GLOBAL INSIGHTS JOURNAL
Jurnal Mahasiswa Program Studi
Ilmu Hubungan Internasional - FISIP - UNJANI
https:/ejournal.fisip.unjani.ac.id/index.php/GIJ
DOI : https://doi.org/10.36859/gij.v2i3.4217
Vol. 02 No. 03 Tahun 2025

Article Informations
*Received*: 30/07/2025; *Accepted*: 25/09/2025; *Published*: 15/10/2025
Corresponding Email:
miftahulfarrasmr@gmail.com

# KEBIJAKAN INDONESIA DALAM KERJA SAMA DENGAN AMERIKA SERIKAT DI BIDANG SIBER TAHUN 2023 – 2024

**Miftahulfarras Muhammad Rachmawiana**

Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Achmad Yani

**Abstrak**

Penelitian ini menganalisis kebijakan Indonesia dalam kerja sama dengan Amerika Serikat di bidang keamana siber pada periode 2023-2024. Dengan menggunakan pendekatan kualitatif dan tipe penelitian eksplanatif, penelitian ini memfokuskan pada faktor internal dan eksternal yang mempengaruhi Indonesia dalam menjalin kerja sama siber. Data diperoleh melalui studi literatur berbasis internet dan wawancara dengan pakar keamanan siber. Hasil penelitian menunjukkan bahwa peningkatan ancaman siber internasional, keterbatasan kapasitas sumber daya manusia di bidang siber, serta pentingnya peran Indonesia di kawasan Indo-Pasifik menjadi faktor pendorong melalui berbagai kegiatan, seperti pertukaran informasi intelijen, pelatihan teknis, perlindungan infrastruktur digital, serta penandatanganan Momerandum Saling Pengertian (MSP) pada 4 Desember 2024. Penelitian ini menegaskan bahwa kerja sama tersebut berkontribusi signifikan terhadap peningkatan ketahanan siber nasional Indonesia sekaligus memperkuat posisi diplomasi siber Indonesia di tingkat internasional.
**Kata Kunci :** Keamanan Siber, Indonesia, Amerika Serikat, Kerja Sama Bilateral, Kebijakan Luar Negeri

***Abstract***

*This study analyzes Indonesia's policy in cybersecurity cooperation with the United States during the 2023–2024 period. Using a qualitative approach and an explanatory research type, the study focuses on internal and external factors influencing Indonesia's decision to engage in cybersecurity cooperation. Data were collected through Internet-Based Research and interviews with cybersecurity experts. The findings indicate that the rise of global cyber threats, limited human resource capacity in the cybersecurity sector, and Indonesia's strategic role in the Indo-Pacific region are the main drivers of this bilateral collaboration. The Indonesia–United States cooperation was carried out through various activities, such as cyber intelligence information exchange, technical training, critical digital infrastructure protection, and the signing of a Memorandum of Understanding (MoU) on December 4, 2024. This study emphasizes that the cooperation significantly contributes to strengthening*

*Indonesia's national cybersecurity resilience and enhances its position in global cyber diplomacy.*
***Keywords*** ***:*** *Cybersecurity, Indonesia, United States, Bilateral Cooperation, Foreign Policy.*

## 1. PENDAHULUAN

Dalam era digital yang berkembang pesat, keamanan siber telah menjadi isu strategis yang krusial bagi stabilitas nasional dan dinamika hubungan internasional. Indonesia, sebagai negara dengan pertumbuhan teknologi yang signifikan, menghadapi tantangan besar dalam melindungi data, infrastruktur kritis, dan menanggulangi ancaman siber yang semakin kompleks. Konteks ini mendorong pentingnya kerja sama internasional, khususnya dengan Amerika Serikat yang memiliki kapabilitas luas di bidang keamanan siber. Ancaman siber global terus meningkat seiring kemajuan teknologi dan perubahan geopolitik. *Global Security Outlook 2024* oleh *World Economic Forum*, yang menyebutkan kesenjangan ketahanan siber global dan peningkatan serangan dari pihak eksternal atau ketiga. Kecerdasan buatan (AI) juga membawa manfaat sekaligus risiko, memperburuk ancaman seperti *phishing* dan *malware* meskipun dapat membantu penanganan serangan.[1]

Di Indonesia, tata kelola keamanan siber masih terfragmentasi dan sektoral, meningkatkan risiko terhadap ketahanan siber. Sebagai respons, pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) pada tahun 2017 untuk mengoordinasikan dan memperkuat pertahanan siber nasional.[2] Meskipun Indonesia menunjukkan kemajuan signifikan dalam keamanan siber, masuk dalam Tier 1 Global Cybersecurity Index (GCI) 2024 dan meningkatkan peringkat e-Government PBB, ancaman siber seperti ransomware, phishing, dan misinformasi terus berkembang, ditunjukkan dengan puluhan ribu kasus phishing dan jutaan konten negatif yang ditindaklanjuti sejak 2019. Oleh karena itu, kolaborasi internasional menjadi

[1] Amara Zahra, "Rapor Tantangan dan Ancaman Kejahatan Siber 2024" *idntimes.com*, 2024, https://www.idntimes.com/news/indonesia/amara-zahra/rapor-tantangan-dan-ancaman-kejahatan-siber-2024.
[2] Damar Apri Sudarmadi and Arthur Josias Simon Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia" *Jurnal Kajian Stratejik Ketahanan Nasional*. 2.2 (2019): 163–183, https://scholarhub.ui.ac.id/jksknhttps://scholarhub.ui.ac.id/jkskn/vol2/iss2/7.

penting untuk memperkuat pertahanan siber Indonesia, berbagi informasi, dan membangun ekosistem digital yang tangguh.[3]

BSSN mempunyai peran krusial dalam mengawasi keamanan siber, mengingat tingginya penggunaan internet di Indonesia mencapai 64,8% populasi menurut APJII 2019 yang turut meningkatkan risiko kejahatan siber. Untuk menjaga keamanan nasional, pemerintah mengambil langkah pengamanan lebih ketat dan aktif berpartisipasi dalam forum internasional seperti Konferensi PBB tentang Kejahatan Transnasional Terorganisir yang menyoroti ancaman siber lintas negara. Dengan posisi strategis dan masyarakat yang beragam, Indonesia cukup rentan, sehingga penguatan kerja sama internasional, baik bilateral maupun regional, menjadi upaya penting dalam melindungi kedaulatan dan kepentingan nasional.[4]

Politik luar negeri bebas aktif Indonesia membatasi aliansi, namun kemandirian dalam keamanan siber bukanlah hal mudah, menjadikan kerja sama dengan negara maju seperti Amerika Serikat krusial untuk akses teknologi dan keahlian. Hubungan bilateral Indonesia-Amerika Serikat telah terjalin erat, diperkuat dengan komitmen untuk meningkatkan hubungan menuju Kemitraan Strategis Komprehensif. Amerika Serikat, sebagai negara adidaya dengan kapabilitas siber yang tinggi dan berbagai lembaga pengelola keamanan siber seperti Department of Homeland Security (DHS), Department of Defense (DoD), Federal Bureau of Investigation (FBI), serta United States Cyber Command (US CYBERCOM), menjadi mitra strategis dalam menghadapi ancaman siber global. Perkembangan situasi ini mendorong penandatanganan Memorandum Saling Pengertian (MSP) antara BSSN dan Department of State Amerika Serikat pada 4 Desember 2024, yang bertujuan memperkuat keamanan siber melalui pertukaran praktik terbaik, peningkatan kapasitas, dan perlindungan infrastruktur digital. MSP ini memiliki nilai strategis tinggi bagi Indonesia dalam alih pengetahuan, penguatan sistem keamanan siber nasional, dan posisi diplomasi siber di

---

[3] Cnnindonesia, "Menkomdigi: Peringkat Keamanan Siber RI Naik, Sejajar AS Hingga Jepang" *cnnindonesia.com*. , 2025, https://www.cnnindonesia.com/teknologi/20250206153253-192-1195388/menkomdigi-peringkat-keamanan-siber-ri-naik-sejajar-as-hingga-jepang.

[4] Afifah Fidina Rosy, "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber" *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan*. 1.2 (2020): 118–129.

Asia-Pasifik.[5] Kerangka kerja sama ini berlandaskan pernyataan bersama kedua pemimpin pada tahun 2023 dan berlaku hingga 4 Desember 2024, tanggal penandatanganan MSP.

## 2. PEMBAHASAN

### 2.1. Kebijakan Luar Negeri Indonesia di Bidang Siber

Kebijakan luar negeri Indonesia mengenai siber memiliki fokus terhadap diplomasi siber sebagai bagian integral dari tata kelola keamanan nasional di era digital ini. Ditujukan untuk menghadapi ancaman yang semakin kompleks dalam ruang siber, perlu dilakukannya kolaborasi internasional serta pembentukan lembaga khusus yang memiliki otoritas dalam isu – isu siber, seperti Badan Siber dan Sandi Negara (BSSN). Pembentukan BSSN merupakan bentuk respon kelesmbagaan terhadap kebutuhan pertahanan dan keamanan siber, selain menjalankan fungsi pengamanan teknis juga mengemban fungsi diplomasi siber.

Ancaman siber yang selalu berkembang dari masa ke masa menjadikan dimensi baru dalam keamanan nasional. Di era globalisasi dan aktivitas internet yang tinggi, serangan siber tidak hanya bersifat teknis tetapi juga berdampak pada stabilitas ideologi, ekonomi, sosial, dan politik negara. Indonesia merupakan negara dengan pengguna internet terbanyak di dunia menghadapi resiko tinggi terhadap berbagai bentuk ancaman siber, baik yang dilakukan oleh aktor negara maupun non – negara.[6]

Badan Siber dan Sandi Negara (BSSN) dibentuk pada 2017 melalui Perpres No. 53 dan diperbarui dengan Perpres No. 133 Tahun 2017 sebagai respons terhadap meningkatnya ancaman di ruang siber.[7] Berada langsung di bawah Presiden, keberadaan BSSN mencerminkan keseriusan pemerintah dalam menangani isu keamanan digital secara khusus. Dalam menjalankan tugasnya, BSSN mengacu pada lima pilar Global Cybersecurity Index (GCI) dan telah merumuskan berbagai kebijakan untuk memperkuat keamanan

---

[5] Beni Sukadis, "Peran Diplomasi Pertahanan Indonesia Dalam Kerjasama Pertahanan Indonesia Dan Amerika Serikat" *Jurnal Mandala : Jurnal Ilmu Hubungan Internasional*. 1.1 (2018): 111–112.

[6] Hidayat Chusnul Chotimah, "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 (2019): 113–114.

[7] Agus Haryanto and Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020" *Global Political Studies Journal*. 7.1 (2023): 61.

siber nasional. Diplomasi siber juga menjadi bagian penting, melalui kerja sama bilateral dengan negara seperti Belanda, Inggris, Australia, dan AS, serta keterlibatan aktif dalam forum regional dan internasional seperti ASEAN, IISS Shangri-La Dialogue, dan CERT International. Namun demikian, tantangan struktural masih dihadapi, seperti koordinasi antarkementerian, kebutuhan sinkronisasi data, dan rendahnya keterlibatan sektor swasta.

Global Cybersecurity Index (GCI) sendiri merupakan indikator global yang dikembangkan oleh ITU untuk mengukur komitmen negara terhadap keamanan siber melalui lima aspek utama: kebijakan hukum, teknis, organisasi, pembangunan kapasitas, dan kerja sama. Indeks ini digunakan untuk menganalisis hubungan antara kesiapan keamanan siber dengan kerugian ekonomi akibat kejahatan digital. Semakin tinggi skor GCI suatu negara, semakin kecil kemungkinan negara tersebut mengalami kerugian besar, yang menunjukkan bahwa kesiapan dan kapasitas yang kuat di bidang keamanan siber dapat mengurangi dampak ekonomi dari kejahatan siber. Oleh karena itu, GCI menjadi alat penting dalam evaluasi kebijakan dan perbandingan antarnegara guna meningkatkan kesiapan keamanan digital secara global.[8]

GCI menjadi dasar gagasan BSSN dalam membangun system keamanan siber nasional yang kuat:

1. Aspek Hukum, BSSN aktif dalam mendorong legasi yang komprehensif. Dimulai membahas mengenai RUU Keamanan dan Ketahanan Siber, BSSN juga mengusulkan RUU Persandian dan RUU Rahasia Negara. Hal tersebut bertujuan untuk menciptakan landasan yuridis yang sesuai dengan dinamika ancaman siber.
2. Aspek Teknis, BSSN yang berfokus terhadap Pembangunan dan penguatan tim tanggap insiden melalui pembentukan Gov-CSIRT, dan BSSN juga menyediakan point of contact Tunggal untuk pelaporan insiden siber di sektor pemerintah.

[8] K Farahbod, C Shayo, and J Varzandeh, "CYBERSECURITY INDICES AND CYBERCRIME ANNUAL LOSS AND ECONOMIC IMPACTS" *Journal of Business and Behavioral Sciences*. 32.1 (2020): 63–71, https://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf#page=63.

3. Aspek Organisasi, BSSN diharapkan mampu menjadi lembaga inti dalam koordinasi keamanan siber lintas negara maupun organisasi.
4. Aspek Pengembangan Kapasitas, BSSN telah menyadari pentingnya literasi dan pengembangan SDM sebagai fondasi utama keamanan siber melalui berbagai kegiatan.
5. Aspek Kerja Sama, BSSN menjadi bagian penting dalam diplomasi siber. Kerja sama bilateral dilakukan dengan berbagai negara dan mengikuti forum-forum internasional.[9]

Dalam upaya memperkuat aspek hukum keamanan siber, pada 7 November 2024, BSSN yang dipimpin oleh Hinsa Siburian mengusulkan Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber ke dalam Program Legislasi Nasional DPR RI. Tujuan utama RUU ini adalah memberikan landasan hukum yang lebih fleksibel bagi BSSN dalam melaksanakan tugasnya. RUU tersebut disusun berdasarkan kajian akademik dan draf yang dikembangkan BSSN, sebagai respons terhadap keterbatasan regulasi yang masih bersifat sektoral, parsial, dan belum mengatur keamanan siber secara sistemik sebagai bagian dari strategi nasional. Landasan yuridis RUU ini mencerminkan kebutuhan mendesak akan regulasi yang komprehensif dalam sistem hukum nasional, terutama untuk aspek pencegahan, penanganan, dan pemulihan insiden siber.[10]

Sebagai langkah konkret, pada 9–11 Juli 2019, BSSN juga mengadakan *Focus Group Discussion* (FGD) terkait penanggulangan dan pemulihan insiden siber di sektor pemerintah, serta secara resmi meluncurkan Gov-CSIRT Indonesia. Tim ini bertanggung jawab dalam layanan triase (identifikasi dan klasifikasi insiden), koordinasi penanganan insiden, serta resolusi teknis hingga pemulihan pascainsiden. Triase mencakup verifikasi jenis serangan seperti malware, phishing, dan DDoS, serta penentuan prioritas berdasarkan tingkat risiko. Koordinasi dilakukan bersama instansi pelapor untuk investigasi dan rekomendasi teknis,

[9] Muh Yusuf S, "Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index" *Al-Ulum: Jurnal Sains Dan Teknologi*. 7.1 (2022): 21–26.
[10] DPR RI and Badan Siber Dan Sandi Negara, *Naskah Akademik Rancangan Undang - Undang tentang Keamanan dan Ketahanan Siber Naskah Akademik.* , vols., 2019, https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf.

sementara resolusi fokus pada pemulihan sistem dan evaluasi kerugian. Selain itu, Gov-CSIRT juga menjalankan kegiatan proaktif seperti *drill test*, *workshop*, serta asistensi pembentukan CSIRT di berbagai instansi untuk memperkuat ketahanan siber nasional.[11]

Untuk memperkuat keamanan siber nasional, BSSN menjalin kerja sama internasional, termasuk dengan *Cyber Security Agency of Singapore* (CSA) sejak 2018, yang diawali dari pertemuan di Forum Shangri-La Dialogue dan dilanjutkan dengan pertemuan teknis di Jakarta untuk saling bertukar informasi kebijakan dan tugas kelembagaan. Selain itu, Indonesia juga bekerja sama dengan Australia melalui forum 2+2 Dialogue dan Ministerial Council on Law and Security, dengan fokus pada pembelajaran dari pembentukan *Australian Cyber Security Centre* (ACSC) dan strategi penanganan insiden siber yang komprehensif.[12] Selain menjalin kolaborasi, BSSN juga menekankan pentingnya literasi dan pengembangan Sumber Daya Manusia (SDM) sebagai fondasi utama ketahanan siber nasional. Tantangan seperti rendahnya kesadaran masyarakat, keterbatasan teknologi, dan kapasitas hukum mendorong BSSN untuk meningkatkan pemahaman publik terhadap ancaman siber melalui literasi digital. Upaya ini dilakukan melalui pelatihan teknis bagi ASN, edukasi publik, serta program pelatihan untuk sektor swasta dan komunitas profesional melalui Cyber Security Awareness Program. BSSN juga rutin menggelar FGD dan seminar yang melibatkan akademisi, praktisi, dan pemangku kepentingan guna memperkuat kapasitas individu dan institusi dalam menghadapi ancaman siber yang terus berkembang.[13]

Indonesia menganut prinsip politik luar negeri bebas aktif sejak 1945, yang menekankan netralitas dan tidak berpihak pada blok kekuatan manapun. Dalam konteks kerja sama siber, Indonesia menjaga independensi di tengah dominasi negara besar seperti Amerika Serikat, Tiongkok, dan

---

[11] Badan Siber Dan Sandi Negara, "Press Release: BSSN Launching Gov-CSIRT, Indonesia Kini Punya Tim Respon Insiden Siber" *Badan Siber dan Sandi Negara*. , 2024, online, Internet, 30 Jun. 2025. , https://www.bssn.go.id/press-release-bssn-launching-gov-csirt-indonesia-kini-punya-tim-respon-insiden-siber/.

[12] Y Wicaksono, "Indonesia-Australia kembali perkuat kerjasama cyber security" *Polkam.go.id*. , 2017, online, Internet, 3 Jul. 2025. , https://polkam.go.id/indonesia-australia-kembali-perkuat-kerjasama-cyber-security/.

[13] Rian Dwi Hapsari and Kuncoro Galih Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis" *Jurnal Konstituen*. 5.1 (2023): 1–17, https://ejournal.ipdn.ac.id/konstituen.

Rusia yang memiliki kepentingan berbeda. Kepentingan nasional Indonesia di bidang siber berfokus pada perlindungan kedaulatan, keamanan, dan stabilitas negara di era digital. Melalui BSSN, Indonesia turut aktif dalam kerja sama regional seperti ASEAN Regional Forum (ARF) guna memperkuat diplomasi siber dan meningkatkan ketahanan terhadap ancaman siber, sekaligus melindungi aset vital negara dan masyarakat di ruang digital.[14]

Pelaksanaan diplomasi siber di Indonesia sendiri melibatkan para aktor yang mencakup sejumlah lembaga pemerintah yang memiliki peran strategis, seperti Kementerian Luar Negeri (Kemlu RI), BSSN, dan Direktorat Tindak Pidana Siber Bareskrim Polri. Kemlu RI berperan sebagai ujung tombak dalam negosiasi dan kerja sama internasional terkait isu siber, melalui inisiasi dialog bilateral, fasilitasi perjanjian, dan pembentukan norma perilaku bertanggung jawab di ruang siber. Contohnya adalah keterlibatan dalam Australia-Indonesia Cyber Policy Dialogue yang menegaskan komitmen bersama untuk menciptakan ruang siber yang terbuka, bebas, dan aman.[15] *United Nations Group of Governmental Experts* (UNGGE), di mana Indonesia menjadi salah satu dari 25 negara anggota yang terlibat dalam perumusan regulasi keamanan informasi global. Kemlu mendorong pembentukan norma internasional, penerapan hukum humaniter siber, dan penguatan kerja sama untuk mencegah konflik digital, serta membangun *Confidence Building Measures*. Dengan demikian, Kemlu RI tidak hanya reaktif tetapi juga proaktif dalam membangun arsitektur keamanan siber regional dan global.

Badan Siber dan Sandi Negara (BSSN) juga memainkan peran strategis dalam kerja sama luar negeri di bidang keamanan siber. Berdasarkan Perpres No. 28/2021, BSSN bertanggung jawab menyusun dan menerapkan kebijakan teknis diplomasi siber, termasuk standardisasi, pemantauan, deteksi, mitigasi, dan penanggulangan serangan siber. BSSN membangun dan memperkuat kerja sama keamanan siber sebagai bagian dari diplomasi teknis Indonesia dan berfungsi sebagai otoritas nasional yang menjadi

[14] Minsi Lestari and Tom Finaldin, "Kerja Sama Antara Indonesia Dan Negara-Negara Di Asia Tenggara Melalui Asean Regional Forum Dalam Bidang Keamanan Siber" *Global Mind*. 4.2 (2023): 27–42.
[15] Jakarta Globe, "Indonesia, Australia Join Hands to Strengthen Cybersecurity" *Jakarta Globe*. (Jakarta, 5 May 2017), https://jakartaglobe.id/news/indonesia-australia-join-hands-to-strengthen-cybersecurity.

penghubung utama dengan lembaga-lembaga siber internasional, baik bilateral maupun multilateral.[16]

Negara lainnya yang menjalin kerjasama di bidang siber oleh Indonesia ialah Amerika Serikat. Mekanisme kerja sama bilateral antara Indonesia dan Amerika Serikat di bidang siber merupakan kerangka strategis yang dirancang untuk memperkuat hubungan kedua negara dalam menghadapi ancaman siber global. Kerja sama ini diwujudkan melalui berbagai forum dialog tingkat tinggi yang melibatkan kepala negara, kementerian luar negeri, lembaga keamanan, dan lembaga terkait siber. Implementasi kerja sama ini mencakup beberapa bentuk kegiatan, antara lain:

1. Pertemuan Delegasi Tingkat Tinggi: Melibatkan para pemimpin dan pejabat dari kedua negara. Sebagai contoh, pertemuan antara Presiden Joko Widodo dan Presiden Barack Obama pada 26 Oktober 2015, di mana disepakati peningkatan kemitraan komprehensif ke tingkat strategis, termasuk perluasan kerja sama di domain siber.[17]
2. Penandatanganan Nota Kesepahaman (MoU) atau Perjanjian Bilateral: Contoh konkret adalah penandatanganan *Letter of Intent* (LoI) berjudul "*Promoting Strong Cyberspace Cooperation*" pada 28 September 2018, yang merupakan langkah penting dalam memperkuat kerja sama bilateral keamanan siber. Selain itu, Kepolisian Indonesia dan Kejaksaan Agung Amerika Serikat juga menandatangani perjanjian kerja sama untuk memperkuat kolaborasi dalam menghadapi kejahatan siber lintas negara pada November 2018, yang difokuskan pada pelatihan teknis dan penguatan kapasitas digital forensik. Puncaknya adalah penandatanganan Memorandum Saling Pengertian (MSP) tentang Penguatan Kerja Sama di Ruang Siber pada 4 Desember

[16] Henike Primawanti and Sidik Pangestu, "Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (Asean) Regional Forum" *Global Mind*. 2.2 (2020): 4–5.
[17] The American Presidency Project, "Join Statement by President Obama and President Joko 'Jokowi' Widodo of Indonesia" *University of California, Santa Barbara*. , 2015, 19 Jul. 2025. , https://www.presidency.ucsb.edu/documents/joint-statement-president-obama-and-president-joko-jokowi-widodo-indonesia.

2024, antara BSSN Indonesia dan *Department of State* (DoS) Amerika Serikat.[18]

3. Pertukaran Delegasi dan Pelatihan Bersama: Ini bertujuan untuk meningkatkan kemampuan deteksi, pencegahan, dan respons terhadap insiden keamanan siber seperti serangan siber, kejahatan dunia maya, dan ancaman terhadap infrastruktur vital serta ekonomi digital. MSP 2024 secara khusus menargetkan pertukaran praktik terbaik, peningkatan kapasitas SDM dan teknologi, serta perlindungan infrastruktur digital. Ruang lingkup kerja sama MSP juga meliputi pertukaran informasi ancaman siber, pengembangan kapasitas melalui pelatihan teknis dan simulasi serangan siber (cyber drill), serta kolaborasi dalam penelitian dan pengembangan teknologi keamanan siber.[19]

Kerja sama ini mencerminkan kesadaran kedua negara bahwa keamanan siber bukan hanya masalah teknis, tetapi juga strategis dan politik. Kedua negara berkomitmen untuk menjaga stabilitas nasional dan pertumbuhan ekonomi dari ancaman siber yang terus meningkat. Evaluasi tahunan akan dilakukan terhadap MSP ini dari 2024 hingga 2028 untuk mengukur efektivitasnya.

## 2.2. Ancaman Siber Global Indonesia dan Amerika Serikat

### Ancaman Siber Global yang dialami Indonesia

Indonesia menghadapi berbagai bentuk tindak pidana kejahatan siber yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, termasuk pornografi online, judi online, pencemaran nama baik, penipuan, pemalsuan informasi elektronik, pemerasan, pengancaman, penyebaran berita bohong, pelanggaran hak cipta, hingga terorisme melalui dunia maya. Ancaman siber juga mencakup segala bentuk gangguan terhadap sistem informasi elektronik, pencurian

[18] Azizah Fitriyanti and Suharto, "Indonesia, US Agree to Promote Strong Cyberspace Cooperation" *ANTARA English News Portal*. , 2018, 20 Jul. 2025. , https://en.antaranews.com/news/119107/indonesia-us-agree-to-promote-strong-cyberspace-cooperation.

[19] U.S. Department of Defense, "Readout of Indonesia–United States Security Dialogue 2021" *U.S. Department of Defense*. , 2021, 21 Jul. 2025. , https://www.defense.gov/News/Releases/Release/Article/2852539/readout-of-indonesia-united-states-security-dialogue-2021/.

data, penyadapan tidak sah, dan penyalahgunaan perangkat informasi elektronik. Meskipun telah memiliki regulasi, Indonesia masih menghadapi tantangan dalam implementasi, koordinasi antar-instansi, dan kapasitas penegakan hukum. Upaya hukum yang dilakukan antara lain adalah kerja sama internasional, seperti dengan Australia melalui *Cyber Crime Investigation Centre* (CCIC).[20]

Meskipun pemerintah telah berupaya menekan ancaman siber, kejahatan siber terus meningkat seiring tingginya akses internet di Indonesia. Pada tahun 2023, ancaman paling sering ialah *web defacement*, *ransomware varian Lock Bit 3.0 brain cipher*, dan kebocoran data (*data breach*) pada sektor pemerintahan dan kesehatan yang menyebabkan gangguan layanan dan data tidak dapat dipulihkan. BSSN mencatat 361 juta anomali lalu lintas digital pada awal 2023, dengan 42% berupa *malware*, 35% *trojan*, dan 9% kebocoran data, yang menunjukkan tingginya ancaman siber global yang tidak diimbangi dengan kebijakan sistem keamanan data digital memadai.[21] Pada Juni 2024, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menangani kasus penipuan oleh anggota jaringan internasional berinisial ZS yang menipu 823 warga negara Indonesia dengan modus lowongan kerja palsu yang menimbulkan kerugian sebesar Rp 59 miliar.[22] Kasus lainnya melibatkan ancaman bagi pusat data nasional Indonesia menyebabkan kebocoran data e-visa di Bali sehingga membuka akses informasi data pelancong secara tak sah, serangan ransomware yang merusak layanan imigrasi, bandara, dan KPU sehingga berdampak pada 40-200 lembaga.[23] Rendahnya sistem keamanan siber di Indonesia juga dikuatkan dengan adanya pemeriksaan dan backup data pada akhir 2024, ditemukan 98% data tidak terbackup yang dapat menjadi peluang bagi peretas untuk mengancam

---

[20] Aditama, Sinaga, and Putri, "Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya dalam Penegakan Hukum Antara Indonesia dan Amerika." *Jurnal Kompilasi Hukum* 10.1 (2025): 58–77. https://doi.org/10.29303/jkh.v10i1.202.

[21] VIRTUS, "Introducting the Anti Cybercrime Formula, a Powerful Way to Defeat Cyber Attack," 2023, online, Internet, 17 Jun. 2025. , https://www.virtusindonesia.com/en/insights/news-articles/detail/introducing-the-anti-cybercrime-formula-a-powerful-way-to-defeat-cyber-attacks?.com.

[22] Arafat and Wirasto, "Kebijakan Kriminal dalam Penanganan Siber di Era Digital : Studi Kasus di Indonesia."

[23] Reuters, "Cyber Attack Compromised Indonesia Data Centre, Ransom Sought," 2024, online, Internet, 17 Jun. 2025. , https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/?.com.

keamanan digital di Indonesia.[24] Sepanjang 2024, Kaspersky mencatat 19,2 juta upaya serangan siber berbasis web di Indonesia, menurun 34,85% dari 29,5 juta insiden pada 2023. Namun, penurunan ini belum mencerminkan peningkatan sistem keamanan siber nasional, mengingat data serangan sejak 2019 menunjukkan tren fluktuatif. Sementara itu, promosi aktif distribusi data ilegal dan penggunaan alat pencuri aset kripto meningkat dari 55 kasus pada 2022 menjadi 129 kasus pada 2024, menandakan ancaman siber yang kian serius. Serangan terhadap BSI dan data pemilih menurunkan kepercayaan investor, sementara kerugian akibat serangan pada aset kripto mencapai sekitar Rp300 miliar pada 2024. Kondisi ini menegaskan urgensi kebijakan yang lebih kuat dalam keamanan siber nasional.[25]

Selain kerugian finansial, serangan siber menimbulkan dampak jangka panjang bagi lembaga pemerintah, seperti pengeluaran tak terduga, penurunan layanan publik, biaya pemulihan sistem, dan pendataan ulang yang mahal. Ancaman global yang menyasar sektor perbankan, energi, komunikasi, dan pemerintahan memperbesar risiko terhadap keamanan nasional. Indonesia menghadapi kebocoran data di sektor kesehatan dan keuangan, serta gangguan layanan pemerintah dan infrastruktur, yang berdampak pada reputasi dan stabilitas negara. Untuk merespons, pemerintah memperkuat regulasi digital melalui Kominfo dan meningkatkan kapasitas BSSN, membentuk unit militer siber, serta mendorong kolaborasi publik-swasta dan audit sistem keamanan. Melalui Perpres No. 28 Tahun 2021, BSSN ditetapkan sebagai otoritas utama keamanan siber nasional, termasuk inisiasi program CTIP bersama perusahaan swasta untuk meningkatkan proteksi data.[26] Meski demikian, penanggulangan ancaman regional belum maksimal karena masih banyak celah keamanan. Oleh karena itu, Indonesia menempatkan kerja sama internasional termasuk dengan Amerika Serikat sebagai pilar penting dalam strategi ketahanan siber.

---

[24] Reuters, "Indonesia President Orders Audit of Data Centres After Cyberattack," 2024, online, Internet, 17 Jun. 2025. , https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/?.com.

[25] Indonesiansentinel, "19 Million Cyberattack Attempts in Indonesia Troughout 2024," 2025, https://indonesiasentinel.com/kaspersky-reports-19-million-cyberattack-attempts-in-indonesia-troughout-2024/.com.

[26] Agung Ikhssani, Cakra Mudra, and Fragmadio Gana Prasidya, "Cybersecurity dan Tata Kelola Intelijen Cybersecurity dan Tata Kelola Intelijen" *Jurnal Kajian Stratejik Ketahanan Nasional*. 7.1 (2024).

**Ancaman Siber yang dialami Amerika Serikat**

Amerika Serikat memiliki kerangka hukum yang komprehensif dalam menghadapi ancaman siber, salah satunya melalui *Computer Fraud and Abuse Act* (CFAA) yang mengatur berbagai bentuk pelanggaran terhadap sistem komputer, termasuk akses ilegal ke komputer pemerintah, peretasan untuk tujuan penipuan, penyebaran malware, penggunaan kata sandi tanpa izin, serta pemerasan berbasis teknologi. Selain CFAA, kebijakan keamanan siber juga diperkuat melalui Digital *Millennium Copyright Act* (DMCA) dan berbagai regulasi federal maupun negara bagian, serta didukung institusi penegak hukum yang kuat dan terkoordinasi.

Undang-undang pidana siber diatur dalam *United States Code* (U.S. Code), yang mencakup sekitar 19 pasal khusus terkait kejahatan siber. Beberapa di antaranya antara lain:

1. 18 U.S.C § 1028 membahas penipuan terkait dokumen identitas dan otentikasi, termasuk pemalsuan dan kepemilikan alat untuk pemalsuan, dengan ancaman hukuman hingga 30 tahun penjara.
2. 18 U.S.C § 1028a mengatur pencurian identitas berat (aggravated identity theft), dengan hukuman penjara 2 hingga 5 tahun tanpa masa percobaan.
3. 18 U.S.C § 1029 meliputi penipuan menggunakan perangkat akses, seperti kartu kredit atau alat elektronik, termasuk peretasan, dengan hukuman 5–20 tahun penjara.
4. 18 U.S.C § 1030 secara khusus mengatur tindakan penipuan dan pelanggaran yang berhubungan dengan penggunaan komputer (termasuk peretasan), dengan hukuman antara 5 hingga 20 tahun.
5. 18 U.S.C § 1037 menyoroti kejahatan siber berbasis email, seperti pengiriman spam, pemalsuan informasi pengirim, dan akses ilegal, dengan ancaman hukuman 3–5 tahun penjara.
6. 18 U.S.C § 1043 mencakup penipuan melalui sarana komunikasi seperti TV, radio, dan internet, dengan hukuman maksimal 20 tahun atau 30 tahun jika merugikan lembaga keuangan, serta denda hingga $1.000.000.

7. 18 U.S.C §§ 1466A, 2251, dan 2252 mengatur kejahatan pornografi anak, mencakup larangan distribusi dan kepemilikan materi eksploitasi seksual anak dalam berbagai bentuk media, dengan hukuman penjara minimal 30 tahun hingga seumur hidup.[27]

Melalui regulasi yang ketat ini, Amerika Serikat menunjukkan komitmen serius dalam menanggulangi kejahatan siber dan memberikan dasar hukum yang kuat bagi penegakan hukum siber di tingkat nasional maupun dalam kerja sama internasional. Amerika Serikat memiliki kesiapan teknologi siber yang sangat tinggi, menjadikan teknologi sebagai kekuatan ekonomi, politik, dan militernya. Pada masa Presiden Obama, dibentuk *US Cyber Command* (*US Cybercom*) sebagai unit militer independen di bawah kendali langsung presiden. Di era Trump, komando ini diberi kewenangan lebih luas untuk melakukan operasi siber strategis demi kepentingan nasional.

Amerika Serikat juga mengembangkan EINSTEIN 3, sistem pendeteksi ancaman siber real-time untuk jaringan pemerintah federal. Selain itu, melalui *Cybersecurity and Infrastructure Security Agency* (CISA), pemerintah aktif memantau dan merespons serangan siber, khususnya pada sektor-sektor vital seperti energi, keuangan, dan pemerintahan. Seluruh inisiatif ini mencerminkan komitmen kuat AS dalam membangun pertahanan siber yang tangguh.[28]

Ancaman siber yang dihadapi Amerika Serikat pada 2019–2024 menyebabkan kerugian besar, baik secara finansial, reputasi, maupun keamanan nasional. Serangan *ransomware* terhadap kota Baltimore tahun 2019 mengakibatkan kerugian hingga 18 juta dolar AS karena lumpuhnya layanan publik. Pada 2020, serangan terhadap perangkat lunak SolarWinds memengaruhi lebih dari 18.000 pelanggan global, termasuk lembaga federal penting. Serangan Colonial Pipeline pada 2021 memicu krisis pasokan bahan bakar di Pantai Timur, sementara kebocoran data akibat peretasan MOVEit

[27] Aditama, Sinaga, and Putri, "Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya dalam Penegakan Hukum Antara Indonesia dan Amerika." *Jurnal Kompilasi Hukum* 10.1 (2025): 58–77. https://doi.org/10.29303/jkh.v10i1.202.

[28] Rangga Dheo Chandra, Andrea Abdul Rahman Azzqy, and Syahrul Awal, "Strategi Keamanan Siber Amerika Serikat di Masa Pemerintahan Joe Biden Terkait Isu State-Sponsored Cyber Espionage" *JOM*. 7.1 (2023): 13–26.

pada 2023 menjadi salah satu yang terbesar, melibatkan 2.700 organisasi dan 93 juta data pribadi.

Kerugian tidak hanya dalam bentuk biaya pemulihan sistem, tetapi juga gangguan layanan dan meningkatnya risiko kejahatan digital seperti pemerasan dan penipuan identitas. Untuk merespons hal ini, pemerintah AS menerapkan strategi komprehensif, salah satunya melalui program *Shields Up* oleh CISA. Program ini mendorong sektor infrastruktur kritis seperti energi, air, dan transportasi untuk meningkatkan pertahanan siber melalui audit keamanan, sistem deteksi dini, dan pelatihan intensif guna memperkuat ketahanan nasional terhadap serangan digital.[29] Melalui kombinasi pendekatan teknis, kebijakan hukum, kerja sama lintas sektor, dan koordinasi internasional, Amerika Serikat berusaha membangun ketahanan siber nasional yang tangguh dan adaptif terhadap berbagai jenis ancaman global yang terus berkembang.

**Pentingnya Keamanan Siber di Wilayah Indo Pasifik Bagi Indonesia dan Amerika Serikat**

Wilayah Indo-Pasifik memiliki signifikansi strategis yang sangat besar bagi Indonesia maupun Amerika Serikat, namun juga menghadirkan tantangan keamanan siber yang kompleks. Bagi Indonesia, kawasan ini merupakan jalur perdagangan maritim yang vital dan memiliki potensi ekonomi digital yang masif. Beberapa sektor yang sangat rentan terhadap ancaman siber di kawasan Indo-Pasifik bagi Indonesia adalah sektor transportasi laut dan pelabuhan, sektor energi dan utilitas, serta sektor komunikasi dan keuangan. Data dari BSSN tahun 2023 menunjukkan bahwa sektor transportasi dan energi menjadi dua dari lima sektor paling terdampak oleh serangan siber, terutama dalam bentuk *phishing*, *ransomware*, dan eksploitasi sistem *Industrial Control Systems* (ICIS) . Sistem digital pelabuhan seperti Tanjung Priok, Pelindo II, dan pelabuhan di Batam sangat bergantung pada software logistik dan konektivitas daring . Jika sistem ini terganggu akibat serangan siber, maka dampaknya akan berantai, dimulai dari terganggunya aktivitas ekspor-impor, keterlambatan logistik

[29] Chris Bronk and Wm Arthur Conklin, "Who's in Charge and How Does it Work? US Cybersecurity of Critical Infrastructure" *Journal of Cyber Policy*. 7 (2022).

nasional, serta kerugian ekonomi miliaran rupiah per hari.[30] Oleh karena itu, menjaga keamanan siber di Indo-Pasifik menjadi krusial untuk melindungi infrastruktur energi dan sistem komunikasi yang esensial, serta untuk mendukung pertumbuhan ekonomi digital nasional dan mempertahankan kedaulatan di tengah persaingan global yang intens.

Sementara itu, bagi Amerika Serikat, stabilitas keamanan siber di Indo-Pasifik sangat penting untuk menegakkan hukum internasional, menjaga stabilitas regional, dan memastikan kelancaran jalur perdagangan laut global. Sejak 2020, Amerika Serikat melalui Menteri Luar Negeri Mike Pompeo menyatakan bahwa klaim maritim China di Laut China Selatan bersifat ilegal dan tidak sesuai dengan hukum laut internasional (UNCLOS). Dalam konteks ini, pengamanan siber di kawasan Indo-Pasifik menjadi sangat penting bagi Amerika Serikat, mengingat tingginya aktivitas intelijen, pengiriman kapal induk, kapal selam, drone, hingga pembom di wilayah tersebut. Perang dagang antara AS dan China juga memperkuat pandangan bahwa kawasan ini bisa menjadi ancaman strategis jika tidak diimbangi dengan kebijakan siber yang kuat. Amerika Serikat memiliki tiga kepentingan utama di Laut China Selatan. Pertama, menegakkan hukum laut internasional berdasarkan UNCLOS. Kedua, menjaga keamanan dan stabilitas kawasan. Ketiga, memastikan jalur perdagangan global tetap terbuka dan bebas, mengingat Laut China Selatan merupakan jalur vital bagi perdagangan internasional.[31]

Sebagai wilayah perairan strategis, sektor pelayaran dan logistik di Indo-Pasifik sangat rentan terhadap ancaman digital. Sistem navigasi berbasis GPS dan perangkat lunak pelabuhan pintar di kawasan Asia Tenggara, Jepang, dan Australia terhubung langsung dengan sistem logistik perusahaan besar asal Amerika seperti FedEx, Maersk, dan ExxonMobil. Serangan siber terhadap titik-titik ini dapat mengacaukan rantai pasok global yang menopang industri manufaktur dan energi AS. Selain itu, infrastruktur energi seperti jaringan pipa dan pelabuhan bahan bakar di kawasan Indo-Pasifik yang menjadi jalur penting bagi armada militer dan

[30] Wahyu Hutomo et al., "Kontribusi Indonesia Dalam Isu Kawasan Indo-Pasifik Melalui Kebijakan Global Maritime Fulcrum." Jurnal Kewarganegaraan 7.1 (2023): 143–153. www.intermestic.unpad.ac.id.
[31] Delanova and Yani, "Dampak Kebijakan Amerika Serikat Di Indo-Pasifik Dalam Menghadapi China Terhadap Keamanan Indonesia." *Jurnal Academia Praja* 5.1 (2022): 79–97.

kapal dagang Amerika masih rentan terhadap serangan ransomware maupun serangan siber destruktif lainnya. Dampaknya bisa sangat besar, mulai dari gangguan operasional hingga kerugian ekonomi yang mencapai ratusan juta dolar akibat pemulihan sistem, terganggunya perdagangan, dan hambatan dalam operasi strategis.[32] Oleh karena itu, keamanan siber di Indo-Pasifik merupakan prioritas utama bagi kepentingan strategis AS.

### 2.3. Kebijakan Indonesia – Amerika Serikat di Bidang Siber Tahun 2023-2024

Faktor utama yang mendorong Indonesia menjalin kerja sama siber dengan Amerika Serikat adalah keunggulan teknologi dan kepemimpinan global AS dalam tata kelola keamanan digital. Amerika dikenal memiliki sistem pertahanan siber yang maju, seperti US Cyber Command, dukungan anggaran besar, serta kapasitas intelijen digital yang kuat. Perbedaan tingkat adaptasi teknologi antara Indonesia dan Amerika juga menjadi alasan penting, terutama dalam konteks penguatan sektor-sektor strategis seperti pertahanan dan ekonomi. Melalui kerja sama ini, Indonesia berharap dapat memperkuat infrastruktur digital nasional dan meningkatkan ketahanan terhadap ancaman siber yang semakin kompleks.

**Variabel Sistemik Ancaman Siber Global Terhadap Indonesia**

Dalam era digital, ancaman siber telah menjadi tantangan global yang tidak mengenal batas wilayah. Dampaknya bersifat sistemik, menyerang berbagai sektor vital seperti listrik, transportasi, perbankan, dan layanan publik lainnya. Indonesia, sebagai negara dengan pengguna internet terbesar keempat di dunia, menghadapi risiko tinggi dari serangan siber berskala besar, termasuk kebocoran data, ransomware, dan disinformasi politik. Serangan semacam ini tidak hanya menyebabkan gangguan teknis, tetapi juga memicu krisis kepercayaan publik, instabilitas ekonomi, dan bahkan ancaman terhadap keamanan nasional.

Sifat lintas batas dari serangan siber menuntut kerja sama internasional yang kuat. Indonesia tidak dapat mengandalkan pendekatan

[32] Delanova and Yani, "Dampak Kebijakan Amerika Serikat Di Indo-Pasifik Dalam Menghadapi China Terhadap Keamanan Indonesia." *Jurnal Academia Praja* 5.1 (2022): 79–97.

domestik semata, melainkan perlu membangun kolaborasi strategis dengan negara-negara yang memiliki kemampuan keamanan digital yang lebih mapan, seperti Amerika Serikat. AS memiliki rekam jejak panjang dalam pengembangan sistem pertahanan siber, termasuk kapasitas deteksi dini, infrastruktur canggih, dan SDM terlatih. Kerja sama ini penting untuk memperkuat kebijakan siber Indonesia, meningkatkan kapasitas teknis, serta mencegah infiltrasi terhadap sistem negara.

Dari hasil wawancara dengan pakar keamanan siber Alfons Tanujaya, diketahui bahwa kerja sama Indonesia-AS sangat krusial untuk mendukung penguatan infrastruktur digital dalam negeri. Tanpa dukungan dari negara-negara dengan kemampuan siber tinggi, Indonesia berisiko mengalami kebocoran informasi strategis yang dapat merusak sektor pertahanan, keuangan, hingga maritim. Meski demikian, pemerintah tetap diharapkan menjaga batasan agar kerja sama tidak mengganggu kedaulatan negara.

Faktor eksternal lain yang mendorong kerja sama ini adalah posisi strategis Indonesia di kawasan Indo-Pasifik. Meningkatnya ketergantungan ekonomi digital dan potensi konflik geopolitik menjadikan wilayah ini rawan terhadap ancaman siber. Sebagai negara dengan kepentingan besar di Indo-Pasifik, Amerika menjadi mitra yang tepat untuk membangun kebijakan siber bersama. Hal ini terealisasi dalam penandatanganan Memorandum of Strategic Partnership (MSP) antara Indonesia dan AS pada tahun 2024, yang menjadi pijakan awal kolaborasi siber di kawasan.

**Variabel Sosial Kurangnya Kepercayaan Masyarakat Terhadap BSSN Minim Tenaga Ahli**

Dalam era digital yang semakin kompleks, Indonesia menghadapi tantangan besar dalam membangun sistem keamanan siber yang andal. Salah satu hambatan utama adalah masih rendahnya kompetensi sumber daya manusia dan belum meratanya adaptasi teknologi keamanan siber, baik di sektor publik maupun privat. Dibandingkan negara-negara tetangga seperti Malaysia, Indonesia masih tertinggal dalam kesiapan infrastruktur dan pengelolaan keamanan digital.

Amerika Serikat dipandang sebagai mitra strategis karena memiliki sejarah panjang dalam pengembangan teknologi siber serta sistem

pertahanan yang sudah mapan sejak era Perang Dingin. Pendekatan multilapis yang diterapkan Amerika melibatkan perangkat teknologi mutakhir, edukasi publik, kemitraan dengan sektor swasta, serta sistem deteksi berbasis kecerdasan buatan menjadi model yang relevan untuk diadopsi. Strategi nasional keamanan siber Amerika bahkan telah dirancang hingga 2030 dengan fokus pada perlindungan infrastruktur kritis dan peningkatan kapasitas SDM.

Indonesia dapat memperoleh banyak manfaat dari kerja sama ini, terutama dalam hal transfer pengetahuan dan penguatan institusi keamanan digital. Di tengah ketergantungan yang semakin tinggi terhadap teknologi informasi di sektor-sektor vital, peningkatan kesadaran kolektif dan pembangunan kapasitas nasional menjadi langkah yang tidak bisa ditunda. Tantangan lainnya adalah memastikan agar kerja sama internasional tetap menjaga batas-batas kedaulatan, dengan regulasi yang jelas terhadap akses data dan sektor strategis seperti pertahanan.

Model pengambilan kebijakan di Amerika menunjukkan pentingnya keseimbangan antara efektivitas dan pengawasan. Awalnya, semua tindakan keamanan siber memerlukan persetujuan presiden. Namun, seiring meningkatnya ancaman digital, kebijakan tersebut direvisi untuk memberi otoritas yang lebih fleksibel kepada lembaga keamanan siber, tanpa mengabaikan prinsip akuntabilitas. Pengalaman ini menjadi cerminan penting bagi Indonesia dalam membangun tata kelola keamanan siber yang responsif namun tetap terkendali.

**Variabel Pemerintah Sistem Politik Demokrasi Indonesia**

Sebagai negara demokrasi terbesar ketiga di dunia, Indonesia menjunjung tinggi prinsip keterbukaan, partisipasi publik, dan akuntabilitas dalam penyelenggaraan pemerintahan. Prinsip-prinsip ini juga tercermin dalam kebijakan keamanan siber. Namun, justru karena sifat demokrasi yang inklusif, pengelolaan keamanan digital menjadi lebih menantang. Negara tidak bisa bertindak sepihak; setiap kebijakan harus melalui proses koordinasi dan mempertimbangkan aspirasi masyarakat, yang kadang membuat respons terhadap ancaman siber menjadi lambat.

Di sisi lain, demokrasi juga menuntut transparansi dan tanggung jawab dalam setiap insiden siber. Sayangnya, penanganan insiden sering kali tidak disertai dengan penjelasan yang jelas atau koordinasi yang efektif, sehingga menurunkan kepercayaan publik. Meski begitu, sistem demokrasi memberi peluang besar bagi kolaborasi lintas sektor antara pemerintah, komunitas teknologi, sektor swasta, dan masyarakat sipil untuk membangun sistem keamanan digital yang lebih tangguh dan partisipatif.

Amerika Serikat, dengan pengalaman dan kapasitas tinggi dalam keamanan siber, menjadi mitra strategis bagi Indonesia. Kerja sama ini tercermin dalam penandatanganan Memorandum Saling Pengertian (MSP) periode 2024–2028, sebagai respons atas meningkatnya ancaman siber global. MSP mencakup pertukaran informasi, pelatihan teknis, simulasi penanganan insiden, serta riset bersama. Fokus utamanya adalah perlindungan infrastruktur informasi kritikal seperti sektor kesehatan, transportasi, dan pemilu.

Dengan latar belakang hubungan diplomatik yang telah berlangsung lebih dari 75 tahun, serta kesamaan nilai demokrasi dan komitmen terhadap hukum internasional, MSP ini menjadi tonggak penting bagi Indonesia dan Amerika dalam menghadapi tantangan siber global. BSSN dan *Department of Homeland Security* (DHS) bertindak sebagai pelaksana utama untuk memastikan kerja sama ini berjalan efektif dan adaptif terhadap dinamika ancaman digital.[33]

Di pihak Indonesia, kerja sama ini juga melibatkan Kementerian Komunikasi dan Digital, Polri, serta sektor swasta. Meski memiliki manfaat besar, implementasi MSP menghadapi sejumlah tantangan, seperti kekhawatiran terhadap intervensi asing dan ketergantungan teknologi luar yang dapat mengancam kedaulatan digital. Perbedaan sistem hukum antara kedua negara juga menyulitkan penyelarasan standar perlindungan data dan

[33] CSIRT, "*Indonesia dan Amerika Serikat Tanda Tangani Kerja Sama Keamanan Siber*" 2024, online, Internet, 17 Jun. 2025. , https://csirt.makassarkota.go.id/posts/indonesia-dan-amerika-serikat-tanda-tangani-kerja-sama-keamanan-siber?.com.

penegakan hukum siber. Oleh karena itu, transparansi, audit bersama, dan pedoman etis menjadi elemen penting dalam pelaksanaannya.[34]

Bagi Indonesia, MSP memiliki nilai strategis sebagai sarana alih teknologi dan penguatan sistem pertahanan digital nasional yang masih rentan. Kerja sama ini mendukung terciptanya ekosistem digital yang aman, khususnya dalam layanan publik dan ekonomi digital. Selain itu, MSP juga mencerminkan peran aktif Indonesia dalam diplomasi keamanan siber kawasan. MSP berlaku selama empat tahun (2024–2028) dengan evaluasi tahunan untuk mengukur dampaknya. Evaluasi mencakup indikator seperti pelatihan bersama, penanganan insiden lintas negara, dan peningkatan sistem keamanan nasional. Jika terbukti efektif, MSP berpeluang ditingkatkan menjadi perjanjian internasional yang mengikat secara hukum.

**Variabel Peran Indonesia dalam Indo Pasifik**

Indonesia memiliki posisi strategis di kawasan Indo-Pasifik, baik secara geografis maupun geopolitik. Sebagai negara kepulauan terbesar yang menjadi penghubung Samudra Hindia dan Pasifik, Indonesia memainkan peran penting dalam jalur perdagangan dan keamanan kawasan. Selain militer dan diplomasi konvensional, Indonesia kini juga terlibat dalam isu-isu non-tradisional seperti keamanan siber. Kompleksitas ancaman digital mendorong perlunya kerja sama internasional, termasuk dengan Amerika Serikat, guna memperkuat posisi Indonesia sebagai aktor utama di Indo-Pasifik.

Kerja sama ini didorong oleh komitmen Indonesia terhadap *ASEAN Outlook on the Indo-Pacific* (AOIP), yang menekankan pendekatan inklusif, transparan, dan kolaboratif dalam menangani isu kawasan, termasuk keamanan digital. AOIP mendorong penguatan konektivitas dan perlindungan infrastruktur informasi di tengah ancaman siber lintas batas. Dalam kerangka ini, kemitraan dengan AS menjadi langkah strategis untuk membangun kapasitas nasional dan menjamin keamanan regional. Transformasi digital yang cepat juga mendorong Indonesia memperkuat

[34] OkeZone, "*AS dan Indonesia Tandatangani MoU Memperkuat Kerja Sama Pertahanan Siber*" 2024, online, Internet, 17 Jun. 2025. , https://techno.okezone.com/read/2024/12/06/54/3092838/as-dan-indonesia-tandatangani-mou-memperkuat-kerja-sama-pertahanan-siber?.com.

ketahanan siber, namun keterbatasan SDM dan teknologi menjadi hambatan. Oleh karena itu, kerja sama dengan AS mencakup pelatihan, asistensi teknis, dan pengembangan kebijakan siber yang adaptif. Indonesia memosisikan diri sebagai mitra aktif dan konstruktif di kawasan, memperkuat stabilitas regional melalui diplomasi digital, sembari tetap menjaga prinsip non-blok dan kemandirian dalam kebijakan luar negerinya.

**Variabel Individu keberhasilan kerjasama Indonesia – Amerika Serikat**

Di balik dinamika politik dan strategi nasional, keberhasilan kerja sama siber Indonesia–Amerika Serikat turut ditentukan oleh peran individu, seperti pemimpin, diplomat, teknokrat, dan ahli siber yang terlibat langsung. Meski jarang terlihat di publik, mereka berperan penting dalam membangun kepercayaan, membuka komunikasi efektif, dan menjaga kesinambungan kerja sama lintas negara.

Tokoh-tokoh Indonesia yang memiliki reputasi internasional di bidang keamanan digital menjadi wajah negara dalam forum global sekaligus penghubung diplomatik. Lewat pendekatan profesional dan personal, mereka menunjukkan keseriusan Indonesia dalam membangun sistem siber yang kuat dan terbuka. Keberhasilan ini juga bergantung pada kemampuan individu menjalin relasi yang setara dan dihormati oleh mitra seperti AS, tanpa bersikap inferior, serta mampu berdialog dan bernegosiasi dengan percaya diri. Di tingkat teknis, insinyur siber, analis forensik digital, dan perancang sistem berperan langsung dalam mewujudkan hasil kerja sama, melalui pelatihan, pertukaran pengetahuan, dan penguatan sistem pertahanan nasional. Mereka membuktikan bahwa kerja sama ini membawa dampak nyata di lapangan.

Dorongan utama Indonesia menjalin kerja sama internasional di bidang siber adalah perlindungan terhadap infrastruktur kritis seperti energi, komunikasi, dan pelabuhan. Letak strategis Indonesia menuntut adaptasi teknologi tinggi yang dibarengi penguatan sistem keamanan siber. MSP Indonesia-AS sendiri bertujuan meningkatkan kapasitas dalam mengurangi risiko dan ancaman siber, khususnya pada sektor vital seperti pertahanan

dan maritim, yang menjadi fokus kerja sama pada periode 2023–2024.[35] Salah satu bentuk kerja sama siber Indonesia–Amerika pada 2023–2024 adalah penandatanganan MoU antara BSSN dan CISA untuk meningkatkan keamanan dan ketahanan sistem transportasi maritim internasional. Kolaborasi ini menunjukkan komitmen kedua negara dalam melindungi infrastruktur maritim dari serangan siber. Melalui kerja sama ini, dilakukan pula latihan bersama yang fokus pada peningkatan keamanan siber maritim dan respons insiden di Indonesia serta kawasan Indo-Pasifik.[36]

Peningkatan kapasitas nasional dilakukan melalui latihan bersama yang menitikberatkan pada peningkatan kemampuan teknis dalam mendeteksi dan merespons serangan siber pada sektor maritim. Kerja sama ini juga memperkuat posisi Indonesia dalam arsitektur keamanan Indo-Pasifik dengan menekankan pentingnya kolaborasi internasional dalam menjaga stabilitas dan keamanan lintas batas. Selain itu, Indonesia menjalin kemitraan strategis dengan perusahaan teknologi global, seperti *Microsoft*, untuk memperkuat perlindungan terhadap sektor-sektor penting negara dari kejahatan siber. Seluruh inisiatif ini merupakan bagian dari strategi nasional untuk menciptakan ekosistem digital yang aman, tangguh, dan berdaulat.

### 2.4. Bentuk Kerja Sama Siber Indonesia-Amerika Tahun 2023-2024

Kerja sama siber Indonesia–Amerika Serikat pada 2023–2024 menitikberatkan pada peningkatan kapasitas intelijen di sektor strategis, khususnya pertahanan dan maritim. Penandatanganan Memorandum Saling Pengertian (MSP) antara Indonesia dan Amerika Serikat untuk periode 2024–2028 merupakan respons terhadap meningkatnya ancaman siber di kawasan dan global. Melalui kerja sama antara BSSN dan *Department of Homeland Security* (DHS), MSP bertujuan memperkuat kolaborasi teknis dan kebijakan dalam mencegah serta menangani insiden siber. Ruang lingkup MSP meliputi pertukaran informasi ancaman, pelatihan teknis, simulasi penanganan

[35] Teddy Putra Ar Rasyid and Wishnu Mahendra Wiswayana, "Upaya Kerjasama Pertahanan Indonesia-Amerika Serikat dalam Mencapai Target Minimum Essential Force Pertahanan Negara Tahun 2020-2021" *Journal of Foreign Affairs*. 8.1 (2016): 1–23.

[36] Homeland Security, "*DHS Bolsters Indo-Pacific Maritime Cybersecurity through Partnership with Indonesia*," 2025, online, Internet, 17 Jun. 2025. https://www.dhs.gov/archive/news/2024/06/18/dhs-bolsters-indo-pacific-maritime-cybersecurity-through-partnership-indonesia?.com.

serangan (*cyber drill*), dan riset bersama dalam teknologi keamanan siber. Fokus utamanya adalah penguatan perlindungan terhadap infrastruktur informasi kritikal (CII), seperti sektor kesehatan, transportasi, dan sistem pemilu. Kolaborasi ini mencerminkan komitmen kedua negara dalam melindungi infrastruktur maritim dari ancaman dan intrusi siber, serta mencakup latihan bersama untuk meningkatkan respons insiden di Indonesia dan kawasan Indo-Pasifik.

Sebagai bagian dari hubungan diplomatik Indonesia–AS yang telah terjalin selama 75 tahun, MSP dikoordinasikan oleh BSSN dan DHS, serta melibatkan lembaga nasional lainnya seperti Kominfo, Polri, dan sektor privat. Meski menjanjikan manfaat strategis, implementasinya tetap harus memperhatikan isu kedaulatan digital dan potensi ketergantungan terhadap teknologi asing.[37]

Perbedaan sistem hukum dan regulasi antara Indonesia dan Amerika Serikat menjadi tantangan dalam menyelaraskan standar perlindungan data dan penegakan hukum siber. Oleh karena itu, transparansi, audit bersama, serta kerangka etika kolaborasi menjadi komponen penting dalam pelaksanaan MSP. MSP memiliki nilai strategis bagi Indonesia, tidak hanya sebagai sarana transfer teknologi dan pengetahuan, tetapi juga sebagai langkah memperkuat ketahanan siber nasional yang masih rawan terhadap serangan digital. Kerja sama ini mendukung terbentuknya ekosistem digital yang aman, khususnya dalam konteks transformasi digital layanan publik dan pertumbuhan ekonomi berbasis teknologi. Di sisi lain, MSP mencerminkan peran aktif Indonesia dalam diplomasi keamanan digital di kawasan Asia-Pasifik.

Periode kerja sama ditetapkan selama empat tahun (2024–2028) dengan evaluasi tahunan untuk menilai efektivitasnya. Evaluasi mencakup indikator seperti jumlah pelatihan bersama, penanganan insiden siber lintas negara, dan penguatan sistem keamanan nasional. Jika berhasil, MSP

[37] CSIRT, "Indonesia dan Amerika Serikat Tanda Tangani Kerja Sama Keamanan Siber." 2024. Online. Internet. 17 Jun. 2025. . https://csirt.makassarkota.go.id/posts/indonesia-dan-amerika-serikat-tanda-tangani-kerja-sama-keamanan-siber?.com.

berpotensi ditingkatkan menjadi perjanjian internasional yang mengikat secara hukum.

## 3. KESIMPULAN

Kerja sama siber antara Indonesia dan Amerika Serikat pada 2023–2024 merupakan langkah strategis yang didorong oleh meningkatnya kompleksitas ancaman siber global, posisi Indonesia yang strategis di Indo-Pasifik, serta keterbatasan infrastruktur dan sumber daya manusia nasional di bidang keamanan siber. Kemitraan ini mencakup pelatihan teknis, pertukaran intelijen, penguatan infrastruktur kritis terutama di sektor maritim dan kolaborasi dengan sektor swasta. Penandatanganan Memorandum Saling Pengertian (MSP) pada 2024 menjadi dasar kerja sama jangka panjang hingga 2028. Melalui inisiatif ini, Indonesia berhasil meningkatkan ketahanan siber nasional, memperluas akses terhadap teknologi mutakhir, dan memperkuat posisinya dalam tata kelola keamanan siber kawasan Indo-Pasifik.

**REFERENSI**


Aditama, Prigel, Elisabeth Aprilia Sinaga, and Citra Anjelika Putri. "Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya dalam Penegakan Hukum Antara Indonesia dan Amerika." Jurnal Kompilasi Hukum 10.1 (2025): 58–77. https://doi.org/10.29303/jkh.v10i1.202.

Apri Sudarmadi, Damar, and Arthur Josias Simon Runturambi. "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia." Jurnal Kajian Stratejik Ketahanan Nasional 2.2 (2019): 163–183. https://scholarhub.ui.ac.id/jksknhttps://scholarhub.ui.ac.id/jkskn/vol2/iss2/7.

Ar Rasyid, Teddy Putra, and Wishnu Mahendra Wiswayana. "Upaya Kerjasama Pertahanan Indonesia-Amerika Serikat dalam Mencapai Target Minimum Essential Force Pertahanan Negara Tahun 2020-2021." Journal of Foreign Affairs 8.1 (2016): 1–23.

Arafat, Muhammad, and Alexander Tito Enggar Wirasto. "Kebijakan Kriminal dalam Penanganan Siber di Era Digital : Studi Kasus di Indonesia." Equality : Journal of Law and Justice 1.2 (2024): 221–241.

Bronk, Chris, and Wm Arthur Conklin. "Who's in Charge and How Does it Work? US Cybersecurity of Critical Infrastructure." Journal of Cyber Policy 7 (2022).

Chandra, Rangga Dheo, Andrea Abdul Rahman Azzqy, and Syahrul Awal. "Strategi Keamanan Siber Amerika Serikat di Masa Pemerintahan Joe Biden Terkait Isu State-Sponsored Cyber Espionage." JOM 7.1 (2023): 13–26.

Chotimah, Hidayat Chusnul. "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 (2019): 113–114.

Cnnindonesia. "Menkomdigi: Peringkat Keamanan Siber RI Naik, Sejajar AS Hingga Jepang." cnnindonesia.com, 2025. https://www.cnnindonesia.com/teknologi/20250206153253-192-1195388/menkomdigi-peringkat-keamanan-siber-ri-naik-sejajar-as-hingga-jepang.

CSIRT. "Indonesia dan Amerika Serikat Tanda Tangani Kerja Sama Keamanan Siber," 2024. Online. Internet. 17 Jun. 2025. . https://csirt.makassarkota.go.id/posts/indonesia-dan-amerika-serikat-tanda-tangani-kerja-sama-keamanan-siber?.com.

Delanova, Mariane Olivia, and Yanyan Mochamad Yani. "Dampak Kebijakan Amerika Serikat Di Indo-Pasifik Dalam Menghadapi China Terhadap Keamanan Indonesia." Jurnal Academia Praja 5.1 (2022): 79–97.

DPR RI, and Badan Siber Dan Sandi Negara. Naskah Akademik Rancangan Undang - Undang tentang Keamanan dan Ketahanan Siber. Naskah Akademik, 2019. https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf.

Farahbod, K, C Shayo, and J Varzandeh. "Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts." Journal of Business and Behavioral Sciences 32.1 (2020): 63–71. https://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf#page=63.

Fitriyanti, Azizah and Suharto, "Indonesia, US Agree to Promote Strong Cyberspace Cooperation" ANTARA English News Portal. , 2018, 20 Jul. 2025. , https://en.antaranews.com/news/119107/indonesia-us-agree-to-promote-strong-cyberspace-cooperation.

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. "Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis." Jurnal Konstituen 5.1 (2023): 1–17. https://ejournal.ipdn.ac.id/konstituen.

Haryanto, Agus, and Satya Muhammad Sutra. "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020." Global Political Studies Journal 7.1 (2023): 61.

Ikhssani, Agung, Cakra Mudra, and Fragmadio Gana Prasidya. "Cybersecurity dan Tata Kelola Intelijen Cybersecurity dan Tata Kelola Intelijen." Jurnal Kajian Stratejik Ketahanan Nasional 7.1 (2024).

Indonesiansentinel. "19 Million Cyberattack Attempts in Indonesia Troughout 2024," 2025. https://indonesiasentinel.com/kaspersky-reports-19-million-cyberattack-attempts-in-indonesia-troughout-2024/.com.

Jakarta Globe. "Indonesia, Australia Join Hands to Strengthen Cybersecurity." Jakarta Globe. Jakarta, 5 May 2017. https://jakartaglobe.id/news/indonesia-australia-join-hands-to-strengthen-cybersecurity.

Lestari, Minsi, and Tom Finaldin. "Kerja Sama Antara Indonesia Dan Negara-Negara Di Asia Tenggara Melalui Asean Regional Forum Dalam Bidang Keamanan Siber." Global Mind 4.2 (2023): 27–42.

Negara, Badan Siber Dan Sandi. "Press Release: BSSN Launching Gov-CSIRT, Indonesia Kini Punya Tim Respon Insiden Siber." Badan Siber dan Sandi Negara, 2024. Online. Internet. 30 Jun. 2025. . https://www.bssn.go.id/press-release-bssn-launching-gov-csirt-indonesia-kini-punya-tim-respon-insiden-siber/.

OkeZone. "AS dan Indonesia Tandatangani MoU Memperkuat Kerja Sama Pertahanan Siber," 2024. Online. Internet. 17 Jun. 2025. . https://techno.okezone.com/read/2024/12/06/54/3092838/as-dan-indonesia-tandatangani-mou-memperkuat-kerja-sama-pertahanan-siber?.com.

Primawanti, Henike, and Sidik Pangestu. "Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian

Nation (Asean) Regional Forum." Global Mind 2.2 (2020): 4–5.
Project, The American Presidency, "Join Statement by President Obama and President Joko 'Jokowi' Widodo of Indonesia" University of California, Santa Barbara. , 2015. Online. Internet.19 Jul. 2025. , https://www.presidency.ucsb.edu/documents/joint-statement-president-obama-and-president-joko-jokowi-widodo-indonesia.
Reuters. "Cyber Attack Compromised Indonesia Data Centre, Ransom Sought," 2024. Online. Internet. 17 Jun. 2025. . https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/?.com.
Reuters. "Indonesia President Orders Audit of Data Centres After Cyberattack," 2024. Online. Internet. 17 Jun. 2025. . https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/?.com.
Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber." Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan 1.2 (2020): 118–129.
S, Muh Yusuf. "Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index." Al-Ulum: Jurnal Sains Dan Teknologi 7.1 (2022): 21–26.
Security, Homeland. "DHS Bolsters Indo-Pacific Maritime Cybersecurity through Partnership with Indonesia," 2025. Online. Internet. 17 Jun. 2025. . https://www.dhs.gov/archive/news/2024/06/18/dhs-bolsters-indo-pacific-maritime-cybersecurity-through-partnership-indonesia?.com.
Sukadis, Beni. "Peran Diplomasi Pertahanan Indonesia Dalam Kerjasama Pertahanan Indonesia Dan Amerika Serikat." Jurnal Mandala : Jurnal Ilmu Hubungan Internasional 1.1 (2018): 111–112.
U.S. Department of Defense, "Readout of Indonesia–United States Security Dialogue 2021" U.S. Department of Defense. , 2021, 21 Jul. 2025. , https://www.defense.gov/News/Releases/Release/Article/2852539/readout-of-indonesia-united-states-security-dialogue-2021/.
VIRTUS. "Introducting the Anti Cybercrime Formula, a Powerful Way to Defeat Cyber Attack," 2023. Online. Internet. 17 Jun. 2025. . https://www.virtusindonesia.com/en/insights/news-articles/detail/introducing-the-anti-cybercrime-formula-a-powerful-way-to-defeat-cyber-attacks?.com.
Wahyu Hutomo, Bagus et al. "Kontribusi Indonesia Dalam Isu Kawasan Indo-Pasifik Melalui Kebijakan Global Maritime Fulcrum." Jurnal Kewarganegaraan 7.1 (2023): 143–153. www.intermestic.unpad.ac.id.
Wicaksono, Y. "Indonesia-Australia Kembali Perkuat Kerjasama Cyber Security." Polkam.go.id, 2017. Online. Internet. 3 Jul. 2025. .

https://polkam.go.id/indonesia-australia-kembali-perkuat-kerjasama-cyber-security/.

Zahra, Amara. “Rapor Tantangan dan Ancaman Kejahatan Siber 2024.” *idntimes.com*, 2024. https://www.idntimes.com/news/indonesia/amara-zahra/rapor-tantangan-dan-ancaman-kejahatan-siber-2024