

## Implementasi Kerja Sama Antara Indonesia dan Tiongkok dalam Memperkuat Keamanan Siber Pada Tahun (2021 – 2023)

Mariana Agnes Shafira  
Universitas 17 Agustus 1945 Jakarta  
agnezhafiraa@gmail.com

### ABSTRAK

*Penelitian ini membahas implementasi kerja sama antara Badan Siber dan Sandi Negara (BSSN) dan Cyberspace Administration of China (CAC) Tiongkok dalam memperkuat keamanan siber periode 2021–2023. Latar belakangnya adalah meningkatnya ancaman siber akibat lonjakan penggunaan internet selama pandemi COVID-19. Penelitian menggunakan metode kualitatif deskriptif dengan studi kasus dan analisis literatur, berlandaskan teori kerja sama bilateral. Hasil penelitian menunjukkan kerja sama ini memperkuat kapasitas SDM, regulasi, dan infrastruktur digital melalui alih teknologi. Meski demikian, tantangan muncul terkait ketergantungan teknologi, transparansi data, dan dinamika geopolitik.*

**Kata Kunci :** Keamanan Siber, Kerja Sama Bilateral, BSSN, CAC

### ABSTRACT

*This study examines the implementation of cooperation between Indonesia's National Cyber and Crypto Agency (BSSN) and China's Cyberspace Administration (CAC) in strengthening Cybersecurity during the 2021–2023 period. The background of this research is the increasing cyber threats caused by the surge in internet usage during the COVID-19 pandemic. The study employs a descriptive qualitative method using case studies and literature analysis, grounded in bilateral cooperation theory. The findings show that this cooperation has strengthened human resource capacity, regulations, and digital infrastructure through technology transfer. Nevertheless, challenges have emerged regarding technological dependence, data transparency, and geopolitical dynamics.*

**Keywords:** Cybersecurity, Bilateral Cooperation, BSSN, CAC

### PENDAHULUAN

Pada akhir tahun 2019, tepatnya bulan Desember, dunia diguncang dengan berita kemunculan virus COVID-19 di Kota Wuhan, Tiongkok. Peristiwa ini menimbulkan kepanikan global karena ditakutkan akan menyebar ke berbagai negara. Kekhawatiran tersebut terbukti ketika pada tanggal 2 Maret 2020, Presiden ke-7 Republik Indonesia, Joko Widodo, secara resmi mengumumkan bahwa virus COVID-19 telah memasuki Indonesia dan menginfeksi masyarakat. Sejak saat itu, pemerintah

Indonesia mengambil langkah darurat berupa pembatasan aktivitas masyarakat, termasuk bekerja, belajar, hingga kegiatan sosial lainnya. Fenomena ini kemudian dikenal sebagai pandemi COVID-19 (Warsino, 2021). Pandemi ini membawa dampak besar terhadap hampir seluruh sektor kehidupan, mulai dari kesehatan, ekonomi, pendidikan, hingga sosial budaya. Salah satu dampak paling signifikan adalah percepatan transformasi digital. Kegiatan yang sebelumnya dilakukan secara tatap muka beralih menjadi daring. Aktivitas seperti bekerja, belajar mengajar, berbelanja, hingga interaksi sosial dilakukan secara online. Pola kerja pun berubah, dari sistem tatap muka di kantor menjadi sistem work from home (WFH). Kondisi ini mendorong masyarakat untuk semakin bergantung pada internet sebagai sarana utama dalam menjalankan aktivitas sehari-hari (Pramadhi, Windijarto, & Ma'ruf, 2021).

Beralihnya hampir seluruh aspek kehidupan ke ranah digital berdampak langsung pada peningkatan jumlah pengguna internet. Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat, pada tahun 2020 pengguna internet di Indonesia meningkat menjadi 196,71 juta jiwa, atau sekitar 73,7% dari total populasi (BSSN, 2021). Angka ini naik drastis dari 171 juta pengguna pada tahun 2019 (SAFEnet, 2020). Secara global, pengguna internet mencapai 4,1 miliar jiwa pada tahun yang sama (Takwin, 2020). Peningkatan ini mencerminkan adanya percepatan adopsi teknologi digital, yang di satu sisi menguntungkan karena menunjukkan kemampuan masyarakat dalam beradaptasi dengan perkembangan zaman. Namun, di sisi lain, lonjakan pengguna internet juga meningkatkan kerentanan terhadap ancaman kejahatan siber. Fenomena meningkatnya penggunaan internet ternyata dimanfaatkan oleh pelaku kejahatan siber. Masih banyak masyarakat Indonesia yang awam dengan keamanan digital, sehingga mudah menjadi korban kejahatan daring. Berbagai bentuk kejahatan seperti phishing, ransomware, pencurian identitas, hingga kebocoran data marak terjadi sepanjang tahun 2020. BSSN mencatat Indonesia berada di posisi kedua dari sepuluh negara dengan jumlah serangan siber tertinggi, dengan total mencapai 38,7 juta serangan (BSSN-IHP, 2021). Selain itu, kasus kebocoran data dalam jumlah besar turut terjadi, antara lain 91 juta data pengguna Tokopedia, 1,2 juta data pengguna Bhinneka, hingga 2,3 juta data pemilih dari Komisi Pemilihan Umum (KPU). Kebocoran ini menimbulkan keresahan publik sekaligus memperlihatkan masih lemahnya sistem pertahanan siber nasional.

Selain insiden kebocoran data, BSSN juga melaporkan adanya 495,3 juta anomali trafik sepanjang tahun 2020. Anomali trafik didefinisikan sebagai kejanggalan dalam lalu lintas jaringan yang bisa menjadi tanda awal terjadinya serangan siber. Anomali tertinggi tercatat pada 10 Desember 2020 dengan jumlah 7,3 juta kasus dalam sehari (Asmarani, 2022). Fakta ini menunjukkan bahwa pandemi tidak hanya menguji Indonesia dalam sektor kesehatan dan ekonomi, tetapi juga dalam keamanan siber. Kondisi tersebut menegaskan bahwa keamanan siber harus ditempatkan sebagai salah satu prioritas utama negara. *Cybersecurity* bukan hanya sekadar isu teknis, melainkan menyangkut kedaulatan negara, perlindungan data masyarakat, dan stabilitas nasional. Jika keamanan siber lemah, maka kerahasiaan data negara maupun masyarakat rentan terekspos dan dimanfaatkan pihak-pihak tertentu, baik aktor non-negara maupun negara lain (Permatasari, 2021). Dalam menghadapi kompleksitas ancaman siber, diperlukan strategi yang komprehensif. Di samping memperkuat infrastruktur domestik, kerja sama internasional menjadi langkah strategis yang penting. Indonesia melalui BSSN kemudian menjalin kolaborasi dengan Cyberspace Administration of China (CAC), lembaga yang dikenal memiliki pengalaman luas dalam mengelola keamanan digital. Tiongkok dipandang sebagai mitra potensial karena memiliki kebijakan Great Firewall of China, yang selama ini digunakan untuk mengendalikan arus informasi dan melindungi ruang siber mereka. Kerja sama BSSN dan CAC sendiri bukanlah hal baru.

Pada tahun 2016, Indonesia melalui Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan (Polhukam) pernah menandatangani kerja sama dengan CAC yang mencakup peningkatan kesadaran keamanan siber, penguatan kapasitas, serta riset bersama dalam bidang *cyber forensics*, hukum siber, dan *counter cyber intelligence*. Pengalaman sebelumnya ini menjadi dasar yang memperkuat kepercayaan Indonesia untuk kembali menjalin kerja sama yang lebih fokus melalui BSSN pada tahun 2021. Nota kesepahaman (MoU) ditandatangani pada 12 Januari 2021 dengan ruang lingkup mencakup pelatihan SDM, transfer teknologi, pertukaran informasi, hingga simulasi penanggulangan krisis siber. Selain untuk memperkuat pertahanan siber, kerja sama ini juga dilatarbelakangi oleh kebutuhan Indonesia dalam mempercepat pembangunan infrastruktur digital. Kerja sama internasional merupakan salah satu instrumen kebijakan luar negeri untuk membangun komunikasi, kepercayaan, dan koordinasi antarnegara. (Angreini & Indrawati, 2020) Proyek Palapa Ring yang menjadi tulang punggung jaringan internet nasional masih membutuhkan penguatan dari sisi

keamanan. Dengan adanya kerja sama ini, diharapkan Indonesia dapat mempercepat transformasi digital secara merata, sekaligus meminimalisir risiko ancaman yang semakin kompleks. Meskipun demikian, kerja sama ini tidak terlepas dari tantangan. Beberapa pihak menilai adanya potensi ketergantungan Indonesia pada teknologi Tiongkok, khususnya dalam hal transfer teknologi. Kekhawatiran lainnya adalah terkait isu transparansi data serta implikasi geopolitik, mengingat hubungan Tiongkok dengan negara-negara Barat yang cenderung tegang. Hal ini menuntut pemerintah Indonesia untuk berhati-hati dalam mengelola kerja sama, agar keuntungan yang diperoleh lebih besar daripada risiko yang ditimbulkan.

Berdasarkan dari latar belakang yang telah penulis coba sampaikan, maka adanya rumusan masalah yang ingin diajukan penulis dalam penelitian tugas akhir ini yaitu “Bagaimana Implementasi dalam program kerjasama antara BSSN dengan CAC untuk memperkuat Keamanan Siber pada tahun 2021 – 2023?”

## **TINJAUAN PUSTAKA**

Penelitian ini menggunakan teori Kerja Sama Bilateral dalam paradigma Liberalisme. Paradigma liberal menekankan pentingnya kebebasan dan kemajuan individu serta memandang negara bukanlah aktor tunggal dalam hubungan internasional. Selain negara, aktor non-negara seperti lembaga internasional maupun organisasi dalam suatu negara juga memiliki peran penting dalam dinamika global (Affianty, 2017). Liberalisme beranggapan bahwa negara, layaknya manusia, tidak dapat berdiri sendiri dan membutuhkan kerja sama untuk memenuhi berbagai kebutuhan. Ketergantungan ini mendorong negara untuk menjalin interaksi dalam rangka mencapai kepentingan bersama dan mengatasi hambatan yang muncul dalam kehidupan berbangsa (Septaningtyas, 2005).

### **Kerjasama Bilateral**

Teori yang digunakan dalam penelitian ini adalah Kerja Sama Bilateral dengan paradigma Liberalisme, yang menekankan kebebasan, kemajuan individu, serta dorongan bagi negara untuk saling bekerja sama demi mencapai kepentingan bersama (Septaningtyas, 2005). Menurut liberalisme, aktor dalam hubungan internasional tidak hanya negara, tetapi juga lembaga non-negara (Affianty, 2017). Kerja sama bilateral merupakan salah satu bentuk kerja sama internasional yang penting di era globalisasi, di mana dua negara saling bergantung untuk memenuhi kebutuhan ekonomi, politik,

maupun keamanan (Bagaskara, 2018; Andre, 2021). Negara, seperti manusia, tidak dapat berdiri sendiri sehingga membutuhkan hubungan timbal balik dengan negara lain untuk menghadapi persoalan nasional, regional, maupun global.

Jenis kerja sama internasional dapat dibedakan menjadi bilateral, regional, dan multilateral (A. S. Putri, 2022). Penelitian ini berfokus pada kerja sama bilateral, karena pembahasan terkait hubungan dua lembaga negara dalam bidang keamanan siber. Indikator utama efektivitas kerja sama bilateral mencakup: tujuan bersama (Keohane, 2016), komunikasi intensif (Keohane & Nye, 2019), transfer teknologi/pengetahuan (Rovira, 2018), implementasi nyata kebijakan (Hollis, 1991), serta keberlanjutan kerja sama (Wendt, 1992). Pola interaksi bilateral dapat berupa kebijakan aktual, persepsi, hingga respon kedua belah pihak, yang menghasilkan kerja sama, persaingan, maupun konflik (Affianty, 2017). Kerja sama bilateral pada dasarnya dilandasi oleh ketergantungan antarnegara dan dapat mencakup bidang politik, ekonomi, sosial-budaya, pertahanan, hingga keamanan. Tujuan utamanya adalah menciptakan perdamaian, menghormati hak serta kedaulatan masing-masing negara, dan memberikan nilai tambah yang saling menguntungkan (Amalia, 2018).

## **PEMBAHASAN**

### **Gambaran Hubungan Negara Indonesia Dengan Tiongkok**

Hubungan Indonesia–Tiongkok mengalami perkembangan pesat sejak dibukanya hubungan diplomatik pada 1950. Walaupun sempat terputus pada 1967 akibat dinamika politik domestik Indonesia, hubungan ini kembali dipulihkan pada 1990 dan sejak itu terus menunjukkan tren positif menuju kemitraan strategis komprehensif (Haykal, 2020). Dalam bidang ekonomi, Tiongkok telah menjadi mitra dagang terbesar Indonesia hampir dua dekade terakhir, dengan kerja sama besar pada perdagangan, investasi, serta pembangunan infrastruktur, seperti proyek Kereta Cepat Jakarta–Bandung, kawasan industri, hingga pelabuhan strategis melalui inisiatif Belt and Road (BRI). Kerja sama juga diperluas ke sektor energi, pertanian, teknologi, ekonomi digital, dan program pengurangan kemiskinan. Selain itu, hubungan sosial-budaya diperkuat lewat pertukaran pelajar, beasiswa, dan kolaborasi akademik yang mendorong kedekatan antar masyarakat kedua negara.

Meski demikian, hubungan Indonesia–Tiongkok menghadapi tantangan, terutama terkait isu Laut Tiongkok Selatan. Indonesia menegaskan pentingnya

kedaulatan nasional dan hukum internasional, namun tetap mengedepankan dialog damai dan diplomasi (Utomo, 2017). Komitmen ini ditegaskan kembali pada April 2025 dalam pertemuan Presiden Xi Jinping dan Presiden Prabowo Subianto, yang menyepakati penguatan kerja sama di berbagai sektor strategis demi masa depan yang saling menguntungkan. Dalam bidang keamanan siber, sebelum menjalin kerja sama dengan Tiongkok, Indonesia berada pada kondisi rentan. Lemahnya infrastruktur teknologi, keterbatasan sumber daya manusia, rendahnya koordinasi antar lembaga, serta minimnya kesadaran publik menyebabkan Indonesia kerap menjadi target serangan siber, seperti kebocoran data, peretasan situs pemerintah, hingga ransomware yang menyerang institusi publik dan swasta (Chotimah, 2019). Kondisi ini mendorong Indonesia membuka peluang kerja sama internasional untuk memperkuat sistem pertahanan digital melalui alih teknologi, pelatihan, dan pengembangan infrastruktur siber yang lebih modern. Sementara itu, Tiongkok telah membangun ekosistem keamanan siber yang kuat dengan regulasi ketat, antara lain *Cybersecurity Law* (CSL), *Data Security Law* (DSL), dan *Personal Information Protection Law* (PIPL) (Indonesia, 2021). Negara ini juga memiliki kapabilitas siber ofensif, dengan kelompok peretas seperti Mustang Panda yang pernah dikaitkan dengan serangan terhadap kementerian dan lembaga Indonesia. Walaupun ada dinamika sensitif di bidang ini, kerja sama Indonesia–Tiongkok dalam keamanan siber mencerminkan upaya bersama untuk menghadapi tantangan ruang digital sekaligus memperkuat kepercayaan strategis kedua negara.

### **Bentuk Kerjasama BSSN dengan CAC**

Kerja sama bilateral Indonesia–Tiongkok dalam bidang keamanan siber secara resmi dimulai dengan penandatanganan *Memorandum of Understanding* (MoU) antara Badan Siber dan Sandi Negara (BSSN) Republik Indonesia dan *Cyberspace Administration of China* (CAC) pada 12 Januari 2021 di Simalungun. Perjanjian ini berlaku selama tiga tahun (2021–2023) dan lahir dari kesadaran bersama atas meningkatnya ancaman kejahatan siber baik di tingkat domestik maupun internasional, yang semakin kompleks terutama pada masa pandemi Covid-19 (BSSN & CAC, 2021). Melalui MoU ini, kedua negara berkomitmen memperkuat pertukaran informasi, berbagi teknologi, dan meningkatkan kapasitas pertahanan digital sebagai bentuk respons terhadap kerentanan yang dihadapi masing-masing pihak.

MoU tersebut memuat tujuh bidang kerja sama strategis. Pertama, pertukaran

informasi mengenai regulasi, hukum, dan tata kelola ruang siber. Kedua, berbagi pengalaman dan praktik terbaik terkait perlindungan infrastruktur informasi vital dan respons terhadap ancaman siber. Ketiga, memfasilitasi dialog multi-pihak yang melibatkan pemerintah, akademisi, industri, dan pemangku kepentingan lainnya guna membangun rasa saling percaya. Keempat, mendorong kunjungan pakar keamanan siber melalui forum akademik, konferensi, simposium, dan seminar. Kelima, menyediakan program pelatihan bersama terkait teknologi pertahanan siber. Keenam, mengembangkan kapasitas di bidang perlindungan data pribadi, manajemen keamanan data, dan respons ancaman. Ketujuh, membuka peluang kerja sama tambahan yang dapat disepakati bersama sesuai kebutuhan.

Selain fokus pada aspek teknis, MoU ini juga menegaskan komitmen kedua negara untuk mendorong pembentukan tata kelola internet internasional yang bersifat multilateral, demokratis, transparan, dan aman. Dengan demikian, kerja sama ini tidak hanya berorientasi pada penguatan kapasitas pertahanan digital, tetapi juga pada pembangunan ruang siber global yang damai, terbuka, dan bertanggung jawab. Perjanjian ini dapat diperpanjang setelah tiga tahun pertama, dengan jaminan bahwa kerahasiaan informasi dan teknologi yang telah dipertukarkan tetap dijaga meskipun kerja sama berakhir.

Secara keseluruhan, MoU BSSN–CAC mencerminkan keseriusan Indonesia dan Tiongkok dalam memperkuat hubungan bilateral di bidang keamanan siber. Kesepakatan ini menjadi langkah penting dalam membangun kepercayaan strategis, memperkuat kerja sama teknis, serta menghadapi ancaman kejahatan digital yang semakin kompleks. Di sisi lain, keberadaan kerangka hukum formal ini juga menjadi landasan bagi keberlanjutan kerja sama di masa mendatang, dengan tujuan akhir mewujudkan ruang siber yang lebih aman dan tertib di tingkat nasional maupun internasional.

### **1. Pertukaran Informasi Dan Dialog Awal**

Kerja sama Badan Siber dan Sandi Negara (BSSN) dengan Cyberspace Administration of China (CAC) resmi dimulai pada 12 Januari 2021 melalui penandatanganan MoU dengan jangka waktu tiga tahun. Pada tahap awal, kedua lembaga menitikberatkan pada pertukaran informasi dasar serta penyelarasan pemahaman terkait regulasi dan kebijakan keamanan siber yang berlaku di masing-masing negara. Pertukaran ini dilakukan melalui mekanisme konferensi virtual dan

pertemuan bilateral yang membahas kerangka regulasi, prioritas keamanan siber, serta strategi yang akan dijalankan dalam implementasi kerja sama (BSSN & CAC, 2021).

Pertukaran informasi dasar yang dilakukan mencakup kebijakan, regulasi, dan prosedur perlindungan ruang siber, termasuk aturan mengenai perlindungan data pribadi, keamanan infrastruktur kritis, dan mekanisme tanggap darurat terhadap insiden siber. Melalui proses ini, kedua negara dapat saling memahami pendekatan yang digunakan mitra mereka dalam menghadapi ancaman digital. Hal ini juga membantu menyusun kerangka kebijakan yang lebih harmonis dan kompatibel sehingga dapat meningkatkan efektivitas kerja sama bilateral di bidang keamanan siber.

Dialog awal juga membahas prioritas keamanan siber masing-masing negara. Indonesia menekankan kebutuhan untuk memperkuat perlindungan data dan penguatan sistem digital nasional, sedangkan Tiongkok lebih memfokuskan pada pengamanan infrastruktur, khususnya terkait implementasi dan perluasan jaringan 5G. Dengan berbagi prioritas ini, kedua negara dapat menyusun strategi kerja sama yang lebih terarah, termasuk perencanaan program pelatihan, workshop, dan pertukaran ahli keamanan siber. Selain itu, pembentukan mekanisme koordinasi juga menjadi bagian penting dari tahap awal kerja sama. Kedua negara menunjuk koordinator yang bertugas memantau jalannya pertukaran informasi, mengelola kegiatan, serta memastikan bahwa rencana yang disepakati dapat terlaksana dengan baik sesuai jadwal. Forum virtual dan pertemuan bilateral yang dilaksanakan turut membuka ruang bagi diskusi kasus nyata dan berbagi pengalaman dalam menangani serangan siber, sehingga memungkinkan masing-masing pihak belajar dari praktik terbaik yang telah diterapkan.

Dialog awal ini juga mengidentifikasi berbagai tantangan yang mungkin muncul selama implementasi kerja sama, seperti perbedaan kebijakan, kendala teknis, hingga hambatan koordinasi. Dengan mengantisipasi tantangan sejak awal, BSSN dan CAC dapat menyiapkan strategi mitigasi agar kerja sama tetap berjalan efektif. Untuk itu, ditetapkan pula indikator keberhasilan yang dapat digunakan untuk mengevaluasi capaian, antara lain efektivitas pertukaran informasi, keberhasilan pelatihan, dan dampak dari program yang dijalankan. Secara keseluruhan, tahap awal kerja sama ini menjadi fondasi penting bagi pembangunan kepercayaan dan

transparansi antara kedua negara. Mengingat isu keamanan siber merupakan isu sensitif dan rentan menimbulkan kecurigaan, adanya komunikasi yang terbuka dan berbasis kepercayaan menjadi kunci keberhasilan kerja sama. Pertukaran informasi yang dilakukan tidak hanya memperkuat rasa saling percaya, tetapi juga membuka jalan bagi kegiatan lanjutan, seperti kunjungan delegasi BSSN ke kantor CAC di Tiongkok serta pelaksanaan workshop bersama yang melibatkan berbagai ahli keamanan siber pada triwulan pertama tahun 2021.

Dengan demikian, tahap awal kerja sama BSSN–CAC tidak hanya berfungsi sebagai sarana pengenalan kebijakan dan regulasi, tetapi juga sebagai pondasi untuk mengembangkan strategi bersama dalam menghadapi ancaman siber yang semakin kompleks. Proses ini sekaligus memperlihatkan bahwa hubungan bilateral di bidang keamanan siber antara Indonesia dan Tiongkok dibangun secara bertahap melalui pertukaran informasi, penyelarasan regulasi, dan pembentukan kepercayaan yang menjadi dasar keberlanjutan kerja sama ke depan.

## **2. Kunjungan Delegasi Dan Workshop**

Pada triwulan pertama tahun 2021, kerja sama Indonesia–Tiongkok di bidang keamanan siber memasuki fase penting dengan dilaksanakannya pertemuan tatap muka pertama antara Badan Siber dan Sandi Negara (BSSN) dengan Cyberspace Administration of China (CAC). Delegasi BSSN yang terdiri dari pejabat tinggi serta para ahli keamanan siber berkunjung langsung ke Tiongkok, yang menjadi tonggak awal bagi kedua negara dalam memperkuat koordinasi menghadapi ancaman siber yang semakin kompleks (BSSN & CAC, 2021). Kunjungan ini tidak hanya bersifat simbolis, tetapi juga memiliki makna strategis karena memperlihatkan komitmen nyata kedua negara untuk membangun mekanisme kerja sama jangka panjang dalam bidang yang krusial. Sebagai bagian dari kunjungan, kedua lembaga menyelenggarakan workshop yang menghadirkan para ahli keamanan siber dari BSSN dan CAC. Workshop ini menjadi forum penting untuk membahas tren ancaman siber terbaru, seperti ransomware, malware canggih, serangan phishing, hingga ancaman terhadap infrastruktur digital.

Melalui diskusi terbuka, kedua pihak saling bertukar pengalaman, berbagi teknik mitigasi, serta mendiskusikan solusi praktis yang dapat diimplementasikan. Forum ini tidak hanya meningkatkan pemahaman teknis, tetapi juga memperluas jejaring profesional antara pakar keamanan siber Indonesia dan Tiongkok, yang ke

depannya dapat memperkuat koordinasi lintas batas. Hasil dari pertemuan tersebut memperlihatkan beberapa poin penting. Pertama, BSSN memperoleh wawasan mendalam mengenai kebijakan dan pendekatan CAC dalam mengelola keamanan siber, termasuk regulasi yang ketat, pemanfaatan big data, penerapan kecerdasan buatan, serta manajemen infrastruktur digital. Kedua, kedua pihak berhasil memetakan potensi kerja sama teknis di masa depan, seperti transfer teknologi, pengembangan sistem deteksi dini serangan siber, pembangunan pusat pelatihan bersama, hingga peningkatan kapasitas sumber daya manusia melalui program pelatihan teknis.

Lebih lanjut, CAC juga memberikan rekomendasi terkait praktik terbaik dalam penanganan insiden siber. Misalnya, kewajiban operator jaringan untuk melaporkan setiap insiden sesuai tingkat keparahan, penyusunan rencana tanggap darurat, serta pelatihan berkala guna meningkatkan kesiapsiagaan. Selain itu, peningkatan kesadaran keamanan siber di tingkat individu maupun organisasi dianggap penting untuk mengurangi risiko human error yang kerap dimanfaatkan pelaku kejahatan siber. Langkah-langkah ini menunjukkan bahwa kerja sama tidak hanya difokuskan pada aspek teknologi, tetapi juga pada penguatan budaya keamanan siber di masyarakat. Dengan demikian, pertemuan tatap muka BSSN dan CAC pada 2021 dapat dipandang sebagai pijakan penting dalam membangun kerja sama bilateral yang lebih konkret di bidang keamanan siber. Kolaborasi ini tidak hanya memperkuat hubungan diplomatik kedua negara, tetapi juga memberikan kontribusi langsung pada peningkatan kapasitas pertahanan digital Indonesia. Ke depan, kerja sama ini berpotensi berkembang menjadi kemitraan strategis yang mencakup transfer teknologi, peningkatan kualitas SDM, serta pembentukan standar bersama dalam menghadapi ancaman siber global.

### **3. Program Pelatihan BSSN dengan CAC**

Pada tahun 2022, kerja sama antara BSSN dan CAC memasuki tahap baru dengan penyelenggaraan program pelatihan bersama setelah adanya pelonggaran pembatasan akibat pandemi Covid-19. Program pelatihan ini dirancang untuk memperkuat kapasitas kedua negara dalam menghadapi ancaman siber melalui kursus intensif yang dapat mencakup teknologi pertahanan siber terbaru. Pelatihan dilaksanakan secara bergiliran di negara Indonesia dan Tiongkok, sehingga dapat memungkinkan para peserta dari kedua negara untuk memperoleh keterampilan

yang praktis dan pengetahuan mendalam dalam bidang keamanan siber (BSSN & CAC, 2022). dengan materi meliputi :

- Teknik Enkripsi

Enkripsi merupakan salah satu teknik fundamental dalam keamanan siber yang berfungsi untuk mengubah data atau informasi penting milik negara menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dengan penerapan enkripsi, kerahasiaan data dapat terjaga karena hanya pihak yang memiliki kunci dekripsi yang dapat mengakses informasi tersebut. Hal ini berperan penting dalam mencegah serta meminimalisasi tindak kejahatan siber, khususnya pencurian data dan penyadapan komunikasi, sehingga informasi strategis negara maupun individu tetap terlindungi.

- Deteksi Intrusi

Deteksi intrusi adalah mekanisme yang digunakan untuk mengidentifikasi, memantau, dan menganalisis aktivitas yang tidak sah atau mencurigakan dalam suatu jaringan atau sistem komputer. Sistem ini memungkinkan adanya peringatan dini apabila terjadi serangan siber, sehingga dapat dilakukan tindakan pengamanan secara cepat. Terdapat dua jenis sistem deteksi intrusi. Pertama, Network-based Intrusion Detection System (NIDS) yang bekerja dengan memantau lalu lintas data pada titik-titik utama jaringan untuk mendeteksi pola akses yang berpotensi berbahaya. Kedua, Host-based Intrusion Detection System (HIDS) yang memfokuskan pemeriksaan pada file sistem operasi, log aplikasi, serta aktivitas tingkat host guna mengidentifikasi perilaku mencurigakan pada perangkat tertentu. Dengan adanya sistem deteksi intrusi, negara dapat meningkatkan kemampuan deteksi dini serta memperkecil risiko kerusakan akibat serangan siber.

- Manajemen Risiko

Manajemen risiko dalam konteks keamanan siber merupakan suatu proses sistematis yang mencakup identifikasi potensi ancaman, analisis tingkat risiko, serta penentuan strategi mitigasi yang tepat. Proses ini dimulai dengan mengidentifikasi kerentanan yang mungkin dieksploitasi oleh pihak tidak bertanggung jawab. Selanjutnya dilakukan analisis untuk menilai kemungkinan terjadinya serangan dan potensi dampak yang ditimbulkan. Berdasarkan hasil analisis tersebut, strategi mitigasi dirancang guna meminimalkan risiko. Strategi

ini kemudian harus diawasi secara berkelanjutan dan disesuaikan dengan perkembangan ancaman yang terus berubah. Dengan manajemen risiko yang efektif, organisasi maupun negara dapat memastikan kesiapan menghadapi potensi serangan siber serta menjaga keberlangsungan operasional digital.

- Respons Insiden

Respons insiden merupakan langkah penanganan yang dilakukan ketika suatu sistem atau jaringan mengalami serangan siber. Proses ini bertujuan untuk mengurangi dampak serangan, memulihkan sistem ke kondisi normal, serta mencegah kejadian serupa di masa mendatang. Tahapan respons insiden mencakup identifikasi insiden untuk memastikan adanya serangan, pengendalian dengan cara mengisolasi serangan agar tidak menyebar lebih luas, pemulihan sistem sehingga dapat kembali berfungsi normal, serta evaluasi menyeluruh guna mengidentifikasi penyebab serangan. Evaluasi ini penting untuk memperbaiki kelemahan sistem serta meningkatkan strategi keamanan yang sudah diterapkan. Dengan adanya mekanisme respons insiden yang sistematis, sebuah negara dapat menjaga ketahanan siber sekaligus meningkatkan kepercayaan publik terhadap keamanan infrastruktur digital.

Peserta dari Indonesia memperoleh pengalaman langsung dari pakar siber Tiongkok, sementara peserta dari Tiongkok mempelajari pendekatan yang diterapkan di Indonesia. Pertukaran instruktur dan materi pelatihan memastikan adanya transfer teknologi, perspektif berbeda, serta peningkatan standar pelatihan sesuai praktik internasional. Program ini juga melibatkan simulasi serangan siber, latihan respons insiden, proyek kolaboratif, dan diskusi kelompok, yang membantu peserta mengembangkan keterampilan teknis sekaligus jejaring profesional.

Selain aspek teknis, pertemuan bilateral dalam rangkaian pelatihan ini juga membahas kebijakan, regulasi, serta adopsi standar tata kelola ruang siber yang baik. Fokus lainnya adalah peningkatan kesadaran publik melalui penyuluhan keamanan siber. Evaluasi dan tindak lanjut dilakukan secara rutin untuk memastikan kualitas pelatihan. Dampak program ini cukup signifikan. Hasil pelatihan memperkuat kemampuan BSSN dalam mendeteksi dan merespons insiden, sekaligus membuka akses terhadap pengalaman Tiongkok dalam membangun sistem keamanan siber berskala besar. Secara praktis, kerja sama ini

berkontribusi pada penurunan jumlah kasus kejahatan siber di Indonesia, dari 4.860 kasus pada 2022 menjadi 3.758 kasus pada 2023, atau turun sebesar 22,11% (Tribrata Polri, 2023).

#### **4. Pengembangan Teknologi Dan Infrastruktur**

Pada pertengahan tahun 2022, kerja sama antara Indonesia dan Tiongkok di bidang keamanan siber memasuki tahap baru dengan fokus pada pengembangan serta implementasi teknologi canggih untuk memperkuat ketahanan siber nasional (BSSN & CAC, 2022). Program ini meliputi pemasangan sistem deteksi ancaman siber di berbagai infrastruktur kritis Indonesia, seperti pusat data, jaringan komunikasi, dan fasilitas pemerintah. Sistem tersebut memungkinkan pemantauan aktivitas jaringan secara real-time, memberikan peringatan dini, serta mempercepat respons terhadap serangan. Implementasi dilakukan bersama tim ahli dari kedua negara dengan penyesuaian sesuai standar internasional.

Selain teknologi, kerja sama ini juga mencakup pelatihan staf lokal, evaluasi berkala melalui simulasi serangan, serta penyusunan kebijakan dan prosedur keamanan siber untuk mendukung efektivitas sistem. Langkah ini menjadi bagian dari strategi nasional Indonesia dalam membangun pertahanan digital yang tangguh terhadap ancaman yang semakin kompleks.

Hasil penting dari fase kerja sama ini adalah pembentukan Computer Security Incident Response Team (CSIRT) di bawah koordinasi BSSN. CSIRT berfungsi menangani insiden, mengurangi dampak serangan, memulihkan sistem, memberikan pelatihan dan sertifikasi, serta menyusun kebijakan keamanan internal (Azhar, 2024). CSIRT terbagi menjadi tiga kategori, yakni Gov-CSIRT untuk instansi pemerintah, Sectoral-CSIRT untuk sektor strategis, dan Enterprise-CSIRT untuk perusahaan swasta, BUMN, maupun lembaga pendidikan.

Implementasi CSIRT telah mendorong pembentukan tim serupa di berbagai kementerian dan lembaga, bahkan PT INTI (Persero) menjadi BUMN pertama yang memperoleh sertifikasi CSIRT dari BSSN. Dengan langkah ini, tujuan akhir BSSN adalah mewujudkan ekosistem keamanan siber nasional yang terintegrasi, cepat tanggap, serta proaktif dalam melindungi data dan infrastruktur kritikal, sehingga Indonesia lebih mandiri dan tangguh dalam menghadapi tantangan digital (Azhar, 2024).

#### **5. Ekspansi Kerjasama Dan Kolaborasi Internasional**

Pada tahun 2023, kerja sama Badan Siber dan Sandi Negara (BSSN) dengan Cyberspace Administration of China (CAC) memasuki tahap ekspansi dan kolaborasi yang lebih luas. Bentuk implementasi kerja sama ini tercermin melalui kunjungan delegasi BSSN dan CAC ke Tsinghua Southeast Asia Center di Bali, serta ke Institut Teknologi Bandung (ITB) dan STIKOM Bali. Kegiatan ini bertujuan untuk memperkuat jejaring akademik, pendidikan, dan pelatihan dalam bidang keamanan siber, sekaligus mempromosikan pengembangan kapasitas dan penyediaan talenta digital. Dalam kesempatan tersebut, BSSN menegaskan bahwa akademisi memiliki peran penting dalam ekosistem keamanan siber Indonesia, sedangkan pihak STIKOM Bali menekankan harapan agar kerja sama dapat terus berlanjut dan memberikan manfaat bagi kedua negara maupun lembaga pendidikan tinggi.

Selain memperkuat hubungan bilateral, kerja sama ini juga memberi BSSN akses terhadap teknologi keamanan siber terkini serta data ancaman global dari perusahaan internasional seperti Microsoft dan IBM. Kolaborasi ini diharapkan dapat meningkatkan kemampuan deteksi dini serangan siber serta mendukung pembangunan infrastruktur digital yang lebih aman dan tangguh. Implementasi kerja sama Indonesia–Tiongkok dalam periode 2021–2023 mencakup beberapa aspek, mulai dari pertukaran informasi, dialog antar lembaga, kunjungan delegasi, program pelatihan, hingga pengembangan kapasitas dalam perlindungan infrastruktur vital dan keamanan data.

Prinsip utama dari Memorandum of Understanding (MoU) yang ditandatangani kedua belah pihak menekankan pentingnya memperkuat hubungan bilateral di bidang keamanan siber dengan tetap menjunjung tinggi prinsip kedaulatan negara, integritas wilayah, dan non-intervensi. MoU ini juga mendorong pembentukan tata kelola internet internasional yang multilateral, demokratis, dan transparan, serta pengembangan ruang siber yang damai, aman, terbuka, kooperatif, dan bertanggung jawab. Pertukaran informasi meliputi regulasi tata kelola ruang siber, kebijakan perlindungan data, hingga praktik terbaik dalam merespons ancaman siber. Sementara itu, dialog akademik dan industri diwujudkan dalam bentuk konferensi, seminar, dan simposium, dengan tujuan membangun rasa saling percaya dan memperkuat kerja sama di bidang keamanan data.

Secara keseluruhan, kerja sama BSSN dan CAC dalam periode 2021–2023

menunjukkan komitmen kuat kedua negara dalam memperkuat kapasitas keamanan siber dan memajukan teknologi informasi. Implementasi MoU tidak hanya mempererat hubungan bilateral, tetapi juga berkontribusi pada pembangunan kapasitas keamanan siber yang lebih baik. Dengan adanya kolaborasi ini, baik Indonesia maupun Tiongkok berharap kerja sama dapat terus berlanjut dan memberikan dampak positif, tidak hanya bagi kepentingan nasional masing-masing, tetapi juga bagi penguatan ekosistem keamanan siber di tingkat internasional.

## **KESIMPULAN**

Berdasarkan hasil penelitian yang dilakukan penulis mengenai kerja sama keamanan siber antara Indonesia melalui Badan Siber dan Sandi Negara (BSSN) dengan Cyberspace Administration of China (CAC) pada periode 2021–2023, dapat disimpulkan bahwa kerja sama tersebut merupakan upaya nyata dalam memperkuat ketahanan siber nasional Indonesia di tengah meningkatnya ancaman siber akibat digitalisasi yang masif selama pandemi COVID-19. Melalui berbagai program, seperti pelatihan, workshop, pertukaran informasi, dan transfer teknologi, kerja sama ini telah berkontribusi pada peningkatan kapasitas sumber daya manusia serta penguatan infrastruktur digital di Indonesia.

Meskipun memberikan banyak manfaat, kerja sama ini juga menghadirkan sejumlah tantangan, antara lain potensi ketergantungan terhadap teknologi asing, isu transparansi data, serta dinamika geopolitik global yang terus berkembang. Oleh karena itu, meskipun kontribusinya signifikan dalam mendukung ketahanan siber nasional, kerja sama ini tetap perlu disertai evaluasi kebijakan dan penguatan regulasi agar Indonesia dapat menjaga kedaulatan data sekaligus memastikan kemandirian teknologi di masa mendatang.

## **DAFTAR PUSTAKA**

- A Wendt. (1992). Anarchy Is What States Make of It. In *Conflict After the Cold War* (pp. 224–245). <https://doi.org/10.4324/9781315664484-30>
- Affianty, D. (2017). Pengantar Ilmu Hubungan Internasional. [https://repository.umj.ac.id/8535/1/DIKTAT-Pengantar Hubungan Internasional.pdf](https://repository.umj.ac.id/8535/1/DIKTAT-Pengantar+Hubungan+Internasional.pdf)
- Amalia, R. (2018). Kerja Sama Maritim Indonesia-Tiongkok Menuju Visi Indonesia Sebagai Poros Maritim Dunia. *EJournal Ilmu Hubungan Internasional*, 6(3),

- 1271–1280.
- Andre, A. (2021). Kerja Sama Internasional: Pengertian, Tujuan, Manfaat, Bentuk dan Contoh. In *Gramedia Blog* (Vol. 02, Issue 02, pp. 41–46).
- Angreini, Y., & Indrawati. (2020). Diplomasi Publik Indonesia Melalui Bali Democracy Forum sebagai Bagian dari Kebijakan Politik Luar Negeri Indonesia. *Global Insight Journal*, 39-58
- Anisya Munatama, & Zhaidah, K. (2023). ANALISIS KERJASAMA BILATERAL SOSIAL POLITIK CHINA DAN INDONESIA DALAM MASA KEPEMIMPINAN JOKO WIDODO 2014 - 2020. 10(1), 77–88.
- Asmarani, A. (2022). Klasifikasi Anomali Trafik Pada Ids Menggunakan Algoritma Naïve Baiyes Dan Random Forest. 51. [https://sintap.unama.ac.id/downloadfile/51256#:~:text=Menurut %5B5%5D dan %5B6,yang menyimpang dari batas normal.](https://sintap.unama.ac.id/downloadfile/51256#:~:text=Menurut%5B5%5D%5B6,yang menyimpang dari batas normal.)
- Azhar, M. (2024). BSSN luncurkan tim tanggap insiden siber (CSIRT) pemerintah daerah.
- Bagaskara, A. M. (2018). Kerjasama Pemerintah Indonesia dan ECPAT dalam Menangani Permasalahan Child Trafficking di Indonesia. *Journal of International Relations*, 4(3), 367–375. <http://ejournal-s1.undip.ac.id/index.php/jihiWebsite:http://www.fisip.undip.ac.id>
- BSSN-IHP. (2021). Laporan Tahun 2020 Honeynet Project BSSN - IHP. BSSN, 86.
- BSSN. (2021). Laporan Hasil Monitoring Keamanan Siber Tahun 2020. Badan Siber Dan Sandi Negara, 3(0251), 1–2.
- BSSN. (2023). kolaborasi BSSN dengan CAC kunjungan ke ITB. [https://www.bssn.go.id/kolaborasi-bssn-dan-cac-agendakan-kunjungan-ke-itb-stikom-bali/?utm\\_source=chatgpt.com](https://www.bssn.go.id/kolaborasi-bssn-dan-cac-agendakan-kunjungan-ke-itb-stikom-bali/?utm_source=chatgpt.com)
- BSSN & CAC. (2021). MOU BSSN dan CAC.
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 10(2), 113–128. <https://doi.org/10.22212/jp.v10i2.1447>
- Febriyani, N. (2023). Keamanan Sistem Informasi Jaringan 5G Di Indonesia Masa Kini Dan Masa Depan. *Researchgate.Net*, April. Keamanan Sistem Informasi Jaringan 5G Di Indonesia Masa Kini Dan%0AMasa Depan%0D
- Haykal, M. F. (2020). DIPLOMASI SIBER INDONESIA TERHADAP TIONGKOK: STUDI KASUS KERJASAMA KEAMANAN SIBER TAHUN 2016. *Academya Education*, 2507(February), 1–9.
- Indonesia, P. (2021). A comparison of *Cybersecurity* regulations: China.
- Kairupan, V. A., & Rahman, A. A. (2022). Analisis Kesadaran *Cybersecurity* Pada Pengguna Media Sosial Di Indonesia. *Jurnal Darma Agung*, 30(1), 1164.

- <https://doi.org/10.46930/ojsuda.v30i1.3167>
- Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. *Politeia : Journal of Public Administration and Political Science and International Relations*, 2(2), 62–82. <https://doi.org/10.61978/politeia.v2i2.211>
- Machlul, M. (2024). Peningkatan Kualitas SDM Melalui Pelatihan Cyber Security Pada Anggota Polisi Daerah Jawa Timur. *Parta: Jurnal Pengabdian Kepada Masyarakat*, 4(2), 150–155. <https://doi.org/10.38043/parta.v4i2.4655>
- Martin Hollis. (1991). *Explaining and Understanding International Relations* (p. 15). <https://philpapers.org/go.pl?id=HOLEAU&proxyId=&u=https%3A%2F%2Fphilpapers.org%2Farchive%2FHOLEAU.doc>
- Nabila Aulia Agustin, & Refania Meilani Firdos. (2024). Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital. *Jurnal Mahasiswa Teknik Informatika*, 3(1), 126–131. <https://doi.org/10.35473/jamastika.v3i1.2841>
- Permatasari, D. (2021). Artikel Kanwil DJKN Sulawesi Selatan, Tenggara, dan Barat. <https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/tantangan-cyber-security-di-era-revolusi-industri-40.html>