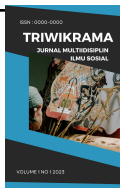
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6, 2025
E-ISSN: 2988-1986
Open Access:



Implikasi APT10 dan Politik Spionase Siber Tiongkok terhadap Keamanan Nasional di Era Otoritarianisme Digital

Andi Audiya Aprilia[1], Agussalim Burhanuddin[2]
[1, 2]Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO

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

odyaprilia12@gmail.com
agus.unhas@gmail.com

This is an open access article under the CC BY-SA license.
Copyright © 2023 by Author. Published by Universitas Pendidikan Ganesha.

A B S T R A K

Artikel ini menganalisis bagaimana kelompok APT 10 yang dituduh disponsori oleh pemerintah China telah menggunakan spionase siber untuk menggambarkan pendekatan Republik Rakyat China terhadap keamanan nasional dalam konteks otoritarianisme digital. Studi ini menggunakan teori sekuritisasi dari Sekolah Kopenhagen, mengintegrasikan konsep otoritarianisme digital dan penyensoran virtual yang memberikan bukti bahwa strategi siber China tidak hanya bersifat teknis, tetapi lebih kepada politik dan ideologis. Artikel ini menggunakan tipe operasi APT 10 dan *Cloud Hopper* sebagai studi kasus untuk berargumen bagaimana dominasi siber digunakan untuk memperkuat kontrol domestik dan memperluas pengaruh internasional melalui apa yang disebut sebagai diplomasi digital Secara metodologis, penelitian ini dilakukan dengan menggunakan analisis kualitatif deskriptif dari literatur, laporan investigasi keamanan siber, dan dokumen kebijakan. Temuan menunjukkan bahwa sekuritisasi siber China berkontribusi pada sistematisasi kontrol otoriter, yang muncul dengan konsekuensi serius bagi demokrasi dan menggeser keseimbangan kekuatan dalam tatanan global keamanan. Ini dibentuk menjadi dinamika baru dari hegemoni hak asasi manusia, kebebasan berbicara, dan pemerintahan transnasional di internet.

Kata Kunci: APT10; Spionase siber; Keamanan Nasional; Otoritarianisme Digital; Tiongkok.

A B S T R A C T

This article analyzes how the APT 10 group accused of being sponsored by the Chinese government has used cyber espionage to illustrate the People's Republic of China's approach to national security in the context of digital authoritarianism. The study uses securitization theory from the Copenhagen School, integrating the concepts of digital authoritarianism and virtual censorship that provide evidence that China's cyber strategy is not just technical, but rather political and ideological. This article uses the APT 10 and Cloud Hopper operation types as case studies to argue how cyber dominance is used to strengthen domestic control and expand international influence through so-called digital diplomacy. Methodologically, the research was conducted using descriptive qualitative analysis of literature, cybersecurity investigation reports, and policy documents. The findings show that China's cyber securitization contributes to the systematization of authoritarian control, which comes with serious consequences for democracy and shifts the balance of power in the security global order. It is shaping up to be a new dynamic of the hegemony of human rights, free speech, and transnational governance on the internet.

Keywords: *APT10; Cyber Espionage; National Security; Digital Authoritarianism; Tiongkok.*

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

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:

1. PENDAHULUAN

Ancaman terhadap keamanan nasional tidak lagi terbatas pada superioritas militer konvensional dan telah merambah kapabilitasnya dalam ranah siber. Keamanan siber kini menjadi salah satu isu utama dalam agenda keamanan nasional sehingga banyak negara-negara adidaya berusaha memanfaatkan kemajuan teknologi untuk menjalankan operasi intelijen, termasuk spionase, sebagai bagian dari strategi geopolitik global. Salah satu aktor utama dalam dinamika ini yaitu Tiongkok yang banyak melebarkan pengaruhnya ke berbagai kelompok peretas untuk melakukan spionase di tingkat global. APT10 adalah sebuah grup peretas (*hacker group*) yang sangat terkenal saat ini.

APT10 (*Advanced Persistent Threat 10*) atau yang juga dikenal sebagai *StonePand*a dan *MenuPass*, merupakan salah satu kelompok peretas paling terkenal yang diduga kuat memiliki afiliasi dengan pemerintah Tiongkok (Anggita, 2023). Aktif beroperasi sejak tahun 2006, APT10 telah melakukan kampanye ekstensif yang menargetkan berbagai sektor dan institusi penting di seluruh dunia melalui operasi seperti *Cloud Hopper*. Fenomena ini memperlihatkan strategi otoritarianisme digital Tiongkok telah berkembang menjadi ancaman global yang serius dan juga menimbulkan pertanyaan kepada pemerintah Tiongkok memaknai dan menanggapi ancaman siber di dua dekade terakhir.

Lebih dari sekadar aspek teknis, strategi siber Tiongkok menyiratkan dimensi politik yang kuat, terutama dalam konteks otoritarianisme digital. Pemerintah Tiongkok secara aktif menyatukan narasi keamanan nasional dengan kontrol informasi domestik, menjadikan ruang siber sebagai arena baru untuk memperkuat stabilitas rezim. Memahami perbedaan antara otoritarianisme digital yang dilakukan secara sengaja dan yang terjadi tanpa niat langsung menjadi hal yang krusial untuk diperhatikan (Pearson, 2024). Untuk menjangkau spektrum praktik otoritarianisme yang lebih luas di ruang digital, pendekatan definisi yang lebih fleksibel menjadi cara yang tepat. Definisi ini memungkinkan kita melihat bahwa teknologi tidak hanya digunakan oleh negara otoriter untuk tujuan represif secara eksplisit, tetapi juga menciptakan efek otoriter melalui struktur dan desain sistem digital itu sendiri.

Critical Terrorism Studies (CTS) mejadi pendekatan yang relevan dalam menganalisis fenomena ini. Teori ini menjelaskan bagaimana label “terorisme” pasca-kebangkitan Taliban sering dikonstruksi oleh negara-negara atau aktor dominan global untuk membenarkan intervensi militer atau kebijakan represif. CTS membantu memahami bahwa ancaman terorisme pasca-Taliban bukan hanya tindakan kekerasan oleh aktor non-negara, tetapi merupakan hasil konstruksi sosial dan politik yang dipengaruhi oleh narasi keamanan global, kebijakan kontra-terorisme yang represif, serta kondisi struktural seperti marginalisasi, konflik identitas, dan intervensi asing.

Konsep *virtual censorship* menjadi kerangka kunci dalam memahami bagaimana Tiongkok mengendalikan informasi di ruang digital domestiknya. Praktik ini tidak hanya dilakukan lewat penyaringan konten atau penggunaan firewall, tetapi juga melalui pembentukan sistem komunikasi digital yang bersifat hirarkis dan berlapis. Dengan tujuan untuk menjaga hegemoni informasi, memisahkan diskursus politik dari arus komunikasi publik yang lebih luas, serta mencegah integrasi antara cyberspace domestik dan asing. Qiu menulis, “*the state tries to*

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

keep the gate between the two cyberspaces" (Qiu, 2000, p. 95), sebuah frasa yang menunjukkan bahwa pemisahan dunia maya tidak hanya bersifat teknis, tetapi merupakan bentuk pertahanan ideologis negara. Ia juga menekankan bahwa *"Internet control in China is not simply a matter of what content is blocked, but how the control mechanisms shape the very structure of cyberspace"* (Qiu, 2000, p. 93). Dengan kata lain, *virtual censorship* bukan sekadar intervensi terhadap isi, melainkan pembentukan ulang terhadap infrastruktur komunikasi digital nasional sebagai alat kontrol sosial dan politik.

Melalui teori *securitization* dari Copenhagen School, konsep otoritarianisme digital berbasis promosi dari Pearson, kerangka transformasi digital Schlumberger et al., dan *virtual censorship* dari Qiu, kita dapat memahami bagaimana negara membingkai isu keamanan siber sebagai ancaman eksistensial. Ancaman ini mencakup isu seperti spionase dan digunakan untuk membenarkan kebijakan luar biasa, seperti peningkatan pengawasan, regulasi ketat terhadap data, dan penguatan kedaulatan siber. Praktik-praktik tersebut pada akhirnya memperkuat otoritarianisme digital yang sistemik di Tiongkok.

Artikel ini bertujuan untuk mengkaji bagaimana tindakan spionase siber oleh APT10 mencerminkan pendekatan keamanan digital Tiongkok di tingkat internasional. Tindakan tersebut juga berperan dalam memperkuat kontrol domestik melalui narasi otoritarianisme digital, baik secara disengaja maupun tidak. Dengan menelaah keterkaitan antara strategi luar negeri dan kebijakan dalam negeri, artikel ini memberikan kontribusi terhadap diskusi akademis mengenai keamanan non-konvensional, transformasi digital, dan penindasan siber dalam rezim otoriter kontemporer.

TINJAUAN PUSTAKA

Konsep otoritarianisme digital merujuk pada penggunaan teknologi digital oleh negara otoriter untuk memperkuat kontrol politik dan sosial. Dalam konteks Tiongkok, konsep ini diwujudkan melalui sensor internet, pengawasan massal, dan ekspor teknologi pengawasan ke negara lain. Sementara itu, keamanan nasional dalam era siber mengacu pada perlindungan data, infrastruktur kritis, dan integritas sistem pemerintahan dari serangan digital. Beberapa penelitian terdahulu telah membahas aspek ini, namun masih sedikit yang mengkaji keterkaitan antara otoritarianisme digital dan ancaman spionase siber lintas negara seperti yang dilakukan oleh APT10.

Dalam kerangka teori *securitization* dari Copenhagen School, isu keamanan dipahami bukan sebagai sesuatu yang objektif, melainkan sebagai konstruksi sosial yang dibentuk melalui "tindakan bicara" (*speech act*) oleh aktor berotoritas seperti negara. Dalam konteks ini, negara dapat menciptakan ancaman berdasarkan kepentingannya sendiri, bukan semata-mata berdasarkan fakta objektif. Penggunaan kecerdasan buatan (AI) dan teknologi digital oleh negara-negara otoriter, khususnya Tiongkok, menjadi instrumen utama dalam menyekuritisasi stabilitas rezim mereka.

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

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Data dikumpulkan melalui studi literatur dari sumber akademik, laporan keamanan siber, dan dokumen kebijakan pemerintah. Analisis dilakukan menggunakan kerangka teoritis *securitization* Copenhagen School yang dikombinasikan dengan konsep otoritarianisme digital dan virtual censorship untuk memahami strategi keamanan siber Tiongkok melalui kasus APT10. Pendekatan studi kasus dipilih karena APT10 merepresentasikan fenomena kompleks yang menggabungkan aspek teknis dan politik dalam konteks geopolitik global. Data primer bersumber dari laporan investigasi keamanan siber dari Mandiant, FireEye, dan lembaga keamanan internasional lainnya, sementara data sekunder berasal dari publikasi akademik dan analisis kebijakan.

3. HASIL DAN PEMBAHASAN

3.1 Model Sekuritas Digital Oleh Tiongkok

Tiongkok menjadi contoh negara yang secara aktif menggunakan *securitization* dalam domain digital. Pemerintah Tiongkok membingkai dunia digital sebagai arena ancaman eksistensial terhadap keamanan nasional. Pernyataan Presiden Xi Jinping bahwa "tanpa keamanan siber, tidak ada keamanan nasional" mencerminkan tindakan bicara menjadi dasar legitimasi bagi implementasi kebijakan seperti UU Keamanan Siber (2017) dan UU Keamanan Data (2021).

Model keamanan siber dari Tiongkok ini mengubah infrastruktur teknologi (sensor, pengawasan, dan penyaringan) menjadi sistem pertahanan politik. Hal ini mencerminkan suatu bentuk sekuritisasi yang menyeluruh, yang tidak hanya bereaksi terhadap ancaman, tetapi juga membangun keunggulan struktural dalam ekosistem ancaman siber. Model ini juga terlihat dengan jelas melalui adanya Great Firewall of China (GFW), yang tidak hanya berfungsi sebagai alat teknis untuk menyaring informasi, tetapi juga merupakan bagian dari rencana keamanan nasional yang lebih luas untuk memperkuat dominasi siber Tiongkok. Dengan cara yang terstruktur, Tiongkok memisahkan ruang siber dalam negeri dari pengaruh eksternal, menciptakan model baru kedaulatan digital yang meningkatkan kemampuan negara untuk mengendalikan aliran informasi dan pandangan masyarakat. Pendekatan ini, sebagaimana dijelaskan dalam studi Herdiana (2023) yang membahas Great Firewall, mencerminkan upaya sistematis Tiongkok untuk mengamankan kedaulatan digital melalui kontrol konten dan pemisahan struktur informasi domestik dari jaringan global. Tulisan tersebut juga menekankan bahwa blokir terhadap konten dari luar negeri, pemantauan berbasis algoritma, serta pengembangan pilihan lokal seperti Baidu dan WeChat merupakan elemen penting dari sistem otoritarian digital yang dirancang dan dijalankan secara terus-menerus.

3.2 APT10: Wajah Spionase Siber Negara Tiongkok

APT10, yang juga dikenal dengan nama MenuPass atau Red Apollo, adalah kelompok Advanced Persistent Threat (APT) yang beroperasi di bawah pengawasan Kementerian Keamanan Negara (MSS) Tiongkok (Zhang et al., 2024). Sejak pertengahan 2000-an, kelompok ini dikenal sebagai pelaku utama dalam spionase siber internasional, dengan sasaran informasi penting di bidang teknologi, pertahanan, dan pemerintahan. Salah satu operasi mereka yang paling signifikan, "Cloud Hopper", menargetkan penyedia layanan TI global dan memperoleh akses ke data klien melalui serangan terhadap rantai pasokan.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

APT10 memanfaatkan cara-cara canggih seperti spear-phishing, perangkat lunak berbahaya khusus seperti PlugX dan QuasarRAT, serta teknik "*Living-Off-the-Land*" yang menggunakan alat resmi sistem untuk masuk dan menghindari deteksi. Serangan mereka dilakukan secara terorganisir, terencana, dan menunjukkan tingkat sumber daya yang hanya dapat dimiliki oleh aktor negara. Keterkaitan mereka dengan MSS menunjukkan bahwa aktivitas APT10 merupakan bagian dari taktik Tiongkok dalam meraih keunggulan geopolitik dan teknologi dengan cara ilegal (Zhang et al., 2024).

Melalui aksinya, APT10 tidak hanya mengganggu keutuhan sistem keamanan nasional negara-negara target, tetapi juga memperkuat posisi kekuatan siber Tiongkok dalam konteks pemerintahan otoriter. Di era ini, informasi diposisikan sebagai sumber daya strategis yang sangat bernilai. Dengan demikian, APT10 merepresentasikan bentuk baru dari pertikaian global di ranah siber.

3. 2.1 Sejarah dan Evolusi APT10: Dari MenuPass hingga Red Apollo

Red Apollo dan *POTASSIUM* adalah kelompok spionase siber yang didukung oleh pemerintah Tiongkok dan telah beroperasi sejak sekitar tahun 2006. Dipercaya bahwa kelompok ini berfungsi di bawah Biro Keamanan Negara Tianjin dari Kementerian Keamanan Negara Tiongkok, serta bekerja sama dengan perusahaan teknologi lokal seperti *Huaying Haitai Science and Technology Development Company* untuk menyamarkan kegiatan mereka. Pada awalnya, APT10 fokus pada pencurian informasi intelektual dan data bisnis penting dari sektor-sektor seperti pertahanan, dirgantara, telekomunikasi, dan lembaga pemerintah di negara-negara yang dianggap saingan Tiongkok, terutama Amerika Serikat, Jepang, dan Eropa.

Pada tahap awal (2006–2014), APT10 memanfaatkan perangkat lunak berbahaya konvensional seperti PlugX, Poison Ivy, dan ChChes, yang disebarkan melalui metode serangan spear-phishing atau dengan mengeksploitasi celah di sistem. Mereka juga menggunakan alat open-source seperti Mimikatz dan PowerSploit untuk memperkuat kemampuan sistem infiltrasi mereka. Puncak perkembangan strategi mereka terjadi selama Operasi *Cloud Hopper* (2014–2017), di mana mereka menargetkan *Managed Service Providers* (MSPs) yang mengelola infrastruktur TI untuk klien-klien di seluruh dunia. Dengan berhasil membobol MSP, APT10 memperoleh akses ke ratusan jaringan klien, termasuk perusahaan teknologi, lembaga pemerintah, dan organisasi kesehatan, sehingga dapat melakukan pencurian data sensitif secara besar-besaran.

Pada tahun 2016 hingga 2018, APT10 meluncurkan berbagai alat baru seperti HAYMAKER, BUGJUICE, dan SNUGRIDE, yang dibuat untuk menghindari deteksi perangkat lunak antivirus serta meningkatkan kemampuan pergerakan lateral di dalam jaringan target. Mereka juga mulai menggunakan infrastruktur *cloud* dan server proxy untuk menyembunyikan lalu lintas *command-and-control* (C2). Selama periode ini, kelompok tersebut semakin sering terhubung dengan kepentingan ekonomi Tiongkok, seperti mendapatkan keunggulan kompetitif untuk perusahaan-perusahaan lokal melalui pencurian hak kekayaan intelektual, termasuk dalam kasus pencurian yang teridentifikasi.

3. 2. 2 Teknik dan Metode Operasional: Malware, Phishing, dan Living-Off-the-Land

APT10, sebuah grup mata-mata siber yang diduga berhubungan dengan Kementerian Keamanan Negara Tiongkok (MSS), terkenal karena penerapan teknik canggih dalam aksinya. Di antara strategi yang paling mencolok adalah pemanfaatan malware, spear-phishing, dan teknik *Living-Off-the-Land* (LOTL). Ketiga strategi ini memungkinkan

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

APT10 untuk mengakses, bergerak dalam jaringan, dan mengambil data sensitif dari sasaran tanpa terdeteksi oleh sistem keamanan yang umum.

a. Malware: Alat Utama dalam Operasi APT10

Malware merupakan salah satu alat utama yang digunakan oleh kelompok *Advanced Persistent Threat* (APT)10 dalam melancarkan operasi siber mereka. APT10, yang juga dikenal sebagai "Stone Panda" atau "MenuPass," adalah kelompok peretas yang diduga memiliki koneksi dengan pemerintah China. Mereka aktif sejak tahun 2009 dan dikenal karena serangan canggih mereka terhadap berbagai sektor, termasuk pemerintahan, militer, dan perusahaan teknologi. Dalam operasinya, APT10 memanfaatkan berbagai jenis malware untuk mencuri data, memantau aktivitas korban, dan mempertahankan akses jangka panjang ke sistem yang diretas. Malware yang digunakan sering kali dirancang khusus untuk menghindari deteksi oleh perangkat keamanan tradisional, sehingga membuatnya sangat efektif dalam operasi spionase siber.

Salah satu malware andalan APT10 adalah PoisonIvy, sebuah *Remote Access Trojan* (RAT) yang memungkinkan penyerang mengambil kendali penuh atas sistem korban. PoisonIvy digunakan untuk mencuri data sensitif, merekam ketikan keyboard, dan mengaktifkan kamera atau mikrofon tanpa sepengetahuan pengguna. Malware ini sering disebarkan melalui *spear-phishing*, di mana korban menerima email yang tampak sah namun mengandung lampiran atau tautan berbahaya. (Zhang et al., 2024). Selain PoisonIvy, APT10 juga dikenal menggunakan malware seperti PlugX dan QuasarRAT, yang memiliki fungsi serupa tetapi dengan teknik penghindaran yang lebih canggih. Penggunaan malware-malware ini menunjukkan betapa APT10 berinvestasi besar dalam pengembangan alat-alat berbahaya untuk mendukung operasi mereka. Selain memanfaatkan malware yang sudah ada, APT10 juga mengembangkan alat khusus untuk menargetkan infrastruktur tertentu. Misalnya, mereka menggunakan malware seperti "RedLeaves" dan "ChChes" yang dirancang khusus untuk menyerang jaringan korporat dan lembaga pemerintah. Malware ini mampu menyebar secara lateral dalam jaringan, mencari sistem penting, dan mengekstrak data tanpa terdeteksi. Kemampuan ini membuat APT10 sangat berbahaya, karena mereka tidak hanya mencuri data tetapi juga dapat mempertahankan kehadiran mereka dalam sistem korban selama berbulan-bulan atau bahkan bertahun-tahun.

Operasi APT10 sering kali terorganisir dan dilakukan dengan rencana yang matang. Mereka terlebih dahulu melakukan survei untuk menemukan sasaran yang memiliki nilai tinggi, lalu meluncurkan serangan dengan perangkat lunak berbahaya pilihan yang sesuai. Setelah berhasil mengakses sistem, mereka menerapkan teknik "*Living-Off-the-Land*" dengan memanfaatkan alat yang telah terdapat di sistem target untuk menghindari kecurigaan. (Hanafi, 2022). Cara ini membuat serangan mereka sukar untuk dilacak dan diatasi. Akibat dari operasi APT10 sangat besar, terutama terkait kerugian finansial dan ancaman terhadap keamanan negara. Banyak perusahaan yang terkena dampak mengalami kebocoran informasi sensitif, termasuk hak kekayaan intelektual serta informasi penting. Pemerintah di berbagai negara telah mengeluarkan peringatan mengenai bahaya APT10, menekankan pentingnya memperkuat pertahanan siber. Tindakan seperti pelatihan kesadaran keamanan, pembaruan sistem secara teratur, dan penggunaan teknologi deteksi yang canggih menjadi sangat penting untuk mengurangi kemungkinan serangan semacam ini.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

Dengan terus berkembangnya teknik dan alat yang digunakan oleh APT10, malware tetap menjadi komponen inti dalam operasi mereka. Kelompok ini terus beradaptasi dengan lingkungan keamanan siber yang semakin ketat, menjadikan mereka salah satu ancaman paling persisten dan berbahaya di dunia maya. Oleh karena itu, Penting untuk memahami metode dan alat yang mereka gunakan untuk mengembangkan strategi pertahanan yang efektif.

b. Spear-Phishing: Gerbang Masuk ke Sistem Target

Spear-phishing merupakan teknik serangan siber yang sangat terarah dan menjadi metode utama kelompok APT10 untuk menginfiltrasi jaringan korban. Berbeda dengan *phishing* konvensional yang menyebar secara massal, *spear-phishing* dirancang khusus untuk menipu individu atau organisasi tertentu dengan pesan yang tampak personal dan meyakinkan. APT10 biasanya melakukan pengintaian mendalam terlebih dahulu seperti menganalisis media sosial, struktur perusahaan, atau kebiasaan komunikasi target untuk membuat email yang sulit dibedakan dari pesan resmi (Deibert, 2013). Misalnya, mereka mungkin menyamar sebagai atasan, rekan kerja, atau mitra bisnis dengan menggunakan alamat email yang mirip asli, disertai lampiran berbahaya atau tautan yang mengarah ke halaman login palsu. Begitu korban terjebak, *malware* seperti PoisonIvy atau PlugX akan diinstal secara diam-diam, memberikan akses penuh kepada penyerang.

Kelompok ini juga kerap memanfaatkan eksploit *zero-day* atau kerentanan yang belum diperbaiki untuk meningkatkan efektivitas serangan. Selain itu, mereka menggunakan teknik "*social engineering*" yang canggih, seperti memanfaatkan isu terkini atau peristiwa penting untuk memancing korban membuka lampiran. Contohnya, email yang mengaku sebagai pemberitahuan kebijakan baru terkait COVID-19 atau undangan seminar palsu. Setelah berhasil masuk, APT10 melakukan lateral movement untuk memperluas cengkeraman dalam jaringan, mencuri kredensial, dan mengakses data sensitif.

Pencegahan serangan *spear-phishing* memerlukan pendekatan multi-lapis, mulai dari pelatihan kesadaran keamanan bagi karyawan, penerapan *multi-factor authentication* (MFA), hingga penggunaan sistem deteksi ancaman berbasis AI. Organisasi juga harus rutin memantau lalu lintas email mencurigakan dan memperbarui sistem untuk menutup kerentanan yang bisa dieksploitasi. Dengan memahami taktik APT10, langkah mitigasi dapat lebih efektif dalam mencegah infiltrasi yang berpotensi merugikan secara finansial dan reputasi.

c. Living-Off-the-Land (LOTL): Menggunakan Alat yang Ada untuk Menyusup

Teknik *Living-Off-the-Land* (LOTL) menjadi salah satu strategi paling canggih yang digunakan kelompok APT10 untuk menghindari deteksi dalam operasi spionase siber mereka. Berbeda dengan serangan konvensional yang mengandalkan *malware* khusus, LOTL memanfaatkan alat-alat sah yang sudah terinstal di sistem target, seperti PowerShell, WMI, PsExec, atau bahkan aplikasi administrasi jaringan. Pendekatan ini membuat aktivitas jahat mereka menyatu dengan lalu lintas sistem normal, sehingga sulit diidentifikasi oleh solusi keamanan tradisional yang hanya berfokus pada tanda-tanda (*signature*) *malware*. APT10 sering kali memulai serangan dengan spear-phishing atau eksploitasi kerentanan untuk mendapatkan akses awal. Setelah masuk, alih-alih menginstal malware yang mencolok, mereka menggunakan skrip PowerShell untuk menjalankan perintah jarak jauh,

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

memanipulasi *Windows Management Instrumentation* (WMI) untuk eksfiltrasi data, atau memanfaatkan RDP (*Remote Desktop Protocol*) untuk bergerak lateral di dalam jaringan. Misalnya, mereka bisa mengekstrak kredensial menggunakan Mimikatz, alat yang sebenarnya dirancang untuk pengujian keamanan lalu menggunakannya untuk mengakses server kritikal tanpa memicu alarm.

Keunggulan LOTL terletak pada kemampuan beradaptasi dengan lingkungan target. Karena alat yang digunakan adalah bagian dari sistem operasi atau aplikasi resmi, serangan ini tidak meninggalkan jejak yang mudah dilacak. Selain itu, banyak organisasi tidak memonitor aktivitas alat-alat sistem secara ketat, sehingga APT10 dapat beroperasi dalam waktu lama tanpa terdeteksi. Mereka bahkan bisa menonaktifkan fitur keamanan lokal dengan perintah *Group Policy Object* (GPO) atau mengubah konfigurasi *firewall* menggunakan netsh semuanya dengan alat bawaan Windows.

Untuk memitigasi ancaman LOTL, organisasi perlu menerapkan pendekatan *Zero Trust*, membatasi hak akses administratif, dan memantau penggunaan alat sistem yang tidak biasa. Solusi *Endpoint Detection and Response* (EDR) juga dapat membantu mengidentifikasi pola aktivitas mencurigakan, seperti eksekusi PowerShell yang tidak wajar atau koneksi jaringan lateral yang tidak terduga. Dengan memahami teknik LOTL, tim keamanan dapat lebih waspada terhadap ancaman terselubung yang memanfaatkan alat sah untuk tujuan jahat.

Teknik LOTL melibatkan penggunaan alat dan fitur sistem yang sah untuk melakukan aktivitas berbahaya tanpa menambahkan perangkat lunak berbahaya baru. Dengan memanfaatkan alat yang sudah ada, penyerang dapat menghindari deteksi oleh perangkat lunak keamanan tradisional yang biasanya mencari tanda-tanda perangkat lunak berbahaya. APT10 memanfaatkan berbagai alat sistem, seperti PowerShell, *Windows Management Instrumentation* (WMI), dan PsExec, untuk mengeksekusi perintah, bergerak lateral, dan mempertahankan akses ke sistem target. Misalnya, PowerShell digunakan untuk menjalankan skrip berbahaya langsung dari memori, sementara WMI memungkinkan eksekusi perintah jarak jauh dan pengumpulan informasi sistem. PsExec, alat administrasi jarak jauh, digunakan untuk mengeksekusi perintah pada sistem lain dalam jaringan tanpa perlu instalasi perangkat lunak tambahan. Penggunaan teknik LOTL memungkinkan APT10 untuk beroperasi dengan sangat tersembunyi, menjadikannya sulit untuk dideteksi dan dihentikan oleh sistem keamanan konvensional.

Kombinasi dari teknik-teknik ini menunjukkan pendekatan canggih dan terkoordinasi yang digunakan APT10 dalam operasi spionase sibernya. Dengan memanfaatkan malware untuk mendapatkan akses awal, spear-phishing untuk menargetkan individu atau organisasi tertentu, dan teknik LOTL untuk bergerak dan beroperasi secara tersembunyi, APT10 mampu mencuri data sensitif dan merusak infrastruktur kritis tanpa terdeteksi. Pendekatan ini menyoroti pentingnya bagi organisasi untuk memiliki sistem keamanan yang kuat dan strategi pertahanan yang dapat mendeteksi dan mencegah teknik-teknik canggih seperti yang digunakan oleh APT10.

Aktivitas spionase siber Tiongkok terhadap proyek F-35 AS menggunakan metode *spear-phishing* yang sangat mirip dengan pola serangan APT10. Dalam kasus ini, seorang warga negara Tiongkok bernama Su Bin, dengan dukungan perwira militer, mengirimkan email berisi malware kepada kontraktor pertahanan AS untuk mencuri data sistem radar dan elektro-optik jet tempur generasi kelima

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

tersebut. (Dheo Chandra et al., 2023). Aksi ini menunjukkan bahwa teknik serangan siber bukan hanya mengincar informasi taktis, tetapi juga dirancang untuk mendukung ambisi Tiongkok dalam mempercepat modernisasi militer domestik serta mengurangi ketergantungan pada ekspor alutsista asing.

Laporan *Center for Strategic and International Studies* (CSIS) tahun 2021 juga menganalisis 160 insiden spionase Tiongkok di Amerika Serikat antara 2000–2021, mengungkapkan peningkatan signifikan aktivitas sejak 2010. Data menunjukkan 76% insiden terjadi dalam dekade terakhir, bertepatan dengan kepemimpinan Xi Jinping sebagai Sekretaris Jenderal Partai Komunis Tiongkok pada 2013.

Aktivitas spionase ini menunjukkan pola sistematis dengan target beragam:

a) Institusi pemerintah (34%): Gedung Putih, Departemen Pertahanan, CIA, FBI, NASA
b) Industri pertahanan: Lockheed Martin, Boeing, Raytheon
c) Sektor sipil (51%): teknologi tinggi, energi, otomotif, universitas, kesehatan
d) Informasi politik (15%): data pejabat dan kandidat politik

Analisis CSIS juga menunjukkan bahwa 74% pelaku spionase adalah warga negara Tiongkok, dengan 42% merupakan pegawai negara atau militer, sementara 26% adalah warga negara AS yang direkrut atau dipengaruhi.

Kemampuan APT10 menunjukkan betapa tingginya kapabilitas siber ofensif Tiongkok, yang tidak hanya mengandalkan eksploitasi teknis, tetapi juga pemahaman mendalam terhadap arsitektur kelembagaan dan ekonomi digital global. Hal ini menempatkan Tiongkok sebagai kekuatan utama dalam arena siber internasional, sekaligus menegaskan bahwa spionase digital adalah instrumen kebijakan luar negeri yang terintegrasi dengan strategi keamanan nasional.

3.3 Kasus Terkemuka: Operasi Cloud Hopper dan Pencurian Data OPM AS

Untuk memahami penerapan teknik operasional APT10 secara konkret, berikut dua studi kasus penting yang menunjukkan cakupan dan dampak dari operasi mereka dalam konteks strategi spionase digital Tiongkok.

Salah satu operasi paling terkenal yang dikaitkan dengan APT10 adalah "*Cloud Hopper*", yang dimulai pada akhir 2016. Dalam operasi ini, APT10 menargetkan penyedia layanan TI terkelola *Managed Service Providers* (*MSP)* di berbagai negara, termasuk Inggris, Amerika Serikat, Jepang, Kanada, Brasil, Prancis, Swiss, Norwegia, Finlandia, Swedia, Afrika Selatan, India, Thailand, Korea Selatan, dan Australia. Dengan mengkompromikan MSP, APT10 tidak hanya memperoleh akses ke sistem perusahaan penyedia layanan, tetapi juga ke data sensitif milik klien-klien mereka yang tersebar di sektor-sektor kritis seperti manufaktur, energi, farmasi, telekomunikasi, dan lembaga pemerintah. (Puyvelde, 2019). Teknik ini memperlihatkan bagaimana APT10 mengeksploitasi hubungan kepercayaan digital dan infrastruktur rantai pasok untuk memaksimalkan cakupan dan efektivitas infiltrasi mereka. Keberhasilan operasi ini menegaskan sifat sistematis dan transnasional dari strategi spionase digital Tiongkok.

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

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:

Selain *Cloud Hopper*, APT10 juga diduga terlibat dalam pencurian data dari Kantor Manajemen Personil AS *Office of Personnel Management* (OPM), yang menyebabkan kebocoran informasi pribadi lebih dari 21 juta individu, termasuk sidik jari dan data keamanan personel pemerintah. Serangan terhadap OPM ini tidak hanya merupakan pelanggaran privasi dalam skala besar, tetapi juga menyoroti kemampuan APT10 dalam menargetkan basis data pemerintah dengan tujuan strategis jangka panjang, seperti pembangunan profil intelijen dan pemetaan jaringan keamanan nasional negara lawan. Kombinasi dari operasi seperti *Cloud Hopper* dan serangan terhadap OPM memperlihatkan bahwa APT10 tidak hanya berfokus pada spionase ekonomi, tetapi juga pada pengumpulan intelijen untuk memperkuat posisi geopolitik dan kemampuan pertahanan nasional Tiongkok.

APT10 dikenal menggunakan berbagai teknik canggih dalam operasinya, mulai dari *spear-phishing* yang menyamar dalam bentuk email sah dengan lampiran berbahaya, hingga pemanfaatan *malware* seperti PlugX, Poison Ivy, dan QuasarRAT untuk mempertahankan kehadiran mereka dalam jaringan target. Mereka juga mempraktikkan teknik "*Living-Off-the-Land*" yang berarti memanfaatkan perangkat bawaan sistem seperti PowerShell dan WMI untuk menjalankan perintah tanpa terdeteksi, serta mengeksploitasi kerentanan dalam perangkat lunak populer seperti *Microsoft Exchange* guna memperoleh akses administratif. Strategi ini menunjukkan kemampuan jangka panjang APT10 dalam menanamkan diri di sistem target untuk mengamati, mempelajari, dan mencuri informasi bernilai tinggi secara diam-diam. Pendekatan tersebut tidak hanya menegaskan kecanggihan teknis kelompok ini, tetapi juga membedakan mereka dari kelompok kriminal siber biasa karena tindakan mereka konsisten dengan misi geopolitik negara, memperjelas fungsi APT10 sebagai instrumen spionase strategis yang dijalankan oleh negara otoriter dalam rangka memperkuat pengaruh dan superioritas digital.

Selain itu, operasi spionase siber Tiongkok terhadap Amerika Serikat dilakukan secara sistematis dan multi-level (Ben Moshe, 2022). Target serangan mencakup lembaga pemerintah, industri pertahanan, universitas, dan perusahaan teknologi. Metode yang digunakan meliputi serangan *malware* langsung, pemanfaatan koneksi bisnis, dan perekrutan individu yang memiliki akses terhadap data sensitif. Dalam konteks ini, APT10 berfungsi sebagai representasi dari pola besar strategi keamanan nasional Tiongkok yang memadukan spionase digital dengan tujuan mempercepat dominasi teknologi global.

3.4 Aspek Etis dan Hak Asasi Manusia dalam Sekuritisasi Siber

Sekuritisasi siber menciptakan dilema normatif fundamental yang mempertanyakan batas-batas antara kepentingan keamanan kolektif dan hak individual dalam ruang digital. Logika keamanan yang memprioritaskan perlindungan dari ancaman siber kerap mengabaikan prinsip proporsionalitas, menciptakan paradoks di mana upaya menciptakan ruang siber yang aman justru mengikis privasi dan kebebasan fundamental (Putri et al., 2022). Praktik sekuritisasi siber telah melegitimasi ekspansi sistem pengawasan massal dengan dalih keamanan nasional, menciptakan apa yang Shoshana Zuboff sebut sebagai "*surveillance capitalism*." Normalisasi pengawasan ini mengubah ekspektasi privasi

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

masyarakat dan menciptakan efek menggigil (chilling effect) terhadap kebebasan berekspresi. Tradisi hukum yang menganggap privasi sebagai hak fundamental mengalami erosi ketika berhadapan dengan imperatif keamanan siber, di mana konsep "*reasonable expectation of privacy*" menjadi semakin terbatas dalam konteks digital.

Sekuritisasi siber tidak hanya mengubah praktik keamanan, tetapi juga struktur kekuasaan dalam masyarakat, menciptakan konsentrasi otoritas pengawasan di tangan negara dan korporasi teknologi yang mengancam prinsip-prinsip demokratis. Penggunaan narasi ancaman siber untuk membenarkan tindakan luar biasa telah menciptakan "*permanent state of exception*" dalam terminologi Giorgio Agamben, di mana keadaan darurat yang seharusnya bersifat sementara menjadi normal baru, mengikis mekanisme *checks and balances* (Ünver, 2018). Atmosfer pengawasan konstan menciptakan dampak psikososial yang signifikan, termasuk *self-censorship*, *paranoia*, dan perubahan perilaku daring yang lebih konservatif. Generasi yang tumbuh dalam era sekuritisasi siber berpotensi mengalami redefinisi ekspektasi privasi secara permanen.

Dalam konteks ini, *UN Guiding Principles on Business and Human Rights* memberikan kerangka etis penting untuk menilai sekuritisasi siber. Pilar pertama menegaskan kewajiban negara untuk melindungi hak asasi dari pelanggaran oleh aktor non-negara, termasuk ketika negara justru berkolaborasi dengan korporasi teknologi. Pilar kedua menekankan tanggung jawab perusahaan dalam melakukan *due diligence* terhadap dampak hak asasi dari teknologi yang mereka kembangkan, serta kewajiban menolak kolaborasi represif. Pilar ketiga menggarisbawahi hak atas pemulihan, meskipun realisasinya di bidang siber menghadapi tantangan besar, mulai dari sifat rahasia operasi pengawasan, hingga keterbatasan yurisdiksi pengadilan.

Pelaksanaan prinsip-prinsip keamanan siber membutuhkan kerangka hukum dan etis yang menjunjung keseimbangan, kebutuhan, dan pendekatan yang paling tidak mengganggu. Selain itu, diperlukan pengawasan independen terhadap kebijakan yang diterapkan oleh negara. Reformasi juga harus mencakup perlindungan data yang menyeluruh, pengawasan yudisial yang kuat, dan tata kelola partisipatif untuk menjaga keseimbangan kekuasaan di era digital.

3.5 Aktualisasi Strategi Siber Tiongkok dalam Forum Internasional

3.5.1 Diplomasi Siber Tiongkok: Membentuk Ulang Norma Digital Global

Tiongkok secara aktif berkontribusi dalam membangun tatanan digital global dengan cara yang sistematis dan terencana. Melalui partisipasinya di berbagai forum internasional, Beijing mendorong prinsip kedaulatan siber, yang menyatakan bahwa setiap negara harus memiliki kontrol penuh atas ruang sibernya masing-masing. Pendekatan ini jelas bertentangan dengan nilai-nilai digital yang diusung oleh negara-negara Barat, seperti kebebasan internet dan pertukaran informasi yang terbuka. Di berbagai forum seperti *United Nations Group of Governmental Experts* (UN GGE), *Shanghai Cooperation Organization* (SCO), dan melalui inisiatif *Belt and Road*

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

terutama *Digital Silk Road* (DSR), Tiongkok secara konsisten mempromosikan model pengelolaan internet yang berbasis negara. Dalam pembahasan UN GGE mengenai keamanan informasi dan komunikasi, Tiongkok selalu menekankan pentingnya kedaulatan negara sebagai prinsip utama dalam pengembangan tata kelola siber di tingkat global. Sudut pandang ini jelas berbeda dari pendekatan yang diambil oleh Amerika Serikat dan mitranya, yang cenderung mendukung model *multi-stakeholder*, dengan peran signifikan dari masyarakat sipil dan sektor swasta.

Dalam kerangka *cyber sovereignty*, Tiongkok menekankan empat elemen utama: hak penuh negara untuk mengatur aktivitas siber di wilayahnya, penolakan terhadap campur tangan asing, penentangan terhadap operasi siber sepihak, dan tanggung jawab negara dalam mencegah wilayahnya digunakan untuk serangan siber (Shen, 2016). Keempat prinsip ini mencerminkan pendekatan kedaulatan yang ketat dalam tata kelola dunia maya. Secara tersirat, pendekatan tersebut menantang doktrin *cyber deterrence* yang banyak dianut oleh NATO dan sekutunya.

Dalam konteks *Shanghai Cooperation Organization* (SCO), Tiongkok berperan sentral dalam merumuskan SCO *Agreement on Cooperation in the Field of International Information Security* yang ditandatangani pada 2009 dan diperkuat melalui berbagai deklarasi berikutnya. SCO menjadi wadah bagi Tiongkok untuk mempromosikan kerangka alternatif tata kelola siber yang menekankan kedaulatan negara dan menolak dominasi informasi yang dianggap sebagai "*information imperialism*" dari Barat. Melalui platform ini, Tiongkok berhasil membentuk koalisi dengan Rusia dan negara-negara Asia Tengah untuk mendukung model tata kelola internet yang restriktif.

Inisiatif *Digital Silk Road* dalam konteks *Belt and Road Initiative* merupakan wujud nyata dari diplomasi siber Tiongkok yang paling ambisius. Melalui DSR, Tiongkok tidak hanya mengedarkan teknologi dan infrastruktur digital, tetapi juga menyodorkan model tata kelola yang fokus pada kontrol negara dan kedaulatan siber (Wowor et al., 2024). Program ini meliputi pembangunan jaringan serat optik, pusat data, infrastruktur kota pintar, dan sistem *e-governance* di lebih dari 60 negara, yang dengan sendirinya menyebarkan standar dan praktik Tiongkok dalam tata kelola digital. Tiongkok dengan cerdik menggunakan DSR untuk menciptakan ketergantungan digital di negara-negara partner, di mana infrastruktur digital dibangun menggunakan standar teknologi Tiongkok dan dioperasikan dengan prinsip-prinsip pengelolaan Tiongkok. Ini menciptakan efek jaringan yang memperkuat kedudukan Tiongkok dalam diskusi tentang pengelolaan digital secara global. Negara-negara yang telah menerima infrastruktur digital dari Tiongkok cenderung lebih mendukung posisi Tiongkok dalam forum-forum internasional. Upaya Tiongkok untuk mengatur regulasi yang membatasi akses internet terlihat dalam berbagai usulan di forum PBB, termasuk Kode Etik Internasional untuk Keamanan Informasi yang pertama kali diajukan bersama Rusia pada tahun 2011 dan telah direvisi beberapa kali. Usul ini mencakup ketentuan yang secara jelas membatasi penyebaran informasi yang dapat "mengganggu stabilitas politik, ekonomi, dan sosial," yang dianggap oleh para pengkritik sebagai sebuah pembenaran untuk sensor internet dan penindasan perbedaan pendapat. Dalam pembicaraan UN GGE, Tiongkok dengan teguh menolak

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

pemahaman luas tentang penerapan hukum humaniter internasional (IHL) di dunia maya, dengan dalih bahwa ini bisa digunakan untuk membenarkan operasi siber yang bersifat menyerang (Moynihan & Patel, 2021). Tiongkok lebih memilih pendekatan yang menekankan penyelesaian sengketa secara damai dan pelarangan penggunaan kekuatan di dunia maya, yang sejalan dengan strategi kebijakan luar negeri secara keseluruhan untuk menjaga status quo sambil memperkuat kekuatan relatif.

Tiongkok juga berperan aktif dalam *International Telecommunication Union* (ITU) sebagai tempat alternatif untuk pembahasan pengaturan siber, di mana negara-negara berkembang memiliki kekuatan suara yang lebih besar dibandingkan forum multi-pemangku kepentingan yang didominasi oleh negara-negara Barat. Melalui ITU, Tiongkok mendorong pendekatan berbasis negara terhadap pengaturan internet dan menentang pemprivatisasian fungsi pengaturan internet yang saat ini dikuasai oleh organisasi berbasis di AS seperti ICANN. Strategi Cina dalam membangun norma-norma siber juga terlihat dalam perjanjian bilateral dan regional yang mendukung prinsip-prinsip kedaulatan siber. Kesepakatan dengan negara-negara seperti Rusia, Iran, dan berbagai negara Afrika secara terus-menerus menekankan penghormatan terhadap kedaulatan siber dan prinsip non-intervensi, yang membentuk dasar untuk kerangka hukum siber internasional alternatif. Sikap Cina yang menolak norma-norma digital Barat juga terlihat dalam penolakan terhadap konsep-konsep seperti "kawasan umum global" di dunia siber dan "kebebasan berekspresi daring" sebagai prinsip universal. (Moynihan & Patel, 2021) Cina berargumen bahwa dunia siber adalah konstruksi buatan yang berada di bawah kedaulatan teritorial, bukan kawasan umum global yang dapat dikelola bersama oleh komunitas internasional. Ini secara mendasar menantang pandangan Barat tentang internet sebagai medium tanpa batas yang melampaui kedaulatan tradisional. Cina juga memanfaatkan potensi ekonominya untuk memperkuat model tata kelola siber yang mereka terapkan. Dalam berbagai perjanjian perdagangan dan kontrak investasi, Cina seringkali menyertakan syarat yang mengharuskan negara mitra untuk menerapkan ketentuan lokal mengenai data Cina, standar keamanan siber, dan regulasi konten. Ini mengarah pada penerapan bertahap praktik tata kelola siber Cina di tingkat regional dan bilateral.

Sebagai respons terhadap sanksi Barat dan pembatasan teknologi, Tiongkok semakin gencar mendorong standar teknologi alternatif dan kerangka tata kelola global. Salah satu contohnya adalah peluncuran *Global Data Security Initiative* pada tahun 2020, yang merupakan upaya untuk menantang dominasi AS dalam isu keamanan data. Inisiatif ini juga mencerminkan keinginan Tiongkok untuk membentuk kerangka alternatif dalam tata kelola data internasional.

Dampak dari diplomasi siber Cina sangat penting untuk masa depan tata kelola internet global. Keberhasilan upaya Cina dalam mempromosikan kedaulatan siber dapat mengakibatkan terbelahnya internet atau yang sering disebut sebagai "*splinternet*" di mana berbagai daerah beroperasi sesuai dengan prinsip tata kelola dan standar teknis

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

yang berbeda. Hal ini dapat mengancam interoperabilitas dan keterbukaan yang merupakan prinsip dasar dari arsitektur internet. Untuk negara-negara yang sedang berkembang, model Tiongkok menawarkan pilihan menarik sebagai alternatif bagi kerangka tata kelola siber yang didominasi oleh Barat, terutama bagi negara-negara yang khawatir tentang pengaruh budaya Barat atau yang memiliki struktur pemerintahan otoriter. Penyediaan teknologi, pendanaan, dan keahlian tata kelola oleh Tiongkok melalui DSR menciptakan paket yang menarik dan sulit untuk disaingi oleh negara-negara Barat. Namun, mengadopsi model tata kelola siber Tiongkok juga membawa risiko, termasuk kemampuan pengawasan yang meningkat, pembatasan terhadap kebebasan berekspresi, dan potensi untuk pemaksaan ekonomi melalui ketergantungan digital. Negara-negara yang secara luas mengadopsi infrastruktur digital Tiongkok dan praktik tata kelola mungkin mendapati diri mereka terjebak dalam pengaruh Tiongkok dengan sedikit pilihan alternatif.

Ke depan, persaingan antara model kedaulatan siber Tiongkok dan pendekatan multi-pemangku kepentingan Barat akan semakin memanas seiring dengan meningkatnya pentingnya teknologi digital dalam bidang ekonomi dan politik. Hasil dari persaingan ini akan sangat memengaruhi karakter tata kelola internet global untuk beberapa dekade mendatang, dengan dampak yang luas terhadap hak asasi manusia, pengembangan ekonomi, dan keamanan internasional.

4. SIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa APT10 bukan sekadar entitas teknis, melainkan instrumen strategis dalam kebijakan keamanan digital tiongkok. Dengan memanfaatkan teknik canggih seperti perangkat lunak berbahaya, spear-phishing, dan pemanfaatan sumber daya yang ada, APT10 menjadi representasi kemampuan Tiongkok untuk melakukan operasi spionase siber berskala internasional yang selaras dengan agenda politik dan teknologi negara itu. Dalam konteks *securitization*, Tiongkok menggambarkan ancaman siber sebagai risiko besar terhadap stabilitas nasional. Metode ini memberikan justifikasi bagi kebijakan represif seperti pengawasan yang meluas, pemisahan ruang digital domestik dari jaringan global, dan pembentukan infrastruktur informasi yang bersifat hierarkis dan tertutup. Tindakan-tindakan tersebut berkontribusi pada terbentuknya sistem otoritarianisme digital yang berkelanjutan dan terorganisir.

Secara global, pendekatan diplomasi siber Tiongkok mendukung model kedaulatan siber yang menekankan pentingnya kontrol negara atas internet dan menolak prinsip-prinsip manajemen yang melibatkan banyak pemangku kepentingan. Melalui berbagai forum seperti UN GGE dan SCO, serta inisiatif *Digital Silk Road*, Tiongkok memperluas pengaruh normatif dan teknologinya kepada negara-negara mitra, yang dapat berpotensi menyebabkan fragmentasi arsitektur internet global atau splinternet. Namun, pendekatan ini juga membawa masalah etis yang serius. Penerapan sekuritisasi siber yang berlebihan dapat mengorbankan hak asasi manusia, termasuk privasi dan kebebasan berpendapat. Dalam hal ini, prinsip-prinsip hukum internasional serta tata kelola yang inklusif menjadi sangat

penting untuk mencapai keseimbangan antara keamanan dan perlindungan hak individu.

Secara keseluruhan, penelitian ini menegaskan bahwa spionase siber yang dilakukan oleh APT10 tidak hanya sekadar alat teknologi, melainkan juga merupakan bagian dari perubahan struktural dalam kekuasaan digital di era rezim otoriter saat ini. Dengan memahami dinamika ini, kita bisa mengembangkan strategi keamanan yang lebih kritis, etis, dan peka terhadap tantangan dalam era otoritarianisme digital.

5. DAFTAR PUSTAKA

Anggita, P. (2023). *LEGALITAS PENGGELEDAHAN KANTONG DIPLOMATIK (DIPLOMATIC BAG) REPUBLIK RAKYAT TIONGKOK DI HOUSTON-TEXAS OLEH PEMERINTAH AMERIKA SERIKAT*.

Ben Moshe, N. (2022). *Chinese Espionage Operations in the United States: And in Israel? 15*, 1–8.

Deibert, R. J. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (illustrate). McClelland & Stewart, 2013.

Dheo Chandra, R., Abdul Rahman Azzqy, A., & Awal, S. (2023). Strategi Keamanan Siber Amerika Serikat di Masa Pemerintahan Joe Biden Terkait Isu State-Sponsored Cyber Espionage. *Balcony*, *7*(1), 13–26.

Hanafi. (2022). *Dasar Cyber Security dan Forensic*. 236. https://eprints.amikom.ac.id/id/eprint/10688/

Moynihan, H., & Patel, C. (2021). Restrictions on online freedom of expression in China The domestic , regional and international implications of China's policies and practices. *Chatham House*.

Pearson, J. S. (2024). *Mendefinisikan Otoritarianisme Digital*. 1–19.

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Puyvelde, D. D. Van. (2019). *Cyber Hype Versus Cyber Reality - How Severe Is The Threat That Chinese Cyber-Attacks Pose To United States ' National Security? July*.

Qiu, J. L. (2000). Virtual Censorship in China: Keeping the Gate Between the Cybersapces. *International Journal of Communications Law and Policy*, *4*, 1–25.

Schlumberger, O., Edel, M., Maati, A., & Saglam, K. (2023). How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition*, 761–783. https://doi.org/10.1017/gov.2023.20

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

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

Ünver, H. A. (2018). Artificial intelligence, authoritarianism and the future of political systems. *EDAM Research Reports*, *July*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331635

Wowor, H. G. A., Sudirman, A., & Hakiki, F. (2024). China's Great Firewall: Cybersecurity as Strategy for Building World Cyberpower. *JISPO Jurnal Ilmu Sosial Dan Ilmu Politik*, *13*(2), 193–232. https://doi.org/10.15575/jispo.v13i2.27713

Zhang, J., Liu, S., & Liu, Z. (2024). Attribution classification method of APT malware based on multi-feature fusion. *PLoS ONE*, *19*(6 June), 1–28. https://doi.org/10.1371/journal.pone.0304066