BAB 6

Diplomasi Siber Asia Tenggara di Tengah Rivalitas AS-China di Indo-Pasifik

Ali Abdullah Wibisono

A. Lanskap Geopolitik, Diplomasi Siber, dan Tantangan bagi ASEAN

Indo-Pasifik adalah teater utama dari langgam persaingan geopolitik antara AS, China, dan Rusia. Ruang siber dan teknologi digital dalam interaksi antarnegara di kawasan Indo-Pasifik telah menjadi "pedang bermata dua", di satu sisi ekonomi digital telah menjadi *booster* perekonomian yang tak dapat dipisahkan dari pertumbuhan ekonomi di kawasan yang ditempati negara-negara dengan kontribusi terbesar pada GDP dunia, tapi di sisi lain ruang siber Indo-Pasifik juga diisi dengan negara-negara yang kompetitif dalam mendayagunakan teknologi digital di ruang siber. Indo-Pasifik terdiri dari 40 negara yang mewakili lebih dari 50% dari GDP dunia menjelang 2040, de-

A. A. Wibisono
Universitas Indonesia, *e-mail*: aliabdullahwibisono@hotmail.com

Wibisono, A. A. (2026). Diplomasi Siber Asia Tenggara di Tengah Rivalitas Amerika Serikat-Tiongkok di Indo-Pasifik. Dalam RR. E. Yustiningrum & E. S. Prihatini (Ed.), *Indonesia dalam Kancah Geopolitik di Indo-Pasifik* (189–231). Penerbit BRIN. DOI: 10.55981/brin.2075.c1723
E-ISBN: 978-602-6303-98-1

ngan GDP akumulatif dari China, Jepang, India, Korea Selatan, dan Australia mencapai lebih dari seluruh Uni Eropa secara keseluruhan (Hurel et al., 2024). Kawasan yang luas dan heterogen ini telah menjadi episentrum dari interaksi strategis dari negara-negara *Five Eyes* di beragam sektor. AS, Inggris, Australia, Kanada, dan negara-negara lain telah memublikasikan strategi mereka untuk Indo-Pasifik, dan membentuk kerja sama keamanan, seperti AUKUS yang berfokus pada aliansi teknologi unggul untuk meningkatkan *interoperability*. Sementara regionalisme yang menjadi episentrum Indo-Pasifik, yaitu ASEAN telah memublikasikan visi Indo-Pasifik mereka sejak 2017.

Dalam hal konstruksi norma keamanan siber—sebagaimana berlangsung pada forum Perserikatan Bangsa-Bangsa (PBB) yang bertajuk *United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (UNGGE) dan *United Nations Open-Ended Working Group on Development in the Field of Information and Telecommunication in the Context of International Security* (OEWG)—AS, China, dan Rusia mengedepankan prioritasnya masing-masing. China memprioritaskan kedaulatan nasional yang menghindari intervensi aktor eksternal negara maupun non-negara dalam pengaturan keamanan siber (dikenal pula sebagai pendekatan *multilateralism*) (Mallick, 2022, 67). Sementara, AS mengedepankan kemitraan negara dengan swasta dan masyarakat sipil dengan negara tunduk kepada aturan-aturan internasional yang disepakati bersama dan mengikat untuk menindak dan menanggulangi kejahatan siber dan kebahayaan lain terhadap informasi dan infrastruktur digital (dikenal pula sebagai *multistakeholderism*).

Sejauh mana persaingan geopolitik AS dan China di ruang siber sebagaimana diutarakan di atas berimplikasi pada keamanan siber Asia Tenggara? Artikel ini menjelaskan bagaimana persaingan geopolitik telah menjadi struktur yang membatasi aktivisme negara-negara Asia Tenggara dalam diplomasi siber mengarah kepada belum terwujudnya arsitektur norma keamanan siber di Asia Tenggara dalam bentuk persepsi ancaman yang sama.

Diplomasi siber adalah instrumen penting dalam keseluruhan kebijakan luar negeri suatu negara atau sekelompok negara untuk menjaga interaksi di ruang siber tidak mengarah kepada konflik dan saling percaya atau *confidence* dapat dibangun dan dijaga sebagai fondasi kerja sama penguatan bersama (Barrinha & Renard, 2017). Diplomasi siber di Asia Pasifik adalah pembahasan yang semakin mengundang penulis untuk melakukan observasi terhadap pembangunan norma dan perkembangan arsitektur keamanan regional (Barrinha & Renard, 2017), bagaimana diplomasi siber dapat berperan membangun saling-percaya dalam ruang siber yang semakin dipenuhi inovasi kecerdasan buatan, *machine learning*, *Internet of Things* (IoT), dan *blockchain* (Radanliev, 2024), peranan diplomasi siber dalam perang siber (Lancelot, 2020), dan bagaimana kebijakan penggentaran atau *deterrence* dapat diintegrasikan dengan diplomasi siber untuk memperkuat pencapaian tujuannya (Manantan, 2021). Namun, belum ada publikasi yang secara spesifik melihat implikasi dari rivalitas AS-China di ruang siber Asia Tenggara, khususnya dalam hal kesenjangan digital antarnegara anggota, dan menciptakan kebutuhan diplomasi siber yang spesifik untuk kawasan yang ditandai dengan kesenjangan digital di antara negara anggotanya.

Penelitian untuk artikel ini bertujuan melihat sejauh mana rivalitas geopolitik AS-China membatasi diplomasi siber negara-negara Asia Tenggara. Diplomasi siber adalah kebijakan yang ditujukan untuk memitigasi bahaya yang muncul dari relasi kompetitif di ruang siber sehingga data-data yang dibutuhkan adalah implikasi ketidakamanan siber di Asia Tenggara sebagai dampak dari rivalitas AS-China di ruang siber, data-data tentang kapabilitas keamanan siber negara-negara ASEAN dan komitmen mereka pada kerja sama internasional untuk keamanan siber, dan data-data tentang arsitektur regional keamanan siber ASEAN. Data-data yang digunakan dalam artikel ini bersumber dari laporan-laporan keamanan siber yang diterbitkan oleh lembaga-lembaga konsultan keamanan siber internasional dan pengukuran indeks keamanan siber yang dikeluarkan oleh lembaga Perserikatan Bangsa-Bangsa bernama *International Telecommunications Union*

(ITU), yaitu *Global Cybersecurity Index* (Indeks GCI) dan *Information and Communication Technology Development Index* (Indeks IDI). Laporan-laporan keamanan siber membantu penelitian ini melakukan observasi terhadap bentuk-bentuk ketidakamanan siber yang mutakhir dihadapi negara-negara di ASEAN dan tingkat intensitas serangan siber yang dihadapi oleh setiap negara. Sementara indeks keamanan dan pembangunan ruang siber berguna untuk mengetahui tingkat komitmen suatu negara kepada pembangunan infrastruktur digital dan keamanan siber. Sementara itu, komitmen negara-negara ASEAN, dan sejumlah negara Indo-Pasifik yang penting, seperti Australia dan Jepang untuk diplomasi siber diukur dengan indeks keamanan siber nasional (*National Cyber Security Index/NCSI*) yang dibuat oleh *Estonian e-Governance Academy* (eGA) yang salah satu komponen pengukurannya adalah kontribusi terhadap keamanan siber global (NCSI, 2023). Artikel jurnal internasional menjadi sumber data-data tentang arsitektur keamanan siber regional, yang menginformasikan penulis tentang arsitektur regional memitigasi ketidakamanan siber dari rivalitas AS-China.

Untuk mengeksplorasi bagaimana persaingan geopolitik di ranah siber memengaruhi keamanan siber Asia Tenggara, dan bagaimana respons ASEAN dalam membentuk tata kelola keamanan siber, artikel ini berlanjut dalam beberapa bagian. Bagian pertama yang mengikuti pendahuluan ini menjelaskan tentang konsep diplomasi siber dan ketidakamanan di ruang siber. Kedua, artikel ini menjelaskan bagaimana rivalitas AS-China bermanifestasi di ruang siber dan teknologi digital. Bagian keempat menjelaskan ketidakamanan siber Asia Tenggara yang ditandai dengan peningkatan kejahatan siber dengan *ransomware* dan *malware* lain dan serangan kelompok peretas non-negara dengan sponsor negara. Bagian kelima mengeksplorasi tata kelola keamanan siber yang telah dibangun ASEAN dan bagaimana hal ini belum menyepakati persepsi ancaman yang sama untuk ancaman yang berasal dari kejahatan siber. Artikel ini berkesimpulan bahwa arsitektur keamanan siber Asia Tenggara berupaya untuk mencegah kawasan ini terlalu condong ke salah satu kekuatan dalam rivalitas

geopolitik, tapi kesenjangan digital di antara negara anggota adalah penghalang besar dari standar bersama keamanan siber regional.

B. Diplomasi Siber dan Ketidakamanan di Ruang Siber

Diplomasi siber adalah serangkaian penerapan negosiasi dalam relasi antarnegara yang bertujuan meregulasi dan menyelesaikan masalah-masalah seputar ruang siber. Masalah yang dihadapi dalam relasi antarnegara di ruang siber tidak jarang melibatkan penyalah-gunaan kemampuan maupun kealpaan yang dapat berujung pada konflik sehingga kajian diplomasi siber juga menginklusi perang siber (*cyber warfare*) dan kesepakatan tentang *rules of engagement* dalam melakukan tindakan tertentu. Diplomasi siber terjadi di masa damai maupun konflik. Di masa damai, diplomasi siber bertujuan memfasilitasi pertukaran informasi dan gagasan untuk isu-isu siber tertentu yang mengarah pada terbentuknya norma-norma siber. Sementara itu, ketika terjadi ketegangan atau konflik di ruang siber, diplomasi siber berperan sebagai strategi resolusi konflik yang mencegah konflik di ruang siber bereskalasi menjadi masalah geopolitik yang lebih serius.

Produk utama dari aktivitas diplomasi siber adalah norma siber. Norma siber adalah nilai dan pedoman yang ditetapkan bersama yang mengarahkan tindakan aktor di ruang siber, yang bertujuan untuk membentuk perilaku etis dan menghentikan aktivitas daring yang tidak bertanggungjawab. Diplomasi siber sangat penting dalam mempromosikan dan menegosiasikan standar perilaku yang membentuk norma siber ini di antara pemerintah maupun aktor swasta. Norma siber tidak selalu tertulis, tapi lebih berperan sebagai aturan tidak tertulis yang dipahami dan diindahkan oleh negara-negara sepemahaman (*likeminded states*). Norma siber yang sudah kokoh karena disepakati tanpa *reserve* dan berkesinambungan membentuk tata kelola atau rezim keamanan siber, yang berwujud regulasi yang diadopsi negara-negara anggota rezim tersebut.

1. *Confidence Building*

Langkah pertama dari diplomasi siber adalah *confidence building* atau membangun kepercayaan, ini penting untuk mencapai kesepakatan antarnegara dan menumbuhkan rasa saling percaya, mengurangi skeptisisme, dan meningkatkan keterbukaan dalam berbagi informasi tentang aktivitas siber masing-masing aktor. *Confidence building* dapat terjadi lewat pertukaran informasi strategis, pelatihan bersama melibatkan tim dari dua atau lebih negara, dan *hotline* untuk menghindari kesalahpahaman dan kesalahan dalam penilaian perilaku.

Keamanan siber atau *cybersecurity* berhubungan erat dengan diplomasi siber tapi keduanya melayani dua fungsi berbeda. Keamanan siber mencegah, mengidentifikasi, dan merespons serangan siber berupa akses tak berizin, peretasan komputer dan pencurian informasi dari sistem, jaringan dan basis data komputer, dengan beragam strategi dan teknologi untuk melindungi data dan membatasi disrupsi di ruang siber.

Diplomasi siber berurusan dengan implikasi diplomatik dari manajemen ancaman-ancaman di ruang siber yang sering kali sulit untuk diidentifikasi dengan pasti dan akurat. Bisa dikatakan, salah satu isu utama dalam keamanan siber adalah identifikasi serangan siber. Diplomasi siber bertujuan untuk mengatasi masalah atribusi atau mencari bukti keterlibatan dalam serangan siber dengan membangun mekanisme untuk membuat orang bertanggung jawab atas operasi siber yang merugikan atau bahkan disruptif.

Untuk memerangi ancaman siber secara efektif, diplomasi siber mendorong kerja sama antara pemerintah dan perusahaan swasta karena sektor swasta memainkan peran utama dalam dunia maya. Oleh karena itu, kolaborasi publik-swasta dapat mempermudah pertukaran pengetahuan dan pengalaman dalam keamanan siber. Diplomasi siber mendorong pengembangan kapasitas di negara-negara berkembang untuk meningkatkan keterampilan dan kekuatan keamanan siber mereka. Bantuan ini dapat berasal dari aktivitas berbagi pengalaman keahlian, pelatihan bersama, dan transfer teknologi.

Bagi negara-negara demokratik, diplomasi siber tidak hanya memfasilitasi negosiasi norma dan resolusi konflik, tapi juga menjaga tindakan-tindakan keamanan siber dalam koridor kebebasan dan hak individual di ruang siber termasuk desentralisasi dan tata kelola internet, kebebasan berekspresi, etika, dan privasi. Keseimbangan antara hak individu di ruang siber dan keamanan siber nasional adalah pertimbangan penting di negara-negara demokratik karena hal tersebut membangun identitas demokrasi itu sendiri, sedangkan tindakan-tindakan keamanan siber oleh pemerintah, seperti pemantauan dan peniadaan akses digital terhadap seseorang atau suatu organisasi yang dianggap berbahaya mengakibatkan erosi dari hak-hak sipil masyarakat.

Diplomasi siber lebih dapat diterapkan dan memberikan manfaat yang maksimal di antara negara-negara yang sudah lebih terbuka dalam hal tata kelola siber nasionalnya kepada negara lain sehingga kebutuhan-kebutuhan keamanan siber yang lebih spesifik dapat dicapai. Di antara negara-negara Asia Tenggara yang beragam dalam hal kapabilitas dan tujuan keamanan sibernya, diplomasi siber lebih diharapkan untuk dapat memfasilitasi peningkatan kapasitas keamanan siber dan dialog yang berkelanjutan untuk mencapai norma-norma bersama.

Saat tulisan ini dibuat, diplomasi siber semakin diperlukan di tengah peningkatan ragam bentuk ancaman di ruang siber menurut karakter operasi siber yang membentuknya. Pertama adalah serangan spionase atau pencurian informasi, yaitu serangan terhadap suatu jaringan komputer atau unit yang bertujuan untuk mengumpulkan data berisi informasi untuk kepentingan kompetitif. Aktor-aktor yang terlibat dalam serangan seperti ini mengirim suatu *malware* atau menggunakan instrumen tertentu untuk mengumpulkan informasi penting yang bisa menguntungkan mereka dari jaringan digital atau unit yang mereka sadap tanpa terdeteksi. Spionase tidak mengakibatkan disrupsi pada jaringan melainkan hanya pencurian informasi. Harga yang ditimbulkan dari kerusakan akibat pencurian informasi bisa sangat tinggi. Bentuk kerusakan yang ditimbulkan spionase dapat

berupa pencurian kekayaan intelektual, pencurian informasi strategis lewat *phising email* atau surel palsu yang memancing penerima surel mengaktifkan *malware* dalam surel palsu tersebut, pencurian identitas, intersepsi percakapan digital (yang belum terenkripsi). Pencurian data pribadi yang tersimpan dalam sistem digital suatu pengelola data seperti lembaga pemerintah juga mengakibatkan kerusakan berupa pembocoran data-data yang dicuri ke ruang publik dengan tujuan keuntungan finansial, yaitu dengan menjual data-data yang sudah dicuri.

2. Serangan Provokatif

Hal ini bertujuan untuk mengomunikasikan pesan atau mengungkap suatu informasi yang memalukan atau memprovokasi/mempolarisasi publik. Seperti halnya spionase, tidak terjadi disrupsi pada jaringan pada serangan provokatif, tetapi serangan provokatif dapat mengakibatkan dampak yang sangat serius bagi stabilitas sosial. Sebagai contoh, pada awal Agustus 2024 terjadi kerusuhan berkekerasan yang di lebih dari 20 lokasi di Inggris Raya sebagai akibat dari disinformasi atau berita bohong yang menyebar di media sosial bahwa seorang tersangka yang ditangkap polisi karena perbuatannya membunuh tiga korban adalah seorang muslim radikal; disinformasi ini kemudian menyebabkan demonstrasi besar-besaran di depan kantor Perdana Menteri Inggris, Keir Starmer, yang kemudian menyebar ke penjuru Inggris Raya, semuanya diwarnai dengan kekerasan yang menarget warga muslim, toko-toko milik orang Asia, dan polisi (Maclellan & Demony, 2024).

3. Serangan Disruptif

Hal ini mengacu kepada operasi siber yang menciptakan kelumpuhan sistem karena berlebihnya beban kerja *server* pada jaringan digital. Serangan disruptif berupaya mengambil alih akses terhadap data yang disimpan dalam jaringan atau unit. Operasi siber disruptif adalah upaya sengaja menghilangkan atau mengganggu kemampuan sistem untuk mencegah akses tidak sah (*unauthorized access*) yang dilakukan aktor peretas. Akses tidak sah atau *unauthorized access* terjadi ketika

suatu aktor mengakses sistem digital tanpa izin dengan mencuri kata sandi, kartu akses, atau instrumen pembuka kunci *firewall* lainnya. Setelah berhasil memasuki sebuah sistem digital, peretas dapat menanam virus untuk mendisrupsi kerja sistem, mengunci akses terhadap data-data yang ada, atau menanam suatu *malware* yang dapat menunggu adanya akses untuk mengakses otoritas yang lebih tinggi dalam mengakses data yang lebih sensitif.

Kerusakan yang diakibatkan serangan disruptif dapat berupa kerusakan data, perusakan laman situs web, *Distributed Denial of Services* atau DDoS (ketidakmampuan sistem melayani perintah pengguna karena terbebani perintah-perintah palsu), atau terkuncinya akses terhadap data yang terjadi akibat pengaplikasian *ransomware*. Serangan disruptif dengan efek paling signifikan dihasilkan oleh *Advanced Persistent Threat*, yaitu serangan yang persisten yang disponsori negara dengan tujuan pencurian data atau disrupsi sistem digital. Ragam serangan disruptif dan pencurian data dapat terjadi karena masuknya *malware* atau program 'jahat' yang menginfiltrasi sistem digital, dan salah satu jalan masuk dari program ini adalah *phising email* atau surel palsu, yaitu surel yang tampak berasal dari lembaga tertentu tapi sebenarnya dibuat oleh peretas. Ketika pengguna mengklik tautan atau *attachment* dari surel tersebut maka *malware* akan menginfiltrasi jaringan. Serangan yang disruptif terhadap jaringan digital berpotensi mengakibatkan kematian atau cidera. Secara hipotetik serangan siber terhadap *air traffic controller* di suatu bandara dapat mengakibatkan dua pesawat bertabrakan di udara dan menewaskan seluruh penumpang.

4. Operasi Destruktif

Operasi serangan kinetik (menggunakan kekerasan fisik seperti senjata api dan bahan peledak) yang berupaya menghancurkan sistem digital dari infrastruktur vital. Serangan ini berusaha menghentikan atau merusak fungsi jaraingan dari sebuah infrastruktur vital, seperti pembangkit listrik, *water purifying system*, sistem perkereta-apian, sistem komunikasi pesawat terbang, dan infrastruktur layanan publik

lainnya yang disrupsinya dapat mengorbankan nyawa pengguna layanan.

Deskripsi, bentuk, dan dampak dari keempat tipe serangan di ruang siber atau jaringan digital tersistematisasi pada Tabel 6.1. Seluruh serangan di ruang siber dapat dilakukan oleh aktor negara maupun non-negara.

Tabel 6.1 Tipe-Tipe Serangan Siber, Lapisan Ruang Siber yang Diserang dan Dampaknya

Jenis Serangan Siber	Karakteristik	Bentuk Serangan	Dampak
Spionase; serangan pada lapisan data	Peretas berupaya mendapatkan akses ke data tanpa otoritas dari pemilik/pengelola sistem.	*Spyware*, *malware*, dan *plug-in* untuk mengumpulkan data, serangan *brute force*, penggunaan ulang kredensial, *phishing* yang memberi jalan bagi *malware* untuk mencuri data.	Dampak reputasi, hilangnya nilai strategis informasi, pencurian kekayaan intelektual, manipulasi dan kebocoran informasi rahasia/sensitif.
Provokasi; serangan pada lapisan sosial atau pengguna ruang siber	Pelaku memanipulasi pengetahuan sosial melalui disinformasi & misinformasi, *deepfake*, untuk menyebarkan informasi yang menyesatkan.	Banjir informasi, penyesatan melalui informasi palsu atau bukti palsu atas tindakan orang/kelompok tertentu, dan eksploitasi isu yang sensitif bagi kelompok tertentu.	Ketidakstabilan sosial dan konflik, aksi terorisme, campur tangan dalam pilihan masyarakat di pemilu, dan perubahan politik yang radikal.

Jenis Serangan Siber	Karakteristik	Bentuk Serangan	Dampak
Disrupsi; serangan pada lapisan sistem operasi	Serangan yang bertujuan menghilangkan atau melemahkan fungsi jaringan digital dan layanannya untuk kepentingan politik atau keuntungan.	Serangan *ransomware* pada infrastruktur kritis, serangan DDoS, dan serangan APT (*Advanced Persistent Threat*).	Kelumpuhan sistem digital yang mengakibatkan gangguan layanan, kerugian ekonomi, kerusakan reputasi, kebocoran data ke publik, dan erosi kepercayaan publik terhadap pemerintah dan keamanan digital. Jika disrupsi dilakukan pada infrastruktur vital, dapat menimbulkan efek kinetik.
Penghancuran; serangan pada lapisan perangkat keras	Serangan kerusakan fisik (kinetik) pada infrastruktur digital.	Serangan senjata api dan bahan peledak pada infrastruktur vital. Biasanya terjadi pada masa perang ketika suatu negara melumpuhkan infrastruktur digital vital dengan serangan kinetik.	Mirip dengan dampak disrupsi sistem. Pada level tertentu, dapat menyebabkan kematian jika serangan melumpuhkan infrastruktur vital yang terhubung dengan layanan publik yang luas, seperti sistem digital di Pengatur Lalu Lintas Udara (ATC).

Serangan siber global tidak menunjukkan tanda-tanda mereda. Semakin tinggi laju digitalisasi sektor-sektor ekonomi dan pemerintahan, semakin banyak pula pelaku penyerangan yang berupaya mendapat untung lewat pencurian dan penjualan data. Lebih fundamental dari tingginya laju digitalisasi, keberlanjutan serangan siber akan terjadi karena karakter-karakter dasar ruang siber yang akan terus bertahan. Pertama, ruang siber bersifat *low cost of entry*,

artinya untuk suatu aktor memiliki efek atau pengaruh pada aktor lain di ruang siber membutuhkan sumber daya yang relatif lebih murah ketimbang di matra-matra lain (darat, laut, udara, dan antariksa) (Green, 2015, 35). Fitur ini membuat ruang siber inheren dengan ketidakamanan, karena aktor-aktor 'jahat' dapat memiliki peluang yang lebih besar dalam melakukan aksinya di ruang siber, meski ini bergantung pada kepemilikan teknologi dan pengetahuan (Brands, 2023; Terry, 2023, 1022).

Kedua, aktor-aktor memiliki anonimitas di ruang siber. Meskipun ragam aplikasi dan portal telah mewajibkan pengiputan data yang dapat diklarifikasi, tapi peluang seseorang atau suatu organisasi—termasuk negara—untuk menyembunyikan atau memalsukan identitas diri masih cukup besar karena penanda pengguna di ruang siber hanyalah *IP address*, yaitu alamat daring dari setiap gawai yang terkoneksi ke internet yang menunjuk pada lokasi geografis gawai yang digunakan untuk melakukan serangan (Warf & Fekete, 2016). Karakteristik dasar ini menciptakan problematika atribusi di ruang siber, yaitu kesulitan untuk membangun alibi yang meyakinkan atas keterlibatan seseorang dalam suatu serangan siber (Rid & Buchanan, 2015).

Terakhir, karakteristik dasar dari ruang siber yang membuatnya inheren dengan ketidakamanan adalah ketimpangan atau asimetrisme. Ruang siber dimanfaatkan oleh aktor dengan beragam kemampuan dan pengetahuan teknis tentang teknologi dan jaringan digital. Sebagian aktor memanfaatkan lemahnya struktur normatif dan legal formal untuk mengambil keuntungan di atas kerugian aktor lain, dan mereka bisa merupakan aktor negara, individu, kelompok, atau geng peretas. Semakin tinggi investasi untuk digitalisasi di suatu sektor semakin menarik pula sektor tersebut bagi para peretas, sebab semakin banyak informasi digital yang disirkulasikan di sektor tersebut dan setiap jaringan digital pasti memiliki kelemahan (*loophole*) yang bisa memberikan jalan masuk bagi penyerang.

Dalam perkembangannya, ketimpangan kekuatan di ruang siber tak kunjung teratasi dan justru dimanfaatkan oleh sebagian

negara dalam mencapai keunggulan atau daya tawar (*leverage*) untuk memengaruhi perilaku negara lain, dan di pihak lain melakukan pemblokiran akses terhadap data dari aktor-aktor yang mereka tidak inginkan. Hal ini membuat dunia menyaksikan apa yang disebut dengan "*splinternet*", yaitu kondisi terfragmentasinya negara-negara di dunia dalam memperlakukan akses data dan aplikasi yang dapat beroperasi dalam jaringan internet yang berada dalam yurisdiksi mereka masing-masing (Hoffmann, Lazanski, & Taylor, 2020).

Diplomasi siber pun mengalami evolusi ke arah yang lebih agresif. Di tengah maraknya penggunaan kekuatan siber tak terkendali oleh negara-negara di dunia untuk pencurian data dan disrupsi jaringan digital, sebagian negara termasuk Australia dan Jepang mengadvokasikan penggunaan penggentaran atau *deterrence* untuk menghadapi pelaku serangan siber yang berhasil teridentifikasi (Manantan, 2021). Sementara atribusi negara tertentu sebagai pelaku atau sponsor serangan siber tidak absolut, Jepang dan Australia menempuh jalan penggentara lewat *naming-and-shaming*, yaitu memublikasikan tuduhan terhadap suatu negara yang mereka identifikasi melakukan serangan siber dengan tujuan mempermalukan dan mendesak negara yang bersangkutan untuk menghentikan serangan mereka jika tidak menginginkan konsekuensi yang lebih parah. Diplomasi siber juga dibuat lebih gencar lewat upaya *digital influencing*, yaitu mendorong negara-negara yang belum ikut serta secara lebih bermakna dalam negosiasi dan perundingan norma siber untuk merumuskan kebijakan mereka, merespons krisis-krisis siber yang penting dan ikut serta dalam perumusan dan penerapan perilaku yang bertanggung jawab di ruang siber.

Diplomasi siber adalah kebijakan yang krusial untuk mendampingi strategi keamanan siber negara. Negara-negara dengan kekuatan siber terbaik di dunia sekalipun mengalami serangan siber yang gencar, bahkan porsi serangan siber terbesar dialami oleh negara-negara dengan kekuatan siber paling mumpuni di dunia. Ketahanan siber mereka dikuatkan dengan aktivisme diplomasi siber yang meningkatkan penguasaan teknik dan teknologi keamanan siber.

Tabel 6.2 yang memperlihatkan perbandingan antara data sebaran serangan siber global dari lembaga konsultan keamanan siber Cyfirma (2023) dan pemeringkatan capaian skor indeks keamanan siber global (*Global Cybersecurity Index*/Indeks GCI) yang dikeluarkan International Telecommunications Union (ITU, 2023).

Tabel 6.2 Sebaran Serangan Siber Dunia Tahun 2023 dan Peringkat Indeks GCI

Negara	Pangsa Serangan Siber Global*	Peringkat Indeks GCI/ Skor GCI**
Jepang	12,5%	7/92
AS	10,8%	5/96,6
India	7,1%	t.d. (tidak tersedia)
Inggris	6,4%	2/92,8
Korea Selatan	5,2%	3/92,7
Singapura	5%	1/97,4
Australia	4,8%	6/94
Prancis	4,1%	10/89,4
Kanada	2,9%	11/87,2

*Pangsa persentase serangan siber global dihitung dari jumlah serangan siber yang terjadi, baik yang berhasil ditanggapi maupun tidak. Dari Situs Web Cyfirma https://www.cyfirma.com/research/singapore-and-southeast-asia-threat-landscape/

**Peringkat Indeks Keamanan Siber Global (GCI) diproses dengan mengubah skor menjadi peringkat. Indeks GCI dibuat oleh International Telecommunications Union (International Telecommunication Union (ITU) Development Sector, 2023)

Sumber: Diolah dari ITU (2023); Cyfirma (2023)

Dapat kita lihat bahwa negara-negara dengan indeks GCI tertinggi di dunia adalah juga target-target utama serangan siber global. Penjelasannya adalah negara dengan komitmen terhadap kapabilitas keamanan siber yang tinggi juga merupakan negara dengan tingkat *networked readiness* yang tinggi atau kemampuan pelayanan lalu lintas digital yang dapat diandalkan, serta melayani banyak pelaku bisnis dan lembaga pemerintah yang terdigitalisasi. Ini merupakan lingkungan yang sangat menarik bagi penyerang-penyerang di ruang siber yang mencari data-data sensitif rahasia perdagangan maupun

rahasia negara. Di saat yang sama, diplomasi siber ikut menguatkan ketahanan siber lewat kerja sama penguatan ragam teknik ketahanan ruang siber tertentu, seperti membangun *back-up memory* yang aman dan memutakhirkan kemampuan *firewall* untuk mengenali *signature* dari *malware* dan *ransomware* yang berusaha menginfiltrasi sistem informasi digital, dan membina budaya kerja yang sesuai dengan prosedur standar untuk menjaga keamanan sistem informasi digital. Kerja sama internasional di bidang keamanan siber dapat membina dan memperkuat praktik-praktik yang dibutuhkan untuk keamanan siber ini.

C. Rivalitas Geopolitik AS-China di Ruang Siber

Rivalitas geostrategis China–AS telah bermanifestasi di ruang siber dan direfleksikan oleh cara keduanya memandang internet sebagai medan kompetisi untuk menyebarkan informasi dan wacana untuk meningkatkan pengaruh global mereka dan mendiskreditkan pihak lain. Baik AS maupun China telah memanfaatkan ruang siber untuk melakukan *digital influencing,* yaitu menyebarkan pandangan dunia mereka kepada khalayak global, sambil melawan dan membantah narasi informasi pihak lain.

Manifestasi dari persaingan antara AS dan China di ruang siber telah lama hadir sejak setidaknya awal abad ke-21, dan mengemuka terutama pada sektor ekonomi politik teknologi digital. Pada awal tahun 2000-an, China disinyalir meluncurkan gelombang serangan terhadap jaringan Departemen Pertahanan AS dalam apa yang disebut oleh AS sebagai Operasi Titan Rain (Doshi & Mcguiness, 2021). Pemerintah di seluruh dunia — AS, Inggris, Prancis, Jerman, Kanada, Australia, Jepang, Korea Selatan, Taiwan, India, dan lebih dari selusin lainnya — telah mengeluh tentang intrusi China ke dalam jaringan pemerintah mereka. Beberapa serangan siber terbesar dalam dekade terakhir dikonfirmasi oleh Jaksa Agung AS William Barr telah dilakukan oleh agen China, termasuk antara lain pencurian catatan dari Kantor Manajemen Personalia AS, Hotel Marriott, asuransi kesehatan Anthem, dan Equifax (Doshi & Mcguiness, 2021). Pada

masa selanjutnya, perusahaan AS melakukan penuntutan hukum terhadap pemerintah dan perusahaan China atas tuduhan melakukan pencurian rahasia dagang dan hak atas kekayaan intelektual melalui serangan siber mereka.

Momentum penting dari upaya AS membendung kekuatan teknologi digital China adalah pelarangan kehadiran produk perusahaan teknologi digital China Huawei dalam infrastruktur digital AS. Pada Mei 2018, pemerintahan Presiden Trump mengeluarkan *Executive Order* yang melarang perusahaan-perusahaan AS untuk melakukan bisnis dengan Huawei, termasuk membeli, mengimpor, mentransfer, melakukan instalasi, melaksanakan kerja sama tanpa persetujuan khusus dari pemerintah (Beckley & Brands, 2022). Meskipun perintah ini hanya ditujukan kepada Huawei, tapi implikasinya luas bagi penguasaan teknologi digital AS atas China, khususnya untuk produk semikonduktor dan peralatan dan jasa pembuatan semi-konduktor. Sebagai contoh, sistem operasi Android dari Google tidak lagi bisa dilisensikan kepada Huawei sehingga ambisi perusahaan itu untuk menguasai pasar ponsel global terbatasi. Lebih dari itu, Huawei memiliki anak perusahaan bernama HiSilicon yang merupakan produsen semikonduktor terbesar di China, yang kemudian tidak lagi bisa mendapat pasokan alat, bahan, dan rancangan semikonduktor dari semua perusahaan AS, termasuk yang beroperasi di Taiwan (Miller, 2022). Langkah pelarangan kehadiran Huawei dalam infrastruktur digital juga diikuti oleh Australia.

Merespons kedigdayaan teknologi digital AS dan juga sebagai upaya membangun keunggulan kompetitif, informasi adalah prioritas teratas dalam pertimbangan keamanan nasional China menurut *Five-Year Plan for Informatisation* di tahun 2013 (Heinl, 2017) maupun di tahun 2021 (Creemers et al., 2022). Ruang siber adalah perpanjangan dari ambisi China untuk membangun kemandirian dan keunggulan, karena ketergantungan pada salah satu pemasok teknologi, sistem operasi atau piranti lunak dipersepsikan sebagai ancaman eksistensial bagi RRC. Hal ini diumpamakan oleh Presiden Xi Jinping seperti membangun 'rumah di atas fondasi milik orang lain':

"*No matter how large an internet company is, no matter how high its market value is, if it is heavily dependent on foreign countries for its core components, and if the "major artery" of the supply chain is in the hands of others, it is like building a house on someone else's foundation. No matter how big and beautiful it is, it may not stand up to wind and rain, and it may be so vulnerable that it collapses at the first blow. The control of core technology by others is our biggest hidden danger.*"

- Xi Jinping, 2018, The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work (Mallick, 2022).

Publikasi lain mendetailkan upaya aktif China menghalau dominasi AS di ruang siber lewat cara-cara ilegal melakukan spionase siber terhadap AS dan juga negara-negara lain, sebagian besar di Eropa dan Asia Tenggara, untuk mengumpulkan informasi publik dan pribadi yang sensitif untuk mencapai tujuan-tujuan nasional mereka; China melakukan operasi pencurian informasi atau spionase dengan melakukan intrusi ke dalam jaringan komputer lawan dan mencuri informasi, memanipulasi data, dan menanam instrumen atau program untuk melakukan operasi lanjutkan di masa yang akan datang (Mallick, 2022).

Keberadaan ragam ancaman dan ketidakamanan ruang siber, ditambah dengan penggunaan instrumen siber dan teknologi digital untuk persaingan keunggulan di antara AS dan China, mengakibatkan ruang siber kawasan Indo-Pasifik yang rawan akan operasi peretasan komputer dan jaringan komputer yang menciptakan disrupsi terhadap ketersediaan, integritas, dan kerahasiaan informasi digital.

D. Ketidakamanan Siber Asia Tenggara

Rivalitas AS-China di ruang siber ikut berpengaruh pada lanskap keamanan siber Asia Tenggara lewat serangan-serangan digital China dan AS dan sekutunya pada jaringan digital Asia Tenggara sebagai bagian dari upaya mencuri informasi strategis. Di masa lalu, AS, Australia, dan Inggris tercatat pernah melakukan spionase digital terhadap Indonesia, termasuk penyadapan pertemuan *UNFCC Bali*

Climate Conference tahun 2007 yang dilakukan atas kerja sama dengan NSA-ASD (intelijen Australia), penyadapan telepon Presiden Susilo Bambang Yudhoyono oleh intelijen Australia dalam kurun waktu 2007–2009, penyadapan jaringan telekomunikasi salah satu perusahaan telekomunikasi di Indonesia pada 2009 oleh GCSB (intelijen Selandia Baru), penyadapan pertemuan tingkat tinggi G-20 tahun 2009 di London, termasuk Presiden Susilo Bambang Yudhoyono dan diplomat Indonesia oleh GCHQ (intelijen Inggris) untuk kepentingan ekonomi, penyadapan kabel optik (internet) bawah laut yang bermuara di Singapura dan membawa data internet beberapa negara di kawasan, termasuk salah satunya Indonesia oleh intelijen Singapura bekerja sama dengan intelijen Inggris, AS, dan Australia. Penyadapan diduga berlangsung selama 15 tahun, dan baru diketahui publik luas pada tahun 2013 setelah pembocoran informasi oleh Edward Snowden (Haripin, 2022; Mengko, 2022, 68–71).

China pun tercatat sebagai sponsor serangan kelompok peretas, seperti Naikon dan SharpPanda. Naikon—dan kelompok-kelompok pelaku *Advanced Persistent Threats* (APT)—menargetkan beberapa pemerintah di Filipina, Vietnam, Thailand, Myanmar, dan Brunei Darussalam untuk mengumpulkan intelijen geopolitik (Baezner, 2018). Demikian pula, SharpPanda juga menggunakan surel *spear phishing* yang canggih, sebuah taktik yang menarget individu dan organisasi tertentu untuk memperoleh informasi rahasia (CPR, 2021). Selain itu, aktor-aktor disruptif juga melakukan operasi infiltrasi jaringan untuk memasang pintu belakang (*backdoor*) pada sistem operasi untuk melakukan operasi pengawasan terhadap pemerintah Asia Tenggara. *Ensign Infosecurity's 2023 Cybersecurity Landscape Report* melaporkan bahwa kelompok-kelompok peretas dari China, Korea Utara, Iran, dan Rusia menarget Singapura, Indonesia, Malaysia, Hong Kong, dan Korea Selatan (Ensign, 2023). Mereka melakukannya dengan ragam motivasi, sebagian besar untuk pencurian dan spionase informasi, sementara lainnya termasuk sabotase dan perusakan jaringan, kejahatan, serta keuntungan finansial.

Namun, rivalitas AS-China berkontribusi pada tantangan keamanan siber Asia Tenggara yang lebih struktural. Pertama, secara umum Asia Tenggara adalah kawasan dengan pertumbuhan ekonomi di atas rata-rata dunia dan sedang gencar mengupayakan digitalisasi. Seluruh pelaku ancaman atau *threat actors* menarget jaringan TIK pemerintah dan perusahaan-perusahaan di sektor-sektor yang sedang mengalami pertumbuhan tinggi, diprioritaskan investasinya oleh pemerintah, dan mengalami laju digitalisasi yang tinggi. Dengan kata lain, risiko keamanan siber akan semakin tinggi seiring dengan investasi dan digitalisasi di suatu sektor meningkat, karena pelaku serangan berusaha meraih profit maksimal lewat penipuan dan pencurian data, maupun mengupayakan efek dramatis dari disrupsi di sektor yang melayani banyak konsumen. Selain itu, profil risiko keamanan siber negara-negara Asia Tenggara juga dipengaruhi oleh faktor risiko geopolitik yang tinggi. Tensi perebutan pengaruh antara AS, China, dan Rusia di kawasan ini tidak kunjung mereda, dan mereka tidak segan menggunakan instrumen siber sebagai alat memengaruhi. Seiring dengan Filipina memperbaiki relasi bilateralnya dengan AS, China menganggap negara itu sebagai potensi tantangan yang harus dikendalikan. Potensi konflik atas Taiwan merupakan titik api konflik yang mungkin terjadi di cakrawala keamanan regional dengan dampak siber yang berpotensi tidak dapat diprediksi. Filipina merupakan target logis bagi serangan siber China jika terjadi konflik atas Taiwan.

Tantangan struktural yang dihadapi Asia Tenggara adalah risiko dan kerawanan yang dibawa oleh transformasi digital yang begitu cepat. Seiring dengan semakin banyaknya organisasi publik dan swasta yang terhubung dengan jaringan 5G, mereka semakin banyak menggunakan teknologi yang mendukung kecerdasan buatan (AI) dan *internet of things* (IoT), sembari bermigrasi ke komputasi awan (*cloud*). Integrasi teknologi digital ini telah memperluas potensi target serangan (*attack surfaces*) yang dapat dimanfaatkan oleh pelaku kejahatan siber.

Selain itu, tantangan struktural lain adalah keberagaman dalam hal kematangan siber, yaitu beragamnya intensitas komitmen dan kemauan politik negara-negara Asia Tenggara untuk terlibat dalam kebijakan siber dan isu-isu keamanan, serta beragamnya rezim politik di negara-negara di kawasan, telah menyebabkan kesenjangan pendekatan yang besar di ruang siber. Misalnya, negara dengan tingkat kematangan siber yang tinggi seperti Singapura cenderung mendorong peningkatan penerapan norma-norma internasional bersama, langkah-langkah peningkatan kapasitas, dan aspek kebijakan siber lainnya, sedangkan negara seperti Myanmar yang perlu meningkatkan kematangan siber secara keseluruhan lebih fokus pada upaya membangun kematangan siber dan fokus pada langkah-langkah perlindungan terhadap infrastruktur nasionalnya. Dengan kata lain, komitmen negara-negara Asia Tenggara terhadap isu-isu kebijakan siber juga bergantung pada kematangan siber mereka. Dalam pengukuran *Networked Readiness Index*, ditemukan bahwa kesiapan konektivitas jaringan digital di negara-negara ASEAN berada pada tingkat yang beragam. Skor negara-negara ASEAN dalam *National Cyber Security Index* (NCSI, 2023) dan *Global Cybersecurity Index* (ITU, 2021) pun tampak beragam.

Asia Tenggara telah terposisikan sebagai salah satu kawasan yang paling diminati aktor-aktor kriminal dan disruptif di ruang siber, baik yang disponsori negara maupun gang peretas yang beroperasi di seluruh dunia. Baik China, Rusia, AS, Jepang, dan Australia sebagai negara-negara kuat di ruang siber berusaha memengaruhi posisi politik dari negara-negara di kawasan sebagai bagian dari persaingan dalam memperebutkan pengaruh. Serangan-serangan siber atau operasi ofensif di ruang siber adalah salah satu instrumen untuk mencuri informasi sensitif, memanipulasi pengetahuan publik, memengaruhi preferensi kerja sama internasional sehingga tentu menjadi salah satu instrumen yang digunakan negara-negara besar lewat kelompok-kelompok peretas.

Di sisi lain Asia, Tenggara juga merupakan kawasan dengan pertumbuhan ekonomi dan digitalisasi yang paling dinamis di dunia,

dan seiring dengan laju digitalisasi dan investasi pada pertumbuhan ekonomi yang kian meningkat maka semakin gencar pula serangan siber dapat diharapkan terjadi. Pengamatan oleh perusahaan konsultan keamanan siber Cyfirma memperlihatkan bahwa dalam Januari–Juni 2023 saja, Asia Tenggara adalah tuan rumah regional dari 2,47% atau sejumlah 66 organisasi yang menjadi korban serangan *ransomware*. Dalam hal jumlah korban *ransomware*, Thailand menempati posisi pertama (17/66), diikuti Indonesia (13/66), Malaysia (12/66), Filipina (11/66), Singapura (8/66), dan Vietnam (5/66). Tabel 6.3 merinci pangsa serangan siber global yang diterima oleh sembilan negara, menempatkan Jepang (12,5%), AS (10,8%), dan India (7,1%) sebagai tiga target serangan teratas dalam daftar tersebut.

Tabel 6.3 Karakteristik Ketidakamanan Siber Negara-Negara ASEAN, Jepang, dan Australia

Negara	Karakteristik Ancaman Siber yang Mengemuka
Singapura	*Phising email* menarget organisasi dan bisnis; serangan APT/ serangan siber oleh peretas berbasis di luar negeri; *ransomware.*
Malaysia	Kebocoran data; serangan siber oleh peretas berbasis di luar negeri; serangan *ransomware*; serangan *phising email* pada bisnis piranti lunak, penerbangan, logistik, TIK, dan pemerintah; serangan oleh *hacktivist* dalam bentuk DdoS, *web defacement*, dan pembocoran data.
Indonesia	Serangan *ransomware* diikuti dengan pembocoran data menarget perbankan dan pemerintah; serangan *phising email* terutama menyerang media sosial, sektor logistik, layanan keuangan, layanan penyedia internet dan surel; serangan DDoS terhadap perusahaan TIK, penyedia internet, layanan informasi, *gaming* dan *retail,* berdurasi sebagian besar lebih dari 3 jam.
Filipina	Serangan *ransomware* diikuti dengan pembocoran data oleh beragam kelompok peretas internasional menarget sektor keuangan, pemerintahan, pendidikan, dan *retail*; serangan DdoS terhadap sektor TIK, penyedia informasi, *gaming*, dan penyedia internet; serangan APT bertujuan pencurian informasi perusahaan di bidang perdagangan dan pemerintahan.
Vietnam	Serangan APT oleh kelompok-kelompok peretas internasional; serangan DdoS dengan durasi lebih dari 3 jam pada perusahaan -perusahaan TIK; serangan *ransomware*; serangan *phising*.

Negara	Karakteristik Ancaman Siber yang Mengemuka
Jepang	Serangan APT; pembocoran data-data perusahaan termasuk basis data pegawai dan informasi kartu kredit.
Australia	Serangan APT menarget sektor perbankan dan keuangan, konglomerasi bisnis; pembocoran data menarget perusahaan pertambangan, dan panel surya; serangan DdoS menarget perusahaan-perusahaan TIK.

Sumber: Diolah dari Cyfirma (2023)

Keberagaman komitmen kepada kebijakan tata kelola keamanan siber dan laju digitalisasi menyebabkan Asia Tenggara yang sebelumnya telah menjadi medan intervensi digital, baik oleh AS maupun China (Mubah et al., 2016). Wilayah Asia Pasifik, khususnya Asia Tenggara, juga memiliki tingkat serangan *malware* dan *ransomware* yang lebih tinggi dari rata-rata dunia. Microsoft menemukan bahwa kawasan ini memiliki tingkat 1,6 atau 1,7 kali lebih tinggi dari rata-rata global (Microsoft, 2022). Kejahatan siber mendominasi profil ancaman keamanan siber di Asia Tenggara. Laporan *ASEAN Cyberthreat Assessment 2021* yang dilakukan Interpol mengidentifikasi hal-hal berikut sebagai ancaman kejahatan siber teratas di Asia Tenggara, yaitu (1) peretasan surel bisnis (*business email compromise*); (2) *phishing*; (3) *ransomware*; (4) peretasan data ekonomi digital; (5) pelaku jasa *crimeware* (*crimeware-as-a-service*); dan (6) penipuan siber. Interpol menempatkan *ransomware* sebagai ancaman paling signifikan di Asia Tenggara, yang berproliferasi dengan kecepatan yang belum pernah terjadi sebelumnya karena *low cost of entry*, dan terjangkau untuk dijalankan para pelaku peretasan. Selain itu, *ransomware-as-a-service* (RaaS), *crimeware-as-a-service* (CaaS), dan *phishing-as-a-service* (PhaaS) juga menjadi populer untuk menghasilkan keuntungan cepat. Ini adalah model bisnis antara operator *ransomware* dan klien mereka. Dalam pengaturan ini, klien yang tidak memiliki keahlian untuk mengembangkan *ransomware*, membayar operator untuk meluncurkan serangan *ransomware*. Sederhananya, RaaS, CaaS, dan PhaaS beroperasi dengan cara yang sama dengan model bisnis perangkat lunak sebagai layanan (*software as a service*/SaaS)

(Baker & Shortland, 2023). Interpol juga melaporkan peningkatan kecenderungan para pelaku kejahatan siber untuk mengeksploitasi semakin meluasnya penggunaan perangkat IoT, dengan menggunakan berbagai taktik untuk memperoleh keuntungan ilegal yang maksimal. Laporan tersebut juga mencatat bahwa informasi sumber terbuka (*open source*)—terdiri dari unggahan informasi dari para pengguna media sosial—sangat penting untuk menyusun taktik penipuan rekayasa sosial yang efektif terhadap individu dan organisasi (Interpol, 2021).

E. Tata Kelola Keamanan Siber yang Telah Dibangun ASEAN

Sejauh mana tata kelola keamanan siber Asia Tenggara merespons rivalitas AS-China? Tata kelola keamanan siber Asia Tenggara dibangun oleh dua pilar utama, yaitu strategi keamanan siber setiap negara di kawasan dan arsitektur keamanan regional yang sejauh ini telah dibangun oleh ASEAN.

Berkenaan dengan strategi keamanan siber dari masing-masing negara di kawasan, Asia Tenggara masih diisi oleh negara-negara yang sangat beragam dalam hal komitmen mereka terhadap keamanan siber. Ruang siber Asia Tenggara diisi oleh oleh tiga kelompok negara berdasarkan komitmen mereka dalam keamanan siber. Kelompok pertama adalah negara-negara yang telah menempatkan keamanan informasi digital sebagai prioritas nasional, dan mengalokasikan investasi yang tinggi sebagai porsi dari Produk Domestik Bruto (di atas rata-rata global untuk porsi PDB pada keamanan siber sebesar 0,13%) untuk keamanan siber dan pengembangan TIK, serta memiliki dependensi terhadap ekonomi digital yang tinggi. Singapura, Malaysia, dan Thailand ada pada kategori pertama ini (Tran Dai & Gomez, 2018). Pada Tabel 6.4, ketiga negara ini meraih tiga peringkat teratas di Asia Tenggara untuk capaian skor indeks *National Cyber Security Index* (NCSI). Meskipun Indonesia lebih baik dari Thailand dalam capaian indeks GCI, tapi capaian Indonesia untuk skor indeks IDI yang mengukur pembangunan TIK nasional masih rendah dan hanya

mencapai peringkat 111 dari 193 negara, menunjukkan kesenjangan digital yang tinggi antarkelompok masyarakat dalam hal akses digital. Hal ini berkontribusi pada literasi digital yang tidak merata dan keamanan siber nasional berpotensi disrupsi.

Pada kategori kedua terdapat negara-negara dengan dependensi yang tinggi pada ekonomi digital tetapi memiliki porsi GDP yang rendah (di bawah rata-rata global, antara 0,03%–0,13% dari GDP). Mereka mengakui kehadiran ancaman tapi memprioritaskan isu-isu lain sehingga mengalokasikan sumber daya yang terbatas untuk keamanan siber dan hanya secara parsial mengupayakan keamanan siber. Negara-negara ini bahwa mengakui kerawanan negara akan serangan siber dan implikasinya, tapi belum mempunyai prioritas yang jelas antara perlindungan infrastruktur dan pengendalian konten informasi digital oleh warganya. Indonesia, Brunei Darussalam, Vietnam, dan Filipina ada pada kelompok kedua ini. Brunei Darussalam menunjukkan komitmen pada kapabilitas keamanan siber yang masih di bawah Indonesia meskipun kesenjangan digital di negara itu jauh lebih kecil. Kelompok ketiga adalah negara-negara yang belum mengakui ancaman keamanan siber sebagai prioritas nasional karena tidak adanya aset yang terancam disebabkan oleh penetrasi internet yang masih rendah. Kamboja, Laos, dan Myanmar ada pada kelompok ini.

Rivalitas AS-China di sektor ekonomi-politik dari teknologi digital tercermin dalam tata kelola ruang siber negara-negara Asia Tenggara. Pada kubu pertama adalah negara-negara pendukung tata kelola model *multistakeholderism* yang mengusung kemitraan pemerintah-swasta dan kebebasan berinternet yang diadvokasikan oleh AS, dan kubu kedua adalah tata kelola model *multilateralism* yang mendukung peran kuat negara berdaulat dalam kemitraan lintas aktor yang diadvokasikan China (Stadnik, 2017). Keberadaan dua macam kecenderungan dalam tata kelola ini di Asia Tenggara dicerminkan oleh laporan Freedom House tahun 2017 tentang kebebasan berinternet di Asia Tenggara, yang menggambarkan bobot kebijakan sensor dan institusionalisasi kendali informasi yang

tinggi di Thailand, Myanmar, dan Vietnam sehingga mendapat label "not free"; sementara Indonesia, Malaysia, Singapura, dan Kamboja mendapat label "partially free"; dan Filipina mendapat label "free" atau menjalankan kebebasan berinternet.

Selain keragaman dalam hal model tata kelola ruang siber, negara-negara Asia Tenggara juga ditandai dengan keberagaman tingkat pengembangan kapabilitas keamanan siber, pengembangan kapasitas TIK, dan kontribusi pada keamanan siber global, sebagaimana tercermin pada Tabel 6.4.

Tabel 6.4 Pengukuran Kapasitas Keamanan Siber dan Pembangunan TIK Negara-Negara ASEAN

Negara	Peringkat GCI*	Peringkat IDI**	Peringkat NCSI***	Global Cyber Security Contribution****
Singapura	4	18	31	83%
Malaysia	5	63	22	83%
Indonesia	24	111	49	17%
Vietnam	25	108	93	33%
Thailand	44	78	45	17%
Filipina	61	101	48	33%
Brunei Darussalam	85	53	88	17%
Myanmar	99	135	152	17%
Laos	131	139	135	17%
Kamboja	132	128	120	17%

*Global Cybersecurity Index (GCI) disusun oleh International Telecommunication Union (ITU) untuk mengukur komitmen 193 negara anggota ITU terhadap keamanan siber dan membantu mereka mengidentifikasi sektor-sektor yang perlu diperbaiki. Pemeringkatan pada tabel ini adalah hasil konversi skor pada indeks GCI menjadi peringkat global.

***Information and Communication Technology* (ICT) *Development Index* (IDI) mengukur tingkat pembangunan sektor Teknologi Informasi dan Komunikasi (TIK) yang dibuat oleh lembaga *International Telecommunications Union* (ITU). Indeks IDI mengukur hingga sejauh mana konektivitas digital bersifat universal dan bermanfaat (*meaningful*). Pemeringkatan pada tabel ini adalah hasil konversi skor pada indeks IDI menjadi peringkat global.

***National Cyber Security Index (NCSI) mengukur pengembangan kapasitas (*capacity building*) cybersecurity yang dibuat oleh Estonian e-Governance Academy (eGA).

**** Global Cyber Security Contribution adalah ukuran yang ada di dalam NCSI untuk mengukur keberadaan perjanjian internasional untuk kejahatan siber, representasi di forum kerjasama internasional, peran sebagai tuan rumah untuk organisasi keamanan siber internasional, kerja sama pembangunan kapasitas keamanan siber dengan negara-negara lain.

Perbedaan komitmen kepada keamanan siber pun mengakibatkan aktivisme diplomasi siber yang berbeda. Tabel 6.4 juga menunjukkan komitmen diplomasi siber dengan angka persentase pemenuhan potensi peran internasional atau *Contribution to Global Cyber Security*. Kontribusi kepada keamanan siber global pada dasarnya merupakan dari regulasi keamanan siber di masing-masing negara, semakin kuat regulasi tersebut semakin baik pula pemenuhan potensi kontribusi kepada keamanan siber global. Tabel 6.5 memerinci capaian pada setiap indikator dari skor kontribusi pada keamanan siber global yang tertera pada Indeks NCSI.

Tabel 6.5 Indikator-Indikator Kontribusi Pada Keamanan Siber Global Negara-Negara ASEAN

Negara Anggota ASEAN	Konvensi Internasional untuk Kejahatan Siber	Perwakilan di Forum Internasional	Tuan Rumah Organisasi Keamanan Siber Internasional	Peningkatan Kapasitas Keamanan Siber Negara lain	Skor total (dalam skala 6)
Singapura	0	1	3	1	5
Malaysia	0	1	3	1	5
Indonesia	0	1	0	0	1
Vietnam	0	1	0	1	2
Filipina	1	1	0	0	2
Brunei Darussalam	0	1	0	0	1
Kamboja	0	1	0	0	1
Laos	0	1	0	0	1

Negara Anggota ASEAN	Konvensi Internasional untuk Kejahatan Siber	Perwakilan di Forum Internasional	Tuan Rumah Organisasi Keamanan Siber Internasional	Peningkatan Kapasitas Keamanan Siber Negara lain	Skor total (dalam skala 6)
Myanmar	0	1	0	0	1
Thailand	0	1	0	0	1

Sumber: Diolah dari Indeks NCSI (NCSI, 2023)

Tabel 6.5 memperlihatkan bahwa mayoritas negara ASEAN belum memiliki komitmen yang besar untuk ikut serta dalam pengembangan norma keamanan siber global. Hanya Singapura dan Malaysia yang memiliki keikutsertaan dalam pembentukan norma keamanan siber global dengan menjadi tuan rumah untuk organisasi keamanan siber internasional dan melaksanakan *capacity-building* untuk keamanan siber negara lain. Negara-negara ASEAN lainnya sebagian besar hanya menjaga keikutsertaan dalam forum kerja sama keamanan siber internasional.

Selain itu, Tabel 6.5 juga menunjukkan ketiadaan konvensi kerja sama penanganan kejahatan siber yang disepakati oleh seluruh negara ASEAN. Hanya Filipina yang tercatat menandatangani konvensi anti-kejahatan siber, yaitu *Budapest Convention* yang disepakati oleh Uni Eropa sejak 2001 untuk mengatur respons negara-negara pengadopsinya terhadap kejahatan siber. Hingga tulisan ini dibuat, satu-satunya perjanjian internasional di bidang kejahatan siber yang bersifat mengikat bagi para pengadopsinya hanya *Budapest Convention* yang berjudul lengkap *2001 European Convention on Cyber-Crime*. Selain negara-negara Uni Eropa, Kanada, Jepang, Afrika Selatan, Australia, dan AS juga ikut memformulasikan konvensi ini. Konvensi ini mengatur tentang harmonisasi legislasi dan jangkauan transnasional dari aparat penegak hukum dalam menindak kejahatan siber lintas batas negara anggota konvensi (Thomas, 2009). Melihat konten dari konvensi yang sangat mengatur substansi legal-formal dan tata kelola yurisdiksi siber negara-negara pengadopsinya, *Budapest Convention* tidak diratifikasi oleh sebagian besar negara ASEAN

yang mengedepankan norma non-interferensi. Negara Asia lain yang menandatanganinya hanya Jepang dan Sri Lanka.

Saat tulisan ini dibuat, lembaga *Ad Hoc Committee on Cybercrime* yang dibuat oleh Majelis Umum Perserikatan Bangsa-Bangsa telah menyepakati draf perjanjian penanggulangan kejahatan siber yang diinisiasi oleh Rusia sejak tiga tahun lalu (Smalley, 2024). Draf perjanjian tersebut dikritik oleh para pemerhati HAM karena komitmennya yang rendah pada penyalahgunaan wewenang investigasi dan pengumpulan alat bukti digital yang dapat menggerus kepercayaan masyarakat pada teknologi digital dan menciptakan risiko kesalahan prosedur pidana kejahatan transnasional.

Pilar nasional yang membangun diplomasi siber di Asia Tenggara adalah instrumen kebijakan keamanan siber yang dikeluarkan oleh masing-masing negara anggota. Diplomasi siber hanya dapat mencapai manfaat optimal jika semua negara telah merumuskan strategi keamanan siber nasional yang merumuskan tujuan-tujuan kebijakan keamanan siber, baik dalam hal pengamanan data, infrastruktur komunikasi digital, integritas dan ketersediaan jaringan atau sistem layanan digital, maupun perlindungan hak-hak fundamental pengguna internet. Dokumen strategi keamanan siber nasional juga menjelaskan posisi pemerintah dalam mengupayakan keseimbangan antara perlindungan kebebasan berekspresi individu dan perlindungan data pribadi dan organisasi dan keamanan nasional. Dengan seluruh negara merumuskan strategi keamanan siber nasional, konvergensi kepentingan dan norma keamanan siber regional. Sebagaimana ditunjukkan pada Tabel 6.6, di Asia Tenggara, sejumlah negara belum memiliki dokumen strategi keamanan siber nasional, termasuk Indonesia, Laos, Kamboja, Myanmar, dan Brunei Darussalam.

Tabel 6.6 Instrumen Kebijakan Keamanan Siber dan Data Negara-Negara ASEAN

ASEAN State	Cyber Security Policy Instrument
Malaysia	Computer Crimes Act 1997
	Communication and Multimedia Act 1998
	Sedition and Defamation Act 1948
	Personal Data Protection Act 2010
	National Cyber Security Policy 2016
	Cyber Security Act 2024
Filipina	Electronic Commerce Policy 2000 (Republic Act 8792)
	Law on Cybercrime Prevention (Republic Act 10175)
	Data Privacy Act 2012 (Republic Act 10173/2012)
	National Cyber Security Plan 2022
Thailand	Hukum konvensional mengatur *lèse-majesté* atau penghinaan terhadap kerajaan.
	Computer Crimes Act 2007 & Computer-Related Crime Act 2016
	Cyber Security Act 2019 (B.E. 2562)
	Personal Data Protection Act (PDPA) 2019
	Electronic Transaction Law 2019
	National Cyber Security Strategy 2017-2021
Vietnam	Cyber Security Law 2018
	Cyber Information Law 2015; Information Technology Law 2006; E-Transactions Law 2005; Protection of Consumers' Rights Law 2010
	Hukum konvensional untuk pemidanaan pengguna internet
	Cyber Security Strategy 2025-2030
Indonesia	UU Informasi dan Transaksi Elektronik
	UU Perlindungan Data Pribadi
	Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017
	Perpres No. 47/2023 tentang Strategi Keamanan Siber Nasional
Singapura	Info-Communications Media Development Authority Act 2016; Broadcasting Act, Electronic Transactions Act; Films Act; Newspaper Act, Postal Services Act
	Spam Control Act
	Internet Domain Act

ASEAN State	Cyber Security Policy Instrument
	Personal Data Protection Act 2012
	Cybersecurity Act 2018
	National Cybersecurity Strategy 2016
Kamboja	Defamation & Sedition Law; Cybercrime Law 2022;
Brunei Darussalam	Sedition Act 1948;
Laos	Prevention and Combating Cybercrime Law; electronic data protection law 2017;
Myanmar	Telecommunications Law; Law Protecting Privacy and Security of Citizens;

Sumber: Diolah dan dikembangkan dari Fitriani et al., 2019

Di Asia Tenggara, Brunei Darussalam adalah satu-satunya negara di kawasan yang tidak memiliki regulasi untuk keamanan siber, kejahatan siber, data pribadi, maupun strategi keamanan siber nasional. Meskipun akselerasi dalam hal transformasi digital telah mendorong negara-negara kawasan untuk merumuskan ragam kebijakan keamanan siber nasional, kesenjangan masih ada dalam respons kebijakan mereka. Selain itu, regulasi dan undang-undang yang diproduksi dan mengatur keamanan siber nasional masih lebih banyak berkutat pada restriksi akses informasi untuk pengguna ruang siber dan teknologi digital. Sejumlah regulasi masih belum sesuai dengan prinsip kebebasan berekspresi dan perlindungan hak atas privasi tapi di negara lain—terutama Filipina—hal ini diprioritaskan. Selain itu, mayoritas substansi dari produk kebijakan keamanan siber nasional berkisar pada pengendalian konten digital dan pemidanaan pembuat/penyebar konten yang dianggap negatif, baik karena menghina negara/kerajaan, mencemarkan nama baik orang lain atau mengandung konten negatif lainnya, ketimbang regulasi untuk perlindungan data pribadi dan infrastruktur komunikasi digital.

Pilar kawasan dari tata kelola keamanan siber Asia Tenggara dibangun oleh ASEAN lewat *ASEAN Cybersecurity Cooperation Strategy* (2017–2020), yang ditindaklanjuti dengan *Cybersecurity Cooperation Strategy 2021–2025* yang menguraikan tentang pendirian *ASEAN*

Cybersecurity Coordinating Committee. Di dalam komite tersebut melekat ragam kolaborasi lintas-sektor untuk isu-isu siber. ASEAN juga mendirikan *ASEAN Ministerial Conference on Cybersecurity* untuk menanggapi ancaman ransomware yang meningkat dalam sesi substantif pertama dari *United Nations Open-Ended Working Group on Development in the Field of Information and Telecommunication in the Context of International Security* (OEWG).

Substansi dari norma-norma keamanan siber Asia Tenggara mengikuti substansi dari norma-norma perilaku siber yang bertanggungjawab yang ditetapkan dalam proses *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (*UNGGE*) tahun 2015 (CSAS, 2017). ASEAN dalam hal ini adalah pelaksana subsidiaritas norma dari apa yang sudah ditetapkan dalam UNGGE (Cloramidine & Wibisono, 2024). Termasuk dalam 11 norma perilaku siber yang bertanggungjawab ini adalah larangan negara untuk membiarkan wilayahnya digunakan untuk tindakan yang salah dengan menggunakan TIK dan mendukung atau melakukan serangan siber yang merusak infrastruktur penting (UNGA, 2021).

Kerangka institusional dan kebijakan ASEAN terkait tata kelola siber secara garis besar masih merupakan turunan dari prinsip fundamental kawasan yang terhimpun dalam *ASEAN Way*, termasuk non-intervensi dalam urusan domestik negara anggota, musyawarah dan mufakat sebagai metode pengambilan keputusan, dan mekanisme institusional yang informal dan tidak mengikat sebagaimana terlihat pada produk kesepakatan berupa memorandum (Ali, 2021). Oleh karena itu, kerja sama siber kawasan di bidang siber juga taat kepada pendekatan formalistik antarpemerintah (*intergovernmental*), ditandai dengan deklarasi, pernyataan dan inisiatif kerja sama yang tidak mengikat, struktur kelembagaan berupa *ASEAN Digital Ministers' Meeting* (ADGMIN), sebelumnya dikenal dengan *ASEAN Telecommunications and Information Technology Ministers* (TELMIN), yang merupakan platform kelembagaan utama di ASEAN untuk kerja sama di sektor TIK. ADGMIN mengemban tugas menentukan arah

garis besar dari kebijakan dan kerja sama ASEAN di ranah digital. Dalam mengemban fungsinya, ADGMIN juga didukung oleh *ASEAN Digital Senior Officials' Meeting*, *ASEAN Telecommunication Regulators' Council* dan *ASEAN ICT Centre* yang masing-masing berupaya memperdalam kerja sama antarnegara ASEAN. Ketaatan pada koridor *ASEAN Way* terlihat pada inisiatif kebijakan yang tak mengikat dan berbasis prinsip non-intervensi urusan-urusan internal.

Ketaatan pada *ASEAN Way* juga terlihat pada *ASEAN Framework on Personal Data Protection* yang mengupayakan penguatan perlindungan data pribadi di kawasan untuk mendukung aliran informasi di kawasan. Alih-alih merumuskan aturan-aturan mengikat yang mengharmoniskan hukum-hukum domestik tentang proteksi data pribadi, *framework* ini mendorong negara-negara anggota untuk merancang dan mengimplementasikan hukum atau kebijakan yang mengatur perlindungan data pribadi di yurisdiksinya masing-masing. Selain itu, negara-negara anggota yang mengimplementasikan *framework* ini dapat mengadopsi pengecualian-pengecualian sesuai dengan kondisi domestik masing-masing. Sangat kontras dengan aturan *General Data Protection Regulation* dari Uni Eropa, *ASEAN Framework on Personal Data Protection* tidak mewujud sebagai aturan mengikat yang harus diterapkan negara-negara anggota ASEAN di yurisdiksinya masing-masing (GSMA, 2018).

Selain selaras dengan *ASEAN Way*, fitur utama kedua dari pendekatan tata kelola siber ASEAN adalah penekanannya pada prinsip sentralitas ASEAN, yaitu gagasan bahwa ASEAN harus tetap berada di pusat arsitektur kelembagaan, yang mendorong inisiatif kerja sama regional yang lebih luas di kawasan Asia-Pasifik. Sentralitas ASEAN merupakan prinsip penting yang menginformasikan pengelolaan hubungan eksternal ASEAN dengan negara-negara kuat, termasuk China, AS, Jepang, Korea Selatan, UE, dan India. Prinsip ini secara bertahap menghasilkan terciptanya sistem mitra dialog yang dilembagakan yang dipimpin ASEAN, yang dapat dilihat sebagai bentuk kerja sama transregional yang berbeda di *Global South* (Mueller, 2020). Sehubungan dengan tata kelola siber, ASEAN menunjukkan

keinginan yang kuat untuk menerapkan dan memperkuat prinsip sentralitas ASEAN melalui mekanisme kelembagaan yang dipimpin ASEAN, seperti *ASEAN Regional Forum* (ARF) dan *ASEAN Plus Three*.

Melalui ARF, ASEAN secara khusus mempromosikan langkah-langkah membangun kepercayaan di ruang siber yang selaras dengan budaya diplomatiknya, yang mendorong deeskalasi dan pencegahan konflik secara bertahap melalui *dialog confidence building* (ARF, 2012). ARF dengan demikian memfasilitasi terciptanya pendekatan kerja sama regional terhadap tata kelola siber yang terutama difokuskan pada ketahanan kemampuan nasional dan rasa saling percaya (Tran Dai & Gomez, 2018), dengan ASEAN berada di pusat kelembagaan dan diplomatik kawasan Asia-Pasifik yang lebih luas.

Alih-alih memilih antara pendekatan tata kelola siber multilateral yang secara eksklusif berpusat pada negara (multilateralism) dan pendekatan multi-pemangku kepentingan berbasis pasar (multistakeholderism), ASEAN berupaya menjadi "perantara" antara pendekatan China dan AS terhadap tata kelola siber (Van Raemdonck, 2021). Sementara ASEAN dan China memang memiliki posisi normatif yang sama pada prinsip-prinsip umum tentang penghormatan terhadap kedaulatan negara dan non-intervensi dalam urusan internal, perbedaan halus antara pendekatan ASEAN dan China terhadap tata kelola siber dapat diamati. Misalnya, China telah lama skeptis tentang pendekatan *multistakeholderism* yang bertentangan dengan penekanan China pada tata kelola siber multilateral yang dipimpin oleh pemerintah yang berdaulat (Rosenbach & Chong, 2019). Sebaliknya, ASEAN telah mulai merangkul gagasan multistakeholderism dalam tata kelola ruang siber. Sebagaimana ditunjukkan dalam *ASEAN Cybersecurity Cooperation Strategy 2021–2025*, ASEAN berupaya untuk mengupayakan pendekatan "multi-disiplin", modular, dan terukur bagi pengembangan kapasitas keamanan siber (ASEAN, 2022). Dengan menyoroti pentingnya pendekatan "multilateral" dan "multi-stakeholder", dokumen ini semakin menunjukkan niat ASEAN untuk menciptakan jalan tengah yang melampaui model tata kelola dunia maya AS dan China.

Jalan tengah antara *multilateralism* dan *multistakeholderism* ini termanifestasikan dalam aktivisme ASEAN membangun kerja sama ekstra-regional di bidang keamanan siber. ASEAN telah membangun kerja sama keamanan siber secara berkelanjutan dengan sejumlah mitra dialog dan organisasi internasional dengan tujuan meningkatkan pertukaran informasi tentang ancaman dan respons terhadap insiden-insiden keamanan siber. Dalam hal ini *ASEAN Regional Forum* (ARF) telah membentuk *Points of Contact Directory*, yaitu sejumlah narahubung yang dapat segera merespons insiden keamanan siber yang membutuhkan koordinasi segera—sebagai bagian dari upaya diplomasi preventif untuk membangun saling percaya (*confidence building measure*). *Points of Contact Directory* tersebut dapat dikategorikan sebagai diplomasi preventif karena bertujuan mencegah terjadi kesalahpahaman dan mispersepsi tentang suatu insiden keamanan yang melibatkan TIK digital yang dapat mengarah kepada eskalasi ketegangan hubungan jika tidak diatasi.

Di sektor kejahatan siber (*cybercrime*) *UN Office on Drugs and Crime* (UNODC) dan Interpol memainkan peranan yang melampaui upaya membangun kesadaran ke arah kolaborasi lintas batas, khususnya di antara penegak hukum, penuntut umum, dan penyidik kejahatan siber. Melalui *Financial Action Task Force* (FATF), UNODC juga bekerja sama dengan sektor keuangan dan bisnis dari negara-negara anggota untuk mengidentifikasi titik-titik rawan (*chokepoint*) mata uang kripto dan layanan pencucian uang terkait yang digunakan oleh penjahat dan sindikat kejahatan siber di Asia Tenggara.

Bekerja sama dengan perusahaan keamanan siber, Interpol juga telah meluncurkan berbagai inisiatif untuk mengadili dan menyelidiki pelaku kejahatan siber yang beroperasi sebagai bagian dari jaringan kejahatan global di Asia Pasifik. Pada bulan Maret 2020, ASEAN membentuk *ASEAN Cybercrime Operations Desk* untuk meningkatkan intelijen kejahatan siber dan mengoordinasikan beberapa operasi multiyurisdiksi untuk menargetkan kejahatan siber.

Namun, ketaatan pada koridor *ASEAN Way* dan membangun kerja sama ekstra-regional sepertinya masih meninggalkan banyak

pekerjaan rumah bagi keamanan siber ASEAN, khususnya dalam menghadapi ancaman kejahatan siber (*cybercrime*). Meskipun terdapat capaian yang semakin banyak di Asia Tenggara berkenaan dengan penanggulangan kejahatan siber, masih terdapat tantangan bagi respons regional yang kolektif dan holistik menghadapi kejahatan siber. Pertama, sejumlah pemerintahan di negara-negara Asia Tenggara belum melihat kejahatan siber sebagai ancaman keamanan (Walsh, 2017).

Kesenjangan dalam perspektif ancaman kejahatan siber berkaitan dengan kesenjangan yang mencolok dalam hal kematangan digital di antara negara-negara anggota ditambah perbedaan prioritas keamanan siber sebagai isu keamanan nasional, secara keseluruhan menurunkan kedalaman implementasi kebijakan-kebijakan keamanan siber regional yang telah diambil (Heinl, 2017). Sebagai contoh, persengketaan di Laut China Selatan telah lama memiliki dimensi siber yang bermanifestasi sebagai spionase atau pencurian informasi di ruang siber, tapi insiden ini tidak pernah dipertimbangkan sebagai insiden keamanan siber dan diperlakukan secara terisolasi dari keseluruhan lanskap keamanan siber (Manantan, 2021). Hal ini memunculkan keraguan di sebagian kalangan terhadap kemampuan ASEAN untuk memenuhi komitmen keamanan siber-nya, terutama karena kemampuan ASEAN menjaga konsolidasi politik di tengah persaingan geopolitik semakin tampak terbatasi.

Dua prioritas ancaman terhadap data di ruang siber adalah konten informasi digital yang mengakibatkan instabilitas politik-keamanan karena ketidaksesuaian dengan diskursus ideologis dominan dan kejahatan siber yang dilakukan aktor-aktor disruptif yang mengancam integritas, aksesibilitas, dan kerahasiaan data. ASEAN menganggap keduanya sama penting. Namun kenyataannya, fokus yang timpang ke salah satu ancaman akan membuat investasi yang kurang pada ancaman yang lain. Indonesia adalah contoh negara dengan prioritas keamanan siber yang masih berkisar pada pengendalian konten informasi digital atau ujaran, keberlangsungan ekonomi digital, dan digitalisasi sektor-sektor masyarakat; sehingga ruang perhatian untuk keamanan jaringan dan data menjadi sempit. Di tahun 2021,

Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa dari 1.261 notifikasi celah keamanan yang mereka kirimkan kepada institusi pemerintah dan lembaga-lembaga pengelola data lain, hanya 72 notifikasi atau 6% yang mendapat tindak lanjut (Yahya & Arbi, 2022). Kemampuan yang rendah dalam merespons kerawanan ini menunjukkan ketiadaan dorongan struktural dari lembaga-lembaga pengelola data untuk menjaga keamanan jaringan dengan serius. Ini kontras berbeda dengan China misalnya, yang menerapkan denda hingga 500.000 yuan bagi lembaga yang mengalami serangan siber yang mengakibatkan kerusakan, kebocoran, atau hilangnya akses terhadap data (Heinl, 2017).

Keberagaman dalam prioritas keamanan siber nasional merupakan fungsi dari tingkat sumber daya finansial dan manusia yang tersedia dari masing-masing negara dan tingkat kemauan politik yang menentukan ambisi dan prioritas di ruang siber. Ada negara yang mau fokus mengupayakan perlindungan infrastruktur informasi vital dan kerangka regulasi, tapi ada pula negara yang lebih memprioritaskan industri digital dalam negerinya dan membangun matra siber untuk angkatan bersenjata. Kunci kesepakatan adalah mencari prioritas bersama, misalnya menanggulangi kejahatan siber yang juga telah menjadi agenda *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC).

Prinsip *ASEAN Way* lain yang juga dapat menjadi tantangan adalah musyawarah dan mufakat, karena prinsip ini dapat mendorong negara anggota untuk menyepakati norma dan aturan demi tercapainya konsensus tanpa pemahaman utuh dari norma tersebut. Lebih mengkhawatirkan dari itu, di tengah karakteristik ruang siber yang ditandai dengan anonimitas pelaku serangan siber, konsensus dapat dihasilkan oleh ketidakjujuran intensi. Hal ini berpotensi terjadi, mengingat negara seperti Vietnam masih sering menjadi sponsor serangan siber di Asia Tenggara. Vietnam sebagai salah satu anggota ASEAN melalui APT32 telah melakukan berbagai macam serangan siber ke negara lain, seperti Australia, Bangladesh, Tiongkok, Denmark, Jerman, India, Iran, Jepang, Nepal, Belanda, Korea Selatan,

Inggris, AS, termasuk di antaranya negara-negara anggota ASEAN, yakni Kamboja, Brunei Darussalam, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, dan Thailand (ETDA, 2022). Integritas dari norma dan aturan apa pun di level regional akan bergantung pada implementasi dan penerjemahannya menjadi aturan di tingkat nasional.

F. Penutup

Rivalitas AS-China di ruang siber menjangkau hingga ruang siber Asia Tenggara dalam dua manifestasi penting. Pertama adalah karakteristik kompetitif dari ruang siber Indo-Pasifik yang terbentuk oleh rivalitas ini. Upaya AS untuk membendung penguasaan ekonomi-politik China atas teknologi digital, sebagai respons terhadap upaya China mencuri informasi rahasia dari perusahaan-perusahaan teknologi AS diikuti dengan tindakan-tindakan spionase yang serupa di Asia Tenggara. Ragam bentuk spionase atau pencurian informasi lewat *phising email* maupun penyadapan digital dilakukan oleh kelompok-kelompok peretas maupun negara yang mengindikasikan keterlibatan China maupun AS dan aliansinya. Namun, Asia Tenggara secara umum telah menyaksikan peningkatan risiko serangan siber dengan pelaku serangan negara lain maupun dari dalam negeri, suatu risiko yang meningkat sebagai hasil dari kombinasi dari laju transformasi digital yang cepat yang tidak diimbangi dengan komitmen untuk membangun kemampuan pencegahan, deteksi, dan pemulihan dari serangan siber serta perlindungan data dan sistem komunikasi digital.

Implikasi kedua dari rivalitas ini adalah fragmentasi antarnegara Asia Tenggara dalam hal tata kelola keamanan siber, yang terderivasikan dari perbedaan preferensi China dan Rusia yang mengedepankan peranan kuat pemerintah negara berdaulat dalam pengendalian informasi digital dan penanganan kejahatan siber dan preferensi tata kelola AS yang mengedepankan pentingnya kemitraan pemerintah dan swasta dalam mengelola data pribadi, kebebasan lalu lintas data lintas yurisdiksi siber, serta penguatan ketahanan infrastruktur dan jaringan digital. Di Asia Tenggara, sebagian besar negara kawasan

mengadopsi peran kuat negara dalam pengendalian konten dan informasi digital dengan pengecualian Filipina. Sebagian negara telah membuat strategi keamanan siber nasional mereka *accessible* bagi dunia internasional, memungkinkan kemitraan keamanan siber yang lebih optimal, tetapi Indonesia, Brunei Darussalam, Laos, Kamboja, dan Myanmar belum mengikuti langkah ini. Perbedaan-perbedaan dalam respons kebijakan ini hadir di atas perbedaan dan kesenjangan kapabilitas keamanan siber sebagaimana direkam oleh indeks GCI, IDI, dan NCSI yang artikel ini sudah tampilkan. Namun secara umum, rivalitas geopolitik—berkombinasi dengan kesenjangan kekuatan digital yang ada—berimplikasi pada absennya standar umum regional yang dapat menjadi referensi keamanan siber, dan keleluasaan negara-negara kawasan untuk melakukan restriksi kebebasan ruang siber dan 'impunitas' lembaga-lembaga yang mengelola dan (semestinya) bertanggungjawab atas keamanan data pribadi.

Menghadapi rivalitas dan fragmentasi model tata kelola ini, ASEAN berusaha membangun "poros"-nya sendiri. ASEAN telah menyepakati sentralitas teknologi digital dan ruang siber bagi inovasi, efisiensi, dan produktivitas bisnis serta kelancaran keseharian hidup warga yang semakin terdigitalisasi (ASEAN, 2021). Membangun arsitektur diplomasi siber global lewat *Cybersecurity Cooperation Strategy 2021–2025* yang menguraikan tentang pendirian *ASEAN Cybersecurity Coordinating Committee* dan operasionalisasi *ASEAN Digital Ministers' Meeting* (ADGMIN). Arsitektur keamanan yang sudah ada di ASEAN, terutama ARF yang memasukkan di dalamnya Jepang, Selandia Baru, Australia, Rusia, India, Korea Selatan, dan bahkan Uni Eropa, juga memfasilitasi ASEAN membangun sentralitas dalam upaya membangun tata kelola keamanan siber Asia Tenggara.

Namun, dalam praktiknya regulasi siber di Asia Tenggara lebih cenderung mengikuti prinsip *multilateralism* karena kedekatan prinsip tersebut dengan nilai-nilai *ASEAN Way*. Keadaan ini mengakibatkan Asia Tenggara belum memiliki kesepakatan yang menyatukan persepsi ancaman terhadap keamanan siber, khususnya dan terutama pada bentuk-bentuk kejahatan siber (*cybercrime*) yang berpotensi menciptakan disrupsi yang berbahaya bagi keselamatan publik

maupun ekonomi nasional, suatu potensi ancaman yang besar di tengah ketimpangan tata kelola siber di antara negara-negara anggota.

Untuk dapat menciptakan *hedging* yang efektif terhadap dampak dari rivalitas AS-China di ruang siber, arsitektur keamanan siber ASEAN perlu mengurangi kesenjangan digital antarnegara-negara di kawasan, mendorong negara-negara anggota untuk merumuskan strategi keamanan siber nasional secara terbuka dan berkala serta menggiatkan pengembangan kapasitas lewat berbagi pengalaman terbaik dalam mendeteksi dini serangan siber dan membangun ketahanan di ruang siber. Hal ini sudah muncul dengan kepemimpinan Singapura sebagai pemimpin dalam kapabilitas keamanan siber di kawasan. Di masa yang akan datang, kolaborasi yang melampaui mitra tradisional dan mengeksplorasi tipe-tipe kerja sama di antara negara-negara dengan pengalaman dan semangat yang sama untuk memajukan solusi-solusi ancaman siber yang diakses sebagai mitra setara.

Diplomasi siber harus dengan dilakukan investasi dan intensitas yang lebih, terutama oleh negara-negara pemimpin di ruang siber termasuk Singapura, Malaysia, dan Indonesia. Aktivisme diplomasi siber di kawasan menjadi penting untuk membangun saling percaya, prediktabilitas, dan stabilitas yang esensial untuk mengurangi kesenjangan digital, mendorong insentif bagi sistem internasional untuk membangun keamanan siber, dan mendorong negara-negara di dunia terlibat dalam diskusi keamanan siber.

Referensi

Ali, H. M. (2021). "Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance. *The Journal of Intelligence, Conflict, and Warfare*, *4*(1), 128–153. doi:https://doi.org/10.21810/jicw.v4i1.2805

ARF. (2012, July 12). 2012 ASEAN Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation on Ensuring Cyber Security [Press release]. https://cil.nus.edu.sg/wp-content/uploads/2020/09/2012-ARF-MFA-Stm-on-Cooperation-in-Cyber-Security.pdf

ASEAN. (2021). *ASEAN Digital Masterplan 2025*. https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

ASEAN. (2022). ASEAN Cyber Security Cooperation Strategy (2021-2025) [Press release]. Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Baezner, M. (2018). *Use of cybertools in regional tensions in southeast asia*. CSS Cyberdefense Hotspot Analyses. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314588/Cyber-Reports-2018-05.pdf?sequence=1&isAllowed=y

Baker, T., & Shortland, A. (2023). Insurance and enterprise: cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *48*(2), 275–299. doi:10.1057/s41288-022-00281-7

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. doi:10.1080/23340460.2017.1414924

Beckley, M., & Brands, H. (2022). *Danger zone: The coming conflict with China*. W. W. Norton and Company.

Brands, H. (2023). *The new makers of modern strategy: From the ancient world to the digital Age*. Princeton University Press.

Cloramidine, F., & Wibisono, A. A. (2024). Global cyber norms subsidiarity (UN GGE and UN OEWG) within ASEAN's Body. *Hasanuddin Journal of Strategic and International Studies (HJSIS)*, *2*(2), 21–37. doi:https://doi.org/10.20956/hjsis.v2i2.35313

CPR. (2021, June 3). Sharppanda: Chinese apt group targets southeast asian government with previoulsy unknown backdoor. https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/

Creemers, R., Dorwart, H., Neville, K., & Schaefer, K. (2022). *Translation. 14th five-year plan for national informatization*. https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-Five-Year-Plan-for-National-Informatization.pdf

CSAS. (2017). *Norms for cybersecurity in Southeast Asia. Policy options for collaborative security in the southeast asian region*. https://ccapac.asia/wp-content/uploads/2022/03/Norms-for-Cybersecurity-in-Southeast-Asia.pdf

Cyfirma. (2023). The changing cyber threat landscape Southeast Asia. https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia/

Cyfirma. (2023, September 8). Singapore and Southeast Asia threat landscape. https://www.cyfirma.com/research/singapore-and-southeast-asia-threat-landscape/

Doshi, R., & Mcguiness, K. (2021). *Huawei meets history: Great powers and telecommunications risk*, *1840–2021*. https://policycommons.net/artifacts/4135986/huawei-meets-history/4944162/

Ensign. (2023). *Cyber threat landscape report july 2023*. https://www.ensigninfosecurity.com/resources/98

ETDA. (2022). Threat group cards: A threat actor encyclopedia. https://apt.etda.or.th/cgi-bin/listgroups.cgi

Fitriani, F., Pareira, C., & Arifin, N. A. (2019). *Towards a resilient regional cyber security: perspectives and challenges in Southeast Asia*. Centre for Strategic and International Studies (CSIS).

Green, J. A. (2015). *Cyber warfare: A multidisciplinary analysis*. Routledge.

GSMA. (2018). *Regional privacy frameworks and cross-border data flows. How ASEAN and APEC can Protect Data and Drive Innovation. September 2018*. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Haripin, M. (2022). *Intelijen dan keamanan nasional di Indonesia pasca-orde baru*. Yayasan Pustaka Obor Indonesia.

Heinl, C. H. (2017). New trends in Chinese foreign policy: The evolving role of cyber. *Asian Security*, *13*(2), 132–147. doi:10.1080/14799855.2017.1286160

Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet. *Journal of Cyber Policy*, *5*(2), 239–264. doi:10.1080/23738871.2020.1805482

Hurel, L. M., Priyandita, G., Basu, A., Tran, B., Vosse, W., & Bareja, M. (2024). Cyber capabilities in the Indo-Pacific: Shared ambitions, different means? *Royal United Services Institute (RUSI) Commentary*.

Interpol. (2021). *Annual report 2021*. Interpol.

ITU. (2021). *Global cybersecurity index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

ITU. (2023). *Measuring digital development. The ICT development index 2023*. https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-2/

Lancelot, J. F. (2020). Cyber-diplomacy: Cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, *4*(4), 240–254. Do i:10.1080/23742917.2020.1798155

Maclellan, K., & Demony, C. (2024, August 6). UK's Starmer vows speedy punishment to quell violent disorder. *Reuters*. https://www.reuters.com/world/uk/uks-starmer-hold-emergency-meeting-riots-intensify-2024-08-05/

Mallick, P. K. (2022). *China in the cyber domain*. Prints Publications Pvt Ltd.

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432–459. doi:10.1080/10357718.2021.1926423

Mengko, D. M. (2022). Intelijen dan Perkembangan Teknologi. In M. Haripin (Ed.), *Intelijen dan Keamanan Nasional di Indonesia Pasca-Orde Baru* (65–90). Yayasan Pustaka Obor Indonesia.

Microsoft. (2022, August 23). Microsoft releases its second edition of Cyber Signals tracking ransomware's new business model. https://news.microsoft.com/apac/2022/08/23/microsoft-releases-its-second-edition-of-cyber-signals-tracking-ransomwares-new-business-model/

Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Simon and Schuster.

Mubah, A. S., Wardahni, A., Ponsela, D. F., & Tsauro, M. A. (2016). Problem dasar kesenjangan digital di Asia Tenggara. *Global Strategis*, *10*(2), 204–220.

Mueller, L. M. (2020). Challenges to ASEAN centrality and hedging in connectivity governance — Regional and National Pressure Points. *Pacific Review*, 1–31. doi:10.1080/09512748.2020.1757741

NCSI. (2023). *National cyber security index 3.0*. https://ega.ee/wp-content/uploads/2023/08/NCSI-3.0_Methodology.pdf

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. Doi:10.1080/01402390.2014.977382

Rosenbach, E., & Chong, S. M. (2019, August). *Governing cyberspace: State control vs. the multistakeholder model*. https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model

Smalley, S. (2024, August 9). UN cybercrime treaty passes in unanimous vote. *The Record*. Retrieved from https://therecord.media/un-cybercrime-treaty-passes-unanimous

Stadnik, I. (2017). What is an international cybersecurity regime and how we can achieve it? *Masaryk University Journal of Law and Technology*, *11*(1), 129–154. doi:https://doi.org/10.5817/MUJLT2017-1-7

Terry, S. M. (2023). The strength of weakness: The Kim dynasty and North Korea's strategy for survival. In H. Brands (Ed.), *The New Makers of Modern Strategy: From the Ancient World to the Digital Age.* (1022–1045). Princeton University Press.

Thomas, N. (2009). Cyber security in East Asia: Governing anarchy. *Asian Security*, *5*(1), 3–23. Doi:10.1080/14799850802611446

Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217–235. Doi: 10.1080/23738871.2018.1487987

UNGA. (2021, July 14). *Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security*. https://digitallibrary.un.org/record/3934214?ln=en&v=pdf#files

Van Raemdonck, N. (2021, May). *Digital dialogue. Cyber Diplomacy in Southeast Asia*. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2ZycxfN1/dd-southeast-asia-nb-fb-nvr-09-05.pdf

Walsh, P. F. (2017). Securing state secrets. In R. Dover, H. Dylan, & M. S. Goodman (Eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (177–193). Palgrave Macmillan UK.

Warf, B., & Fekete, E. (2016). Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, *20*(2), 143–157. doi:10.1080/13562576.2015.1112113

Yahya, A. N., & Arbi, I. A. (2022, September 18). 1.261 notifikasi dikeluarkan sepanjang 2022, BSSN: Bentuk Pencegahan Serangan Siber. *Kompas.com*. https://nasional.kompas.com/read/2022/09/18/08493131/1261-notifikasi-dikeluarkan-sepanjang-2022-bssn-bentuk-pencegahan-serangan