususnya pasca-pandemi adalah serangan *ransomware* terhadap *Colonial Pipeline* yang terjadi di tahun 2021. Peristiwa ini memicu gangguan besar pada distribusi bahan bakar yang berada di Pantai Timur dan menimbulkan respons tangkas dari pemerintah, termasuk peluncuran strategi keamanan siber baru. Pada Maret 2023, AS secara resmi merilis *National Cybersecurity Strategy* sebagai penguatan usaha melindungi infrastruktur penting dan memperkuat kolaborasi dengan sektor swasta juga mitra internasional.

Sementara itu, Tiongkok dipilih dalam penelitian ini karena kedudukannya yang cukup menarik untuk dikaji, dimana Tiongkok merupakan negara pertama yang terkena dampak COVID-19 serta memiliki pendekatan yang sangat berbeda dalam hal keamanan digital. Pemerintahan Tiongkok mengatakan bahwa mereka menganut prinsip "kedaulatan siber" atau *cyber sovereignty*. Kedaulatan siber merupakan strategi yang mengontrol negara atas ruang digital domestiknya secara penuh. Strategi ini terlihat dalam beberapa kebijakan Tiongkok, termasuk pembaruan Undang-Undangan Keamanan Siber dan pembatasan perusahaan teknologi asing. Salah satu peristiwa penting yang menunjukkan strategi Tiongkok terhadap *cybercrime* adalah ketika adanya tuduhan terhadap kelompok Hafnium, yang diduga bekerja sama dengan Pemerintah Tiongkok, atas peretasan sistem email *Microsoft Exchange* yang terjadi pada awal tahun 2021. Peristiwa ini mengakibatkan reaksi dunia yang beragam dan menjadi puncak masalah dalam meningkatnya ketegangan keamanan digital antara Tiongkok dengan negara-negara Barat.

Kedua negara ini memiliki kekuatan ekonomi dan teknologi terbesar di dunia, sehingga keduanya memiliki posisi yang strategis dalam menentukan standar, kebijakan, serta tata kelola global mengenai keamanan siber. Namun, keduanya memiliki metode yang berbeda dalam hal penanganan ancaman kejahatan siber. Di tengah ketegangan geopolitik mereka, strategi AS dan Tiongkok dalam menghadapi kejahatan siber merefleksikan kepentingan nasional sekaligus ambisi global mereka. Meskipun kedua ini memiliki perhatian yang besar mengenai isu keamanan siber, strategi dan kebijakan kedua negara ini dalam menghadapi kejahatan siber memiliki perbedaan yang cukup signifikan jika dilihat dari segi strategi, kebijakan, dan tata kelola kelembagaannya. Perbedaan-perbedaan ini menimbulkan pertanyaan mendalam mengenai kebijakan masing-masing negara dalam menanggulangi kejahatan siber yang semakin kompleks dan meningkat pasca-pandemi.

Melalui studi kasus kedua negara ini, jurnal ini memiliki tujuan untuk meneliti, menganalisis, dan membandingkan strategi AS dan Tiongkok dalam menghadapi kejahatan siber pasca-pandemi COVID-19, serta meninjau bagaimana kebijakan lokal mereka menunjukkan strategi politik luar negeri mereka di ranah siber. Fokus penelitian ini meliputi kebijakan, aktor-aktor yang terlibat, bentuk kerja sama internasional serta tantangan yang dihadapi oleh masing-masing negara dalam menjaga keamanan siber mereka. Melalui penelitian ini, diharapkan dapat memberikan dan memperoleh pemahaman yang lebih mendalam mengenai kebijakan dan

implikasi strategis dari masing-masing strategi dalam menghadapi kejahatan siber yang bersifat lintas batas.

KAJIAN TEORITIS

a. Teori Keamanan non-Tradisional

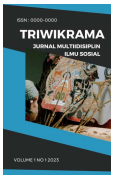
Teori keamanan non-tradisional diciptakan sebagai respons terhadap keterbatasan paradigma keamanan tradisional yang selama ini selalu berfokus pada ruang lingkup militer dan negara yang dimana kedua hal ini menjadi satu-satunya aktor utama. Pendekatan tradisional lebih suka mengenali keamanan hanya pada konteks pertahanan dari serangan bersifat fisik seperti serangan bersenjata atau konflik antarnegara. Namun pada realitanya, global menjadi semakin kompleks dan dinamis, sehingga mengharuskan adanya strategi yang lebih terbuka dan menyeluruh. Dalam hal ini, teori keamanan non-tradisional memperluas cakupan pengertian mengenai keamanan dengan mencantumkan berbagai macam ancaman kontemporer yang tidak bersifat militer, seperti terorisme, perubahan iklim, krisis kesehatan global, perdagangan manusia, serta kejahatan siber. Teori ini menekankan akan pentingnya konsep keamanan manusia atau *human security*, yang memprioritaskan perlindungan terhadap aspek-aspek mendasar dalam kehidupan masyarakat, seperti hak asasi manusia, ekonomi, kesehatan, dan Lingkungan. Dalam artian lain, keamanan tidak hanya diukur berdasarkan kemampuan pertahanan suatu negara, tetapi juga dilihat dari sejauh mana negara tersebut mampu untuk menjamin kelangsungan hidup, kesejahteraan, dan martabat masyarakatnya dalam menyikapi berbagai risiko non-militer.

Dalam penelitian Firmansyah (2020), ditekankan bahwa saat ini, isu-isu keamanan non-tradisional termasuk salah satu perhatian utama dalam kajian hubungan internasional, khususnya karena saat ini berbagai macam negara semakin saling terhubung, rumit, dan rawan terhadap ancaman tanpa batas seperti kejahatan siber atau serangan digital yang saat ini telah menjadi ancaman tingkat tinggi. Serangan semacam ini bisa saja menjatuhkan infrastruktur penting seperti sistem layanan kesehatan, jaringan perbankan, transportasi, sektor pertahanan, hingga sektor keamanan negara. Dampak yang ditimbulkan tidak hanya bersifat teknis, melainkan bisa juga menjadikan rasa kepercayaan masyarakat terhadap institusi negara menjadi menurun. Selain itu hal ini juga dapat mengganggu keseimbangan nasional secara komprehensif.

Salah satu artikel yang dipublikasikan oleh *IP Defense Forum* (2020) menyebutkan bahwa kejahatan siber merupakan bentuk ancaman yang bersifat non-fisik, namun memiliki kemampuan untuk menimbulkan kerusakan yang sangat besar. Di saat konflik bersenjata atau konflik militer dapat dilihat secara fisik, serangan siber biasanya tidak dapat dikenali secara langsung dan dapat terjadi dalam skala besar serta bersamaan. Maka dari itu, berbagai negara yang ada di dunia saat ini diharuskan untuk menciptakan strategi keamanan yang lebih adaptif dan responsif terhadap jenis ancaman seperti ini. Namun, strategi itu dituntut tidak hanya melibatkan institusi negara dan militer, tetapi juga membutuhkan kerja sama lintas sektor, seperti kerja sama internasional, kerja sama dengan sektor swasta, serta keikutsertaan yang aktif dari masyarakat lokal.

b. Teori Kejahatan Transnasional

Kejahatan transnasional adalah bentuk aksi kriminal yang memiliki dampak lintas batas negara dan melibatkan jaringan kejahatan internasional. Bersamaan dengan majunya teknologi informasi, bentuk kejahatan ini semakin meningkat dan rumit (Andi, 2023). Kejahatan transnasional tidak hanya meliputi perdagangan manusia, narkotika, dan senjata ilegal, tetapi juga menyebar ke lingkup kejahatan siber. Dalam dunia digital, para pelaku kejahatan siber



dapat melakukan aksinya dari berbagai juru dunia dan menyerang targetnya dari negara mana saja tanpa harus hadir secara fisik atau *face-to-face*. Hal ini menyebabkan sulitnya penegakan hukum dan memperlebar tantangan otoritas hukum antarnegara. Kejahatan siber yang dikenali sebagai bentuk baru dari kejahatan lintas negara mengharuskan adanya tanggapan dari negara-negara yang terkoordinasi. Ancaman ini menjadi contoh nyata akan kejahatan transnasional bersifat siber karena cara kerjanya yang dilakukan individu maupun kelompok dari suatu negara yang menargetkan negara lain untuk menyebarkan *malware*, melakukan pencurian informasi, atau menjatuhkan sistem digital pemerintahan.

Menurut Andi (2023), kejahatan transnasional siber tidak dapat ditangani oleh satu pihak saja, melainkan harus melibatkan berbagai negara. Negara-negara harus memperkuat kerja sama internasional dan diplomasi keamanan untuk membentuk tanggapan bersama untuk menghadapi ancaman ini. Strategi yang efektif harus melibatkan koordinasi antar lembaga penegak hukum, badan intelijen, organisasi internasional, hingga sektor swasta. Melalui berbagai kerja sama lintas negara dan lintas sektor Sistem keamanan global yang kuat dan adaptif dapat dibentuk untuk menanggulangi kejahatan transnasional di era digital.

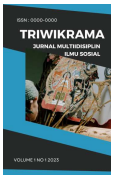
c. Teori Tata Kelola Keamanan Siber

Tata kelola keamanan siber mengacu pada penyusunan kebijakan dan sistem pengelolaan yang mendalam untuk memproteksi infrastruktur digital suatu negara. Strategi ini tidak hanya mengharuskan penggunaan teknologi yang canggih, tetapi juga mengharuskan perencanaan, pelaksanaan, pemantauan, dan evaluasi kebijakan keamanan informasi secara sistematis. Tata kelola keamanan siber meliputi regulasi, pembagian tanggung jawab antar lembaga, pelatihan sumber daya manusia, penerapan prinsip transparansi, serta akuntabilitas dalam menghadapi ancaman siber, baik dari dalam negeri maupun luar negeri.

Menurut laporan *DataGuard* (2023), tata kelola keamanan siber merupakan seperangkat sistem organisasi dan kebijakan yang dibentuk untuk mengurangi risiko serta menjaga keamanan informasi secara strategis. Tata kelola yang efektif ditekankan untuk bersifat terbuka, melibatkan koordinasi antara Pemerintah, sektor swasta, dan masyarakat lokal. Hal ini bertujuan untuk menciptakan sistem lingkungan keamanan digital yang kuat dan Tangguh. Negara yang memiliki tata kelola kuat, tentunya akan menjadi lebih siap menanggapi serangan siber dengan cepat dan efisien. Sebagai contoh, AS melalui *National Cybersecurity Strategy* 2023 menegaskan bahwa pentingnya regulasi keamanan siber yang terkoordinasi dan berbasis kerja sama. Strategi ini mencerminkan bahwa keamanan siber bukan sekedar isu teknis, melainkan juga bagian integral dari kebijakan nasional dan diplomasi internasional, khususnya dalam konteks menanggulangi kejahatan siber yang melibatkan aktor negara asing. Maka dari itu, integrasi keamanan siber ke dalam sistem pemerintahan dan kerangka hubungan internasional menjadi sangat penting dalam mempertahankan kedaulatan digital negara.

METODE PENELITIAN

Penelitian ini akan menggunakan metode kualitatif dengan pendekatan studi kasus. Data akan dikumpulkan melalui studi literatur, dan analisis dokumen. Studi literatur akan dilakukan untuk mengumpulkan informasi mengenai keamanan siber, analisis strategi Amerika Serikat dan Tiongkok, serta isu-isu terkait. Analisis dokumen akan dilakukan terhadap peraturan perundang-undangan, laporan penelitian, dan dokumen resmi lainnya.



HASIL DAN PEMBAHASAN

A. Strategi Amerika Serikat dalam Menanggulangi Kejahatan Siber Pasca-Pandemi

Saat terjadinya pandemi COVID-19, AS menghadapi kenaikan yang signifikan dalam kasus kejahatan siber. Berdasarkan laporan dan data dari FBI pada tahun 2020, AS mengalami kerugian hingga lebih dari $4 miliar akibat kejahatan siber. Setelah melakukan peninjauan, target utama dari para pelaku kejahatan siber ini adalah sektor-sektor penting seperti layanan kesehatan (*U.S. Department of State*, 2023). Seiring dengan hal ini, jumlah korban kejahatan siber juga melonjak drastis menjadi sebesar 69% jika dibandingkan dengan tahun sebelumnya. Ancaman ini memicu pemerintah AS untuk membentuk strategi keamanan siber yang lebih menyeluruh. Sehingga pada Maret 2023, Presiden AS saat itu, yaitu Biden, meluncurkan *National Cybersecurity Strategy* (NCS), yang menyoroti pentingnya kerja sama antara sektor publik dan swasta serta penyesuaian tanggung jawab dalam menjaga keamanan ruang siber.

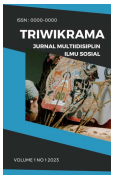
1) Kebijakan Nasional Utama dan Peran Kelembagaan Nasional

AS membentuk kebijakan dalam dokumen strategis yang menjadi panduan dan acuan dalam menanggulangi ancaman siber, yaitu *National Cybersecurity Strategy* (NCS) 2023. Strategi ini memodifikasi strategi nasional dengan menekankan pada pentingnya tanggung jawab yang menyeluruh dan kolaboratif antara pemerintah, sektor swasta, dan masyarakat lokal dalam menanggulangi ancaman kejahatan siber yang semakin kompleks pasca-pandemi. NCS menegaskan pembaruan dan peningkatan sistem pertahanan nasional dengan cara mengintegrasikan prinsip *Zero Trust Architecture*[3], yang bertujuan untuk memperketat kontrol akses dan mengurangi risiko dari dalam maupun luar sistem. Di samping itu, NCS juga menjadikan sektor swasta sebagai mitra utama mereka dalam menghadapi kejahatan siber, melalui penguatan prosedur berbagai informasi dan pelaporan kejadian secara tepat dan terbuka. NCS juga menciptakan fokus baru pada perlindungan infrastruktur kritikal, terlebih pada sistem yang mengalami tingkat kerentanan tinggi selama masa *Work from Home* (WFH) atau kerja dari rumah dan digitalisasi yang marak selama pandemi COVID-19. Maka dari itu, sebagai usaha dalam menghadapi peningkatan serangan *ransomware* dan eksploitasi sistem IT, NCS meningkatkan pengembangan teknologi deteksi dini dan respons cepat yang terhubung antara lembaga pemerintah dengan sektor swasta. Dalam aspek kerja sama, NCS tergolong sebagai strategi yang membuka peluang kerja sama internasional untuk melacak dan menindak pelaku kejahatan siber, serta menyesuaikan kebijakan agar tetap adaptif terhadap perkembangan teknologi baru yang dimana teknologi ini sering kali digunakan oleh pelaku kejahatan siber. Dengan demikian, NCS yang didasari oleh prinsip kerja sama multi-sektor dan inovasi teknologi mencerminkan tindakan AS yang lebih cepat tanggap dan adaptif ketika menanggulangi kejahatan siber yang mengalami pertumbuhan pesat pasca-pandemi.

Seiring dengan kebijakan dalam NCS 2023, AS juga mengandalkan peran aktif berbagai lembaga negara yang memiliki tugas khusus pada bidang penegakan hukum dan keamanan siber, sebagai upaya dalam menanggulangi kejahatan siber. Lembaga negara yang terlibat antara lain adalah, *Department of Justice* (Departemen Kehakiman), *Federal Bureau of Investigation* (FBI), dan *Cybersecurity and Infrastructure Security Agency* (CISA), dimana lembaga-lembaga ini berada di garis terdepan dalam menangani ancaman siber.

Departemen Kehakiman dimandatkan untuk menuntut para pelaku kejahatan siber, termasuk kasus yang bersifat lintas negara dengan melakukan kolaborasi internasional. Mereka membentuk unit khusus seperti *Computer Crime and Intellectual Property Section* (CCIPS) yang

[3] *Zero Trust Architecture* (ZTA) merupakan sebuah konsep keamanan jaringan yang tidak memiliki perangkat, pengguna, bahkan sistem yang otomatis dipercaya, baik dalam maupun luar perimeter jaringan.



berfokus pada investigasi teknis kejahatan siber, pengembangan kebijakan, dan pelatihan petugas penegak hukum. Unit ini bertujuan untuk mengantisipasi, mengusut, dan mengajukan tuntutan kepada para pelaku kejahatan siber dengan berkolaborasi bersama lembaga pemerintah lainnya, sektor swasta, institusi akademik, dan mitra luar negeri (U.*S. Department of Justice*, n.d.).

Di sisi lain, di bawah Departemen Kehakiman, terdapat FBI yang memiliki peran sebagai lembaga investigasi utama di AS. FBI memiliki unit khusus yang disebut *Cyber Division*, dengan tugas untuk mengurus berbagai kasus seperti *ransomware*, kejahatan digital yang melibatkan aktor negara lain, dan serangan siber terhadap infrastruktur kritikal. *Cyber Division* berada pada baris terdepan jika menyangkut upaya AS untuk menginvestigasi dan mengadili kejahatan siber, termasuk terorisme berbasis siber, spionase, intrusi *computer*, dan penipuan siber berskala besar. Selain itu, FBI juga memiliki platform bernama *Internet Crime Complaint Center* (IC3) sebagai tempat pengumpulan laporan masyarakat serta penganalisis tren serangan siber secara nasional (Tempo.co, 2023). Sementara itu, CISA merupakan salah satu bagian dari *Department of Homeland Security* (DHS) yang cenderung memiliki fokus utama pada pencegahan dan peningkatan sistem pertahanan siber. CISA dimandatkan untuk menelaah, mengorganisir, dan meminimalisir risiko terhadap infrastruktur siber dan fisik yang selalu diandalkan oleh masyarakat lokal AS (*Cybersecurity and Infrastructure Security Agency*, 2024).

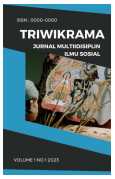
2) Undang-Undang terkait Kejahatan Siber

Upaya AS dalam menangani kejahatan siber didasari oleh Undang-Undang (UU) penting yang menjadi landasan hukum dalam penegakan serta pencegahan tindak kejahatan siber. Salah satu UU terkait adalah *Computer Fraud and Abuse Act* (CFAA), yang telah menjadi landasan utama dalam penindakan berbagai kasus kejahatan siber semenjak diresmikan pada tahun 1986. UU ini pada mulainya dirancang untuk mengatasi akses ilegal pada komputer milik pemerintah dan lembaga keuangan. Akan tetapi, seiring dengan pesatnya perkembangan teknologi, CFAA memperluas cakupannya hingga mencakup pelanggaran data, peretasan, penipuan secara *online*, hingga serangan *malware* dan *ransomware*. Dalam konteks pandemi, UU ini diberlakukan untuk menindak pelaku kejahatan siber yang mengambil kesempatan melalui ketergantungan masyarakat terhadap layanan digital, seperti penipuan berbasis COVID-19 yang sering terjadi selama masa *lockdown*.

3) Kerja Sama Internasional

Selain daripada kebijakan dan regulasi domestik, dalam menghadapi ancaman kejahatan siber khususnya pasca-pandemi, AS juga menyoroti pentingnya kolaborasi internasional sebagai bagian dari strategi efektif yang disinggung dalam *National Cybersecurity Strategy* 2023. Kejahatan siber memiliki sifat transnasional, sehingga kerja sama internasional merupakan fondasi utama bagi AS untuk menghadapinya, terlebih lagi pada masa pasca-pandemi yang dimana ancaman kejahatan siber semakin meningkat dan canggih. Cara kerjanya yang melintasi batas negara, menggunakan yuridiksi yang berbeda, dan menargetkan siapa saja membuat upaya penegakan hukum dan pencegahan sangat membutuhkan koordinasi global.

AS aktif terlibat dalam forum-forum internasional yang berfokus pada tata kelola siber dan norma-norma negara di ranah digital. AS menunjukkan dukungannya terhadap upaya-upaya internasional dalam menetapkan norma-norma tanggung jawab negara di dunia siber melalui keikutsertaannya dalam dua forum penting PBB, yaitu *Open-Ended Working Group* (OEWG) dan *Group of Governmental Experts* (CGE). Dalam OEWG, AS menggerakkan mekanisme seperti direktori "*Point of Contact*" secara global, yang dimana hal ini meliputi fungsi diplomasi, cara kerja, dan kebijakan untuk memantau juga merespons fenomena siber dengan cepat. Sedangkan dalam CGE, AS mendorong perkembangan norma tanggung jawab negara-negara di



ranah digital, seperti pencegahan serangan yang menargetkan infrastruktur sipil dan menghormati hukum internasional.

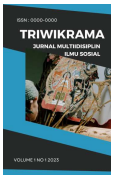
Selain keaktifannya di PBB, AS juga memainkan peran aktif dalam G7 dan G20, dimana isu keamanan siber sering kali menjadi agenda penting. AS memiliki peran yang penting, dimana AS menerapkan prinsip tata kelola siber dan mendukung program *Counter Ransomware Initiative* yang berfokus pada akuntabilitas dan pencegahan terjadinya serangan *ransomware* pada institusi kesehatan. Selain itu, AS juga mengakui penerapan hukum internasional di dunia digital, melarang pencurian hak kekayaan intelektual lintas negara, serta mendorong negara-negara lain untuk meratifikasi Konvensi Budapest yang menjadi standar hukum internasional.

AS menjalin kerja sama bilateral bersama dengan Jepang, Korea Selatan, Australia, dan Uni Eropa melalui perjanjian yang meliputi pertukaran intelijen pelatihan penegak hukum, dan pengembangan kemampuan deteksi serta tanggapan terhadap fenomena siber. Sedangkan secara multilateral, AS memberikan kontribusi dalam berbagai kerangka kerja internasional, yang dimana salah satunya adalah Konvensi Budapest mengenai Kejahatan Siber. AS telah meratifikasi konvensi ini semenjak tahun 2006 dan menjadikannya sebagai acuan hukum internasional dalam menanggulangi kejahatan siber lintas yuridiksi. Konvensi Budapest mengatur dan menetapkan harmonisasi hukum domestik, menyediakan mekanisme bantuan hukum timbal balik, serta jaringan kontak yang beroperasi setiap hari tanpa henti untuk mempercepat pertukaran bukti elektronik antarnegara. Di samping Konvensi Budapest, AS juga mendukung inisiasi multilateral yang baru seperti *Counter Ransomware Initiative* yang bertujuan untuk menghubungkan 50 negara lebih demi membanguni kebijakan tanggap *ransomware* secara bersama-sama.

Pada dasarnya, strategi AS berfokus pada bentuk keamanan siber yang berlandaskan kerja sama antara sektor publik dan swasta, transparansi, dan juga tanggung jawab bersama-sama. Strategi ini telah cukup dijelaskan pada *National Cybersecurity Strategy* 2023 yang menekankan keterlibatan industri, peningkatan ketahanan infrastruktur digital, dan penguatan kerja sama internasional yang didasari oleh nilai demokratis. Kemudian mengenai strategi multilateral, AS menjadikan forum internasional seperti G7, G20, PBB, dan Konvensi Budapest sebagai pilar utama dalam menanggulangi kejahatan siber pasca-pandemi.

B. Strategi Tiongkok dalam Menanggulangi *Cyber Crime* Pasca-Pandemi

Semasa pandemi COVID-19, Tiongkok juga dihadapkan dengan ancaman dan kasus kejahatan siber yang meningkat pesat. Adanya peningkatan penggunaan digital selama pandemi, baik di bidang pendidikan, perdagangan, bahkan pemerintahan, mengakibatkan ruang siber Tiongkok menjadi target utama para pelaku kejahatan siber, baik lokal maupun non-lokal. *Qihoo 360 Technology* pada tahun 2021 melaporkan bahwa serangan institusi pemerintah dan infrastruktur vital di Tiongkok melonjak secara signifikan. Kenaikannya mencapai angka 60% jika dibandingkan dengan tahun sebelumnya. Di samping itu, terjadinya pandemi juga mengakibatkan maraknya penyebaran *hoax* dan penipuan daring menyangkut kesehatan, vaksin, serta bantuan sosial. Untuk menanggapi hal ini, pemerintah Tiongkok dengan tanggap merumuskan kebijakan nasional dan penguatan kerangka hukum serta kelembagaan yang berfokus pada kejahatan siber. Strategi yang dilakukan oleh pemerintah Tiongkok diawasi dengan ketat dan dijalankan melalui reformasi kelembagaan, serta diplomasi digital yang didasari oleh prinsip "*cyber sovereignty*" agar negara tetap memiliki kontrol yang baik terhadap informasi dan infrastruktur digital.



1) Kebijakan Nasional Utama dan Peran Kelembagaan Nasional

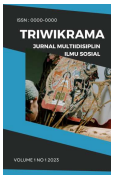
Pasca-pandemi, Tiongkok mulai meningkatkan kekuatan strategi negara terhadap keamanan siber melalui kebijakan nasional yang terpusat dan terkoordinasi. Strategi ini berlandaskan prinsip "*cyber sovereignty*" atau kedaulatan negara yang bersifat komprehensif atas ruang siber, seperti pengontrolan data, infrastruktur, dan dinamika internet. Salah satu kebijakan nasional utama Tiongkok adalah *China's Cybersecurity Strategy* tahun 2021. Kebijakan ini dibentuk oleh *Cyberspace Administration of China* (CAC). Strategi ini difokuskan untuk mengontrol data, melindungi infrastruktur penting, penguatan sistem manajemen risiko digital, hingga peningkatan kapabilitas negara dalam mendeteksi dan menangani ancaman siber secara mandiri (Lee, 2022). Dalam konteks penanganan kejahatan siber pasca-pandemi, strategi ini menjadi sangat penting karena pesatnya kenaikan aktivitas digital selama pandemi mengakibatkan tingginya eksposur terhadap serangan siber. Kebijakan ini juga menyoroti pentingnya "*integrated cybersecurity governance*", yang merupakan koordinasi lintas sektor dan institusi dengan tujuan untuk menyusun sistem pertahanan siber yang menyeluruh. Pemerintah Tiongkok juga memajukan ketahanan teknologi dengan mengembangkan ekosistem keamanan siber nasional, seperti bidang semikonduktor, enkripsi, dan kecerdasan buatan.

Di samping itu, lembaga CAC yang telah disebutkan sebelumnya, merupakan peran utama dalam kelembagaan nasional Tiongkok di bawah naungan Komite Sentral Partai Komunis Tiongkok dengan tanggung jawab untuk menyusun dan merancang kebijakan nasional, melakukan pengawasan terhadap pelaksanaan UU keamanan siber, hingga pengoordinasian operasi lintas pemerintah mengenai kejahatan siber (Lee, 2022). Maka dapat disimpulkan bahwa CAC, merupakan peran sentral dalam merumuskan dan melaksanakan kebijakan keamanan siber. CAC juga bertanggung jawab untuk menyeimbangkan kebijakan antar lembaga, terkhusus ketika kejahatan digital melonjak di masa pandemi yang menjadi masa pergeseran aktivitas ke ruang siber. CAC menjadi acuan dalam menanggapi fenomena siber yang melibatkan tindak kriminal seperti pencurian data, serangan terhadap sistem layanan kesehatan dan penipuan finansial daring yang terus meningkat pada saat pandemi. Selain itu, ada pun lembaga lainnya seperti *Ministry of Public Security* (MPS) atau Kementerian Keamanan Publik yang memiliki peran krusial dalam menginvestigasi kasus kejahatan siber yang biasanya berupa penipuan dan pencurian data, menegakkan hukum, hingga mengadili pelaku kejahatan siber. Dalam hal ini, peran kelembagaan merupakan elemen penting yang perlu dikuatkan dan dikoordinasikan dalam upaya negara Tiongkok untuk menanggulangi ancaman siber khususnya pasca-pandemi, dimana kejahatan siber yang bersifat dinamis mengalami lonjakan yang sangat pesat. Lembaga negara harus bertindak dengan efektif dan selalu siap siaga untuk menghadapi kasus-kasus kejahatan siber serta meningkatkan pertahanan digital Tiongkok pasca-pandemi.

Selain itu, Tiongkok juga mengikutsertakan sektor swasta dalam upayanya untuk memperkuat keamanan siber di Tiongkok. Dalam kampanye tahunan "*Cybersecurity Week*" yang diadakan semenjak tahun 2014, Tiongkok mendukung Perusahaan teknologi seperti Huawei, Tencent, dan Alibaba untuk meningkatkan sistem keamanan serta membagikan data kasus yang terjadi kepada pemerintah Tiongkok untuk deteksi dini ancaman.

2) Undang-Undang terkait Kejahatan Siber

Mengenai UU yang berkaitan dengan kejahatan siber, pemerintah Tiongkok telah menyusun kerangka hukum yang menyeluruh dalam mengatur keamanan siber dan menghadapi berbagai tindak kejahatan siber. Landasan dasar regulasi ini adalah *Cybersecurity Law* yang mulai diberlakukan pada tahun 2017. UU ini mengatur tentang kewajiban perlindungan data bagi penyedia layanan digital, penguatan pengawasan negara terhadap dinamika dan aktivitas siber, serta mengharuskan perusahaan lokal hingga asing untuk menyimpan data penting di



dalam negeri (*Standing Committee of the National People's Congress*, 2017). UU ini mendorong pentingnya audit keamanan yang dilakukan secara berkala serta pengendalian risiko terhadap sistem informasi penting nasional. *Cybersecurity Law* menjadi semakin relevan semenjak pasca-pandemi akibat meningkatnya tindak kriminal di ruang siber. Berbagai bentuk serangan dilakukan oleh para pelaku kejahatan siber seperti penipuan pembayaran elektronik serta serangan kepada institusi kesehatan dan pendidikan. Melalui UU ini, pemerintah Tiongkok menegaskan para penyedia layanan digital untuk memiliki sistem perlindungan siber yang kuat serta membuka akses untuk pemerintah bisa masuk dengan tujuan mengawasi, mencegah, dan menanggapi suatu fenomena siber yang dianggap mengancam kestabilan sosial dan ekonomi.

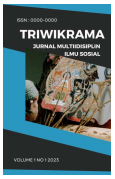
Di sisi lain, sebagai salah satu upaya dalam melakukan perluasan perlindungan data pribadi dan penindakan terhadap oknum yang menyalahgunakan data, pemerintah Tiongkok meresmikan regulasi *Data Security Law* dan *Personal Infromation Protection Law* (PIPL), yang dimana keduanya dibentuk pada tahun 2021. Kedua UU ini, membantu menguatkan hukuman terhadap pelaku kejahatan siber dan memperjelas tanggung jawab penyedia layanan digital dalam menjaga data pribadi pengguna. UU ini menjadi cukup krusial dalam menangani kasus kejahatan siber mengingat tingginya tingkat kenaikan kasus selama pandemi. Regulasi yang jelas dan menyeluruh tentunya sangat diperlukan untuk memberikan kejelasan hukum untuk meningkatkan kapabilitas negara dalam memberikan respons terhadap fenomena kejahatan siber. Maka dari itu, dengan adanya UU ini, pemerintah Tiongkok dalam membentuk sistem pertahanan digital tidak hanya berfokus pada pencegahan, tetapi juga untuk menegakkan hukum agar menjadi lebih kuat dan terorganisir.

3) Kerja Sama Internasional:

Pemerintah Tiongkok cukup menyadari bahwa kejahatan siber adalah tantangan sulit di kancah internasional yang tidak mudah untuk ditangani secara unilateral. Maka dari itu, pemerintah Tiongkok menjadi semakin aktif dalam memajukan kolaborasi secara internasional sebagai salah satu upaya untuk menangani kejahatan siber pasca-pandemi. Meningkatnya penggunaan digital akibat COVID-19 berdampingan dengan serangan siber yang juga meningkat, sehingga, kerja sama internasional menjadi elemen penting dalam pencegahan, pendeteksian, dan respons suatu negara terhadap kejahatan siber agar menjadi lebih kuat dan efektif.

Negara Tiongkok dapat dikatakan aktif terlibat dalam berbagai forum multilateral terkait keamanan siber, seperti *Shanghai Cooperation Organization* (SCO), BRICS, dan *ASEAN Regional Forum* (ARF). Terkait dengan SCO, pemerintah Tiongkok menekankan kolaborasi pertukaran informasi intelijen siber dan kenaikan kapasitas penegakan hukum siber yang dilakukan melalui latihan gabungan. SCO juga berperan untuk memfasilitasi penyusunan kerangka kerja kolektif dalam penanganan ancaman siber regional. Kemudian mengenai BRICS, pemerintah Tiongkok memanfaatkan forum ini untuk menekankan pembentukan *Working Group on Security in the Use of ICTs* dengan tujuan untuk menguatkan keyakinan dalam penggunaan teknologi informasi dan komunikasi, serta memperluas prinsip kedaulatan siber yang menjadi landasan tata kelola digital. Selain itu, forum lainnya yang diikut oleh Tiongkok adalah ARF sebagai platform untuk melaporkan kekhawatiran mengenai serangan siber lintas negara. ARF juga menekankan tentang pentingnya penguatan kerja sama teknis yang efektif dan kebijakan antarnegara Asia Tenggara.

Di samping forum internasional, pemerintah Tiongkok juga terbuka dengan kerja sama perjanjian bilateral dan multilateral bersama dengan negara dari seluruh penjuru dunia yang berlandaskan kerja sama keamanan informasi. Salah satu contoh kerja sama strategis dan efektif yang telah dilakukan adalah kerja sama dengan Rusia, yang dimana kedua negara ini menandatangani perjanjian kerja sama di bidang keamanan informasi meliputi pertukaran data



intelijen siber dan koordinasi kebijakan keamanan digital (Kremlin, 2021). Kerja sama ini mencerminkan strategi "blok" ketika menghadapi dominasi norma Barat dalam tata kelola siber global. Selain itu, pemerintah Tiongkok juga memperkuat kerja samanya dengan negara-negara berkembang seperti Afrika dan Asia Selatan. Bentuk kerja sama yang dilakukan adalah berupa bantuan teknis dalam pembangunan kapasitas siber dan pembuatan UU yang selaras dengan prinsip kedaulatan siber. Kerja sama ini juga membantu Tiongkok untuk memperluas keamanan digitalnya ke negara-negara mitra yang membutuhkan infrastruktur dan dukungan kebijakan siber.

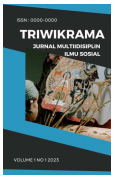
Maka dari itu, dapat disimpulkan bahwa Tiongkok memberlakukan strategi keamanan siber yang sifatnya terpusat dan dikendalikan oleh negara, tercipta dari adanya prinsip kedaulatan siber. Strategi ini telah tercantum dalam kebijakan utama nasional yang kemudian diperkuat oleh lembaga-lembaga nasional seperti CAC dan MPS. Selain itu, pemerintah Tiongkok juga menguatkan kerangka hukum siber domestik melalui mendorong kolaborasi internasional dengan ikut terlibat dalam forum-forum internasional seperti SCO, BRICS, dan ARF. Meskipun sering kali terdapat perbedaan ideologis dan institusional, Tiongkok dan mitranya tetap memandang bahwa keamanan siber merupakan isu strategis nasional yang berfokus pada keamanan teknis, geopolitik, diplomasi, dan pertahanan negara.

C. Perbandingan Strategi Amerika Serikat dan Tiongkok

Berdasarkan penjelasan mengenai strategi AS dan Tiongkok dalam menangani kejahatan siber pasca-pandemi di atas, dapat disimpulkan bahwa meskipun kedua negara tersebut memiliki sistem politik dan filosofi yang berbeda, tetapi AS dan Tiongkok mencerminkan beberapa persamaan dalam strategi penanganan kejahatan siber pasca-pandemi. AS dan Tiongkok mengakui bahwa kejahatan siber merupakan ancaman nasional yang serius, memperkuat kebijakan melalui strategi domestik, melindungi infrastruktur penting, dan melibatkan sektor swasta dalam penguatan sistem pertahanan digital. Di samping itu, ada pun perbedaan yang cukup mencolok, yaitu mengenai strategi tata kelola negara. AS condong kepada bentuk keterbukaan dan kolaborasi dengan berbagai pihak, ketika Tiongkok condong pada kedaulatan siber dan kontrol negara. Selain itu, struktur kelembagaan kedua negara ini pun juga menunjukkan sebuah perbedaan, dimana AS memiliki struktur kelembagaan yang bersifat desentralisasi dan terbuka dengan melibatkan lembaga seperti CISA, NSA, dan FBI, sedangkan Tiongkok menitik pusatkan kewenangannya pada lembaga seperti CAC yang langsung dinaungi oleh Partai Komunis. Kemudian dalam hal kerja sama internasional, AS turut aktif dalam mendorong standar global seperti Konvensi Budapest serta memperluas peluang kerja sama melalui G7 dan G20, sedangkan Tiongkok memanfaatkan kerja sama bilateral dan keikutsertaannya dalam forum lain seperti SCO dan BRICS yang berfokus pada prinsip non-intervensi.

Meskipun keduanya bersaing dalam hal dominasi norma global, tetapi keduanya tetap membuka ruang diplomasi dalam forum PBB seperti UN, CGE, dan OEWG. Dampak dari pandemi membuat digitalisasi global menjadi semakin kuat dan mendorong negara-negara untuk membanguni sistem keamanan siber yang lebih tangguh dan canggih. Upaya-upaya strategis yang diambil dan digunakan oleh kedua negara ini pun tidak hanya sebagai bentuk respons mereka terhadap kejahatan siber, tetapi sebagai bentuk penguatan posisi mereka dalam memperebutkan dominasi atas tata kelola ruang digital global di era pasca-pandemi.

Triwikrama: Jurnal Ilmu Sosial
Volume 9 No.2 Tahun 2025
E-ISSN: 2988-1986
Open Access:



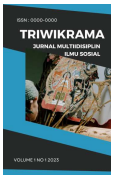
KESIMPULAN

Perkembangan teknologi informasi dan komunikasi telah menjadi pilar utama transformasi global di berbagai bidang seperti ekonomi, pendidikan, pemerintahan, bahkan kesehatan. Namun, berdampingan dengan meningkatnya ketergantungan terhadap teknologi digital, timbul sebuah ancaman baru yang sangat serius, yaitu kejahatan siber. Kejahatan siber menjadi semakin nyata semenjak masa pandemi COVID-19, yang dimana pada saat itu hampir seluruh kegiatan masyarakat beralih ke ruang digital. Masa peralihan ini membuat eksposur terhadap berbagai bentuk kejahatan siber kian meningkat, seperti *hoax*, pencurian data, penipuan daring, dan serangan *ransomware*. Dalam konteks ini, dua negara paling berpengaruh di dunia, yaitu AS dan Tiongkok memiliki peran penting dalam menunjukkan bagaimana mereka menanggapi tantangan tersebut, yang dalam studi ini dianalisis secara spesifik pasca-pandemi. AS sebagai negara dengan lingkungan digital yang cukup kompleks dan transparan, harus menghadapi kenaikan kasus kejahatan siber yang cukup tinggi selama pandemi. FBI pada tahun 2020 melaporkan bahwa kerugian yang dialami oleh AS akibat kejahatan siber mencapai hingga lebih dari 4 miliar dolar AS, dengan target sektor-sektor penting seperti layanan kesehatan dan pendidikan. Sadar akan urgensi situasi dan kondisi tersebut, pemerintah AS melalui dokumen strategis mereka, *National Cybersecurity Strategy* 2023, menyoroti terkait pembagian tanggung jawab antara sektor publik dan swasta, peningkatan ketahanan infrastruktur digital, serta reformasi kebijakan terhadap aktor utama di bidang teknologi. Kemudian peran lembaga seperti CISA, FBI, dan NSA juga menjadi sangat penting dalam melaksanakan tugas dan fungsinya. AS juga menganggap kerja sama internasional tidak kalah penting untuk menanggulangi kejahatan siber, dimana AS terlibat aktif dalam forum-forum di PBB dan kerja sama internasional lainnya.

Di sisi lain, Tiongkok memiliki strategi terpusat yang berlandaskan prinsip kedaulatan siber. Dalam dokumen strategi Tiongkok, yaitu *China's Cybersecurity Strategy* 2021, ditegaskan bahwa kedaulatan penuh atas ruang siber domestik itu sangat penting. Tiongkok mendorong perlindungan terhadap infrastruktur penting, pengelolaan data domestik, dan peningkatan kapasitas sumber daya manusia di bidang keamanan siber. Kebijakan ini dijalankan secara ketat oleh CAC dan MPS, yang merupakan dua lembaga utama dengan peran sebagai penyusun kebijakan, pengawas, dan penindak hukum atas pelaku kejahatan siber. Adapun kerangka hukum seperti *Cybersecurity Law* (2017), *Data Security* (2021), dan *Personal Information Protection Law* (2021) sebagai penunjang implementasi strategi ini dan secara kolektif memberikan kekuatan hukum dalam melakukan pengontrolan arus data, membatasi kegiatan praktik Perusahaan non-lokal, dan membuat standar perlindungan informasi pribadi. Tiongkok juga turut aktif terlibat dalam hal kerja sama internasional, terutama dengan negara-negara berkembang melalui BRICS dan SCO yang berfokus untuk memperluas pengaruh Tiongkok dalam tata kelola siber secara global.

Kedua negara ini sama-sama telah menyadari akan tingginya ancaman kejahatan siber pasca-pandemi dan telah membuat strategi domestik yang komprehensif bagi masing-masing negara. Namun, perbedaan yang cukup mencolok dari strategi keduanya adalah, AS condong mengutamakan keterbukaan, kerja sama internasional, dan tanggung jawab bersama, di saat Tiongkok condong mengutamakan kontrol negara, kedaulatan siber, dan regulasi ketat terhadap dinamika digital.

Secara keseluruhan, analisis ini menunjukkan bahwa strategi AS dan Tiongkok dalam menangani kejahatan siber pasca-pandemi tidak dapat dipisahkan dari konteks sistem politik dan dinamika kebijakan luar negeri masing-masing. Keduanya mencoba menghadapi tantangan dan ancaman yang sama dengan strategi yang berbeda, dimana AS dengan strateginya yang liberal dan institusionalis, di saat Tiongkok dengan strateginya yang *state-centric* dan



autoritarian. Namun, yang menjadi kesamaan disini adalah bahwa kejahatan siber merupakan tantangan bersama yang serius dan membutuhkan atensi khusus serta respons yang tanggap dan efektif. Kerja sama bersama negara-negara lain pun turut diperlukan dalam menanggulangi isu ini. Dalam hal ini, AS dan Tiongkok bisa saja menjadi contoh bagi negara-negara lain untuk merumuskan kebijakan yang sesuai dengan kondisi domestik masing-masing, sekaligus aktif dalam memperkuat tata kelola global ruang siber yang inklusif, adil, dan aman bagi seluruh penggunanya.

DAFTAR PUSTAKA

Astra Security. (n.d.). *Cybercrime statistics*. GetAstra. Retrieved from https://www.getastra.com/blog/security-audit/cyber-crime-statistics

Bitsight. (n.d.). *Cybersecurity governance*. Retrieved from https://www.bitsight.com/glossary/cybersecurity-governance

Budianto, A. (2023). *Strategi keamanan cyber Amerika Serikat* [PDF]. Retrieved from https://www.researchgate.net/publication/361929090_STRATEGI_KEAMANAN_CYBER_AMERIKA_SERIKAT

Chinalawtranslate. (2016). *Cybersecurity Law of the People's Republic of China*. Retrieved from https://www.chinalawtranslate.com/en/2016-cybersecurity-law/

CNN Indonesia. (2022). *Serangan siber di Indonesia tembus 1,6 miliar sepanjang 2021*. Retrieved from https://www.cnnindonesia.com/teknologi/20220125111550-192-749559/serangan-siber-di-indonesia-tembus-16-miliar-sepanjang-2021

CNBC Indonesia. (2021). *Begini cerita lengkap hacker serang pipa BBM terbesar AS*. Retrieved from https://www.cnbcindonesia.com/market/20210512081206-17-245188/begini-cerita-lengkap-hacker-serang-pipa-bbm-terbesar-as

Cyber Defense Review. (2024). Iasiello, E. J. *Strategic Competition and Cybercrime: How the PRC's Approach Challenges the West*, 9(3), Fall 2024. Retrieved from https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Iasiello_CDRV9N3-Fall-2024.pdf

Cyberthreat.id. (n.d.). *AS dan Sekutunya Salahkan China di Balik Peretasan Microsoft Exchange Server*. Retrieved from https://cyberthreat.id/read/12107/AS-dan-Sekutunya-Salahkan-China-di-Balik-Peretasan-Microsoft-Exchange-Server

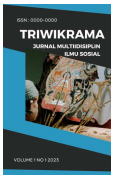
Dataguard. (n.d.). *Cyber security governance*. Retrieved from https://www.dataguard.com/cyber-security/governance

Diplomacy.edu. (n.d.). *What's new with cybersecurity negotiations (OEWG 2021-2025): Second substantive session*. Retrieved from https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-second-substantive-session

Eurojust. (n.d.). *The Budapest Convention on Cybercrime and Cross-border Access to Electronic Evidence*. Retrieved from https://www.eurojust.europa.eu/publication/budapest-convention-cybercrime-and-cross-border-access-electronic-evidence

G7 Italy. (2024). *G7 Foreign Ministers' Meeting Communique: Addressing global challenges and fostering partnerships*. Retrieved from https://g7g20-documents.org/database/document/2024-g7-italy-ministerial-meetings-foreign-ministers-ministers-language-foreign-ministers-meeting-communique-addressing-global-challenges-fostering-partnerships

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19



IP Defense Forum. (2022, December). *Melawan Ancaman Keamanan Nontradisional*. Retrieved from https://ipdefenseforum.com/id/2022/12/melawan-ancaman-keamanan-nontradisional/

Kemenpora RI. (2025). *Keamanan Siber* [PDF]. CSIRT Kemenpora. Retrieved from https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

Lee, K. (2022). *Cyberspace Governance and China's Role* [PDF]. Ifri. Retrieved from https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/lee_cyberspace_governance_china_2022.pdf

Legal Wires. (n.d.). *Understanding cyber laws in the globalised world: From the Budapest Treaty to the UN*. Retrieved from https://legal-wires.com/columns/understanding-cyber-laws-in-the-globalised-world-from-the-budapest-treaty-to-the-un

Media Indonesia. (2023). *Ini Pengertian dan Perbedaan Malware, Ransomware, Social Engineering, dan Ancaman Siber Lainnya*. Retrieved from https://mediaindonesia.com/teknologi/581649/ini-pengertian-dan-perbedaan-malware-ransomware-social-engineering-dan-ancaman-siber-lainnya

Microsoft. (2021). *HAFNIUM targeting Exchange Servers*. Microsoft Security Blog. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

MOFA Japan. (2024). *Diplomatic Bluebook 2024*. Retrieved from https://www.mofa.go.jp/policy/other/bluebook/2024/en_html/chapter3/c030103.html

National Security Council. (2023). *National Cybersecurity Strategy*. White House Archives. Retrieved from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Proxsis IT. (n.d.). *Mengenal Zero Trust Architecture: Pengertian, Prinsip dan Cara Penerapannya di Dunia Modern*. Retrieved from https://it.proxsisgroup.com/mengenal-zero-trust-architecture-pengertian-prinsip-dan-cara-penerapannya-di-dunia-modern/

Tempo.co. (2023). *Sejarah FBI dan Apa Saja Tugas-Tugasnya*. Retrieved from https://www.tempo.co/internasional/sejarah-fbi-dan-apa-saja-tugas-tugasnya-67172

Third Way. (n.d.). *U.S. Global Cybercrime Cooperation: A Brief Explainer*. Retrieved from https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer

U.S. Department of Homeland Security. (n.d.). *Cybersecurity*. Retrieved from https://www.dhs.gov/topics/cybersecurity

U.S. Department of Justice. (n.d.). *About CCIPS*. Retrieved from https://www.justice.gov/criminal/criminal-ccips/about-ccips

U.S. Department of State. (2023). *Cybercrime*. Retrieved from https://www.state.gov/cybercrime/

Universitas Brawijaya. (n.d.). *Bab II - Tinjauan Teoritis dan Kerangka Konseptual* [PDF]. Retrieved from https://repository.ub.ac.id/id/eprint/111833/2/BAB_II.pdf

Universitas Hasanuddin. (2023). *Bab 1-3 Tesis B012181076* [PDF]. Retrieved from https://repository.unhas.ac.id/id/eprint/27035/1/B012181076_tesis_11-05-2023%20bab%201-3.pdf

Universitas Mulawarman. (n.d.). *Jurnal Hubungan Internasional Interdependen*. Retrieved from https://e-journals.unmul.ac.id/index.php/JHII/article/view/1891/1435

Springer. (n.d.). *Cybersecurity*. In *Encyclopedia of Big Data*. Retrieved from https://link.springer.com/referenceworkentry/10.1007/978-3-319-74336-3_257-1