

**KERJA SAMA INDONESIA DAN AMERIKA SERIKAT DALAM
MENANGANI KEAMANAN SIBER TAHUN 2018-2024**

SKRIPSI



**UNIVERSITAS
ISLAM
INDONESIA**

Oleh:

MOHAMMAD RAVEL RESI TAMA

21323272

**PROGRAM STUDI HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL BUDAYA
UNIVERSITAS ISLAM INDONESIA**

2025

**KERJA SAMA INDONESIA DAN AMERIKA SERIKAT DALAM
MENANGANI KEAMANAN SIBER TAHUN 2018-2024**

SKRIPSI

Diajukan kepada Program Studi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia
Untuk memenuhi sebagian dari syarat guna memperoleh

Derajat Sarjana S1 Hubungan Internasional



Oleh:

MOHAMMAD RAVEL RESI TAMA

21323272

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL BUDAYA

UNIVERSITAS ISLAM INDONESIA

2025

HALAMAN PENGESAHAN

Kerja Sama Indonesia Dan Amerika Serikat Dalam Menangani Keamanan Siber Tahun 2018-2024

Dipertahankan di depan Dewan Penguji Skripsi Prodi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia

Untuk memenuhi sebagian dari syarat-syarat dalam memperoleh
derajat Sarjana S1 Hubungan Internasional



Mengesahkan
Program Studi Hubungan Internasional
Fakultas Ilmu Sosial Budaya
Universitas Islam Indonesia



Dewan Penguji

- 1 Enggar Furi Herdianto, S.I.P., M.A.
- 2 Tri Inov Haripa, S.Hub.Int., M.A.
- 3 Mohammad Rezky Utama, S.IP., M.Si.
- 4 Karina Utami Dewi, S.I.P., M.A.

Tanda Tangan

PERNYATAAN INTEGRITAS AKADEMIK

Dengan ini saya menyatakan bahwa skripsi ini adalah hasil karya ilmiah independen saya sendiri, dan bahwa semua materi dari karya orang lain (dalam buku, artikel, esai, disertasi, dan di internet) telah dinyatakan, serta kutipan dan parafrase diindikasikan dengan jelas.

Tidak ada materi selain yang digunakan selain yang termuat. Saya telah membaca dan memahami peraturan dan prosedur universitas terkait plagiarisme.

Memberikan pernyataan yang tidak benar dianggap sebagai pelanggaran integritas akademik.

29 Desember 2025,



Mohammad Ravel Resi Tama

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Shalawat serta salam senantiasa penulis haturkan kepada Nabi Muhammad SAW sebagai suri teladan bagi seluruh umat manusia dan rahmat bagi seluruh alam. Skripsi ini berjudul “Kerja Sama Indonesia dan Amerika Serikat dalam Menangani Keamanan Siber Tahun 2018–2024”, yang disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Hubungan Internasional, Universitas Islam Indonesia. Dalam proses penyusunan skripsi ini, penulis menyadari bahwa penyelesaiannya tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada berbagai pihak yang telah membantu dan mendukung penulis selama proses penyusunan skripsi ini, yaitu:

1. Allah SWT yang telah memberikan ridho serta kemudahan kepada penulis dalam mengerjakan skripsi ini.
2. Kepada seluruh dosen Prodi Hubungan Internasional yang telah memberikan seluruh ilmu pengetahuan kepada penulis sehingga sampai di titik ini.
3. Ibu Karina Utami Dewi, SIP., MA. selaku Kaprodi Hubungan Internasional.
4. Bapak Enggar Furi Herdianto, S.I.P., M.A. dan Tri Inov Haripa, S.Hub.,Int., M.A. selaku dosen pembimbing yang sudah sabar menuntun penulis dalam menyelesaikan skripsi ini serta memberikan dukungan sehingga penulis dapat menyelesaikan skripsi ini.

5. Keluarga penulis, Ayah Tama, Bunda Desty, Kakak Gita, Adik Bram, Adik Anya serta ibunda tercinta penulis, Alm. Mamah Yani, selaku penyemangat dan pendukung utama penulis dalam segala hal yang penulis lakukan. Skripsi ini penulis persembahkan untuk mereka. Terimakasih sudah berjuang sekuat tenaga untuk memberikan kehidupan yang layak serta pendidikan yang tinggi sehingga penulis bisa bertumbuh dewasa menjadi pribadi yang lebih baik. Kesuksesan dan segala hal baik yang penulis dapatkan tentu saja didapatkan dari do'a yang terpanjatkan setiap hari nya dari Ayah, Bunda, Kakak, dan Adik-Adik.
6. Untuk diri saya sendiri, Mohammad Ravel Resi Tama. Apresiasi sebesar-besarnya karena telah berjuang untuk menyelesaikan apa yang telah dimulai. Tidak mudah untuk bertahan sampai di titik ini, namun terimakasih untuk tetap hidup dan merayakan dirimu sendiri, walaupun sering kali merasa lelah. Tetaplah jadi manusia yang selalu mau untuk berjuang dan mencoba menjadi sebaik mungkin.
7. Kepada seseorang yang kehadirannya sangat berarti dalam perjalanan akademik penulis, Ronna Puspita Sari S.Hub.Int, terima kasih atas kesabaran, waktu, dan perhatian yang tak pernah terputus. Terima kasih telah menemani penulis dalam suka dan duka, mendengarkan setiap keluhan, serta memberikan dukungan dan keyakinan untuk terus bertahan dan tidak menyerah hingga skripsi ini akhirnya terselesaikan.
8. Terima kasih kepada sahabat seperjuangan Rizal Muhamad Ramli S.Kom., Daffa Naufal Fernanda S.T., dan Pradika Tohar Nugroho S.H., yang telah menjadi teman berbagi cerita dan perjuangan sejak tahun 2015 sampai saat

ini. Terima kasih juga kepada sahabat Kos Kamadino Rizal, Indra, Pandu, Haikal yang telah menjadi teman seperjuangan sejak awal perkuliahan tahun 2021 hingga saat ini. Terima kasih atas semangat, dukungan, dan kebersamaan yang telah diberikan sehingga proses perkuliahan dapat dilalui dengan penuh makna.

DAFTAR ISI

SKRIPSI	i
HALAMAN PENGESAHAN	iii
PERNYATAAN INTEGRITAS AKADEMIK	iv
KATA PENGANTAR	v
DAFTAR ISI	viii
DAFTAR GAMBAR	x
ABSTRAK	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	7
1.3 Tujuan Penelitian	7
1.4 Cakupan penelitian	8
1.5 Tinjauan Pustaka	9
1.6 Kerangka Pemikiran	11
1.7 Argumen Sementara	12
1.8 Metode Penelitian	13
<i>1.8.1 Jenis Penelitian</i>	13
<i>1.8.2 Subjek dan Objek Penelitian</i>	14
<i>1.8.3 Metode Pengumpulan Data</i>	14
<i>1.8.4 Proses Penelitian</i>	14
1.9 Sistematika Pembahasan	15
BAB 2	16
2.1 Faktor Pendorong Kerja Sama Indonesia dan Amerika Serikat	16
2.2 Kerja Sama Indonesia dan Amerika Serikat dalam Menangani Keamanan Siber	19
2.3 Dampak Serangan Siber di Indonesia dan Amerika Serikat	24
BAB 3	28
3.1 <i>Similarity or Complementary of State Interest, Purposes, and Needs</i> (Kesamaan atau Keselarasan Kepentingan, Tujuan, dan Kebutuhan negara)	28
<i>3.1.1 Kondisi Indonesia</i>	30
<i>3.1.2 Kondisi Amerika Serikat</i>	33
<i>3.1.3 Persamaan Kepentingan, Prinsip, dan Tujuan Indonesia dan Amerika Serikat</i>	37

3.2	<i>Equitable Distribution of Costs, Risks, Burdens, and Rewards among the Partners to a Collaborative Undertaking</i> (Pembagian yang adil atas biaya, risiko, beban, dan manfaat di antara mitra dalam suatu kerja sama). 40	
3.3	<i>Trust that Commitments will be fulfilled, Low Probability of Defections</i> (Kepercayaan bahwa komitmen akan dipenuhi, dengan probabilitas rendah terjadinya pengkhianatan)	47
3.3.1	<i>Dokumen Kesepakatan Formal</i>	49
3.4	<i>Interactions Conducted on the basis of Approximate Reciprocity, Reability and Reputation for Predictability</i> (Interaksi yang dilakukan berdasarkan prinsip timbal balik yang mendekati kesetaraan, keandalan, dan reputasi yang dapat diprediksi)	55
3.4.1	<i>Bentuk-Bentuk Aktivitas Kerjasama Siber antara Indonesia dan Amerika Serikat</i>	58
BAB 4		64
4.1	Kesimpulan	64
4.2	Rekomendasi	65
DAFTAR PUSTAKA		67

DAFTAR GAMBAR

Gambar 3. 1 Tren serangan siber di Indonesia 2018-2024	31
Gambar 3. 2 Laporan serangan siber di AS 2018-2024	34
Gambar 3. 3 Top 5 Negara Sumber dan Tujuan Kejahatan Siber	37
Gambar 3. 4 Alokasi Anggaran dan Realisasi Anggaran BSSN 2019-2024	45
Gambar 3. 5 Pertemuan antara Indonesia dan Amerika Serikat	50
Gambar 3. 6 Indikator Perjanjian Kinerja dalam Kerangka BSSN (2024)	53

ABSTRAK

Penelitian ini mengkaji hubungan kerja sama keamanan siber antara Indonesia dan Amerika Serikat pada periode 2018–2024. Meningkatnya ancaman digital di tingkat global, seperti ransomware, kebocoran data, serangan terhadap infrastruktur vital, serta aktivitas kelompok kriminal dan aktor negara mendorong kedua negara untuk membangun kolaborasi strategis. Studi ini menggunakan metode kualitatif deskriptif melalui analisis pustaka dan dokumen, serta menggunakan teori Kerja Sama Internasional K.J. Holsti guna menelusuri motivasi, dinamika proses, dan bentuk implementasi kerja sama yang dilakukan kedua pihak. Temuan penelitian menunjukkan bahwa Indonesia dan Amerika Serikat memiliki kepentingan yang sejalan dalam memperkuat kemampuan nasional, membangun kepercayaan strategis, serta mengembangkan mekanisme pertukaran informasi untuk menghadapi ancaman siber lintas negara. Implementasi kerja sama tercermin dalam penandatanganan *Letter of Intent (LoI)* pada 2018, perpanjangan perjanjian pada 2021, hingga penandatanganan *Memorandum of Understanding (MoU)* pada Desember 2024. Bentuk kolaborasi tersebut meliputi penyelenggaraan pelatihan keamanan siber, peningkatan kemampuan manajemen insiden, pertukaran intelijen siber, penguatan regulasi, serta dukungan teknologi dan peningkatan sumber daya manusia.

Kata-kata kunci: Indonesia, Amerika Serikat, Keamanan Siber, Kerja Sama Internasional.

ABSTRACT

This study examines the cyber security cooperation between Indonesia and the United States during the period 2018–2024. Increasing global digital threats, such as ransomware, data leaks, attacks on vital infrastructure, and the activities of criminal groups and state actors, have prompted both countries to establish strategic collaboration. This study uses a descriptive qualitative method through literature and document analysis, as well as K.J. Holsti's International Cooperation theory to explore the motivations, dynamics of the process, and forms of cooperation implementation carried out by both parties. The findings show that Indonesia and the United States have aligned interests in strengthening national capabilities, building strategic trust, and developing information exchange mechanisms to deal with cross-border cyber threats. The implementation of cooperation is reflected in the signing of a Letter of Intent (LoI) in 2018, the extension of the agreement in 2021, and the signing of a Memorandum of Understanding (MoU) in December 2024. This collaboration includes conducting cybersecurity training, improving incident management capabilities, exchanging cyber intelligence, strengthening regulations, and providing technological support and human resource development.

Keywords: Cybersecurity, Indonesia, International Cooperation, United States.

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Indonesia telah menjadi salah satu negara yang paling rentan terhadap serangan siber karena populasi pengguna internetnya yang tumbuh sangat cepat dan sistem regulasi yang terus berkembang. Sudah sangat jelas bahwa negara ini merupakan sumber dan target puluhan juta serangan siber setiap tahunnya (Brown 2019). Dengan 202 juta pengguna internet, Indonesia sekarang merupakan salah satu penggerak ekonomi digital terbesar di Asia Tenggara. Ekonomi digital nasional telah memberikan kontribusi sebesar USD 70 miliar pada tahun 2021 saja, dan diproyeksikan akan mencapai USD 146 miliar pada tahun 2025. Namun demikian, kemajuan digital yang cepat ini juga diikuti dengan peningkatan ancaman keamanan siber atau keamanan siber (Daeng dkk. 2023).

Karena perkembangan teknologi dan variasi penggunaannya yang meningkat, insentif ekonomi dan politik untuk mengeksploitasi jaringan dengan tujuan jahat juga meningkat, sehingga negara sangat memperhatikan keamanan siber (Putra 2022). Aktor siber yang canggih dan negara-bangsa menggunakan kerentanan untuk mencuri data dan uang, serta berusaha membangun kemampuan untuk mengganggu, menghancurkan, atau mengancam penyediaan layanan vital. Untuk menjaga keamanan negara, sangat penting untuk melindungi diri dari serangan-serangan ini. Setiap serangan siber, terlepas dari ukurannya, harus diidentifikasi, diawasi, dan dihentikan karena merupakan ancaman bagi keamanan negara kita. Semua orang, termasuk individu dan keluarga, usaha kecil dan besar, *State, Local, Tribal, and Territorial (SLTT)*, dan pemerintah federal, bertanggung

jawab untuk melindungi ruang siber. Aktor ancaman siber kehilangan kekuatan dengan mencegah serangan atau memitigasi penyebaran serangan secepat mungkin (Cybersecurity and Infrastructure Security Agency, t.t.).

Teknologi tidak hanya memberikan peluang besar untuk inovasi dan efisiensi, tetapi juga meningkatkan ancaman siber. Tidak hanya individu yang sekarang menjadi sasaran serangan siber, tetapi juga lembaga besar, perusahaan multinasional, dan pemerintah. Ini berdampak pada ekonomi dan mengganggu stabilitas sosial dan politik negara. Peningkatan serangan siber di seluruh dunia menunjukkan fenomena ini. Misalnya, serangan pada jaringan pipa kolonial Amerika Serikat pada tahun 2021 (Judijanto 2024).

Dari 2016 hingga 2024, kebocoran data di Indonesia meningkat secara signifikan, dengan sektor pemerintah menjadi target utama. Pada tahun 2024, terjadi gangguan besar akibat peretasan Pusat Data Nasional Sementara. Ini berdampak pada komunikasi pendidikan, imigrasi, dan lembaga. Untuk meningkatkan keamanan siber, termasuk pelatihan, pertukaran informasi, dan pengembangan strategis nasional, Kementerian Luar Negeri, Siblis dan Badan Siber Sandi Negara bekerja sama dengan beberapa negara lain, termasuk Australia dan Amerika Serikat guna meningkatkan keamanan siber meliputi pertukaran informasi, pelatihan, serta pengembangan strategis nasional (Erlinda 2025).

Badan Siber Sandi dan Negara (BSSN) adalah lembaga pemerintah yang berada di bawah tanggung jawab presiden. Pembentukan BSSN diharapkan dapat membantu menangani masalah dan tantangan yang muncul dalam era siber saat ini dan di masa depan serta meningkatkan komitmen bidang keamanan siber untuk memerangi ancaman siber di Indonesia. BSSN dibentuk karena bidang keamanan

siber merupakan salah satu bidang yang perlu didorong dan diperkuat oleh pemerintah untuk mendorong pertumbuhan ekonomi nasional dan menjaga keamanan nasional (Sudarmadi 2019).

Pada 28 September 2018, Direktur Jenderal Amerika dan Eropa Kementerian Luar Negeri RI, Muhammad Anshor, dan Duta Besar Amerika Serikat untuk Indonesia, Joseph Donovan, menandatangani *Letter of Intent (LoI)*, yang bertujuan untuk meningkatkan kerja sama di bidang siber, seperti yang dijanjikan saat Presiden Joko Widodo berkunjung ke Amerika Serikat pada Oktober 2015. Perwakilan dari berbagai lembaga dan kementerian Indonesia, seperti Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan; Badan Siber dan Sandi Negara; Kepolisian Negara Republik Indonesia; dan unit terkait di Kementerian Luar Negeri, hadir juga di acara penandatanganan (Fitriyani 2018).

Tujuan kerja sama ini meliputi bidang-bidang seperti pengembangan strategi ruang siber nasional, kemampuan manajemen insiden nasional, kemampuan dan kerja sama dalam penanggulangan kejahatan siber, kolaborasi dengan berbagai pemangku kepentingan, peningkatan kesadaran akan keamanan siber, dan kolaborasi dengan berbagai organisasi pemerintah (Chotimah 2019).

Pada 1 Oktober 2021, pemerintah Indonesia dan Amerika Serikat telah menyetujui nota diplomatik yang secara resmi memperpanjang masa berlaku LoI Siber selama 3 (tiga) tahun sampai 1 Oktober 2024. Bidang kerja sama tersebut antara lain membangun strategi siber nasional, peningkatan kemampuan manajemen insiden nasional, peningkatan kapasitas kerja sama dan kejahatan siber, kemitraan antar pemangku kepentingan; peningkatan kesadaran keamanan siber

dan kerja sama di organisasi regional dan multilateral (Direktur Jenderal Amerika dan Eropa 2021).

Pada Senin, 4 Desember 2024, Duta Besar Amerika Serikat untuk Indonesia Kamala Shirin Lakhdhir dan BSSN Hinsu Siburian menandatangani nota kesepahaman (MoU) tentang kekuatan kerja sama di bidang siber (Nugraha 2024). Sejak 2022, Amerika Serikat telah memberikan bantuan keamanan siber senilai sekitar empat juta dolar kepada Indonesia. Dalam dua tahun terakhir, Amerika Serikat juga telah bekerja sama erat dengan BSSN untuk memperkuat kerja sama bilateral. Selain itu, kedua negara menyelenggarakan pelatihan keamanan siber. Pelatihan ini berfokus pada pencegahan ancaman siber secara bersamaan, memperluas kolaborasi dengan industri AS, dan membangun proyek keamanan siber (Reditya 2024).

Serangan siber besar yang menargetkan platform perdagangan mata uang kripto di Indonesia, menurut Kaspersky, menyebabkan kerugian sekitar Rp300 miliar (\$19 juta) dan merusak reputasi platform tersebut. Kaspersky juga menyaksikan peningkatan aktivitas "*drainer*" di web gelap pada tahun 2024. *Drainer* adalah alat berbahaya yang dimaksudkan untuk mencuri aset kripto pengguna, seperti token dan *Non-Fungible Token (NFT)*. Alat penguras baru muncul setiap tahun dan diiklankan secara aktif di berbagai platform web gelap. Jumlah utas diskusi khusus tentang penguras di web gelap meningkat dari 55 pada tahun 2022 menjadi 129 pada tahun 2024. Ini menunjukkan minat dan penggunaan yang meningkat oleh penjahat siber (Raidi 2025).

Pada Juni 2024, *Department of Homeland Security (DHS)* Amerika Serikat dan pemerintah Indonesia bekerja sama di Surabaya. Ini menunjukkan komitmen

kedua negara untuk meningkatkan kerja sama keamanan siber dan melindungi infrastruktur maritim penting dari serangan siber berbahaya, yang telah ditingkatkan sebagai bagian dari Kemitraan Strategis Komprehensif. DHS menyelenggarakan latihan dan lokakarya tabletop yang berhasil bekerja sama dengan Kedutaan Besar Amerika Serikat di Jakarta, pemerintah Indonesia, dan berbagai otoritas pelabuhan maritim Indonesia (Security 2024).

Fokus latihan adalah peningkatan keamanan siber maritim dan kemampuan untuk menangani insiden di Indonesia dan wilayah Indo-Pasifik. Kolaborasi untuk meningkatkan kerja sama yang erat dengan mitra di kawasan Indo-Pasifik melalui diskusi terfokus mengenai protokol respons insiden, berbagi informasi, dan menentukan kerja sama bilateral di masa mendatang untuk mencegah ancaman siber terhadap infrastruktur maritim penting saat ini dan di masa mendatang (Security 2024).

Kerja sama siber Indonesia dan Amerika Serikat cenderung memiliki tingkat kedekatan dan efektivitas yang lebih tinggi dibandingkan kerja sama Indonesia dengan negara lain, misalnya dengan Tiongkok. Meskipun hubungan siber Indonesia–Tiongkok juga terus berkembang, fokus utama kerja samanya lebih mengarah pada pembangunan kapasitas teknologi, transfer teknologi, investasi infrastruktur digital, serta pengembangan industri digital. Kerja sama ini dijalankan berdasarkan prinsip penghormatan terhadap kedaulatan negara di ruang siber dan komitmen untuk mendukung tata kelola internet internasional yang multilateral, demokratis, dan transparan, sekaligus mendorong keamanan data serta terciptanya lingkungan siber yang damai, aman, terbuka, kooperatif, tertib, dan bertanggung jawab (Arianto dkk. 2023).

Perbedaan intensitas kerja sama keamanan siber Indonesia dengan Amerika Serikat dan dengan Tiongkok terlihat jelas dari fokus kebijakan serta aktor yang terlibat dalam masing-masing hubungan bilateral. Kemitraan Indonesia dan Amerika Serikat bersifat lebih strategis dan menyeluruh, ditandai dengan dialog kebijakan yang rutin, mekanisme berbagi informasi, serta upaya bersama untuk memperkuat ketahanan siber nasional. Selain itu, hubungan diplomatik Indonesia–Amerika Serikat juga menegaskan adanya kesamaan kepentingan dalam memperkuat ketahanan siber, memajukan nilai-nilai demokrasi, dan menjaga stabilitas kawasan (Azhari 2025).

Keamanan siber Amerika Serikat dianggap sulit untuk diretas karena penjagaan yang ketat terhadap teknologi negara adidaya yang semakin berkembang. Hal ini berkaitan dengan ekonomi karena ekonomi dan informasi saling terkait dan menjadi prioritas kebijakan luar negeri Amerika Serikat (Jayakarta 2024). Amerika Serikat sangat memperhatikan pembangunan kekuatan siber nya. Negara ini menganggap siber sebagai domain baru dalam politik internasionalnya dan memberikan perhatian keamanan yang sama dengan domain darat, laut, dan udara. Karena itu, pemerintah Amerika Serikat telah mengembangkan berbagai kebijakan dan strategi untuk menjaga keamanan ruang siber. Ini dilakukan tidak hanya untuk menciptakan pertahanan siber yang kuat untuk menghadapi tantangan zaman modern, tetapi juga untuk mengantisipasi kurangnya aturan ruang siber dalam hukum internasional (Triwahyuni dan Wulandari 2016).

Amerika Serikat dan Indonesia adalah negara demokrasi. Mereka dapat bekerja sama dalam kemitraan demokratis, yang dapat membangun dan

memperdalam hubungan untuk mengatasi perbedaan dan perpecahan dengan tanggung jawab dan kedewasaan. Hubungan pemerintah yang lebih baik antara Indonesia dan Amerika Serikat membutuhkan kerja sama. Para pemimpin lembaga pemerintah juga sering bertemu dan lebih mengenal satu sama lain. Kepentingan strategis Indonesia dengan Amerika Serikat didasarkan pada dua hal: kerja sama keamanan dalam hubungan bilateral Amerika dengan Indonesia dan peningkatan kerja sama kedua negara untuk membangun arsitektur keamanan baru untuk wilayah Asia Pasifik dengan Amerika Serikat yang telah membuka banyak kerja sama di sana (Putra 2022).

Pengembangan dan penguatan infrastruktur, sarana prasarana, dan kemampuan sumber daya manusia dalam bidang keamanan siber membutuhkan kerja sama internasional. Ini termasuk kerja sama bilateral, regional, dan internasional. Diharapkan peningkatan kerja sama dalam teknologi informasi dan *cybersecurity* juga akan membuka peluang untuk pengembangan industri media baru terkait teknologi informasi di Indonesia sebagai bagian dari pengembangan industri strategis nasional (Budi dkk. 2021).

1.2 Rumusan Masalah

Mengapa Indonesia dan Amerika Serikat Melakukan Kerja Sama Dalam Menangani Serangan Siber Tahun 2018-2024?

1.3 Tujuan Penelitian

Penelitian ini menyelidiki kerja sama antara Indonesia dan Amerika Serikat dalam menangani serangan siber. Berikut adalah tujuan dari penelitian ini:

1. Mengidentifikasi hal-hal yang mendorong kedua negara untuk bekerja sama satu sama lain dalam bidang keamanan siber.
2. Melihat bagaimana proses kerja sama antara Indonesia dan Amerika Serikat dalam menghadapi ancaman dan meningkatkan kapasitas keamanan siber nasional selama tahun 2018–2024.
3. Melihat apa bentuk kerja sama antara Indonesia dan AS dalam menghadapi ancaman keamanan siber tahun 2018–2024.

1.4 Cakupan penelitian

Penelitian ini berfokus pada kerja sama bilateral antara Indonesia dan Amerika Serikat di bidang keamanan siber, khususnya terkait proses kerja sama dari perjanjian *LoI* hingga penandatanganan *MoU*. Tahun 2018 dipilih sebagai awal penelitian karena menjadi titik penting dimulainya kerja sama keamanan siber yang lebih terstruktur antara Indonesia dan Amerika Serikat. Pada tahun yang sama, kedua negara menandatangani *LoI* untuk meningkatkan kerja sama di ruang siber. *LoI* ini bertujuan untuk meningkatkan kapasitas nasional, meningkatkan struktur BSSN, dan meningkatkan strategi keamanan siber dan manajemen insiden. Dalam menghadapi ancaman siber yang semakin meningkat, Indonesia mengambil langkah menuju kerja sama internasional yang lebih teratur, seperti yang ditunjukkan oleh penandatanganan *LoI* ini (antaranews.com 2018).

Sepanjang tahun 2024, perusahaan keamanan siber Kaspersky mendeteksi 19.171.977 upaya serangan siber berbasis web di Indonesia. Ini adalah penurunan 34,85% dari 29.426.930 insiden yang dilaporkan pada tahun sebelumnya (Raidi 2025). Penelitian ini akan membahas proses kerja sama antara Indonesia dan

Amerika Serikat dalam meningkatkan keamanan siber, termasuk sejauh mana kerja sama ini membantu mencegah, mendeteksi, dan menanggapi serangan siber. Selain itu, penelitian ini juga akan mengidentifikasi dampak yang dihadapi dalam menjalankan kerja sama.

1.5 Tinjauan Pustaka

Dalam jurnal yang berjudul “Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber” karya Afifah Fidina Rosy. Penelitian ini membahas cara kerja sama internasional dapat membantu Indonesia memperkuat keamanan nasional dan meningkatkan kemampuan keamanan sibernya. Menurut penelitian ini, peningkatan penggunaan internet bersama dengan meningkatnya ancaman kejahatan siber menjadikan keamanan siber sebagai masalah yang tidak biasa yang membutuhkan perhatian khusus.. Indonesia melakukan kerja sama internasional untuk menangani ancaman lintas batas secara bilateral dengan Belanda, Inggris, Australia, dan Amerika Serikat, serta melalui forum multilateral seperti *ASEAN Regional Forum (ARF)* dan *ASEAN Political-Security Community (APSC)*. Secara keseluruhan, jurnal ini menunjukkan bahwa Indonesia menggunakan kebijakan nasional dan diplomasi siber internasional untuk memperkuat keamanan nasional di era digital (Rosy 2020).

Jurnal kedua berjudul *"Cyber Cooperation between Indonesia and the United States in Addressing the Threat of Cyberterrorism in Indonesia"* karya Bimo Arya Putra. Jurnal ini menekankan bahwa pembangunan kapasitas dan pertukaran informasi adalah strategi utama, tetapi belum ada hasil yang signifikan dari penerapan strategi ini. Selain itu, propaganda, komunikasi terenkripsi, dan

penggalangan dana melalui media sosial dan mata uang digital adalah bahaya utama yang dihadapi Indonesia. Selain itu, ditekankan bahwa pusat penyaringan terorisme siber (*Cyberterrorism Screening Center*) yang sebanding dengan *Federal Bureau of Investigation (FBI)* harus didirikan, serta mekanisme yang memungkinkan Indonesia dan Amerika Serikat berbicara satu sama lain secara langsung dan cepat untuk meningkatkan hasil kerja sama. Jurnal ini juga berfokus pada kerja sama bilateral antara Indonesia dan Amerika Serikat dalam menghadapi ancaman serangan siber dan terorisme digital, dengan menekankan aspek hubungan internasional dan diplomasi keamanan siber (Putra 2022).

Jurnal ketiga berjudul "Studi Perbandingan Hukum Pidana Dalam Penanganan Kejahatan Siber: Perspektif Indonesia dan Amerika Serikat" karya Yunita Sekar Ety Arabel, Ida Musofiana. Jurnal ini membahas bagaimana Indonesia dan Amerika Serikat menangani kejahatan siber. Fokus utamanya adalah perbedaan antara kerangka hukum kedua negara, kapasitas lembaga penegak hukum, dan tingkat kesadaran masyarakat tentang kejahatan siber. Selain itu, jurnal ini menyoroti masalah yang dihadapi Indonesia, seperti kekurangan sumber daya, definisi hukum yang tidak jelas, dan rendahnya kesadaran masyarakat tentang kejahatan siber. Jurnal ini juga menyarankan reformasi hukum, peningkatan edukasi masyarakat, dan kerja sama antar lembaga untuk meningkatkan penanganan kejahatan siber di Indonesia. Selain itu, jurnal ini membahas sejumlah studi yang berkaitan dengan hukum siber dan masalah sosial-politik di berbagai negara (Arabel dan Musofiana 2024).

Penelitian saat ini berbeda dari penelitian sebelumnya dalam hal konsep dan teori yang digunakan karena penelitian sebelumnya tidak menggunakan teori kerja

sama internasional seperti yang ada dalam penulisan ini. Penelitian ini juga akan menganalisis menyeluruh tentang sejarah, perkembangan, kerja sama, dan keberhasilan hubungan Indonesia-Amerika Serikat dalam menangani keamanan siber dari 2019 hingga 2024. Penelitian sebelumnya juga belum membahas tahun 2018-2024. Maka dari itu penulis membuat penelitian ini.

1.6 Kerangka Pemikiran

Buku yang berjudul *“International Politics: A Framework for Analysis” fifth edition* karya K. J. Holsti memperkenalkan teori kerja sama internasional yang menyatakan sejumlah dimensi dalam politik internasional dan kebijakan luar negeri, seperti arah umum kebijakan luar negeri serta pola pilihan yang diambil, dapat dijelaskan melalui kondisi sistem internasional. Namun demikian, sebagian besar proses perumusan kebijakan luar negeri pada dasarnya berfokus pada upaya penyelesaian persoalan-persoalan praktis yang muncul baik di tingkat domestik maupun internasional. Kebijakan luar negeri tidak terlepas dari tujuan dan nilai tertentu. Para pengambil keputusan yang bertindak atas nama suatu komunitas melakukannya dengan tujuan untuk mengubah, mempertahankan, ataupun menata kembali lingkungan internal dan eksternal, termasuk aturan, struktur, serta distribusi biaya dan manfaat yang terbentuk dalam hubungan-hubungan tertentu (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 118).

Dalam bukunya Holsti mendefinisikan bahwa kondisi-kondisi yang berpotensi mendorong serta menopang terwujudnya kerja sama dan koordinasi kebijakan meliputi:

1. *Similarity or complementary of state interest, purposes, and needs*
(Kesamaan atau Keselarasan Kepentingan, Tujuan, dan Kebutuhan negara)
2. *Equitable distribution of costs, risks, burdens, and rewards among the partners to a collaborative undertaking* (Pembagian yang adil atas biaya, risiko, beban, dan manfaat di antara mitra dalam suatu kerja sama).
3. *Trust that commitments will be fulfilled, low probability of defections*
(Kepercayaan bahwa komitmen akan dipenuhi, dengan probabilitas rendah terjadinya pengkhianatan).
4. *Interactions conducted on the basis of approximate reciprocity, reability and reputation for predictability* (Interaksi yang dilakukan berdasarkan prinsip timbal balik yang mendekati kesetaraan, keandalan, dan reputasi yang dapat diprediksi) (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 434).

Ditinjau dari ke empat poin definisi kerja sama internasional menurut Holsti dapat disimpulkan bahwa Kerja Sama Indonesia dan Amerika Serikat dalam Menangani Serangan Siber dapat membentuk kerja sama.

1.7 Argumen Sementara

Menurut K.J. Holsti, kerja sama internasional dapat diartikan sebagai adanya kesesuaian serta sifat saling melengkapi antara kepentingan, tujuan, dan kebutuhan Indonesia dan Amerika Serikat. Pembagian biaya, risiko, dan beban yang proporsional, disertai dengan distribusi manfaat yang adil di antara para mitra dalam suatu upaya kerja sama. Kepercayaan bahwa komitmen akan dipenuhi, dengan probabilitas rendah terjadinya pengkhianatan. Pola interaksi yang didasarkan pada prinsip timbal balik, keandalan, dan reputasi, guna menciptakan

tingkat prediktabilitas dalam hubungan kerja sama (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 434).

Teori kerja sama internasional K.J. Holsti dalam bukunya *"International Politics: A Framework for Analysis"* menyatakan bahwa: "Kerja sama internasional dapat dirumuskan secara sederhana sebagai suatu proses di antara negara-negara yang saling terhubung untuk menemukan solusi atas permasalahan melalui pendekatan bersama. Menurut teori Holsti, kerja sama ini juga mencerminkan keinginan untuk mengkoordinasikan kebijakan dan strategi, dengan Indonesia mengupayakan transfer pengetahuan dan teknologi, sementara Amerika Serikat berkepentingan menjaga stabilitas regional dan memperkuat aliansi di kawasan Indo-Pasifik. Oleh karena itu, kerja sama siber antara Indonesia dan Amerika Serikat dapat dipahami sebagai implementasi teori Holsti, yaitu bagaimana membangun hubungan kerja sama ketika negara-negara mengakui bahwa kepentingan dan tujuan mereka saling melengkapi dan dapat dicapai melalui interaksi yang terlembagakan.

1.8 Metode Penelitian

1.8.1 Jenis Penelitian

Dalam penulisan ini menggunakan metode kualitatif dengan pendekatan deskriptif. Ini bertujuan untuk menggambarkan fenomena secara menyeluruh. Fokus utama dari metode ini adalah untuk memahami "apa" dan "bagaimana" fenomena yang diteliti melalui pengumpulan data non-numerik seperti observasi dan analisis dokumen. Tujuan dari metode tersebut guna memberikan gambaran

yang komprehensif tentang situasi atau kondisi tertentu dari sudut pandang subjek yang terlibat.

1.8.2 Subjek dan Objek Penelitian

Subjek dari penelitian ini yaitu negara Indonesia dan objek dari penelitian ini yaitu kerja sama Indonesia dan Amerika Serikat dalam menangani keamanan siber tahun 2018-2024.

1.8.3 Metode Pengumpulan Data

Penulis melakukan metode pengumpulan data lewat studi pustaka untuk memahami teori-teori terkait keamanan siber serta studi kasus kerja sama yang dilakukan Indonesia dan Amerika Serikat pada tahun 2018-2024. Melalui data sekunder adalah jenis data yang dikumpulkan melalui sumber seperti berita tentang masalah serupa, buku ilmu hubungan internasional, jurnal penelitian terdahulu, dan pernyataan resmi dari pemerintah, serta dokumen laporan yang berisi literatur dan fakta yang bisa digunakan bermanfaat guna mendukung penelitian ini dan memungkinkan proses pemahaman yang mendalam. Sumber-sumber tersebut diperoleh melalui proses selektif melalui akses data ke alamat situs web yang dapat dipercaya.

1.8.4 Proses Penelitian

Identifikasi dan pemilihan kasus tentang bagaimana pemerintahan Indonesia dan Amerika Serikat dalam melakukan kerja sama untuk menangani keamanan siber. Setelah itu melakukan pengumpulan data melalui analisis dokumen, dan studi pustaka. Analisis data menggunakan teori kerja sama Internasional oleh K.J Holsti. Kemudian membuat kesimpulan serta saran.

1.9 Sistematika Pembahasan

Bab pertama membahas pengetahuan tentang keamanan serta kejahatan siber yang ada di Indonesia dan Amerika Serikat. Latar belakang, rumusan masalah, tujuan penelitian, cakupan penelitian, tinjauan pustaka, kerangka pemikiran argumen sementara, metode penelitian serta sistematika pembahasan.

Bab kedua membahas kerja sama Indonesia dan Amerika Serikat tahun 2018-2024. Dalam bab ini juga membahas dampak serangan siber, sejarah kerja sama serta faktor pendorong kerja sama di Indonesia dan Amerika Serikat.

Bab ketiga membahas analisis Kerja Sama Indonesia dan Amerika dalam Menangani Keamanan Siber Tahun 2018-2024 menggunakan teori kerja sama Internasional Oleh K.J Holsti dalam bukunya yang berjudul *“International Politics: A Framework for Analysis” fifth edition*.

Bab keempat membuat kesimpulan dari analisis kerja sama tersebut dalam konteks keamanan siber antara Indonesia dan Amerika Serikat serta membuat saran untuk dimasa mendatang.

BAB 2

KERJA SAMA INDONESIA DAN AMERIKA SERIKAT DALAM MENANGANI KEAMANAN SIBER

2.1 Faktor Pendorong Kerja Sama Indonesia dan Amerika Serikat

Serangan siber dapat bervariasi. Serangan *malware*, *phishing*, dan *ransomware* menjadi lebih umum dan dapat mempengaruhi individu maupun perusahaan besar. *Malware* adalah perangkat lunak apa pun yang digunakan untuk mendapatkan akses tidak sah ke sistem teknologi informasi untuk mencuri data, mengganggu layanan sistem, atau merusak jaringan TI dengan cara apapun. *Ransomware* adalah jenis *malware* yang diidentifikasi oleh data atau sistem tertentu oleh penyerang hingga mereka membayar atau tebusan. *Phishing* adalah penipuan online yang mendorong orang untuk membagikan data pribadi dengan cara yang menipu atau palsu (Insight In News 2024).

Di Indonesia, ancaman keamanan siber semakin kompleks dan beragam, dengan berbagai jenis serangan yang menargetkan individu, kelompok, hingga infrastruktur kritis. Salah satu ancaman paling berbahaya adalah serangan ransomware, di mana penyerang mengenkripsi data korban dan meminta tebusan untuk pemulihannya. Karena banyaknya lembaga yang belum memiliki sistem keamanan yang memadai, sektor kesehatan, keuangan, dan pendidikan paling rentan. Selain itu, phishing dan rekayasa sosial juga sering terjadi. Dalam skenario ini, penyerang memanfaatkan email, SMS, atau media sosial untuk berpura-pura sebagai orang yang dipercaya untuk mencuri informasi sensitif seperti kata sandi

atau data keuangan. Serangan ini menjadi lebih mudah dilakukan karena masyarakat tidak tahu cara menjaga keamanan digital (Insight In News 2024).

Selain itu, penipuan online semakin meningkat, termasuk investasi palsu, penjualan barang palsu, dan pinjaman ilegal, terutama seiring dengan peningkatan penggunaan layanan *fintech* di Indonesia. Data pribadi seperti nomor identitas, alamat, dan informasi keuangan sering dicuri dan dijual di internet gelap, yang merupakan masalah besar di kedua sektor swasta dan pemerintah. Selain itu, serangan terhadap infrastruktur penting seperti transportasi, energi, dan telekomunikasi dapat menyebabkan gangguan yang signifikan terhadap layanan publik, terutama dalam kasus di mana sistem yang digunakan sudah tua atau mengalami masalah keamanan.

Sebaliknya, propaganda dan disinformasi digital menjadi semakin mengkhawatirkan. Hoaks dan manipulasi data melalui media sosial dapat menyebabkan ketidakstabilan sosial dan politik. Baik aktor negara maupun non-negara sering menggunakan ancaman ini untuk mempengaruhi opini publik, yang membuat lebih penting untuk meningkatkan literasi digital dan perlindungan siber di Indonesia (Insight In News 2024).

Pada saat ini, lebih dari 800 orang telah menjadi korban akibat serangan *ransomware* di AS, yang telah berdampak besar pada berbagai sektor. Salah satu kelompok *ransomware* yang terlibat dalam serangan ini adalah kelompok yang bernama *Play*. Dampaknya meluas ke banyak industri, menyebabkan gangguan operasi dan kerugian finansial yang signifikan. Selain itu, pelanggaran data menjadi masalah yang sangat penting, karena banyak kasus di mana data penting lembaga disusupi dan informasi pribadi sensitif dijual secara ilegal (TRIAD 2025).

Indonesia telah menghadapi jutaan serangan siber dan menjadi salah satu target utama di kawasan Asia, sehingga cyberterrorism muncul sebagai tantangan serius bagi pemerintah dalam menjaga keamanan nasional di ruang siber. Upaya pengembangan kapabilitas penanggulangan ancaman tersebut masih menghadapi berbagai kendala struktural, seperti lemahnya regulasi hukum siber, rendahnya koordinasi antara sektor pemerintah dan swasta, belum terintegrasinya tata kelola keamanan siber nasional, ketiadaan standar perlindungan infrastruktur vital, serta keterbatasan kualitas dan kuantitas sumber daya manusia di bidang keamanan siber (Khoirunnisa dkk. 2024).

Di Amerika Serikat, penyelenggaraan keamanan siber ditangani oleh sejumlah institusi utama, yakni Departemen Keamanan Dalam Negeri (DHS), Departemen Pertahanan (DoD), dan Biro Investigasi Federal (FBI). DHS berperan sentral dalam menjaga keamanan internal siber melalui koordinasi dengan lembaga pemerintah, sektor swasta, dan mitra internasional, sementara FBI menjalankan fungsi intelijen domestik dan penegakan hukum untuk menghadapi kejahatan siber, terorisme, serta ancaman intelijen asing.

Perbandingan tersebut menunjukkan bahwa kapasitas keamanan siber Indonesia masih tertinggal dibandingkan Amerika Serikat, baik dari sisi kelembagaan, mekanisme operasional, maupun kerangka hukum. Sebagai negara maju yang lebih awal mengembangkan sistem keamanan siber, Amerika Serikat memiliki tata kelola yang lebih komprehensif dan modern, sehingga penting bagi Indonesia untuk merefleksikan serta mempelajari praktik yang diterapkan. Kesadaran ini mendorong kedua negara memperkuat kerja sama keamanan siber,

yang diwujudkan secara konkret melalui penandatanganan Letter of Intent (LoI) Indonesia–Amerika Serikat pada tahun 2018 (Putra 2022).

2.2 Kerja Sama Indonesia dan Amerika Serikat dalam Menangani Keamanan Siber

Meningkatnya ancaman siber memicu diplomasi siber antara Indonesia dan AS. Serangkaian serangan siber telah terjadi di Indonesia yang menargetkan infrastruktur pemerintah dan data vital, menunjukkan kelemahan sistem digitalnya. Ancaman ini berasal dari banyak sumber, bukan hanya dari pihak berwenang negara, tetapi juga dari kelompok kejahatan dunia maya dan individu yang memiliki kemampuan teknis yang luar biasa. AS memberikan bantuan yang sangat diperlukan untuk memperkuat kemampuan pertahanan siber Indonesia dengan menggunakan pengalaman dan teknologi canggihnya di bidang keamanan siber. Memperkuat infrastruktur siber Indonesia, meningkatkan keamanan data, dan melindungi infrastruktur penting dari ancaman siber yang berkembang adalah tujuan dari kerja sama ini (Khoirunnisa dkk. 2024).

Pemerintah Indonesia dan AS telah mencapai konsensus untuk meningkatkan kerja sama di ruang siber (*cyberspace*). Selanjutnya, tahap negosiasi diwujudkan melalui penandatanganan *Letter of Intent (LoI)* pada 28 September 2018, di Jakarta. Muhammad Anshor, Direktur Jenderal Amerika dan Eropa Kementerian Luar Negeri, dan Joseph R. Donovan Jr., Duta Besar AS untuk Indonesia, menandatangani dokumen Pernyataan Kehendak tentang Memajukan Kerja Sama Ruang Siber yang Erat. Sebagaimana disepakati selama kunjungan Presiden Joko Widodo ke AS pada Oktober 2015, penandatanganan LoI merupakan

bukti komitmen kedua negara untuk meningkatkan kerja sama di ruang siber. Dirjen Muhammad Anshor menekankan bahwa kerja sama internasional di ruang siber, termasuk dengan AS sangat penting untuk menangani berbagai tantangan dan masalah siber yang terus berkembang (Suminar 2018).

Pembentukan LoI antara Indonesia dan AS yang membahas dunia maya juga didorong oleh faktor-faktor politik, yaitu kepedulian AS terhadap kemajuan teknologi Tiongkok dan masalah Indo-pasifik, di mana AS berharap Indonesia dapat menjadi mitra AS dalam mengatasi masalah yang dianggap menantang. Misalnya, BSSN telah bekerja sama dengan Amerika untuk menyelenggarakan investigasi online *Homeland Security Investigation (HSI)* virtual yang akan berlangsung dari 14 hingga 16 Maret 2022. Kedutaan Besar Amerika menganjurkan BSSN untuk berpartisipasi dalam kegiatan ini. Personel yang ditugaskan oleh BSSN berada di Direktorat Strategi dan Sandi Keamanan Siber. Hasil dari kegiatan ini antara lain untuk meningkatkan kemampuan untuk menyelidiki, mengatasi, dan menganalisis bukti digital dalam upaya memerangi kejahatan transnasional dan perdagangan manusia, berbicara tentang kejahatan transnasional, forensik digital, dan investigasi situs gelap serta berbagi informasi dan praktik terbaik dalam upaya yang melibatkan jaringan siber (Putra 2022).

Indonesia bekerja sama dengan AS dalam bidang keamanan siber karena mendesak harus meningkatkan kemampuan pertahanan siber nasional untuk menghadapi ancaman siber yang semakin kompleks. Peretasan kerangka data pemerintah Indonesia yang terjadi beberapa waktu lalu adalah bukti pentingnya partisipasi ini. Serangan ini menyoroti kerentanan dalam infrastruktur digital Indonesia dan menyoroti seharusnya kemajuan keamanan siber melalui inovasi dan

kemampuan yang lebih maju. Negara-negara Gabungan akan memberikan inovasi terbaru dalam keamanan siber kepada Indonesia melalui asosiasi ini. Misalnya, Indonesia dapat terlibat dalam upaya teritorial untuk meningkatkan keamanan siber dan mengamankan informasi penting dari ancaman global melalui Wacana Pengaturan Siber ASEAN-AS (Khoirunnisa dkk. 2024).

Kementerian Luar Negeri Indonesia mengumumkan bahwa Indonesia dan AS akan meningkatkan kerja sama siber. Pengembangan strategi nasional, kemampuan untuk mengelola insiden nasional, kemampuan untuk bekerja sama dan menangani kejahatan siber, dan peningkatan kesadaran keamanan siber adalah bidang-bidang kerja sama siber (antaranews.com 2018). AS dan Indonesia adalah negara demokrasi. Mereka dapat bekerja sama dalam kemitraan demokratis, yang dapat membangun dan memperdalam hubungan untuk mengatasi perbedaan dan perpecahan dengan tanggung jawab dan kedewasaan.

Untuk menciptakan Hubungan pemerintahan yang lebih baik antara Indonesia dan AS dibutuhkan kerja sama. Para pemimpin lembaga pemerintah juga sering bertemu dan lebih mengenal satu sama lain. Kepentingan strategis Indonesia dengan AS didasarkan pada dua hal yaitu kerja sama keamanan dalam hubungan bilateral Amerika dengan Indonesia dan peningkatan kerja sama kedua negara untuk membangun arsitektur keamanan baru untuk wilayah Asia Pasifik dengan AS yang telah membuka banyak kerja sama di sana (Chotimah 2019).

Indonesia dapat meningkatkan kerja sama keamanan masa depan dengan AS melalui kerja sama siber dalam beberapa masalah non-militer yang dapat mempengaruhi keamanan nasional kedua negara tetapi tidak dapat diselesaikan secara sepihak karena alasan transnasional (Ariesta 2019). Ini dilakukan melalui

pelatihan keamanan siber yang berfokus pada penanggulangan ancaman siber secara bersamaan, membangun kolaborasi dengan industri AS, dan mendukung inisiatif keamanan siber. Seiring dengan meningkatnya penggunaan teknologi digital di berbagai sektor, ancaman siber di Indonesia terus meningkat. Ini termasuk berbagai serangan yang dapat sangat mengganggu individu, kelompok, dan pemerintah (Insight In News 2024).

Pada 26 Juli 2019, di Jakarta, Indonesia, *Information System and Technology Exchange (ISTX)* tahunan ketiga diselesaikan oleh anggota angkatan darat, udara, dan laut AS dan Indonesia. Sebagai bagian dari Program Kemitraan Negara Bagian Garda Nasional Hawaii, pertukaran ini adalah salah satu dari sekitar 22 latihan tahunan yang dilakukan kedua negara. Salah satu proyek terbaru adalah ISTX, yang bertujuan untuk berbagi praktik terbaik, membantu pengembangan doktrin keamanan siber, dan meningkatkan kapabilitas keamanan siber untuk secara efektif mempertahankan dan melindungi infrastruktur informasi siber penting dari virus berbahaya dan intrusi siber (Sersan Staf Katie Gray 2019).

Pada tanggal 4 Desember 2024 terdapat kerja sama bilateral antara Indonesia dan AS yaitu Memorandum Saling Pengertian (MSP) antara Pemerintah Republik Indonesia dan Pemerintah AS tentang Peningkatan Kerja Sama di Ruang Siber (Badan Siber dan Sandi Negara 2024a). Hubungan bilateral antara AS dan Indonesia mencapai tonggak baru dengan penandatanganan *Memorandum of Understanding (MoU)* baru untuk meningkatkan kerja sama di bidang keamanan siber. Tujuan dari nota kesepahaman tersebut adalah untuk meningkatkan kerja sama dalam melawan ancaman siber, meningkatkan ketahanan digital, dan menciptakan ekosistem keamanan siber yang lebih kuat di Indonesia. MoU ini juga

mencakup rencana pelatihan keamanan siber yang mencakup berbagai elemen penting, seperti penanggulangan ancaman bersama, pengelolaan pusat data, dan pengembangan proyek keamanan siber strategis. Kolaborasi ini adalah langkah strategis dalam membangun ketahanan siber yang lebih baik di Indonesia. Dengan bantuan dan dukungan AS, diharapkan dapat lebih efektif dalam menghadapi tantangan siber yang semakin kompleks (Sari 2024).

Nota Kesepahaman yang telah disepakati akan memfasilitasi dan mendorong kerja sama serta pengembangan kemampuan siber nasional, termasuk BSSN yang saat ini berfungsi sebagai Badan Siber Nasional. BSSN adalah titik fokus Indonesia yang dibentuk untuk melaksanakan tugas-tugas yang berkaitan dengan keamanan siber. MoU tersebut berfokus pada beberapa topik kerja sama: strategi siber nasional, kemampuan manajemen insiden nasional, peningkatan kemampuan dan kerja sama dalam memerangi kejahatan siber, dan, terakhir, kesepakatan nasional untuk melakukannya (Jakarta 2025).

Peningkatan status kerja sama dari *Statement of Intent* menjadi *Memorandum of Understanding* dan Memorandum Saling Pengertian (MSP) pada 4 Desember 2024 menandai langkah konkret penyamaan standar keamanan, koordinasi penanganan insiden lintas batas, serta penguatan pertukaran data strategis antara kedua negara. Ancaman siber yang bersifat lintas negara menjadi faktor eksternal yang menekan kedua negara untuk bekerja sama. Dalam hal ini, yang menentukan bukanlah keselarasan tujuan, tetapi persepsi Indonesia bahwa kebijakan dan kapasitas AS dapat memberikan manfaat langsung bagi penguatan ketahanan sibernya. Begitu pula AS menilai keterlibatan Indonesia sebagai elemen yang mendukung perluasan agenda keamanan siber regionalnya.

2.3 Dampak Serangan Siber di Indonesia dan Amerika Serikat

Semua jenis serangan digital yang ditujukan untuk mencuri data, mengganggu operasi, atau merusak sistem teknologi disebut sebagai ancaman siber. Di Indonesia, risiko ini meningkat seiring dengan pesatnya digitalisasi di berbagai industri. BSSN melaporkan bahwa jumlah serangan siber di Indonesia meningkat sebesar dua puluh persen dalam tiga tahun terakhir. Mulai dari phishing, malware, hingga ransomware yang semakin canggih, ada banyak jenisnya (IT GRC 2025).

Serangan siber memengaruhi banyak aspek kehidupan bernegara dan bisnis. Data pribadi seperti data kependudukan dan keimigrasian sering menjadi target utama peretas, yang membuat pelanggaran privasi menjadi salah satu konsekuensi paling serius. Kegiatan yang melanggar hukum, seperti pencurian identitas dan penipuan, dapat dimanfaatkan untuk bocoran data. Selain itu, serangan siber mengakibatkan kerugian moneter yang signifikan, yang mencakup biaya pemulihan data, kompensasi bagi pihak terdampak, denda hukum, dan kehancuran reputasi organisasi atau perusahaan di mata publik. Peretasan data juga memiliki konsekuensi yang signifikan, termasuk gangguan operasional, karena dapat menyebabkan penundaan pelayanan publik, kehilangan akses ke informasi penting, atau bahkan kegagalan sistem yang signifikan. Selain itu, serangan siber dapat membahayakan keamanan nasional jika digunakan untuk spionase atau sabotase. Data yang dicuri dapat digunakan untuk melakukan serangan lebih lanjut atau melemahkan posisi strategis negara (Jogja 2024).

Serangan siber dan kejahatan siber menyebabkan berbagai jenis kerugian, tergantung pada jenis korbannya. Untuk korban korporasi, mereka menyebabkan kerugian ekonomi dalam bentuk penurunan laba, kehilangan nilai pasar, tuntutan hukum, dan kerusakan reputasi. Untuk korban individu, kerugian siber dan kejahatan siber menyebabkan stres dan gangguan psikologis, pencurian identitas, dan kerugian finansial. *Federal Bureau of Investigation (FBI)* menerima 5 juta keluhan tentang serangan siber antara tahun 2018 dan 2024, dengan total kerugian yang dilaporkan \$56,7 miliar (USAFacts team 2025).

Ransomware membuat sektor-sektor penting seperti penyedia layanan kesehatan offline selama pandemi. Kerentanan teknologi dan kurangnya perhatian pengguna terhadap keamanan memberikan peluang bagi pelaku kejahatan siber untuk mendapatkan keuntungan ilegal, meskipun berisiko rendah, tetapi berhadiah besar. Negara-negara seringkali memiliki regulasi yang buruk dan penegakan hukum yang buruk. Pencurian kekayaan intelektual adalah salah satu jenis kejahatan yang dapat mengganggu inovasi di AS dan merugikan bisnis hingga miliaran dolar, sementara *ransomware* adalah salah satu jenis kejahatan yang dapat mengganggu sektor-sektor penting, mengancam keamanan ekonomi dan nasional, serta mengganggu kehidupan sehari-hari orang Amerika (United States Department of State, t.t.).

Serangkaian serangan *ransomware* yang tidak pernah terjadi sebelumnya melanda AS pada tahun 2019. Dengan potensi kerugian lebih dari \$7,5 miliar, serangan ini dapat berdampak pada setidaknya 966 lembaga pemerintah, lembaga pendidikan, dan penyedia layanan kesehatan, termasuk 113 lembaga negara bagian dan negara bagian, 764 penyedia layanan kesehatan, 89 universitas, perguruan

tinggi, dan distrik sekolah. Selain itu, ada 1.233 sekolah individu yang berpotensi terkena dampak. Serangan siber di AS tidak hanya menyebabkan ketidaknyamanan finansial, tetapi juga merupakan ancaman besar terhadap kesehatan, keselamatan, dan bahkan nyawa manusia. Terutama pada sektor publik seperti rumah sakit, lembaga pemerintah, dan lembaga pendidikan, dampaknya sangat besar (Lab 2019).

Banyak sekali, catatan medis tidak dapat diakses atau bahkan hilang secara permanen. Akibatnya, pasien darurat harus dialihkan ke rumah sakit lain. Penerimaan pasien baru dihentikan, prosedur bedah dibatalkan, dan tes diagnostik ditunda. Selain itu, layanan darurat 911 terganggu, yang mengharuskan pusat pengiriman menggunakan peta dan catatan kertas untuk memantau responden di lapangan. Bahkan beberapa penjara tidak dapat membuka pintu sel dari jarak jauh, polisi kehilangan akses ke sistem pemeriksaan latar belakang dan data kriminal, dan sistem pengawasan, pemindai lencana, dan akses ke gedung ditutup. Kehilangan akses ke data penting seperti alergi dan obat-obatan siswa akan berdampak pada sekolah juga (Lab 2019).

"Fakta bahwa tidak ada kematian terkait *ransomware* yang terkonfirmasi pada tahun 2019 semata-mata karena keberuntungan, dan keberuntungan itu mungkin tidak berlanjut hingga tahun 2020" kata Fabian Wosar, CTO Emsisoft. Pendidikan, sektor kesehatan, dan pemerintah harus memperbaiki diri. Di antara konsekuensi lainnya termasuk penghentian transaksi properti, penundaan tagihan utilitas, penundaan hibah untuk lembaga nirlaba, gangguan pada situs web dan platform pembayaran online, serta gangguan pada layanan email dan telepon. Selain itu, batas waktu pembayaran pajak harus diperpanjang, penerbitan SIM,

pembayaran vendor, dan aktivitas pendidikan seperti pencatatan nilai siswa akan terganggu. Seperti yang ditunjukkan oleh semua ini, serangan siber memiliki dampak sosial dan ekonomi yang jauh lebih luas daripada hanya kehilangan uang (Lab 2019).

BAB 3

ANALISIS KERJA SAMA INDONESIA DAN AMERIKA SERIKAT

DALAM MENANGANI KEAMANAN SIBER TAHUN 2018-2024

3.1 *Similarity or Complementary of State Interest, Purposes, and Needs*
(Kesamaan atau Keselarasan Kepentingan, Tujuan, dan Kebutuhan negara)

Ketika memahami kerja sama keamanan siber antara Indonesia dan AS, langkah pertama adalah melihat apakah kedua negara memiliki kepentingan dan tujuan yang selaras. Keselarasan ini menjadi dasar penting bagi terbentuknya kerja sama, karena kerja sama hanya dapat muncul jika kedua negara memandang bahwa tujuan atau kepentingan mereka dapat dicapai secara bersamaan. Dalam lanskap keamanan siber global, Indonesia menempati posisi yang perlu mendapatkan perhatian serius dari tahun ke tahun. Dimana keamanan negara ini seringkali dianggap rapuh dan kurang siap menghadapi eskalasi ancaman digital. Jauh dari periode tahun sebelum 2018-2024, insiden siber dengan skala luas sebenarnya sudah mulai tercatat.

Pada tahun 2018, Indonesia juga menghadapi lonjakan ancaman siber yang sangat tinggi. Hal ini ditandai dengan adanya lebih dari 50 juta serangan siber. Jumlah ini menunjukkan kenaikan sekitar 240% dibandingkan tahun sebelumnya. Serangan tersebut datang dari berbagai sumber, seperti ancaman pada perangkat mobile, trojan perbankan, adware, riskware, serta malware (Badan Siber dan Sandi Negara 2019b).

Dari keseluruhan serangan, sekitar 77,12% menargetkan individu, sedangkan 22,88% sisanya menargetkan sektor bisnis. Skala serangan yang besar

ini menempatkan Indonesia pada posisi ke-20 negara dengan jumlah ancaman siber terbanyak di dunia. Dalam hal ini, AS menerapkan strategi yang lebih matang melalui kemitraan publik–swasta (PPP) yang berguna dalam memperkuat perlindungan terhadap infrastruktur informasi kritis (Healey 2017; Christensen dan Petersen 2017).

Berdasarkan *Executive Order* 13636, pemerintah AS mengatur mekanisme sukarela bagi Departemen Keamanan Dalam Negeri, Departemen Kehakiman, serta lembaga pertahanan untuk berbagi informasi ancaman dengan sektor swasta. Dalam hal ini, Departemen Keamanan Dalam Negeri bertugas sebagai koordinator dengan membentuk forum konsultatif mengenai keamanan siber. Selain itu, AS juga merumuskan kerangka kerja dasar yang bertujuan untuk menekan risiko serangan siber terhadap infrastruktur informasi kritis (The White House 2013).

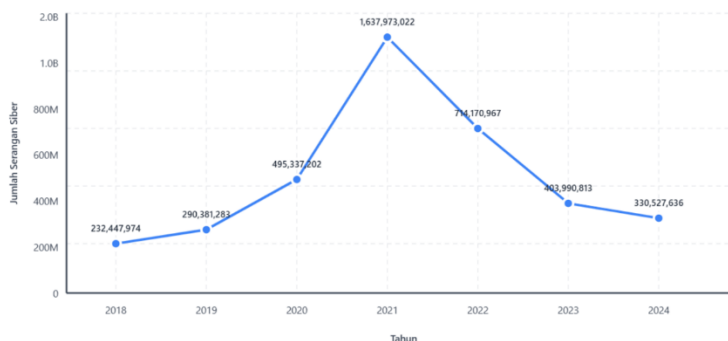
Kemudian di periode tahun 2018-2019, barulah Indonesia dan AS giat membuka peluang kerja sama di bidang *cybersecurity*. Dalam hal ini, USINDO berperan sebagai jembatan yang mempertemukan kampus-kampus AS dengan instansi pemerintah Indonesia. Hal ini ditandai pada Agustus 2018, dimana University of Maryland bertemu dengan BSSN dan Universitas Pertahanan Indonesia (UNHAN) untuk membahas program pelatihan untuk meningkatkan kemampuan para pejabat pemerintah, khususnya dalam hal keamanan siber (Humas Unhan 2024). Kemudian, dalam pertemuan penting dengan Menteri RISTEKDIKTI, University of Maryland juga mengajukan usulan untuk mengadakan konsultasi dan pelatihan *cyber security* (USINDO 2019). Hal ini menegaskan bahwa keamanan siber adalah salah satu fokus utama yang dipilih untuk memperkuat hubungan pendidikan dan strategis antara kedua negara.

Holsti menjelaskan bahwa konflik dalam hubungan internasional berakar pada ketidaksesuaian tujuan antarnegara. Konflik terjadi ketika upaya suatu negara dalam mencapai atau memaksimalkan tujuan politiknya justru mengganggu, membatasi, atau merugikan kepentingan serta nilai yang dianggap penting oleh negara lain. Apabila perbedaan kepentingan tersebut menyangkut nilai strategis dan kepentingan vital, negara cenderung menempuh langkah-langkah koersif, seperti penggunaan ancaman atau peningkatan kapasitas kekuatan, sebagai sarana untuk mempertahankan kepentingannya (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 432).

3.1.1 Kondisi Indonesia

Pada periode 2018–2024, kepentingan nasional Indonesia di bidang siber dapat dilihat dari meningkatnya kerentanan negara terhadap ancaman digital yang berdampak langsung pada keamanan, ekonomi, dan kedaulatan data. Kerja sama siber antara Indonesia dan AS, yang dibangun di atas landasan hubungan strategis kedua negara, dipandang sebagai pintu masuk untuk memperdalam kolaborasi keamanan ke depan. Selain itu, kerja sama siber juga berfungsi sebagai *force multiplier* yang memperkuat posisi politik dan militer Indonesia sesuai kepentingan nasionalnya (Ariesta 2019).

Gambar 3. 1 Tren serangan siber di Indonesia 2018-2024



Sumber: Laporan Tahunan ID-SRTII BSSN 2018-2024 dan dihimpun kembali oleh Penulis (2025) (CNN Indonesia 2019; Badan Siber dan Sandi Negara 2019a; 2020; 2021; 2022; 2023; 2024b)

Berdasarkan gambar 3.1 terlihat adanya peningkatan terhadap jumlah serangan siber yang menargetkan Indonesia. Jika dilihat pada gambar 3.1, laporan pemantauan keamanan internet yang dikeluarkan oleh Badan Siber dan Sandi Nasional (BSSN) menunjukkan bahwa di Indonesia terjadi 232.447.974 serangan siber sepanjang 2018 (CNN Indonesia 2019).

tahun 2019 memiliki jumlah serangan sebanyak 290 juta, kemudian naik menjadi 495 juta di tahun 2020. Dalam hal ini, lonjakan terjadi pada 2021, sebelum akhirnya menurun menjadi 714 juta di tahun 2022, 404 juta pada 2023, dan 331 juta di tahun 2024. Garis pola ini memperlihatkan bahwa meskipun terjadi penurunan setelah 2021, intensitas ancaman siber tetap tinggi dan konsisten dari tahun ke tahun.

Pada tahun 2019, Indonesia mulai memperlihatkan kerentanannya dalam menghadapi eskalasi ancaman digital ketika berbagai insiden serangan siber mengganggu layanan publik maupun sektor swasta. Dari sisi keamanan, hal ini

menegaskan bahwa perlindungan infrastruktur vital dan data masyarakat merupakan prioritas nasional yang tidak bisa diabaikan. Kemudian di tahun 2020, pandemi COVID-19 mendorong percepatan transformasi digital yang sangat masif, di mana kegiatan masyarakat, layanan publik, dan aktivitas ekonomi beralih ke ruang digital. Situasi ini menimbulkan celah keamanan yang lebih luas, tetapi sekaligus menegaskan pentingnya ekonomi digital sebagai salah satu penopang utama pertumbuhan Indonesia. Ambisi Indonesia untuk menjadi ekonomi digital terbesar di Asia Tenggara pada 2030 semakin relevan dalam konteks ini. Kemudian di tahun 2021, kasus peretasan dan kebocoran data semakin marak, termasuk yang menargetkan institusi pemerintah dan layanan komersial. Situasi ini tidak hanya berdampak pada keamanan data, tetapi juga merusak stabilitas politik karena kepercayaan publik terhadap kapasitas negara dalam melindungi warganya terancam menurun.

Pada tahun 2022, data dari BSSN (2022) mencatat lebih dari 714 juta menandakan angka yang sangat besar dan menjadi bukti nyata bahwa kepentingan nasional Indonesia dalam menjaga stabilitas digital tidak dapat dilepaskan dari diplomasi internasional, baik melalui pertukaran informasi intelijen siber, kerja sama penegakan hukum lintas batas, maupun pembangunan kapasitas kelembagaan. Dimana hal ini selaras dengan perubahan Kemitraan Strategis AS-Indonesia yang telah diperluas ke isu-isu regional dan global, termasuk pembahasan isu siber. Sedangkan, di tahun 2023, serangan ransomware kembali menjadi perhatian serius, terutama yang menimpa sektor kesehatan dan keuangan, sehingga menimbulkan kerugian ekonomi sekaligus mengancam keselamatan publik. Hal ini memperlihatkan bahwa isu keamanan siber sudah menjadi bagian dari isu politik

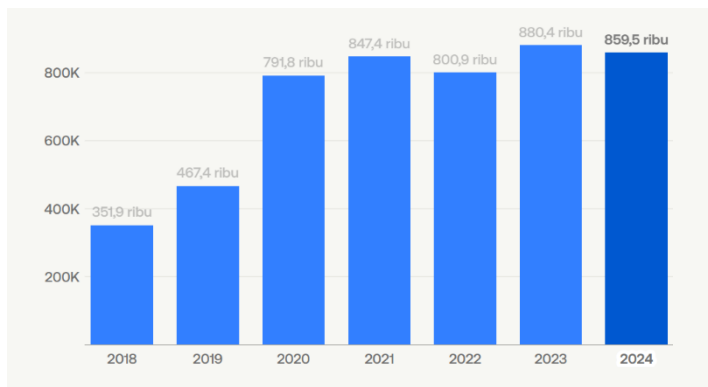
karena melibatkan kepercayaan masyarakat terhadap negara serta membutuhkan regulasi yang kokoh (Indrawan 2019).

Kepentingan ini membuat Indonesia harus menghadapi tuntutan untuk memperkuat diplomasi siber baik di tingkat regional seperti ASEAN maupun di forum global di 2024. Posisi Indonesia sebagai mitra penting di Indo-Pasifik, negara demokrasi besar, dan pemimpin ASEAN memberikan pertimbangan dan pengaruh strategis dalam upaya diplomasi ini (Putra 2022). Fungsinya adalah untuk memastikan kepentingan nasionalnya terlindungi dari dampak serangan siber lintas negara. Hal ini menegaskan bahwa Indonesia dituntut untuk memerlukan strategi pertahanan siber yang berkelanjutan dan kerja sama internasional untuk melindungi kepentingan nasional, baik dari sisi keamanan, ekonomi, politik, maupun diplomasi.

3.1.2 Kondisi Amerika Serikat

Pada periode 2018–2024, kepentingan nasional AS di bidang siber dapat dilihat dari meningkatnya kerentanan negara terhadap ancaman digital yang berdampak langsung pada keamanan, ekonomi, dan perlindungan data warganya. Dalam strategi Indo-Pasifiknya, AS menempatkan Indonesia sebagai mitra utama karena tiga alasan, diantaranya: (1) statusnya sebagai demokrasi besar ketiga; (2) kepemimpinan dalam ASEAN, (3) lokasi geografisnya yang strategis di tepi Laut Cina Selatan (Kurlantzick 2018).

Gambar 3. 2 Laporan serangan siber di AS 2018-2024



Sumber: Laporan IC3 Tahun 2018-2024 (USAFacts team 2025; Federal Bureau of Investigation 2019; 2020; 2021; 2022; 2023; 2024)

Berdasarkan gambar 3.2 terlihat adanya peningkatan signifikan jumlah *complaints* atau pengaduan masyarakat dan kerugian finansial akibat kejahatan siber di AS. Biro Investigasi Federal (FBI) menerima 5 juta pengaduan tentang serangan siber antara tahun 2018 dan 2024, dan kerugian yang dilaporkan mencapai \$56,7 miliar (USAFacts team 2025). Pada tahun 2019, jumlah *complaints* tercatat sekitar 467 ribu dengan kerugian sekitar 3,5 miliar dolar AS (Federal Bureau of Investigation 2019).

Angka ini naik pada 2020 menjadi lebih dari 790 ribu *complaints* dan terus meningkat hingga mencapai 880 ribu laporan dengan kerugian lebih dari 12,5 miliar dolar AS pada 2023. Lonjakan terbesar terjadi pada 2024, ketika jumlah kerugian mendekati 17 miliar dolar AS hanya dari serangan ransomware besar, ditambah lebih dari 1,2 miliar upaya peretasan terhadap infrastruktur kritis (Federal Bureau of Investigation 2024). Pola ini menunjukkan bahwa meskipun jumlah *complaints* cenderung stabil di kisaran 800 ribu sejak 2020, nilai kerugiannya terus meningkat

tajam. Dimana hal ini menandakan ancaman yang semakin serius terhadap ekonomi nasional.

Pada tahun 2019, AS mulai memperlihatkan kerentanannya melalui serangan *ransomware* terhadap *Perceptics*, yang mengakibatkan kebocoran data biometrik warga dan mendorong *United States Congress* untuk mempertanyakan keamanan teknologi pengenalan wajah (U.S. Department of Homeland Security dan Office of Inspector General 2020). Dari sisi keamanan, hal ini mempertegas bahwa perlindungan data pribadi dan infrastruktur vital merupakan prioritas utama kepentingan nasional. Kemudian pada 2020, pandemi COVID-19 memperburuk kondisi karena lonjakan serangan *ransomware* hingga 148% dan pencurian data penelitian vaksin (Federal Bureau of Investigation 2020).

Situasi ini tidak hanya berdampak pada kesehatan publik, tetapi juga menunjukkan bahwa kompetisi geopolitik merambah ruang digital. Memasuki 2021, ancaman siber semakin meningkat dengan target yang meluas ke sektor energi, keuangan, dan pemerintahan. Serangan berskala global ini memperlihatkan bahwa kemampuan domestik AS tidak cukup untuk menghadapi kejahatan digital yang bersifat lintas batas. Sejalan dengan prinsip *Confidence-Building Measures (CBMs)* di ranah siber yang diadvokasi UN GGE, kerja sama antarnegara memegang peran penting demi memupuk transparansi, menjaga stabilitas, dan mencegah timbulnya konflik (Pawlak 2016).

Di tahun 2022, serangan *ransomware* tetap menekan sektor kesehatan, menegaskan pentingnya kerja sama internasional dalam melindungi sektor vital. Kemudian, laporan FBI (2023) mencatat 880 ribu kasus dengan kerugian lebih dari 12,5 miliar dolar AS. Penipuan investasi dan *business email compromise (BEC)*

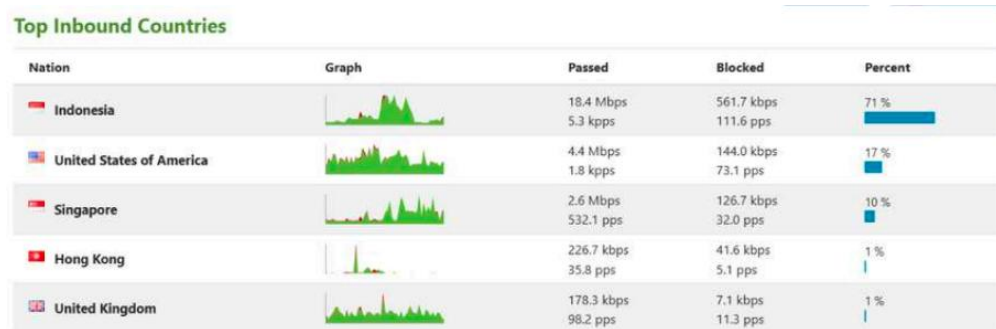
menjadi modus paling merugikan, sementara ransomware mengalami kenaikan tajam hingga 74% dibanding tahun sebelumnya. Hal ini memperlihatkan bahwa isu keamanan siber tidak lagi menjadi masalah teknis, tetapi sudah menjadi isu politik dan ekonomi yang menuntut regulasi lebih kokoh serta koordinasi lintas negara (Federal Bureau of Investigation 2023).

Pada 2024, dengan lebih dari 3.200 serangan *ransomware* besar yang menargetkan sektor kesehatan, energi, dan pemerintahan, AS menghadapi ancaman langsung terhadap keamanan nasional. Dalam hal ini, lebih dari seperempat serangan berasal dari aktor negara asing, terutama dalam bentuk spionase digital untuk mencuri data strategis. Situasi ini memperlihatkan bahwa AS dituntut untuk memperkuat diplomasi siber, baik dalam kerangka bilateral dengan mitra strategis maupun melalui forum multilateral seperti NATO dan Interpol. Dalam konteks bilateral misalnya, komitmen untuk memperkuat kerja sama siber, yang diikat dalam instrumen seperti LoI pada tahun 2015 lalu mampu menjadikan kemitraan AS dengan Indonesia sebagai langkah strategis (Putra 2022).

Hal ini dilandasi oleh kepentingan bersama kedua negara dalam menghadapi tantangan keamanan siber dan menciptakan kesejahteraan. Dimana kondisi tersebut memperlihatkan kepentingan nasional AS dalam bidang siber, sehingga perlunya strategi pertahanan siber berkelanjutan untuk menjaga keamanan, ekonomi, dan stabilitas politik dari ancaman digital lintas negara.

3.1.3 Persamaan Kepentingan, Prinsip, dan Tujuan Indonesia dan Amerika Serikat

Gambar 3. 3 Top 5 Negara Sumber dan Tujuan Kejahatan Siber



Sumber: Laporan Tahunan Kamsiber (KOMINFO CSIRT 2024).

Berdasarkan penjelasan pada sub-bab 3.1.1 dan 3.1.2, terlihat bahwa Indonesia dan AS memiliki kesamaan kepentingan nasional di bidang siber pada periode 2018–2024. Keduanya menghadapi peningkatan signifikan dalam jumlah serangan siber, baik berupa peretasan, *ransomware*, maupun pencurian data yang menargetkan infrastruktur utama, layanan publik, sektor kesehatan, dan keuangan. Hal ini menunjukkan bahwa baik Indonesia maupun AS sama-sama menempatkan keamanan siber sebagai isu strategis yang berhubungan langsung dengan perlindungan keamanan nasional, stabilitas politik, dan keberlangsungan ekonomi.

Sebelum penandatanganan *Letter of Intent* (LoI) pada 2018 hingga terbentuknya *Memorandum of Understanding* (MoU) pada 2024, kerja sama keamanan siber antara Indonesia dan Amerika Serikat dipengaruhi oleh berbagai faktor strategis dan teknis yang berkembang seiring meningkatnya ancaman di ruang digital global. Salah satu pendorong utamanya adalah semakin kompleks dan

lintas batasnya ancaman siber, yang mendorong kedua negara menyadari pentingnya kolaborasi dalam melindungi infrastruktur kritis, data pemerintahan, serta sistem keuangan dan layanan digital. Ancaman-ancaman tersebut tidak lagi dapat ditangani secara unilateral oleh masing-masing negara. Hal ini tercermin dalam pandangan bahwa kerja sama internasional menjadi kebutuhan untuk merespons “beragam tantangan dan permasalahan siber yang terus mengalami perkembangan”, yang kemudian menjadi landasan awal penandatanganan LoI pada tahun 2018 (Antara News 2018). Selain itu, Indonesia masih menghadapi keterbatasan dalam kapasitas sumber daya manusia serta penguasaan teknologi di bidang keamanan siber. Oleh karena itu, Indonesia membutuhkan dukungan teknis, program pelatihan, dan alih pengetahuan dari mitra yang memiliki kemampuan dan pengalaman lebih maju, seperti Amerika Serikat (Rachmawiana 2025).

Secara diplomatik dan strategis, Indonesia dan Amerika Serikat memiliki kepentingan yang sejalan dalam menjaga stabilitas kawasan Indo-Pasifik serta memperkuat tatanan internasional berbasis aturan. Kesamaan kepentingan tersebut mendorong penguatan kerja sama di bidang digital sebagai bagian integral dari hubungan bilateral yang lebih luas dalam kerangka *Comprehensive Strategic Partnership* (DISKOMINFO KOTA MAKASSAR 2024). Selain itu, Amerika Serikat sejak awal menunjukkan komitmen untuk memberikan bantuan serta program pelatihan di bidang keamanan siber yang memperkuat kolaborasi teknis jauh sebelum penandatanganan MoU tahun 2024, termasuk dukungan pendanaan dan kegiatan pelatihan yang mulai berjalan sekitar tahun 2022 (Rahman Asmardika 2024).

Dari sisi prinsip, Indonesia dan AS sepakat untuk menekankan pentingnya perlindungan data pribadi dan kedaulatan digital. Indonesia menekankan kedaulatan data sebagai bagian dari kedaulatan negara, sementara AS menekankan perlindungan data warga negara dan infrastruktur utama sebagai aspek hak-hak sipil dan keamanan nasional. Walaupun konteks politik dan kapasitas berbeda, kedua negara tersebut sepakat bahwa perlindungan data merupakan nilai penting yang harus dijaga dalam tata kelola digital.

Dari sisi tujuan, baik Indonesia maupun AS sama-sama memandang kerja sama internasional sebagai jalan yang tidak bisa dihindarkan dalam menghadapi ancaman siber lintas batas. Indonesia aktif dalam forum ASEAN dan berbagai kerja sama regional, sementara AS memperluas diplomasi sibernya melalui NATO, Interpol, serta kerja sama bilateral dengan mitra strategis. Hal ini sejalan dengan pandangan Holsti yang menekankan bahwa kepentingan nasional tidak hanya bersifat *inward-looking*, tetapi juga terkait dengan upaya negara menjaga stabilitas eksternal melalui kerja sama internasional. Hal tersebut menjelaskan bahwa meskipun memiliki kapasitas berbeda, Indonesia dan AS memiliki tujuan yang sama, yaitu menciptakan ekosistem digital yang aman, stabil, dan mendukung kepentingan nasional di tengah meningkatnya ancaman siber global.

Kedekatan kepentingan Indonesia dan AS semakin tampak melalui peningkatan status kerja sama keamanan siber. Pada 4 Desember 2024, Pemerintah Indonesia lewat Badan Siber dan Sandi Negara (BSSN) bersama Pemerintah AS melalui Kedutaan Besar di Jakarta resmi menandatangani *Memorandum of Understanding (MoU)* dan *Memorandum Saling Pengertian (MSP)* (Badan Siber dan Sandi Negara 2024a). Penandatanganan ini dilakukan oleh Kepala BSSN Hinsa

Siburian dan Duta Besar AS untuk Indonesia Kamala Shirin Lakhdhir. Melalui MoU dan MSP tersebut, kedua negara meneguhkan komitmen untuk memperluas kerjasama mereka, terutama dalam pertukaran informasi, pelatihan, penelitian, dan kerja sama internasional yang bertujuan untuk menghadapi ancaman siber.

Sejak tahun 2018, telah terlaksana 41 kegiatan bersama yang mencakup berbagai hal, mulai dari berbagi informasi tentang serangan terbaru hingga peningkatan kemampuan dalam mendeteksi insiden. Ruang lingkup kerja sama yang diperluas meliputi penyusunan strategi dan tata kelola keamanan siber, peningkatan kualitas sumber daya manusia dan teknologi, pelibatan aktor-aktor terkait, penguatan kesadaran publik, serta koordinasi di forum internasional yang relevan. Inisiatif ini sekaligus mencerminkan nilai yang sama-sama dijunjung oleh Indonesia dan AS, yakni demokrasi, keberagaman, serta komitmen terhadap tatanan internasional berbasis aturan, yang telah menjadi dasar hubungan diplomatik kedua negara selama 75 tahun terakhir (DISKOMINFO KOTA MAKASSAR 2024).

3.2 *Equitable Distribution of Costs, Risks, Burdens, and Rewards among the Partners to a Collaborative Undertaking* (Pembagian yang adil atas biaya, risiko, beban, dan manfaat di antara mitra dalam suatu kerja sama).

Salah satu implementasi penting dari kerja sama ini tercermin melalui pemberian hibah USTDA untuk studi kelayakan penerapan teknologi Open RAN dengan tujuan menghubungkan 1.621 desa di Indonesia yang belum mendapatkan layanan telekomunikasi (U. S. Embassy Jakarta 2024). Dalam konteks kerja sama siber, perlu ditegaskan bahwa Open RAN adalah arsitektur jaringan berbasis perangkat lunak yang sangat bergantung pada keamanan sistem. Karena itu,

dukungan AS di sektor ini bukan hanya perluasan layanan telekomunikasi, tetapi juga penguatan infrastruktur informasi yang dikategorikan sebagai infrastruktur kritis. Dalam hal ini, perusahaan AS seperti Mavenir, Parallel Wireless, dan IBM terlibat dalam penyediaan perangkat keras sekaligus transfer keahlian teknis.

Meskipun 1.621 desa belum memiliki layanan telekomunikasi, memang bisa diartikan bahwasannya akses internet di sana sangat terbatas atau bahkan tidak ada. Namun, ini tidak otomatis membuat wilayah tersebut bebas dari kejahatan atau pelanggaran siber. Kejahatan bisa menargetkan warga desa, meski pelakunya berada di tempat lain. Contohnya adalah adanya penipuan SMS, pencatutan data kependudukan, atau penyalahgunaan identitas kepada bank. Dimana data penduduk, bantuan sosial, layanan kesehatan & keuangan, dan catatan kependudukan tetap masuk ke sistem nasional.

Pelanggaran bisa terjadi pada level server pemerintah, bukan di desa tersebut. Warga yang keluar-masuk desa tetap menggunakan internet di luar wilayahnya. Risiko kejahatan siber mengikuti perilaku digital individu, bukan lokasi desanya. Maka dari itu, perlu dipahami bahwa keamanan siber tidak hanya berkaitan dengan ada atau tidaknya internet di suatu wilayah, tetapi mencakup perlindungan atas seluruh sistem yang memproses, menyimpan, dan mengalirkan data. Siber sendiri merupakan suatu ranah yang mampu membuat masyarakat untuk saling terhubung melalui suatu jaringan, untuk menjalankan beragam aktivitas rutin mereka (Kementerian Pertahanan Republik Indonesia 2014).

Protokol jaringan, data server, dan layanan cloud merupakan bagian dari ekosistem yang tetap membutuhkan perlindungan, bahkan ketika *user* berada di lokasi dengan akses internet yang terbatas. Dalam hal ini, Open RAN relevan dalam

kerangka keamanan siber karena sifatnya yang berbasis perangkat lunak membuatnya lebih rentan terhadap manipulasi kode, intersepsi data, dan gangguan pada integritas jaringan. Sehingga, implementasi teknologi ini dalam kerja sama Indonesia dan AS menuntut adanya standar pengamanan, audit teknis, serta peningkatan kapasitas nasional agar infrastruktur yang baru dibangun tidak hanya memperluas konektivitas, tetapi juga memiliki ketahanan siber yang memadai. Sehingga, meskipun desa-desa tersebut belum atau bahkan tidak cukup memiliki layanan internet, pembangunan infrastruktur telekomunikasinya sudah masuk dalam ruang siber nasional.

Selain arus teknologi, transaksi juga terlihat dari arus keahlian. Lokakarya keamanan siber selama empat hari yang berfokus pada perlindungan pelabuhan strategis Indonesia, dengan pendampingan pakar dari SANS Institute, menjadi bentuk penguatan kapasitas teknis yang bergerak dari satu negara ke negara lain (U. S. Embassy & Consulates in Indonesia 2025). Kegiatan serupa muncul melalui kuliah umum pakar keamanan siber Amerika, Beau Woods, di berbagai perguruan tinggi Indonesia. Arus keahlian berfungsi untuk memastikan bahwa transaksi kerja sama benar-benar diarahkan pada peningkatan kemampuan pertahanan siber.

Arus regulasi dan standar juga membentuk transaksi yang penting. Lokakarya yang diselenggarakan US-ASEAN *Business Council* menjadi wadah dialog strategis bagi peningkatan kapasitas aktor pemerintah dan industri, termasuk dalam adopsi ASEAN *Cybersecurity Assessment Maturity Model (ACAM)* (Kementerian Keuangan Republik Indonesia 2025). Selain itu, pembahasan protokol arus data lintas batas dalam kerangka perjanjian perdagangan baru membantu menyediakan dasar hukum bagi transfer data digital. Regulasi dan

standar ini merupakan inti dari transaksi siber karena menyediakan mekanisme perlindungan data dan interoperabilitas, sehingga menjadi komponen substansial dalam kerja sama keamanan siber bilateral.

Hasil transaksi kerja sama ini memberikan kontribusi yang jelas bagi kedua negara. Bagi Indonesia, manfaatnya mencakup peningkatan kapasitas nasional melalui peningkatan keterampilan personel keamanan siber (BSSN dan KPLP), penguatan perlindungan infrastruktur seperti pelabuhan strategis, akses terhadap teknologi jaringan yang lebih aman seperti Open RAN, serta peningkatan kematangan keamanan siber melalui implementasi Strategi Keamanan Siber Nasional (SKSN). Bagi AS, transaksi ini memberikan akses komersial ke pasar telekomunikasi Indonesia, membangun ekosistem digital berbasis regulasi yang mendukung kepentingan regional, dan memperkuat keamanan jalur perdagangan maritim penting dalam rantai pasok global (Khoirunnisa dkk. 2024). Artinya adalah, hasil kerja sama tetap terkait langsung dengan keamanan siber, bukan untuk mencari keuntungan ekonomi atau teknis saja.

Dalam alokasi pendanaan, MSP menjelaskan pada Paragraf 5 bahwa kerja sama Indonesia dan AS bermaksud untuk menanggung biaya masing-masing terkait dengan kegiatan mereka, kecuali jika diputuskan lain secara bersama-sama. Prinsip pembiayaan ini menunjukkan komitmen berbagi beban yang setara dan memastikan keberlanjutan inisiatif-inisiatif yang disebutkan di atas, dimana masing-masing pihak bertanggung jawab atas sumber dayanya sendiri dalam mendukung transaksi dan arus kerja sama yang telah disepakati.

BSSN sendiri mencatat dalam Peraturan Sekretaris Utama No. 1 Tahun 2024 bahwasannya pelaksanaan anggaran untuk kegiatan-kegiatan kerja sama

internasional harus mengikuti prinsip-prinsip akuntabilitas dan tata kelola keuangan negara yang efektif, efisien, transparan, dan tertib, dengan Pejabat Pembuat Komitmen (PPK) dan Pejabat Penanda Tangan Surat Perintah Membayar (PPSPM) yang ditunjuk secara resmi memegang peran kunci dalam memastikan setiap pengeluaran anggaran dilakukan secara sah dan dapat dipertanggungjawabkan (Badan Siber dan Sandi Negara 2024c). Artinya, dana yang dialokasikan untuk mendukung transaksi kerja sama dengan AS, baik yang berasal dari APBN maupun dari hibah luar negeri, harus dikelola melalui mekanisme perbendaharaan negara yang ketat.

Setiap tahapan, mulai dari perencanaan, komitmen, verifikasi, hingga pembayaran, wajib dilakukan oleh pejabat yang berwenang sesuai dengan ketentuan tersebut. Hal ini memastikan bahwa aliran pendanaan dalam kerja sama ini memiliki landasan hukum dan administrasi yang kuat, sehingga meminimalisir risiko dan mendukung prinsip keberlanjutan yang ditekankan dalam kerangka kerja sama. BSSN sendiri memiliki anggaran pribadi yang berbeda setiap tahunnya, berikut ini adalah arus anggaran milik BSSN dari tahun ke tahun:

Gambar 3. 4 Alokasi Anggaran dan Realisasi Anggaran BSSN 2019-2024



Sumber: LKJ tahun 2024 (Badan Siber dan Sandi Negara 2024c)

Anggaran ini menunjukkan tren yang sangat positif, baik dari sisi besaran alokasi maupun efektivitas penyerapannya. Alokasi anggaran BSSN mengalami peningkatan yang signifikan dari tahun 2019 hingga puncaknya pada tahun 2024, yang mencerminkan pengakuan pemerintah terhadap peran strategis dan beban kerja BSSN yang terus bertumbuh, termasuk dalam mengelola kerja sama internasional seperti dengan AS.

Jika dilihat dari Gambar 3.4, realisasi anggaran BSSN konsisten mendekati atau bahkan mencapai 100% setiap tahunnya, dengan persentase penyerapan yang sangat tinggi. BSSN mencatat pencapaian mereka selalu di atas 96% dan bahkan menyentuh 99,95% pada tahun 2022. Capaian ini menunjukkan kapabilitas tata kelola keuangan BSSN yang sangat baik, di mana mekanisme dan prinsip-prinsip dalam Peraturan Sekretaris Utama No. 1 Tahun 2024 telah diimplementasikan secara efektif untuk memastikan dana yang dialokasikan dapat dimanfaatkan secara optimal, tepat sasaran, dan akuntabel. Ketika BSSN memiliki kinerja anggaran yang kuat, BSSN memiliki fondasi fiskal yang solid untuk mendanai kontribusinya

dalam kerja sama dengan AS. Kemampuan penyerapan anggaran yang tinggi membuktikan bahwa BSSN memiliki kapasitas institusi dan prosedur yang mapan untuk mengelola aliran dana yang kompleks, baik dari APBN maupun dari mitra internasional, sesuai dengan prinsip *sharing cost* yang disepakati dalam MSP.

Dalam perspektif jangka panjang, kerja sama ini mencerminkan suatu perubahan dalam pola hubungan bilateral Indonesia–AS. Dimana mekanisme yang dibangun tidak lagi terbatas pada hubungan transaksional penjual–pembeli, tetapi kedua negara kini bergerak menuju kemitraan yang lebih erat berbasis penciptaan bersama serta penyusunan standar bersama. Bagi Indonesia, perubahan ini menghadirkan peluang untuk membangun ekosistem digital yang lebih resilien sekaligus memperkuat posisi strategis dalam tata kelola keamanan siber kawasan ASEAN.

Sementara itu, bagi AS, perubahan ini menjamin kehadiran mitra digital yang stabil dan aman di Asia Tenggara, sejalan dengan strategi Indo-Pasifik (IPEF), serta memastikan bahwa norma-norma siber yang berkembang mencerminkan kepentingan bersama. Dalam hal ini, jaringan transaksi siber yang terbentuk memainkan peran penting dalam memperkuat mekanisme pertahanan kolektif, meningkatkan stabilitas kawasan, serta memberikan perlindungan lebih optimal terhadap infrastruktur vital dan ekosistem digital kedua negara dari ancaman yang bersifat transnasional.

Kerja sama keamanan siber antara Indonesia dan Amerika Serikat menunjukkan adanya pembagian risiko dan beban melalui mekanisme pertukaran informasi dan koordinasi teknis secara bilateral. Hal ini tercermin dalam peningkatan hubungan kerja sama kedua negara yang diformalkan melalui

penandatanganan MoU BSSN dan pemerintah Amerika Serikat pada 4 Desember 2024. Dalam kerangka kerja sama tersebut, kedua pihak sepakat untuk melakukan koordinasi serta berbagi informasi guna menekan ancaman, risiko, dan potensi serangan siber, sehingga penanganan ancaman tidak lagi ditanggung secara sepihak oleh masing-masing negara. Melalui pendekatan ini, Indonesia dan Amerika Serikat secara bersama-sama memikul tanggung jawab dalam meningkatkan keamanan siber dan ketahanan infrastruktur digital masing-masing (Badan Siber dan Sandi Negara 2024a).

3.3 *Trust that Commitments will be fulfilled, Low Probability of Defections* **(Kepercayaan bahwa komitmen akan dipenuhi, dengan probabilitas rendah terjadinya pengkhianatan)**

Holsti menjelaskan bahwa aspek etika yang berkaitan dengan arah kebijakan, peran, tujuan, dan tindakan dalam kebijakan luar negeri sering kali sudah melekat dalam berbagai pertimbangan lainnya. Hubungan antara etika dan hasil kebijakan luar negeri kerap terlihat terlalu disederhanakan, salah satunya karena cara pejabat pemerintah menyampaikan kebijakan tersebut kepada publik. Dalam banyak pernyataan resmi, kebijakan luar negeri lebih sering dijelaskan sebagai tujuan ideal atau doktrin tertentu, bukan sebagai persoalan nyata yang perlu dihadapi dan diselesaikan.

Pada praktiknya, para pembuat kebijakan tidak selalu mengambil keputusan terutama berdasarkan pertimbangan etika, sebagaimana organisasi bisnis yang menyelesaikan masalah dengan berpedoman pada aturan hukum atau prinsip etika. Meski demikian, nilai-nilai moral dan etika tetap berperan penting dan terus

memengaruhi cara pemerintah bersikap dan bertindak terhadap negara lain (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 392-393).

Pada MoU 2024 paragraf 1 menyebutkan untuk mendorong kemitraan dan menyediakan suatu kerangka kerja guna memperkuat kerja sama dan pengembangan kapasitas di ruang siber antara para peserta, maka berdasarkan Laporan Kinerja BSSN (2024), kerja sama antara Indonesia dengan AS di bidang keamanan siber telah berkembang menjadi suatu kemitraan yang komprehensif dan implementatif. Dimana hal tersebut secara signifikan berkontribusi terhadap pencapaian posisi Indonesia sebagai role model dengan skor sempurna 100 dalam Global Cybersecurity Index (GCI) 2024. Kerjasama bilateral ini secara konkret diwujudkan melalui serangkaian aktivitas yang selaras dengan pilar-pilar inti GCI, terutama dalam aspek Pengembangan Kapasitas dan Teknis, dimana BSSN aktif menerima transfer ilmu pengetahuan dan keahlian mutakhir dari pihak AS, mencakup pelatihan lanjutan untuk operasi keamanan siber, pembangunan dan penguatan kapabilitas *Security Operation Center (SOC)*, serta peningkatan kompetensi dalam penanganan dan tanggap insiden siber yang berdampak langsung pada peningkatan kematangan Gov-CSIRT dan Nat-CSIRT Indonesia (Badan Siber dan Sandi Negara 2024c).

Selain itu, kerja sama ini juga diperkuat melalui Perjanjian Kerja Sama (PKS) yang bersifat formal dan operasional. Dimana fungsinya adalah memfasilitasi terciptanya ruang berbagi informasi intelijen ancaman siber secara lebih terstruktur, disertai dengan partisipasi aktif dalam latihan siber bersama atau *joint cyber exercises* yang bertujuan mempertajam kesiapsiagaan nasional dalam menghadapi serangan siber yang kompleks. Dalam hal ini, keaktifan Indonesia

dalam jejaring keamanan siber global yang didukung oleh kemitraan dengan AS ini tidak hanya memperkuat pilar kerja sama tetapi juga menegaskan posisi Indonesia sebagai mitra yang kredibel dan setara dalam diplomasi siber internasional (Badan Siber dan Sandi Negara 2024c).

3.3.1 *Dokumen Kesepakatan Formal*

Dalam era perkembangan teknologi informasi yang semakin pesat, kerja sama internasional di bidang keamanan siber menjadi instrumen penting bagi negara-negara untuk menjaga kepentingan nasional. Indonesia melalui Badan Siber dan Sandi Negara (BSSN) menilai bahwa ancaman siber bersifat lintas batas sehingga tidak bisa diatasi hanya dengan kebijakan dalam negeri (Ilaina dan Nugraha 2025). Atas dasar itu, dibutuhkan perjanjian formal dengan negara mitra, terutama AS yang memiliki keunggulan teknologi serta pengalaman dalam menangani isu keamanan siber. Kerja sama ini tidak hanya memperkuat kapasitas teknis Indonesia dalam menghadapi berbagai ancaman, tetapi juga memberikan nilai tambah bagi posisi diplomatik Indonesia di forum internasional.

Sebagai wujud konkret, kedua negara menandatangani dokumen formal berupa Memorandum Saling Pengertian (MSP) dan *Memorandum of Understanding (MoU)* pada tahun 2024 yang menjadi landasan penguatan hubungan bilateral di bidang keamanan siber. Namun demikian, juga perlu ditekankan bahwa kerjasama formal ini bukan dimulai dari nol, tetapi merupakan penguatan dan kelanjutan dari komitmen yang telah dibangun sebelumnya, salah satunya melalui penandatanganan LoI pada tahun 2015 yang menjadi kerangka awal kerja sama siber di dunia maya (Fatihah 2022).

Gambar 3. 5 Pertemuan antara Indonesia dan Amerika Serikat



Sumber: (Badan Siber dan Sandi Negara 2024a).

Dalam hal ini, kedua Memorandum yang ditandatangani oleh Pemerintah Indonesia dan AS pada tahun 2024 memiliki peran penting dalam memperkuat hubungan strategis kedua negara di bidang keamanan siber. Dokumen ini tidak hanya berfungsi sebagai simbol kerja sama diplomatik, tetapi juga menjadi dasar hukum yang mengatur bentuk kerja sama teknis dan kebijakan. MSP ditulis dengan visi untuk mendorong kemitraan dan menyediakan suatu kerangka kerja untuk memperkuat kerja sama dan pengembangan kapasitas di ruang siber antara Indonesia dan AS.

MSP dilatar belakangi oleh semangat memperingati 75 tahun hubungan diplomatik serta komitmen untuk memperkuat Kemitraan Strategis Komprehensif, dan mencatat dengan baik keberhasilan kerja sama siber sebelumnya yang dimulai sejak 2018. Jejak kerja sama yang diinisiasi tahun 2018 dapat ditelusuri kembali ke LoI tahun 2015 (Pawlak 2016). Dokumen awal ini merefleksikan niat sungguh-sungguh kedua negara di ranah siber dan berfungsi sebagai fondasi bagi pengaturan yang lebih konkret di kemudian hari, yakni MSP dan MoU tahun 2024.

Pada MoU paragraf 3 menyebutkan dimana bentuk kerja sama diwujudkan melalui instansi penjuru, yaitu BSSN untuk Indonesia dan Departemen Luar Negeri AS (DoS) untuk AS, yang akan menyusun pengaturan pelaksanaan lebih lanjut. Namun, status hukum MSP ditegaskan secara jelas dimana dokumen ini bukanlah sebuah perjanjian internasional dan tidak menciptakan hak atau kewajiban berdasarkan hukum internasional maupun domestik. Pelaksanaannya tunduk dan harus konsisten dengan hukum serta kewajiban internasional masing-masing negara.

MSP juga memiliki masa berlaku selama 5 (lima) tahun sejak ditandatangani, dan dapat diakhiri oleh salah satu pihak dengan pemberitahuan tertulis minimal 1 (satu) bulan sebelumnya. Dalam MoU paragraf 2 menyebutkan dimana area kerjasama yang disepakati mencakup pertukaran pengalaman dan praktik terbaik dalam penyusunan strategi serta tata kelola keamanan siber nasional, peningkatan kapasitas sumber daya manusia dan teknologi, serta perlindungan infrastruktur informasi vital (IIV) yang berhubungan langsung dengan keamanan nasional (Badan Siber dan Sandi Negara 2024b).

Kemitraan dalam MSP dan MoU 2024 tetap fokus pada bidang-bidang prioritas yang telah ditetapkan dalam LoI 2015, seperti strategi siber nasional, penanganan insiden, pemberantasan kejahatan siber, dan peningkatan literasi keamanan siber (Putra 2022). Hal ini menunjukkan konsistensi sekaligus vertikalisasi agenda kerja sama dari masa ke masa. Selain itu, Memorandum ini juga mengatur mekanisme pelaksanaan kerja sama melalui pertukaran pandangan, kunjungan pejabat dan pakar, serta program pelatihan yang diarahkan untuk memperkuat kemampuan teknis dalam menghadapi risiko dan insiden siber. Ruang

lingkupnya juga melibatkan peran pemangku kepentingan non-pemerintah, termasuk akademisi, sektor industri, dan lembaga penelitian untuk mendukung implementasi program. Sehingga, hal tersebut mampu memberikan manfaat yang lebih luas bagi ekosistem digital nasional.

Pada tingkat global, Memorandum ini memberi peluang bagi Indonesia dan AS untuk memperkuat posisi di forum internasional terkait keamanan siber, termasuk melalui penelitian bersama, pengembangan teknologi baru, dan koordinasi berbagi informasi demi meminimalkan ancaman lintas negara. Dalam hal ini, dokumen ini menegaskan upaya kedua negara untuk membangun hubungan yang tidak hanya menekankan aspek teknis, tetapi juga mencakup dimensi diplomasi, regulasi, dan politik internasional, sekaligus memperkuat posisi Indonesia sebagai mitra yang relevan dalam tata kelola keamanan siber global.

Kesepakatan formal yang terdapat dalam MoU 2024 menyebutkan bahwa kerja sama menyepakati pertukaran data, informasi, dan dokumentasi terkait kekayaan intelektual yang ditetapkan bersama. Kerja sama ini mencakup berbagi informasi nonrahasia serta praktik terbaik guna mendukung efektivitas proses pemeriksaan dan pendaftaran paten, desain industri, dan merek, baik dalam rangka meningkatkan efisiensi operasional lembaga kekayaan intelektual maupun memperkuat perlindungan dan penegakan hak kekayaan intelektual.

Kerja sama juga sepakat untuk melakukan kolaborasi dalam penyelenggaraan program pengembangan kapasitas yang diarahkan pada peningkatan administrasi kelembagaan, penguatan sumber daya manusia, serta peningkatan kualitas pemeriksaan paten, desain industri, dan merek. Selain itu, kerja sama ini bertujuan memperkuat perlindungan, pemanfaatan, dan penegakan

hak kekayaan intelektual serta mendorong peran strategis perlindungan kekayaan intelektual dalam mendukung inovasi, alih teknologi, komersialisasi, dan pertumbuhan ekonomi (Ministry of Foreign Affairs 2024).

Gambar 3. 6 Indikator Perjanjian Kinerja dalam Kerangka BSSN (2024)

Sasaran Strategis		Indikator Kinerja Sasaran Strategis		Target
Perspektif Penerima Layanan				
SS.A.1	Meningkatnya Keamanan Siber Indonesia	IKSS.A.1.1	Global Cybersecurity Index (GCI)	94,88
SS.A.2	Meningkatnya Kapasitas Keamanan Siber dan Sandi	IKSS.A.2.1	Persentase Rekomendasi Hasil Operasi Keamanan Siber, Operasi Keamanan dan Pengendalian Informasi, dan Operasi Sandi yang Termanfaatkan	97%
		IKSS.A.2.2	Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan Keamanan Siber dengan skor minimal 2,59	100%
Perspektif Proses Bisnis				
SS.B.1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang Berkualitas	IKSS.B.1.1	Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi	85%
		IKSS.B.1.2	Nilai Kualitas Kebijakan (NKK) Bidang Keamanan Siber dan Sandi	78
SS.B.2	Terpenuhinya Kerja Sama Keamanan Siber dan Sandi	IKSS.B.2.1	Persentase Pencapaian Kerja Sama Keamanan Siber Internasional	100%
SS.B.3	Meningkatnya Kualitas Operasi Keamanan Siber dan Sandi	IKSS.B.3.1	Persentase Penyelenggaraan Operasi Keamanan Siber, Operasi Keamanan dan Pengendalian Informasi, dan Operasi Sandi Sesuai Standar	100%
SS.B.4	Meningkatnya Kualitas Hasil Pembinaan Keamanan Siber dan Sandi	IKSS.B.4.1	Jumlah Computer Security Incident Response Team (CSIRT) Organisasi yang Difasilitasi Pembentukannya	156
Perspektif Penguatan Internal				
SS.C.1	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi pada Pelayanan Publik	IKSS.C.1.1	Indeks Reformasi Birokrasi	80
Perspektif Anggaran				
SS.D.1	Meningkatnya Pengelolaan Keuangan BSSN yang Akuntabel	IKSS.D.1.1	Indeks Kualitas Pelaksanaan Anggaran	92
		IKSS.D.1.2	Opini BPK	WTP

Sumber: LKJ BSSN (Badan Siber dan Sandi Negara 2024b)

Arah kebijakan BSSN juga menekankan optimalisasi kerja sama lintas sektor, baik dengan lembaga pemerintah, pihak swasta, maupun mitra luar negeri,

untuk membangun ekosistem keamanan siber yang lebih komprehensif. Hal ini menunjukkan bahwa Indonesia telah menyiapkan instrumen kelembagaan dan kerangka kebijakan yang relatif konkret sebagai landasan bagi kerja sama siber, termasuk dengan AS. Namun demikian, apabila ditinjau dari arah kebijakan pertahanan secara lebih luas, fokus Indonesia masih cenderung pada pembangunan kapasitas domestik dan penyelesaian tantangan internal.

Hadirnya dokumen formal berupa MSP/MoU antara Pemerintah Indonesia dan Pemerintah AS juga mencerminkan komitmen kedua negara dalam memperkuat kerja sama strategis di bidang keamanan siber. Dokumen ini memberikan kerangka aturan yang lebih jelas dengan menetapkan tujuan untuk memperkuat kerja sama dan pengembangan kapasitas, menegaskan BSSN dan Departemen Luar Negeri AS sebagai instansi penjuru, serta merinci area kerja sama yang mencakup berbagi praktik terbaik, peningkatan kapasitas sumber daya manusia, pertukaran informasi ancaman siber, dan kolaborasi di forum internasional. Kemudian, adanya aturan mengenai kerahasiaan informasi (Paragraf 7) dan penyelesaian masalah melalui konsultasi (Paragraf 6) juga menjadi elemen penting yang membangun kepercayaan dan mengelola ekspektasi kedua belah pihak. Meskipun demikian, karakter MSP ini secara tegas dinyatakan bukan sebagai perjanjian internasional yang mengikat secara hukum (*non-binding*), sebagaimana diatur dalam Paragraf 9 MSP.

Status ini mencerminkan sifat kerja sama yang masih didasarkan pada kehendak politik dan kepentingan strategis masing-masing, ketimbang kewajiban hukum yang memaksa. Dimana efektivitas aturan dalam MSP sangat bergantung pada kemauan politik (*political will*) dan mekanisme implementasi lebih lanjut dari

masing-masing pihak, ketimbang pada kekuatan hukumnya. Artinya, MSP berfungsi sebagai kerangka kerja kooperatif (*soft law*) yang fleksibel, yang bisa diinterpretasikan bahwa keterikatan kedua negara untuk bekerja sama didasarkan pada tanpa adanya ikatan hukum yang kaku. Hal ini selaras dengan pendekatan Indonesia yang berhati-hati dan menitikberatkan pada kemandirian, dan tetap membuka ruang bagi AS untuk memajukan agenda keamanan sibernya di kawasan melalui kemitraan.

3.4 *Interactions Conducted on the basis of Approximate Reciprocity, Reability and Reputation for Predictability* (Interaksi yang dilakukan berdasarkan prinsip timbal balik yang mendekati kesetaraan, keandalan, dan reputasi yang dapat diprediksi)

Keberlanjutan konflik dan kekerasan antarnegara sering kali mendorong anggapan bahwa politik internasional pada dasarnya merupakan arena perebutan kekuasaan, serta bahwa ketiadaan otoritas supranasional yang mampu menegakkan perdamaian menjadikan perdamaian universal sebagai sesuatu yang sulit diwujudkan. Meskipun frekuensi krisis dan perang tidak memberikan alasan untuk bersikap terlalu optimistis, Holsti menekankan bahwa dalam praktiknya, negara-negara pada umumnya berinteraksi melalui mekanisme timbal balik yang tidak selalu berujung pada kekerasan. Lebih lanjut, Holsti menjelaskan bahwa konflik dan kerja sama tidak selalu merupakan dua bentuk hubungan yang saling bertentangan, karena hubungan politik internasional hampir selalu mengandung unsur konflik dalam kadar tertentu (Holsti, K. J. (Kalevi Jaakko) 1987, halaman 432-433).

Jika dilihat dari sisi eksternal, AS dengan kapasitas hukum dan infrastruktur siber yang lebih maju telah memberikan pengaruh signifikan terhadap Indonesia melalui berbagai inisiatif bilateral. Contohnya, adanya *Letter of Intent* dan program pelatihan yang diselenggarakan BSSN bersama Kedutaan Besar AS di Jakarta mendorong Indonesia untuk memperkuat regulasi dan strategi siber domestik, termasuk penanganan terorisme siber, peningkatan kapasitas sumber daya manusia, dan mekanisme pertukaran informasi yang lebih sistematis (Golose 2022; Putra 2022).

Pada 2019, Indonesia mencatat 290,3 juta serangan siber dan mengalami kenaikan hingga 2020 (lihat gambar 3.1). Meskipun sempat menurun, angka yang dicapai tetap tinggi, sehingga, menempatkan Indonesia dalam posisi yang mengkhawatirkan sebagai negara sumber sekaligus target utama serangan digital. Dimana hal tersebut mirip dengan tantangan yang dihadapi oleh AS. Kesamaan pola ancaman dengan AS hanya berfungsi sebagai latar situasional, sementara keputusan bekerja sama tetap bertumpu pada persepsi manfaat yang ditawarkan kebijakan pihak lain. Namun, kapasitas pertahanan Indonesia secara internal masih tertinggal. Dari sisi internal, kerangka hukum dan strategi keamanan siber nasional dinilai lemah karena belum memiliki regulasi spesifik maupun kemitraan strategis dengan sektor swasta (Fatihah 2022). Akibatnya, infrastruktur digital nasional sangat rentan, sebagaimana dibuktikan oleh rangkaian kebocoran data massal, seperti data pengguna eHAC, BPJS Kesehatan, dan e-commerce (Afifa 2021).

Hal tersebut memaksa Indonesia harus menyesuaikan kebijakan dengan kondisi domestik yang berbeda. Situasi tersebut memperkuat persepsi Indonesia bahwa dukungan teknis dan regulatif dari AS dapat membantu menutup celah

kapasitas nasional. Pengalaman menghadapi ancaman ekstremisme siber, pengembangan regulasi melalui *National Action Plan for Countering Extremism*, serta penerbitan Peraturan Presiden tentang Penanggulangan Terorisme memengaruhi bagaimana AS menilai dimensi sosial-politik dalam strategi kontra-sibernya yang biasanya lebih teknokratis (Anwary 2022; Ramadhan 2023). Hal ini menunjukkan bahwa meskipun pengaruh AS lebih dominan, interaksi kebijakan kedua negara bersifat timbal balik.

Selain itu, Indonesia juga belajar dari kerangka kebijakan siber AS yang komprehensif, termasuk *National Strategy to Secure Cyberspace* dan *International Strategy for Cyberspace*, serta struktur komando yang melibatkan DHS, FBI, dan USCYBERCOM untuk mengelola ancaman siber secara nasional (Chen 2013; Langevin dkk. 2008). Kerangka ini menjadi acuan bagi Indonesia untuk menata ulang kelembagaan, membangun Desk Resiliensi Siber dan Informasi Nasional di bawah Kemenkopolhukam, dan akhirnya membentuk BSSN.

Dua konsep kedaulatan siber yang bertolak belakang membentuk interaksi kebijakan internasional. Konsep pertama, *'Sovereignty as a Principal'* yang dianut AS dan Inggris, bersifat lunak dan memperbolehkan operasi siber tanpa izin di wilayah negara lain selama tidak termasuk intervensi atau penggunaan kekuatan, sebagaimana dioperasionalkan melalui strategi bertahan ke depan dan doktrin CYBERCOM (Taichman 2021; Eichensehr 2019). Konsep kedua, *'Sovereignty as a Rule'* yang didukung Indonesia, Prancis, dan Belanda, bersifat kaku dan menuntut penghormatan penuh terhadap kedaulatan negara di dunia maya, di mana pelanggaran terhadapnya dianggap sebagai tindakan melawan hukum internasional (Fatihah 2022).

Indonesia juga menyadari perbedaan paradigma ancaman siber, di mana AS telah menetapkan *cyber threat* sebagai ancaman strategis nomor satu, sementara Indonesia dalam Perpres No. 97 Tahun 2015 masih mengkategorikan ancaman siber sebagai ancaman non-militer. Kesadaran ini mendorong rekomendasi untuk mengklasifikasikan ancaman siber sebagai ancaman militer atau hibrid, serta menetapkan domain siber sebagai domain pertahanan baru (Billo dan Chang 2004).

Indonesia menyesuaikan diri dengan praktik internasional dan standar keamanan siber global, sementara AS memperluas jangkauan kerjasamanya ke Asia Tenggara dan mempertimbangkan pengalaman Indonesia dalam menghadapi aspek sosial, budaya, dan regulatif dari ekstremisme siber. Dalam hal ini, Indonesia berada dalam posisi adaptif terhadap AS sebagai pemimpin tata kelola siber global, sementara AS tetap memanfaatkan pengalaman Indonesia untuk menyempurnakan strategi regionalnya. Perubahan ini menegaskan bahwa kebijakan siber masing-masing negara tidak berdiri sendiri, tetapi merupakan hasil kompromi, penyesuaian, dan persepsi manfaat timbal balik dari kebijakan negara lain (Chou dkk. 2018).

3.4.1 Bentuk-Bentuk Aktivitas Kerjasama Siber antara Indonesia dan Amerika Serikat

Kerjasama siber bilateral antara Indonesia dan AS dalam periode 2018-2024 termanifestasi dalam beberapa bentuk yang saling melengkapi. Dasar kerjasama ini telah berkembang dari kerangka awal seperti LoI 2015 menjadi kesepakatan yang lebih formal. Bentuk pertama dan yang mendasar adalah penguatan kerangka kerja sama dan dialog kebijakan melalui instrumen hukum bilateral. Puncak perkembangan ini adalah penandatanganan nota kesepahaman atau kemitraan keamanan (MoU/MSP) antara Kepala BSSN dan Duta Besar AS

untuk Indonesia pada akhir tahun 2024, yang bertujuan memperkuat dan memformalkan seluruh area kerjasama yang telah berjalan. Kerangka ini memfasilitasi dialog strategis dan menjadi payung hukum bagi aktivitas-aktivitas praktis berikutnya.

Bentuk kedua adalah program pembangunan kapasitas dan pelatihan. Ini merupakan area kerjasama yang sangat aktif. AS berkomitmen memberikan bantuan teknis dan pelatihan untuk meningkatkan kemampuan sumber daya manusia siber Indonesia. Sebagai contoh konkret, pada tanggal 14-16 Maret 2022, BSSN bersama *Homeland Security Investigations (HSI)* AS menyelenggarakan kegiatan '*HSI Online Investigation Virtual*' (Imran 2023). Kegiatan ini berfokus pada pengembangan kemampuan investigasi digital, diskusi mengenai kejahatan transnasional dan digital forensik, serta pertukaran praktik siber terbaik. Selain itu, pada periode 14 Maret - 27 Mei 2022, diselenggarakan '*English Language Program for Cyber Professionals in Indonesia*' yang ditujukan untuk meningkatkan kemampuan bahasa Inggris personel BSSN, sehingga mendukung partisipasi mereka dalam program *capacity building* internasional (Putra 2022). Program-program pelatihan lainnya dilaksanakan melalui mekanisme webinar dan pelatihan yang dijalankan melalui koordinasi Kedutaan Besar AS di Jakarta.

Bentuk ketiga adalah berbagi informasi dan kerja sama operasional. Mekanisme yang telah dibangun antara BSSN dan Kedutaan AS mencakup *information sharing* terkait ancaman siber yang ada dan potensial. Aktivitas ini menjadi tulang punggung kerjasama sehari-hari, dengan fokus pada berbagi informasi kerawanan, identifikasi program *APT (Advanced Persistent Threat)* pada sistem IT pemerintah, serta antisipasi serangan siber (Putra, 2022). Kerja sama ini

juga meluas ke penanganan *cyberterrorism*, di mana BSSN berkerja sama dengan Badan Nasional Penanggulangan Terorisme (BNPT). BNPT sendiri memiliki kerjasama terpisah dengan AS melalui MoU tentang *Counter-terrorism*, yang menciptakan sinergi dalam penanganan ancaman siber yang terkait terorisme (Bramantoro 2018).

Bentuk keempat adalah kerja sama teknis-operasional di bidang pertahanan dan keamanan. Sebenarnya hal ini sudah digaungkan sejak lama, berdasarkan penelitian milik (Rizal dan Yani 2016), TNI juga pernah menjalin kerja sama dengan beberapa pihak yang kompeten di ranah teknologi informasi, termasuk Institut Teknologi Del (IT Del) di Sumatera Utara. Kemitraan yang direncanakan dari tahun 2014 hingga 2017 ini meliputi tiga program utama, yaitu pengembangan model perang siber, penyelenggaraan seminar mengenai intelijen dan operasi siber militer, serta pelaksanaan kamp atau akhir pekan siber. Kemitraan TNI dengan IT Del pada periode 2014–2017 ini juga menjadi contoh dari landasan awal bagi penguatan pemahaman teknis mengenai operasi dan pertahanan siber, sehingga mendukung kesiapan TNI ketika kemudian memasuki kerja sama siber bilateral dengan AS pada periode-periode selanjutnya. Bentuk kerja sama terbaru mencakup koordinasi langsung dengan lembaga penegak hukum dan keamanan AS, seperti FBI, yang dijembatani oleh Kedutaan Besar AS. Dimana kerja sama berkembang ke ranah latihan militer gabungan. Panglima TNI Jenderal Agus Subiyanto menginisiasi penambahan materi latihan siber dalam latihan gabungan bilateral *Super Garuda Shield*, sebagaimana didiskusikan dengan pimpinan militer AS (Jenderal Charles Q. Brown) pada November 2024 (Nugroho 2025). Inisiatif ini bertujuan untuk meningkatkan penguasaan teknologi dan kapabilitas pertahanan

siber TNI, serta merefleksikan perluasan cakupan kerja sama dari aspek civilian ke aspek keamanan nasional dan pertahanan yang lebih luas.

Jika tidak ada kerangka pengikat, suatu negara berpotensi bertindak sepihak demi kepentingan domestiknya sendiri dan mengabaikan kepentingan mitra lain. Karena itu, aturan berperan ganda, yakni sebagai pedoman yang mengarahkan jalannya interaksi sekaligus sebagai batasan yang menentukan perilaku apa saja yang diperbolehkan maupun yang dilarang dalam kerja sama internasional. Prinsip dasar ini juga relevan ketika dikaitkan dengan hubungan Indonesia dan AS dalam bidang keamanan siber.

Dalam konteks Indonesia, pengaturan mengenai ranah siber sebenarnya telah berkembang sejak sebelum 1999 melalui perangkat hukum yang ditujukan untuk memberikan landasan bagi transaksi elektronik dan pemanfaatan teknologi informasi. Adanya *cyber law* dimaksudkan agar tersedia pijakan hukum yang dapat mendukung regulasi lain ketika kejahatan berbasis teknologi mulai meningkat (Wahyuni 2022).

Dua regulasi yang relevan adalah UU Hak Cipta No. 19 Tahun 2002 serta UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, yang disahkan pada 25 Maret 2008 dan terdiri dari 13 bab serta 54 pasal. Kerangka ini kemudian diperkuat melalui PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang selanjutnya digantikan oleh PP No. 71 Tahun 2019 (BPK 2019). Perubahan ini menjadi penting dalam kerja sama internasional karena memperbarui standar mengenai sistem elektronik, klasifikasi data, kewajiban penyelenggara sistem elektronik, dan tata kelola perlindungan data, sehingga

memberikan konteks regulatif yang lebih mutakhir bagi interaksi Indonesia dengan negara mitra.

Dalam penelitian ini, penulis berpendapat bahwa aturan mengenai kerja sama antara Indonesia dan AS dalam bidang siber pada dasarnya masih bersifat umum dan belum dituangkan dalam mekanisme bilateral yang terperinci. Pada tahap awal, kerangka kerja sama lebih terlihat sebagai bagian dari aspirasi strategis AS yang disampaikan melalui *International Strategy for Cyberspace* (2011), yang menekankan pentingnya membangun kemitraan internasional untuk menghadapi ancaman bersama dan menjaga stabilitas global (THE WHITE HOUSE 2011).

Salah satu dari tujuh prioritas dalam dokumen tersebut adalah memperkuat aliansi dan kemitraan internasional, yang secara tidak langsung membuka ruang bagi Indonesia untuk diposisikan sebagai mitra. Hal ini sejalan dengan doktrin Departemen Pertahanan AS yang juga menempatkan penguatan aliansi internasional sebagai tujuan strategis dalam menghadapi ancaman kolektif. Kerangka awal ini membuat aturan yang ada cenderung berfungsi sebagai landasan strategis AS di kawasan, bukan sebagai bentuk kesepakatan formal yang mengikat kedua negara.

Namun, analisis ini perlu diperluas dengan mengkaji perkembangan strategis dan pendekatan terbaru AS. *International Strategy for Cyberspace* (2011) kini telah diperbarui dan diterjemahkan ke dalam dokumen-dokumen strategis. Strategi Keamanan Nasional (NSS) AS Oktober 2022 mengukuhkan visi dunia yang ‘bebas, terbuka, aman, dan sejahtera’, dengan memprioritaskan kepemimpinan dalam ekonomi digital dan teknologi baru (The White House 2022). Dimana Strategi Keamanan Siber Nasional (NCS) 2023 yang digalakkan

Departemen Luar Negeri AS bertujuan menjalin kemitraan global untuk mewujudkan ekosistem digital yang terbuka, tangguh, terlindungi, dan menghormati hak asasi manusia (U.S. Department of State 2024).

Dalam hal ini, pendekatan ganda NCS, yang mendistribusikan kembali tanggung jawab pertahanan siber antara pemerintah dan sektor swasta serta menyelaraskan insentif untuk investasi jangka panjang, menjadi landasan regulasi dan kebijakan baru bagi kerja sama AS dengan mitra seperti Indonesia.

BAB 4

PENUTUP

4.1 Kesimpulan

Penelitian ini menunjukkan bahwa kerja sama keamanan siber antara Indonesia dan AS pada periode 2019–2024 lahir sebagai respons terhadap meningkatnya ancaman digital yang semakin rumit dan berskala lintas negara. Kondisi tersebut membuat kedua negara memiliki kepentingan yang sejalan untuk memperkuat pertahanan siber nasional masing-masing. Indonesia menghadapi lonjakan signifikan serangan siber yang menasar instansi pemerintah, layanan publik, dan infrastruktur vital, sementara AS mengalami pertumbuhan serangan ransomware, pencurian data, serta aktivitas spionase digital yang memberi dampak serius bagi keamanan nasional dan perekonomiannya.

Kesamaan kepentingan ini kemudian mendorong terbentuknya kolaborasi bilateral yang berkembang secara bertahap, bermula dari *Joint Statement* hasil pertemuan Presiden Joko Widodo dan Presiden Barack Obama pada Oktober 2015. Selanjutnya penandatanganan *Letter of Intent (LoI)* pada tahun 2018 dan perpanjangan kerja sama pada 2021, hingga penguatan hubungan melalui penandatanganan *Memorandum of Understanding (MoU)* dan Memorandum Saling Pengertian (MSP) pada 2024. Implementasinya mencakup pelatihan keamanan siber, pertukaran intelijen digital, peningkatan kualitas sumber daya manusia, penguatan kemampuan manajemen insiden, serta dukungan terhadap teknologi dan regulasi keamanan siber.

Temuan penelitian menegaskan bahwa kerja sama ini tidak hanya memperkuat ketahanan siber Indonesia, tetapi juga meningkatkan posisi negara dalam ranah diplomasi siber internasional. Lebih jauh, pola interaksi kedua negara konsisten dengan teori kerja sama internasional K.J. Holsti, yang menekankan bahwa kolaborasi tercipta karena keselarasan tujuan, kebutuhan timbal balik, adanya aturan bersama, serta manfaat yang diperoleh kedua pihak. Dengan demikian, kerja sama siber antara Indonesia dan AS merupakan bentuk kolaborasi strategis yang berkembang sebagai jawaban atas dinamika ancaman digital global dan sebagai upaya menjaga keamanan, stabilitas, serta kepentingan nasional di era digital.

4.2 Rekomendasi

Peneliti menyarankan agar pemerintah Indonesia memperkuat undang-undang keamanan siber nasional untuk selaras dengan standar internasional dan meningkatkan kapasitas sumber daya manusia melalui pelatihan, sertifikasi, dan pendidikan berkelanjutan. Selain itu, sangat penting untuk membangun pusat tanggap insiden siber yang berkolaborasi dengan mitra internasional, termasuk AS, agar serangan dapat dideteksi lebih cepat dan diatasi lebih baik. Bagi AS, kerja sama dengan Indonesia harus lebih dari sekadar pertukaran informasi, yang mana harus diperluas melalui transfer teknologi dan dukungan untuk penguatan infrastruktur digital. Langkah-langkah ini akan membuat kerja sama bilateral lebih berkelanjutan sekaligus berkontribusi pada stabilitas keamanan digital di wilayah Indo-Pasifik.

Peneliti juga menyadari bahwa skripsi ini memiliki keterbatasan, terutama karena data yang digunakan lebih banyak berasal dari laporan sekunder dan studi pustaka. Akibatnya, analisis belum dapat sepenuhnya menangkap dinamika kerja sama di lapangan. Penelitian lebih lanjut disarankan untuk dilakukan setelah 2025, melakukan penelitian komparatif tentang kerja sama internasional dengan negara lain, dan menggunakan metode kuantitatif untuk mengukur dampak kerja sama internasional terhadap penurunan serangan siber dan peningkatan ketahanan digital Indonesia.

DAFTAR PUSTAKA

- Afifa, Laila. 2021. "6 Major Data Breach Cases in Indonesia in Past 1.5 Years - Sci En.tempo.co." <https://en.tempo.co/read/1501851/6-major-data-breach-cases-in-indonesia-in-past-1-5-years>.
- Antara News. 2018. "Indonesia, US agree to promote cyberspace cooperation." *Antara News*. <https://en.antaranews.com/news/119060/indonesia-us-agree-to-promote-cyberspace-cooperation>.
- antaranews.com. 2018. "Indonesia, US Agree to Promote Cyberspace Cooperation." Antara News, September 29. <https://en.antaranews.com/news/119060/indonesia-us-agree-to-promote-cyberspace-cooperation>.
- Anwary, Ichsan. 2022. "The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia." *International Journal of Cyber Criminology* 16 (2): 216–27.
- Arabel, Yunita Sekar Ety, dan Ida Musofiana. 2024. "STUDI PERBANDINGAN HUKUM PIDANA DALAM PENANGANAN KEJAHATAN SIBER: PERSPEKTIF INDONESIA DAN AMERIKA SERIKAT." *Jurnal Hukum dan Kewarganegaraan* 6 (11).
- Arianto, Adirio, Dairatul Maarif, M Muhadjir, dan Raynor Argaditya. 2023. "Indonesia-China Cooperation For The Development And Improvement of Digital Technology 4.0 in The Field of Security And Economy." *Global Komunika : Jurnal Ilmu Sosial Dan Ilmu Politik* 5 (2): 44–53. <https://doi.org/10.33822/gk.v5i2.5537>.
- Ariesta, Marcheilla. 2019. "Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia." medcom.id, Juli 2. <https://www.medcom.id/internasional/asia/nN9wJq3k-keamanan-siber-jadi-perhatian-khusus-indonesia-dan-australia>.
- Azhari, Muhamad Al. 2025. "Indonesia's National Cyber and Crypto Agency Meets with US Cyber Envoy Steve Lang to Deepen Bilateral Cybersecurity Cooperation - Jakarta Daily." Indonesia's National Cyber and Crypto Agency Meets with US Cyber Envoy Steve Lang to Deepen Bilateral Cybersecurity Cooperation - Jakarta Daily. <https://www.jakartadaily.id/tech-media/16215252547/indonesias-national-cyber-and-crypto-agency-meets-with-us-cyber-envoy-steve-lang-to-deepen-bilateral-cybersecurity-cooperation>.
- Badan Siber dan Sandi Negara. 2019a. "Laporan Hasil Monitoring Keamanan Siber Tahun 2019." Pusat Operasi Keamanan Siber Nasional.
- Badan Siber dan Sandi Negara. 2019b. "LAPORAN KINERJA BSSN 2018."
- Badan Siber dan Sandi Negara. 2020. "Laporan Hasil Monitoring Keamanan Siber Tahun 2020." Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. 2021. "Laporan Hasil Monitoring Keamanan Siber Tahun 2021." Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. 2022. "Laporan Hasil Monitoring Keamanan Siber Tahun 2022." Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.

- Badan Siber dan Sandi Negara. 2023. "Laporan Hasil Monitoring Keamanan Siber Tahun 2023." Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. 2024a. "Indonesia Dan Amerika Serikat Tanda Tangani Kerja Sama Keamanan Siber - WwW.Bssn.Go.Id." Desember 5. <https://bssn.go.id/indonesia-dan-amerika-serikat-tanda-tangani-kerja-sama-keamanan-siber/>.
- Badan Siber dan Sandi Negara. 2024b. "Laporan Hasil Monitoring Keamanan Siber Tahun 2024." Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara.
- Badan Siber dan Sandi Negara. 2024c. "Laporan Kinerja Badan Siber Dan Sandi Negara Tahun 2024." Badan Siber dan Sandi Negara. <https://bssn.go.id/laporan-kinerja-badan-siber-dan-sandi-negara-tahun-2024/>.
- Billo, Charles, dan Welton Chang. 2004. "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation-States." *Institute for Security Technology Studies at Dartmouth College, Hanover*.
- BPK. 2019. "Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik." DATABASE PERATURAN. <https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019>.
- Bramantoro, Toni. 2018. "BNPT dan Lembaga Kontra Terorisme Amerika Serikat Jalin Kerjasama." *Tribunnews.com*, September 15. <https://www.tribunnews.com/nasional/2018/09/15/bnpt-dan-lembaga-kontra-terorisme-amerika-serikat-jalin-kerjasama>.
- Brown, Helen. 2019. "Indonesia Focused on Cyber Resilience, Open to Foreign Cooperation." *Digital Economy*, November 12. <https://digital.australiaindonesiacentre.org/news/insights/indonesia-focused-on-cyber-resilience-open-to-foreign-cooperation/>.
- Budi, Eko, Dwi Wira, dan Ardian Infantono. 2021. "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0." *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3 (Desember): 223–34. <https://doi.org/10.54706/senastindo.v3.2021.141>.
- Chen, Thomas M. 2013. "An Sssessment of the Department of Defense strategy for Operating in Cyberspace." *Army War College, Carlisle Barracks, PA: Strategic Studies Institute*. (United States).
- Chotimah, Hidayat Chusnul. 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): 113–28. <https://doi.org/10.22212/jp.v10i2.1447>.
- Chou, Cheng-Hui, Chi-Che Wu, Kuan-Chu Lu, dkk. 2018. "Modbus Packet Analysis and Attack Mode for SCADA System." *Journal of ICT, Design, Engineering and Technological Science* 2 (2): 30–35. <https://doi.org/10.33150/JITDETS-2.2.1>.

- Christensen, Kristoffer Kjærgaard, dan Karen Lund Petersen. 2017. "Public–Private Partnerships on Cyber Security: A Practice of Loyalty." *International Affairs* 93 (6): 1435–52. <https://doi.org/10.1093/ia/iix189>.
- CNN Indonesia. 2019. "BSSN: 232,45 Juta Serangan Siber 'Serbu' Indonesia di 2018." CNN Indonesia, April 26.
- Cybersecurity and Infrastructure Security Agency. t.t. "Cyber Threats and Advisories." Diakses 15 September 2025. <https://www.cisa.gov/topics/cyber-threats-and-advisories>.
- Daeng, Yusuf, Jimmy Levin, Muhammad Razzaq Prayudha, Nindy Putri Ramadhani, dan Susanto Imanuel. 2023. *Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia*. 3 (6): 1135–45.
- Direktur Jenderal Amerika dan Eropa. 2021. "KALEIDOSKOP DITJEN AMERIKA EROPA." DITJEN AMERIKA EROPA KEMENTERIAN LUAR NEGERI.
- DISKOMINFO KOTA MAKASSAR. 2024. "Indonesia dan Amerika Serikat Tanda Tangani Kerja Sama Keamanan Siber." <https://csirt.makassarkota.go.id/posts/indonesia-dan-amerika-serikat-tanda-tangani-kerja-sama-keamanan-siber>.
- Eichensehr, Kristen E. 2019. "Decentralized Cyberattack Attribution." *AJIL Unbound* 113: 213–17. <https://doi.org/10.1017/aju.2019.33>.
- Erlinda, Eka. 2025. "Diplomasi Indonesia Menanggulangi ancaman digital." *Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi* 2 (3): 229–42. <https://doi.org/10.62383/konstitusi.v2i3.852>.
- Fatihah, Citra Yuda Nur. 2022. "Indonesia's Approach on Cyberattack Attribution through its Foreign Policy." *Global Legal Review* 2 (2): 121. <https://doi.org/10.19166/glr.v2i2.5140>.
- Federal Bureau of Investigation. 2019. "2019 Internet Crime Report." Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2019_ic3Report.pdf.
- Federal Bureau of Investigation. 2020. "2020 Internet Crime Report." Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2020_ic3Report.pdf.
- Federal Bureau of Investigation. 2021. "2021 Internet Crime Report." Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf.
- Federal Bureau of Investigation. 2022. "2022 Internet Crime Report." Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf.
- Federal Bureau of Investigation. 2023. "2023 Internet Crime Report." Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.
- Federal Bureau of Investigation. 2024. "2024 Internet Crime Report." Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
- Fitriyani, Azizah. 2018. "Indonesia, US Agree to Promote Strong Cyberspace Cooperation." Antara News, Oktober 1. <https://en.antaranews.com/news/119107/indonesia-us-agree-to-promote-strong-cyberspace-cooperation>.

- Golose, Petrus Reinhard. 2022. "Cyber Terrorism- A Perspective of Policy Analysis." *International Journal of Cyber Criminology* 16 (2): 149–61.
- Healey, Jason. 2017. "Who's in Control: Balance in Cyber's Public-Private Sector Partnerships." *Georgetown Journal of International Affairs* 18 (3): 120–30.
- Holsti, K. J. (Kalevi Jaakko). 1987. *International Politics: A Framework for Analysis*. Fifth edition. Prentice-Hall.
- Ilaina, Asy Syuraya Arba, dan Imam Fadhil Nugraha. 2025. "KESENJANGAN KAPABILITAS KEAMANAN SIBER INDONESIA DALAM MITIGASI SERANGAN SIBER PADA LAYANAN PUBLIK DIGITAL TAHUN 2020-2025." *Triwikrama: Jurnal Multidisiplin Ilmu Sosial* 8 (6).
- Imran, M. Fadil. 2023. "CyberCriminology: An analysis of the Indonesian and the United States Police Perception." *International Journal of Cyber Criminology* 17 (2).
- Indrawan, Jerry. 2019. "Cyberpolitics Sebagai Perspektif Baru Memahami Politik di Era Siber [Cyberpolitics as A New Perspective in Understanding Politics in The Cyber Era]." *Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10 (1): 1–16. <https://doi.org/10.22212/jp.v10i1.1315>.
- Insight In News. 2024. "US And Indonesia Sign Memorandum Of Understanding To Strengthen Cyber Cooperation." <https://www.insightinnews.com/index/read/1435/us-and-indonesia-sign-memorandum-of-understanding-to-strengthen-cyber-cooperation>.
- IT GRC, Proxis. 2025. "Tren Ancaman Siber di Indonesia Meningkat? Berikut Fakta yang Harus Diketahui - IT Proxis Group." Proxis IT GRC. <https://it.proxisgroup.com/tren-ancaman-siber-di-indonesia-meningkat-berikut-fakta-yang-harus-diketahui/>.
- Jakarta, U. S. Embassy. 2025. "Amerika Serikat dan Indonesia Gelar Dialog Keamanan ke-21." Kedutaan Besar dan Konsulat AS di Indonesia, Mei 7. <https://id.usembassy.gov/id/amerika-serikat-dan-indonesia-gelar-dialog-keamanan-ke-21/>.
- Jayakarta, Denapoleon. 2024. "STRATEGI KEAMANAN SIBER AMERIKA SERIKAT DALAM PERANG DAGANG DENGAN CHINA." *Diplomacy and Global Security Journal: Jurnal Mahasiswa Magister Hubungan Internasional* 1 (1): 90–98. <https://doi.org/10.36859/dgsj.v1i1.2862>.
- Jogja, Kanwil Kemenkum. 2024. "Peretasan Pusat Data Nasional: Ancaman, Dampak, Dan Solusi Keamanan." Kanwil Kemenkumham DIY, Juli 1. <https://jogja.kemenkum.go.id/pusat-informasi/informasi-lain/artikel/peretasan-pusat-data-nasional-ancaman-dampak-dan-solusi-keamanan>.
- Judijanto, Loso. 2024. "National Security Strategies Amidst Increasing Global Cyber Threats: A Multilateral Approach." *Synergisia* 1 (2): 11–18. <https://doi.org/10.62872/2wph4p15>.
- Kementerian Keuangan Republik Indonesia. 2025. *US-ASEAN Business Council Sambut Positif Upaya Dialog dan Kerja Sama Indonesia-AS*. <https://www.kemenkeu.go.id/informasi-publik/publikasi/berita-utama/USABC-Sambut-Positif-Dialog-Indonesia-AS>.
- Kementerian Pertahanan Republik Indonesia. 2014. "Pedoman pertahanan siber." <https://www.kemhan.go.id/pothan/wp->

- content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.
- Khoirunnisa, Minar Silvi, dan Evelin Angelina Rizqi Surya. 2024. "Implementation of Cyberspace Cooperation between Indonesia and United States A Combating Cyberterrorism in Indonesia, 2019–2023." *Ilomata International Journal of Social Science* 5 (3): 660–78. <https://doi.org/10.61194/ijss.v5i3.1173>.
- Kurlantzick, Joshua. 2018. *Keeping the U . S . -Indonesia Relationship Moving Forward*.
- Lab, Emsisoft Malware. 2019. "The State of Ransomware in the US: Report and Statistics 2019." Emsisoft | Cybersecurity, Desember 12. <https://www.emsisoft.com/en/blog/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/>.
- Langevin, James R., Michael T. McCaul, Scott Charney, dan Harry Raduege. 2008. *Securing Cyberspace for the 44th Presidency: Defense Technical Information Center*. <https://doi.org/10.21236/ADA489361>.
- Ministry of Foreign Affairs. 2024. "JURNAL PERJANJIAN INTERNASIONAL." *Ditjen HPI cq. Setditjen HPI secara berkala (kuartal) dan memuat Perjanjian Internasional yang ditandatangani oleh Pemerintah Indonesia IV*.
- Nugraha, Fajar. 2024. "Hadapi Ancaman, Indonesia-AS Sepakati Kerja Sama Keamanan Siber." METRO TV. <https://www.metrotvnews.com/read/KdZCW5Jj-hadapi-ancaman-indonesia-as-sepakati-kerja-sama-keamanan-siber>.
- Nugroho, Novali Panji. 2025. "Indonesia Akan Belajar Keamanan Siber ke Tentara Singapura | tempo.co." Tempo, Juli 22. <https://www.tempo.co/politik/indonesia-akan-belajar-keamanan-siber-ke-tentara-singapura-2049567>.
- Pawlak, Patryk. 2016. "Confidence-Building Measures in Cyberspace : Current Debates and Trends." *International Cyber Norms: Legal, Policy & Industry Perspectives*.
- Putra, Bimo Arya. 2022. "Cyber Cooperation between Indonesia and the United States in Addressing the Threat of Cyberterrorism in Indonesia." *International Journal of Multicultural and Multireligious Understanding* 9 (10): 22–23.
- Rachmawiana, Miftahulfarras Muhammad. 2025. *KEBIJAKAN INDONESIA DALAM KERJA SAMA DENGAN AMERIKA SERIKAT DI BIDANG SIBER TAHUN 2023 – 2024*. 2 (3). <https://doi.org/10.36859/gij.v2i1.4217>.
- Rahman Asmardika. 2024. "AS dan Indonesia Tandatangani MoU Memperkuat Kerja Sama Pertahanan Siber." okezone. <https://ototekno.okezone.com/read/2024/12/06/54/3092838/as-dan-indonesia-tandatangani-mou-memperkuat-kerja-sama-pertahanan-siber>.
- Raidi. 2025. "19 Million Cyberattack Attempts in Indonesia Throughout 2024." *Indonesia Sentinel*, Februari 8. <https://indonesiasentinel.com/kaspersky-reports-19-million-cyberattack-attempts-in-indonesia-troughout-2024/>.
- Ramadhan, Iqbal. 2023. "ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities." *Journal of Social and Political Sciences* 6 (4): 1–10. <https://doi.org/10.31014/aior.1991.06.04.440>.

- Reditya, Tito Hilmawan. 2024. "AS dan Indonesia Tanda Tangan Nota Kesepahaman Perkuat Kerja Sama Siber." KOMPAS.com, Desember 5. <https://www.kompas.com/global/read/2024/12/05/220000870/as-dan-indonesia-tanda-tangani-nota-kesepahaman-perkuat-kerja-sama-siber>.
- Rizal, Muhamad, dan Yanyan Yani. 2016. "Cybersecurity Policy and Its Implementation in Indonesia." *JAS (Journal of ASEAN Studies)* 4 (1): 61. <https://doi.org/10.21512/jas.v4i1.967>.
- Rosy, Afifah Fidina. 2020. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security." *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan* 1 (2): 118–29. <https://doi.org/10.54144/govsci.v1i2.12>.
- Sari, Rita Puspita. 2024. "AS dan Indonesia Tandatangani MoU Perkuat Kerja Sama Siber." cloud computing. <https://event.cloudcomputing.id/berita/event.cloudcomputing.id>.
- Security, Homeland. 2024. "DHS Bolsters Indo-Pacific Maritime Cybersecurity through Partnership with Indonesia | Homeland Security." Homeland Security. <https://www.dhs.gov/archive/news/2024/06/18/dhs-bolsters-indo-pacific-maritime-cybersecurity-through-partnership-indonesia>.
- Sersan Staf Katie Gray. 2019. "US and Indonesia 'Threat Hunt' during Information Exchange." U.S. Indo-Pacific Command. <https://www.pacom.mil/Media/NEWS/News-Article-View/Article/1921079/us-and-indonesia-threat-hunt-during-information-exchange/>.
- Sudarmadi, Damar Apri. 2019. "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia." *Jurnal Kajian Strategik Ketahanan Nasional* 2 (2). <https://doi.org/10.7454/jkskn.v2i2.10028>.
- Suminar, Agustina. 2018. "Indonesia-Amerika Serikat Sepakat Majukan Kerja Sama Ruang Siber." <https://www.suarasurabaya.net/infoteknologi/2018/Indonesia-Amerika-Serikat-Sepakat-Majukan-Kerja-Sama-Ruang-Siber/>.
- Taichman, Elya. 2021. "Defend Forward & Sovereignty: How America's Cyberwar Strategy Upholds International Law." *University of Miami Inter-American Law Review* 53 (1). <https://repository.law.miami.edu/umialr>.
- THE WHITE HOUSE. 2011. "INTERNATIONAL STRATEGY FOR CYBERSPACE."
- The White House. 2013. "Executive Order -- Improving Critical Infrastructure Cybersecurity." Whitehouse.Gov, Februari 12. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
- The White House. 2022. "National security strategy." Oktober 12. <https://stratml.us/pdfs/NSS2022.pdf>.
- TRIAD, CloudSEK. 2025. "Analyzing Recent Cyber Attacks in the United States Coinciding with Columbus Day Celebration | CloudSEK."
- Triwahyuni, Dewi, dan Tine Agustin Wulandari. 2016. "STRATEGI KEAMANAN CYBER AMERIKA SERIKAT." *Jurnal Ilmu Politik dan Komunikasi* VI (1).

- U. S. Embassy & Consulates in Indonesia. 2025. "Kedutaan Besar AS Selenggarakan Lokakarya Keamanan Siber untuk Amankan Pelabuhan Strategis." [Siaran Pers]. Kedutaan Besar dan Konsulat AS di Indonesia, September 8. <https://id.usembassy.gov/id/kedutaan-besar-as-selenggarakan-lokakarya-keamanan-siber-untuk-amankan-pelabuhan-strategis/>.
- U. S. Embassy Jakarta. 2024. "Amerika Serikat dan Indonesia Bermitra dalam Penerapan Jaringan Generasi Berikutnya." Kedutaan Besar dan Konsulat AS di Indonesia, Februari 22. <https://id.usembassy.gov/id/amerika-serikat-dan-indonesia-bermitra-dalam-penerapan-jaringan-generasi-berikutnya/>.
- United States Department of State. t.t. "United States International Cyberspace & Digital Policy Strategy." Diakses 4 Desember 2025. <https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>.
- U.S. Department of Homeland Security dan Office of Inspector General. 2020. *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*. <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf>.
- U.S. Department of State. 2024. "The United States international cyberspace & digital policy strategy: Towards an innovative, secure, and rights-respecting digital future." Mei 6.
- USAFacts team. 2025. "How Many Cyberattacks Occur in the US?" USAFacts. <https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us/>.
- USINDO. 2019. "President's report on programs and activities: May 2018–May 2019."
- Wahyuni, Willa. 2022. "Mengenal Cyber Law dan Aturannya." hukumonline.com. <https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/>.