pISSN : 2460-4208
eISSN : 2549-7685

MENGUKUR KEAMANAN SIBER INDONESIA MELALUI INDIKATOR PILAR KERJASAMA DALAM *GLOBAL CYBERSECURITY INDEX* (GCI)

Feline Cloramidine[1], Muhammad Badaruddin[2]
[1]Researcher at the Center for Politics and Governance Studies (CPGS) Universitas Bakrie, Jakarta.
[2]Director at the Center for Politics and Governance Studies (CPGS) Universitas Bakrie, Jakarta
Email: fcloramidine@gmail.com/feline.cloramidine@ui.ac.id, Muhammad.badaruddin@bakrie.ac.id

[*]Korespondensi: fcloramidine@gmail.com/feline.cloramidine@ui.ac.id

(Submission 25-10-2022, Revissions 10-05-2023, Accepted 15-05-2023).

Abstract

The revolution of digital technology has changed the landscape of international relations. Communication patterns between countries are becoming more transparent, multi-channel, and involving various parties with dynamic participation from non-state actors. These changing conditions benefit our lives while bringing new challenges that must be managed together internationally. This study discusses Indonesia's ability to manage its cyberspace which is assessed through the Global Cybersecurity Index (GCI) variable. Researchers are interested in analyzing Indonesia's commitment in meeting GCI guidelines, especially on indicators from the pillars of international cooperation that have succeeded in obtaining maximum assessment points from Indonesia's GCI score. Although, from some of the indicators mentioned it is not clearly illustrated whether it is achieved well or not. This research was conducted with qualitative methods, especially case studies to analyze cases systematically and also literature study data collection techniques. To achieve this goal, this article prepared by describing the importance of the pillars of international cooperation in improving Indonesia's global cybersecurity index score in the first part. Then we presented a map of cyberattacks against Indonesia from 2018 to 2020 and compared it with the increase in Indonesia's GCI score in the same period. This paper also describe the dynamics of relations between Indonesian ministries and institutions with their international partners for the third part. Finally, in the fourth part, this paper examine the advantages and disadvantages of Indonesia's efforts to improve the performance of its international cooperation in order to improve the level of its cybersecurity.

Keywords: *cybersecurity; international cooperation; global cybersecurity index; cyber threat; international telecommunication union.*

Abstrak

Revolusi teknologi digital telah mengubah lanskap hubungan internasional. Pola komunikasi antar negara menjadi lebih transparan, *multi-channel*, dan melibatkan berbagai pihak dengan partisipasi yang dinamis dari aktor non-negara. Kondisi yang berubah ini menguntungkan kehidupan kita sekaligus membawa tantangan baru yang harus dikelola bersama secara internasional. Penelitian ini membahas tentang kemampuan Indonesia dalam mengelola ruang sibernya yang dinilai melalui variabel *Global Cybersecurity Index* (GCI). Peneliti tertarik untuk menganalisis komitmen Indonesia dalam memenuhi pedoman GCI, khususnya pada indikator-indikator dari pilar kerjasama internasional yang berhasil mendapatkan poin penilaian maksimal dari skor GCI Indonesia. Meskipun, dari beberapa indikator yang disebutkan tidak tergambar dengan jelas apakah tercapai dengan baik atau tidak. Penelitian ini dilakukan dengan metode kualitatif, khususnya studi kasus untuk menganalisis kasus secara sistematis dan juga teknik pengumpulan data studi kepustakaan. Untuk mencapai tujuan tersebut, artikel ini disusun dengan menggambarkan pentingnya pilar kerjasama internasional dalam meningkatkan skor indeks keamanan siber global Indonesia pada bagian pertama. Kemudian kami memaparkan peta serangan siber terhadap Indonesia dari tahun 2018 hingga 2020 dan membandingkannya dengan peningkatan skor GCI Indonesia pada periode yang sama. Tulisan ini juga menggambarkan dinamika hubungan kementerian dan lembaga Indonesia dengan mitra internasionalnya untuk bagian ketiga. Terakhir, pada bagian keempat, makalah ini mengkaji apa keuntungan dan kerugian yang didapatkan dari upaya Indonesia dalam meningkatkan kinerja kerjasama internasionalnya dalam rangka meningkatkan tingkat keamanan sibernya.

Kata Kunci: keamanan siber; kerjasama internasional; *global cybersecurity index;* ancaman siber; *international telecommunication union.*

PENDAHULUAN

Setiap negara yang berdaulat tentu memiliki kewajiban untuk melindungi warga negara dan teritorinya. Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Alinea ke-4 menegaskan bahwa pemerintah Indonesia berkewajiban untuk melindungi segenap bangsa Indonesia. Perlindungan pemerintah Indonesia terhadap warga Indonesia yang dimaksud ialah perlindungan yang meliputi seluruh aspek, termasuk diantaranya ialah perlindungan terhadap keamanan data dan aktivitas yang terhubung melalui internet, atau yang dikenal sebagai keamanan siber. Keamanan siber saat ini dianggap sebagai domain keamanan baru bagi sebuah negara layaknya keamanan yang telah ada sebelumnya, yakni laut, darat, udara, dan ruang angkasa.

Urgensi keamanan siber sebagai domain baru ini ditegaskan oleh Kepala Badan Siber dan Sandi Negara (BSSN), Hinsa Siburian, bahwa keamanan siber merupakan domain yang juga diatur dalam pembukaan UUD Tahun 1945. "Waktu itu hanya terpikir darat, laut, dan udara, tetapi menjadi wadah Pembukaan UUD 1945 yaitu negara ini harus hadir untuk melindungi bangsa Indonesia dan seluruh tumpah darah Indonesia yakni darat, laut, udara, ruang angkasa nanti ditambah ruang siber" (Nursaid, 2022). Keamanan siber merupakan keamanan yang muncul sebagai bentuk perlindungan dari ruang siber. Sedangkan ruang siber merupakan ruang yang terhubung dengan koneksi internet serta menghubungkan banyak perangkat (*devices*) di dalamnya. Siburian menyebutkan bahwa ruang siber ialah sistem elektronik yang terhubung dengan koneksi internet hingga membentuk sebuah ruang baru, di luar ruang fisik seperti laut, darat, udara, dan luar angkasa dimana di dalamnya terjalin interaksi ekosistem sosial dan ekonomi secara digital. Bahkan dalam perkembangannya, ruang siber menempatkan diri sebagai pusat dari ruang yang lain, karena ruang siber merupakan ruang yang menghubungkan perangkat yang ada pada ruang yang lainnya. Oleh karena itu, keamanan siber juga menjadi pusat dari bentuk keamanan lainnya yang mana keamanan siber dapat menimbulkan ancaman baik yang berupa fisik maupun non-fisik.

Eksistensi ruang siber dan keamanan siber berprogres saling mempengaruhi bersama perkembangan teknologi, termasuk diantaranya teknologi persenjataan. Saat ini, teknologi informasi dan komunikasi berbasis internet dianggap sebagai alat persenjataan baru karena dalam ruang siber semua orang dapat terkoneksi sehingga kemungkinan orang lain untuk mengalami ancaman juga jauh lebih besar. Dalam ruang siber, baik negara yang sedang berkonflik maupun tidak, dapat mengalami ancaman karena aktor dalam ruang siber bukan hanya negara, komunitas, organisasi maupun perusahaan saja, melainkan juga individu tertentu dapat menjadi aktor penyebab terjadinya ancaman bagi keamanan siber.

Tingkat keamanan siber berbanding lurus dengan banyaknya jumlah perangkat yang terkoneksi dengan internet. Adanya revolusi teknologi membentuk pola perilaku masyarakat yang baru, dimana masyarakat saling terhubung tanpa mengenal batas dengan perangkat yang dimilikinya. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat, jumlah pengguna internet di Indonesia dalam periode waktu 2019-2020 (Q2) terdapat sebanyak 196,7 juta pengguna dengan jumlah penduduk di Indonesia ialah 266,7 juta jiwa. Jumlah tersebut meningkat dari tahun sebelumnya, yaitu pada tahun 2018 pengguna internet di Indonesia berjumlah 171,17 juta dengan jumlah penduduk sebanyak 264,16 juta jiwa dengan presentase peningkatan dari angka 64,8% menjadi 73.7% (Irawan, Yusufianto, Agustina, Dean, & etc., 2020). Meningkatnya data pengguna internet di Indonesia setiap tahun membuktikan bahwa masyarakat Indonesia juga tidak terlepas dari sisi positif dan negatif dari penggunaan internet itu sendiri.

Menurut Siburian (2020), "…kemajuan teknologi berbanding lurus dengan ancaman siber, baik secara teknis maupun sosial". Ini dapat dibuktikan dari serangan siber ke Indonesia yang terus mengalami peningkatan. Pada tahun 2018, BSSN bersama *Indonesian Honeynet Project* (IHP) melaporkan bahwa telah terjadi sebanyak 12,8 juta total serangan (Direktorat Deteksi Ancaman BSSN, 2018). Dilaporkan pula oleh *Indonesia Security Incident Response Team on Internet Infrastructure* (Id-SIRTII), bahwa pada tahun yang sama telah terjadi sebanyak 232,4 juta total percobaan serangan yang masuk (ID-SIRTII/CC, 2018). Pada tahun 2019, BSSN dan IHP kembali melaporkan adanya

pISSN : 2460-4208
eISSN : 2549-7685

98,2 juta serangan total di Indonesia (Direktorat Deteksi Ancaman BSSN, 2019). Sementara berdasarkan data yang disampaikan oleh Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) BSSN, tercatat sebanyak 290,3 juta total percobaan serangan yang masuk ke Indonesia (Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2019)**.** Kemudian pada tahun 2020, Pusopkamsinas BSSN telah mencatat sebanyak lebih dari 423 juta serangan siber di Indonesia periode Januari-November 2020. Total serangan ini naik drastis dari tahun-tahun sebelumnya. Hal ini merupakan bagian dari dampak yang ditimbulkan oleh pandemi Covid-19 yang tersebar di seluruh dunia, dimana banyaknya perangkat yang terhubung memicu terjadinya ancaman siber di Indonesia (Media Indonesia, 2020)**.**

Jumlah serangan siber di Indonesia berbanding lurus seiring dengan peningkatan jumlah pengguna internet di Indonesia. Naiknya angka serangan siber di Indonesia juga tidak terlepas dari bagaimana komitmen pemerintah menangani isu keamanan siber. Hal ini dapat dibuktikan dari skor *Global Cybersecurity Index* (GCI) Indonesia yang terus membaik setiap tahunnya. Seperti yang disampaikan oleh mantan ketua Badan Siber dan Sandi Negara (BSSN), Djoko Setiadi, berdasarkan data GCI yang dikeluarkan oleh *International Telecommunication Union* (ITU), pada tahun 2018, indeks GCI Indonesia naik pada peringkat 41 dari 175 negara dan berada pada peringkat 9 di kawasan Asia-Pasifik (Ristianto, 2019)**.** Kemudian pada tahun 2020, peringkat GCI Indonesia semakin membaik. Indonesia berada pada peringkat 24 dari 194 negara di seluruh dunia dan peringkat ke 6 di kawasan Asia-Pasifik dengan skor 94,88 (ITU, 2021).

Fakta bahwa ancaman siber merupakan ancaman yang melibatkan banyak pihak dan merupakan ancaman inti yang menghubungkan ancaman yang satu dengan lainnya, menjadikan perwujudan keamanan siber tidak dapat dilakukan secara sendiri, Dibutuhkan kerjasama dengan aktor lainnya. Urgensi kerjasama tersebut disampaikan oleh Menteri Luar Negeri Retno Marsudi, yang menekankan bahwa *cyber diplomacy* menjadi salah satu bagian yang penting dan mendasar untuk mengatasi tantangan, serta permasalahan yang muncul sebagai akibat dari perkembangan teknologi siber yang tidak mungkin terlepas dari masyarakat (Hakim, 2017). Urgensi kerjasama juga disampaikan oleh Kepala BSSN, bahwa "Politik luar negeri Indonesia merupakan politik bebas dan aktif. Untuk teknologi, dari manapun dan oleh siapapun, selama berguna untuk kepentingan bangsa dan negara. BSSN tidak dapat mengkoordinir semua kepentingan, tetapi apa yang baik dan terbaik untuk kita adalah kita perlu melakukan kerjasama, terutama di bidang teknologi informasi saat ini." (Indotelko.com, 2019).

Penelitian ini disusun penulis mencoba memetakan bagaimana komitmen pemerintah Indonesia dalam menjaga keamanan sibernya serta meningkatkan skor GCI-nya melalui standar penilaian 5 pilar GCI yang dicanangkan oleh ITU. Penulis juga melakukan kajian pada pilar kerjasama dari 4 pilar lainnya, yang mana kerjasama merupakan salah satu fokus utama dalam kajian Ilmu Hubungan Internasional.

- **Keamanan Siber**

Terpusatnya ruang siber dan keamanan siber yang menghubungkan domain satu dengan lainnya membuat ruang siber dan keamanan siber menjadi sangat krusial. Perkembangan teknologi komunikasi yang menghubungkan banyak orang melalui perangkat yang dimilikinya membuat eksistensi ruang siber dan keamanan siber tidak dapat dipandang sebelah mata. Salah satu cara yang dapat dilakukan untuk membuat negara beserta komposisi di dalamnya tetap aman ialah dengan melakukan kerjasama. Kepala BSSN menyatakan bahwa kerjasama merupakan salah satu pilar yang dicanangkan oleh *International Telecommunication Union* (ITU) melalui 5 (lima) pilar *Global Cybersecurity Index* (GCI). Urgensi kerjasama dalam keamanan siber sendiri mengacu pada bagaimana setiap negara memiliki intensitas ancaman yang sama dalam ruang siber serta membutuhkan kualitas dan kuantitas solusi yang sama atau yang dikenal sebagai *collective security* dan *mutual interest* guna mengembangkan prinsip keamanan yang sama, termasuk diantaranya ialah pembangunan kapasitas Sumber Daya Manusia (SDM) dan juga sumber daya teknologi bersama untuk mengurangi intensitas ancaman yang masuk. Dalam kerangka ini, penulis menggunakan teori liberalisme, dimana variabel-variabel dalam teori ini sesuai dengan kasus yang dianalisis.

pISSN : 2460-4208
eISSN : 2549-7685

Ini sesuai dengan apa yang dinyatakan oleh Immanuel Kant, bahwa institusi internasional selalu mendorong adanya rezim internasional dan keamanan kolektif yang dapat mendorong adanya perdamaian dan kerjasama. Rezim internasional merupakan seperangkat aturan, norma, dan prosedur yang mana ekspektasi dari setiap aktor terbungkus menjadi satu dalam area isu yang sama. Sedangkan konsep keamanan kolektif merujuk pada formasi dari kesamaan aliansi dari aktor utama dalam institusi internasional.

Keamanan siber, menurut Kaspersky merupakan praktik untuk melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya. Keamanan siber juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik. Ini berlaku dalam berbagai konteks, dari bisnis hingga komputasi seluler. *International Telecommunication Union* (ITU) mendefinisikan keamanan siber sebagai rangkaian alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, *best practices*, asuransi dan teknologi yang dapat digunakan untuk melindungi lingkungan siber, organisasi, dan aset pengguna.

Sebagai organisasi yang menangani isu-isu keamanan siber dunia, ITU juga mengukur komitmen negara-negara anggotanya dalam menjaga keamanan sibernya melalui 5 (lima) pilar *Global Cybersecurity Index* (GCI), yaitu: *legal measures, technical measures, organizational measures, capacity development measures,* dan *cooperation measures* (ITU, 2019). Dalam konteks regulasi, keamanan siber merupakan segala bentuk tindakan yang dilakukan oleh negara untuk melindungi segala aset penting yang ada dalam ruang siber. Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan siber secara lebih rinci mendefinisikan Keamanan Siber Nasional sebagai segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor.

Keamanan siber pada dasarnya merupakan sebuah bentuk tindakan negara untuk melindungi ruang sibernya. *National Institute of Standards and Technology* (NIST) membagi lima kerangka yang dapat digunakan untuk merinci bagaimana upaya sebuah negara dapat melindungi ruang sibernya. Kelima kerangka tersebut ialah: (1) *Identify*, merinci seluruh daftar keperluan, perangkat lunak dan data yang digunakan; (2) *Protect*, segala bentuk perlindungan terhadap perangkat yang digunakan; (3) *Detect*, langkah pendeteksian dari segala aktivitas yang ada pada perangkat; (4) *Respond*, segala bentuk respon yang ditunjukkan atas segala aktivitas yang masuk dalam perangkat; dan (5) *Recover*, segala bentuk tindakan yang dilakukan guna memulihkan aktivitas berbahaya yang dapat membahayakan perangkat maupun ruang siber.

- **Pilar Kerjasama**

Keamanan siber merupakan salah satu isu global yang tidak terpaku pada batas-batas wilayah maupun sektoral. Karena untuk mengatasi ancaman kejahatan siber yang masuk, diperlukan adanya pendekatan *multi-stakeholder* dengan *input* dari berbagai sektor dan disiplin, termasuk bilateral, multilateral dan partisipasi internasional, kerjasama sektor publik dan privat, kerjasama antar agensi dan *best practice.* Kerjasama yang baik dapat berfungsi untuk membangun kapabilitas keamanan siber yang jauh lebih kuat, membantu untuk menggertak segala ancaman dan kejahatan *online* serta membantu untuk mencapai investigasi dan presekusi yang jauh lebih baik terhadap aktor yang mencurigakan. Kerjasama merupakan pilar ke-5 dalam GCI yang komitmennya dapat diukur melalui banyaknya jumlah kerjasama kemitraan, kerangka kerjasama dan juga jaringan berbagai informasi terkait dengan keamanan siber. Bagaimana indikator dalam pilar kerjasama dalam *Global Cybersecurity Index* (GCI) itu dirumuskan, hal tersebut bisa dilihat pada Tabel 1:

pISSN : 2460-4208
eISSN : 2549-7685

Tabel 1. Indikator Pilar Kerjasama dalam GCI

Disiplin	Indikator penilaian 1	Indikator penilaian 2
Kerjasama bilateral	Apakah negaramu memiliki kesepakatan/perjanjian bilateral dengan negara lain?	Jika iya, apakah pembagian informasi merupakan bagian dari perjanjian?
		Apakah pembangunan kapasitas juga menjadi bagian dari perjanjian?
Apakah negaramu berpartisipasi dalam mekanisme internasional terkait dengan keamanan siber?		
Kerjasama multilateral	Apakah negaramu memiliki kesepakatan/perjanjian multilateral dengan negara lain?	Jika iya, apakah pembagian informasi merupakan bagian dari perjanjian?
		Apakah pembangunan kapasitas juga menjadi bagian dari perjanjian?
Kerjasama sektor publik dan privat	Apakah negaramu memiliki kesepakatan/perjanjian antara sektor publik dan privat?	Apakah negaramu memiliki kesepakatan/perjanjian antara sektor publik dan privat terkait dengan perusahaan dalam negeri?
		Apakah negaramu memiliki kesepakatan/perjanjian antara sektor publik dan privat terkait dengan perusahaan dalam negeri?
Apakah negaramu memiliki kerjasama internasional antar-agensi dari 2 badan pemerintahan yang berbeda?		

(Sumber : GCI Guidelines for Members, diolah oleh penulis)

METODE

Metode penelitian merupakan sebuah alat atau instrumen yang digunakan oleh peneliti untuk membantu dalam proses penelitian dan juga sebagai prosedur atau tata cara ilmiah yang digunakan oleh peneliti untuk memperoleh dan mengumpulkan data-data penelitian. Dalam tulisan ini, penulis menggunakan metode penelitian kualitatif, yaitu penelitian yang dapat dikonstruksi sebagai strategi penelitian yang biasanya menekankan pada kata-kata daripada kuantifikasi terhadap pengumpulan dan analisis data. Penelitian kualitatif biasanya merupakan penelitian yang menekankan pada pendekatan induktif dalam hubungannya antara teori dan penelitian, dimana teori merupakan hasil dari penelitian dari data-data yang telah dikumpulkan (Bryman, 2012, p. 36).

Penelitian kualitatif pada dasarnya ialah penelitian yang bersifat interpretif, yakni penelitian dimana penulis memiliki pandangan kritis terhadap penerapan model-model ilmiah untuk mempelajari dunia sosial yang telah banyak dipengaruhi oleh tradisi intelektual yang berbeda (Bryman, 2012, p. 28). Dalam penelitian kualitatif, fenomena-fenomena yang terjadi, baik dalam konteks alamiah maupun sosial merupakan fenomena yang dikonstruksi dan menjadi produk sosial. Itu berarti bahwa fenomena yang terjadi dan makna di dalamnya terus dilakukan oleh aktor-aktor sosial (Bryman, 2012, p. 33). Dalam penelitian ini, penulis menggunakan teknik pengumpulan data studi kepustakaan. Teknik studi kepustakaan ialah teknik pengumpulan data yang merujuk pada data-data yang relevan dengan tema penelitian, yang telah ada sebelumnya. Data tersebut dapat berupa buku, artikel jurnal, situs resmi, dan juga sumber-sumber dari internet.

pISSN : 2460-4208
eISSN : 2549-7685

PEMBAHASAN

A. Realita Keamanan Siber di Indonesia

Keamanan siber telah menjadi isu yang patut diperhitungkan, baik oleh negara maupun masyarakat. Saat ini, ruang siber telah menjadi domain yang menghubungkan satu domain dengan domain lainnya, yang mana domain siber juga menjadi domain pusat dari domain lainnya. Keamanan siber menjadi sangat krusial untuk diperhatikan sebagai tanggung jawab negara untuk melindungi kedaulatan bangsanya, serta sebagai tanggung jawab seluruh lapisan masyarakat untuk dapat lebih sadar dalam menjaga keamanan perangkat yang dimilikinya. Perkembangan informasi, komunikasi, dan teknologi yang merata ke seluruh dunia, tidak terkecuali Indonesia, berbanding lurus dengan segala ancaman yang masuk ke dalam ranah ruang siber dan kemudian bisa saja berkembang menjadi ancaman fisik. Berdasarkan informasi yang disampaikan oleh Menteri Komunikasi dan Informatika tahun 2019, Rudiantara, Indonesia menjadi target serangan nomor 2 setelah Mongolia (Umah, 2019).

Seiring berjalannya waktu, pertumbuhan jumlah penduduk di Indonesia terus mempengaruhi pertumbuhan jumlah pengguna internet di Indonesia. Ketika terjadi transisi global sebagai akibat pandemi *Coronavirus Disease* 2019 (Covid-19), situasi ini turut mempengaruhi perkembangan pengguna internet dan masuknya serangan siber di Indonesia. Semakin banyaknya jumlah perangkat yang terhubung akibat dari banyaknya aktivitas yang dilakukan secara daring, membuat banyak sektor-sektor penting menjadi target serangan siber. Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa setidaknya terdapat 10 sektor yang rentan terhadap serangan siber. Sektor tersebut di antaranya ialah sektor hukum; energi dan sumber daya mineral (SDM); transportasi; keuangan dan perbankan; kesehatan; teknologi informasi dan komunikasi; pertanian; pertahanan dan industri strategis; layanan darurat; dan sumber daya air (Koran Sindo, 2019).

Banyaknya sektor yang menjadi target serangan siber dan banyaknya jumlah serangan siber yang masuk ke Indonesia dalam rentang waktu tahun 2018-2020, memunculkan pertanyaan: bagaimana sebenarnya komitmen yang dilakukan oleh pemerintah Indonesia dalam menanggulangi isu ini? Apalagi, jika dilihat dari data yang telah disampaikan sebelumnya, bahwa komitmen keamanan siber di Indonesia cenderung membaik dari tahun ke tahun. Namun faktanya, Indonesia dapat dikatakan masih memiliki ketidakpastian hukum terkait dengan keamanan siber. Selain itu, Indonesia juga belum memiliki fasilitas pengembangan SDM siber yang maksimal. Jadi, wajar kalau kemudian ada asumsi: apa yang sebenarnya masih kurang dari negara Indonesia untuk melengkapi komitmen yang ada?

Sementara di sisi lain, Indonesia berhasil menunjukkan performanya untuk sampai pada angka 24 dari 194 negara dalam indeks *Global Cybersecurity Index* (GCI) tahun 2020. Tidak hanya itu, Indonesia juga berhasil meraih posisi ke-enam dalam lingkup negara Asia-Pasifik. Dengan posisi tersebut, Indonesia berhasil memperoleh poin-poin yang terbilang baik untuk kelima indikator pilar GCI. Perolehan skor yang didapat Indonesia adalah 94,88 yang meliputi 18,48 skor untuk *legal measures*, 19,08 untuk *technical measures*, 17,84 untuk *organizational measures*, 19,48 untuk *capacity development*, dan 20,00 untuk *cooperative measures* (ITU, 2021).

Besarnya poin pilar kerjasama yang diperoleh Indonesia tentu menjadi alasan utama mengapa Indonesia bisa sampai pada titik ini dalam mempertahankan komitmennya. Sebab, pilar kerjasama GCI juga memastikan bagaimana setiap negara mempelajari negara lain dalam mengatur kemanan sibernya. Termasuk dalam hal legalitas, penguatan kapasitas sumber daya, penguatan kapasitas teknologi, dan juga pengelolaan organisasi (*best practices*). Dengan dimaksimalkannya komitmen kerjasama, maka Indonesia juga berkesempatan untuk menyerap poin-poin penting dari keempat pilar lainnya.

B. Komitmen Keamanan Siber Indonesia Melalui Pilar Kerjasama Dalam GCI

Kerjasama merupakan salah satu pilar dalam *Global Cybersecurity Index* (GCI) untuk mengukur komitmen negara-negara anggota *International Telecommunication Union* (ITU) terhadap keamanan sibernya. Adanya kerjasama dalam merespon isu keamanan siber merupakan suatu tindakan yang terbentuk karena adanya *collective security* dari negara-negara di dunia, terutama negara anggota ITU. Kerjasama dianggap sebagai langkah yang efektif dalam menjaga ruang siber, karena dengan kerjasama negara-negara dapat dengan perlahan memenuhi indikator dari pilar-pilar lainnya.

Pilar kerjasama dalam GCI terbagi menjadi beberapa disiplin indikator, diantaranya: kerjasama bilateral, kerjasama multilateral, partisipasi internasional dengan keamanan siber dan juga kerjasama antar agensi baik secara publik maupun privat, serta kerjasama lokal maupun internasional.

1) Kerjasama Bilateral

Kerjasama bilateral merupakan kerjasama yang melibatkan negara Indonesia dengan satu negara lain atau satu instansi dengan instansi pada negara lain. Tujuan dari adanya kerjasama bilateral ialah memastikan keamanan ruang siber dari kedua negara yang bersepakat. Kerjasama yang dilakukan tentunya merupakan kerjasama yang timbal balik atas dasar kebutuhan yang sama. Adapun yang dilakukan Indonesia dalan kerjasama bilateral adalah sebagai berikut:

a. Kerjasama antara Indonesia dan Inggris Raya. Ini merupakan salah satu kerjasama yang berhasil disepakati melalui penandatanganan *Memorandum of Understanding* (MoU) oleh Kepala Badan Siber dan Sandi Negara (BSSN) Periode 2018-2019, Dr. Djoko Setiadi dan pemerintah Inggris Raya. Momentum ini terjadi pada acara pertemuan Wakil Menteri Luar Negeri Abdurrahman Mohammad Fachir dengan Menteri Muda Urusan Asia dan Pasifik Kementerian Luar Negeri Inggris Raya yaitu The Rt. Hon. Mark Field, MP pada tanggal 14 Agustus 2018 di kantor Kementerian Luar Negeri, Jakarta Pusat. Dalam pertemuan tersebut, terdapat beberapa poin yang disepakati oleh kedua negara, diantaranya: a) Implementasi dan pengembangan strategi keamanan siber nasional; b) Pengelolaan insiden siber; c) Kejahatan siber; d) Pelatihan dan kampanye kesadaran keamanan siber; e) Peningkatan kapasitas (Biro Hukum dan Humas BSSN, 2018).
b. Kerjasama terkait dengan keamanan siber yang disepakati oleh pemerintah Republik Indonesia dan Australia melalui MoU yang secara resmi ditandatangani oleh Kepala Badan Siber dan Sandi Negara (BSSN) periode 2018-2019, Djoko Setiadi, Duta Besar Negara Australia untuk isu siber serta Departemen Luar Negeri dan Perdagangan Australia, Tobias Freakin yang disaksikan oleh Presiden Republik Indonesia Joko Widodo dan Perdana Menteri Australia Scott Morrison pada tanggal 31 Agustus 2018. Tujuan utama dilakukannya kerjasama kedua negara adalah untuk memenuhi salah satu prioritas BSSN, yaitu kemitraan nasional dan internasional serta untuk mempromosikan kemitraan dan menyediakan kerangka kerjasama dalam bidang siber. Kedua negara terlibat dalam kerjasama yang saling menguntungkan dengan poin-poin sebagai berikut**:** a) Berbagi informasi dan *best practice;* b) Peningkatan kapasitas dan penguatan koneksi; c) Kerjasama dalam bidang ekonomi digital; dan d) Penanganan kejahatan siber (Biro Hukum dan Hubungan Masyarakat, 2018). Kerjasama ini berlanjut hingga pertemuan ke-3 *Dialog Kebijakan Siber Indonesia-Australia* pada tanggal 2 September 2020. Dialog dihadiri oleh beberapa petinggi negara dari kedua belah pihak dengan tujuan untuk membicarakan kerjasama siber dan kemitraan kedua negara dalam bidang keamanan siber.
c. Kesepakatan kerjasama yang ditandai dengan *Letter of Intent* di bidang keamanan siber yang dilakukan oleh BSSN dan Menteri Luar Negeri Belanda pada 3 Juli 2018 di Kementerian Luar Negeri Republik Indonesia. Kerjasama ini menghasilkan beberapa poin, diantaranya adalah: a) Saling berbagi informasi dalam bidang hukum; b) Kebijakan nasional dan strategi kebijakan manajemen yang terkait dengan ranah siber; c) Pertukaran sudut pandang, pengalaman, pembelajaran dan penerapan terbaik terkait ranah siber; d) Penguatan kapasitas dan perbantuan kelembagaan; e) Pengembangan teknologi di bidang keamanan siber melalui jaringan dan program pelatihan dan pendidikan; f) Pertukaran kunjungan kenegaraan; g) Analisis dan studi lapangan; h) Seminar dan konferensi (Biro Hukum dan Humas, 2018). Kerjasama tersebut masih berupa kerjasama *Letter of Intent* (LoI) dan belum berupa *Memorandum of Understanding* (MoU), yakni masih berbentuk surat permintaan atau kertas konsep yang berupa perjanjian yang menguraikan poin-poin utama dari kesepakatan yang telah diusulkan serta berfungsi sebagai "perjanjian untuk menyetujui" antara dua pihak. Kerjasama Indonesia dengan Belanda dalam bidang keamanan siber kemudian berlanjut dalam Pertemuan ke-1 *Dialog Keamanan Siber antara Indonesia dan Belanda* atau *The* 1st *Cybersecurity Dialogue Indonesia-Belanda* yang digelar secara daring dari Ruang NCC BSSN, Jakarta Selatan pada 21

Januari 2021. Pertemuan tersebut dihadiri oleh Kepala Badan Siber dan Sandi Negara Republik Indonesia (BSSN RI), Hinsa Siburian yang menjadi ketua Delegasi Republik RI dan juga Duta Besar Siber Belanda, Nathalie Jaarsma (Biro Informasi dan Hukum Kemenko Kemaritiman dan Tim Komunikasi Pemerintah Kemkominfo, 2021).

Bagaimana indikator kerjasama bilateral yang dilakukan oleh Indonesia mengikuti indikator penilaian dalam *GCI Guideliness,* bisa dilihat pada Tabel 2.

Tabel 2. Indikator Kerjasama Bilateral dalam GCI

Negara yang bekerjasama	**Indikator yang perlu dipenuhi**			
	Apakah negara Indonesia memiliki kesepakatan kerjasama keamanan siber bilateral dengan negara lain?	**Apakah berbagi informasi merupakan bagian dari kesepakatan ?**	**Apakah pembangunan kapasitas merupakan bagian dari kesepakatan?**	**Apakah *"mutual legal assistance"* merupakan bagian dari kesepakatan ?**
Indonesia-Inggris Raya	✓	✓	✓	✓
Indonesia-Australia	✓	✓	✓	✓
Indonesia-Belanda	✓	✓	✓	✓

(Diperoleh dari berbagai sumber, diolah oleh penulis)

2) Kerjasama Multilateral

Kerjasama multilateral, merupakan kerjasama yang melibatkan beberapa negara dengan tujuan kolektif yang sama, yakni menjaga ruang siber, menanggulangi serangan siber yang masuk dan mencegah ancaman-ancaman yang mungkin terjadi di masa mendatang. Biasanya, kerjasama multilateral juga melibatkan organisasi-organisasi internasional layaknya ASEAN.

Kerjasama multilateral Indonesia dilakukan oleh Badan Siber dan Sandi Negara (BSSN) di bawah naungan *Association of Southeast Asian Nations* (ASEAN)-JAPAN *Cyber Exercise*. Kerjasama ini merupakan salah satu bentuk implementasi kolaborasi yang dilakukan oleh kelompok negara anggota ASEAN dengan Jepang untuk sama-sama menghadapi isu dalam lingkup siber seperti penanganan insiden, *capacity building*, dan *sharing* informasi di bidang keamanan siber dari masing-masing negara yang terlibat (Chotimah, 2019). Terpilihnya Jepang dalam melakukan kerjasama, karena Jepang dinilai memiliki kualitas pengembangan SDM dan sumber daya teknologi yang baik.

Tujuan dari kegiatan ini adalah untuk meningkatkan kerjasama dan berbagi informasi di bidang keamanan siber antar negara anggota ASEAN dan Jepang, serta institusi-institusi yang terlibat dalam pelaksanaan *cyber exercise*. Sedangkan sasaran dari kegiatan ini adalah untuk meningkatkan kapabilitas dan kesiapan dalam koordinasi penanggulangan insiden keamanan siber di tingkat nasional pada setiap negara ASEAN, membangun metode komunikasi untuk berbagi informasi secara aman antara para peserta dan antarnegara ASEAN, terjalinnya kerjasama dan komunikasi yang baik antarnegara ASEAN dan Jepang dalam keamanan siber (Bagian Komunikasi Publik, 2019).

3) Partisipasi Indonesia Dalam Mekanisme Internasional Terkait Dengan Keamanan Siber.

Partisipasi Indonesia dalam mekanisme internasional merupakan salah satu indikator yang dinilai dalam *GCI Guideliness* untuk pilar kerjasama. Indikator ini merujuk pada partisipasi

pISSN : 2460-4208
eISSN : 2549-7685

Indonesia dalam forum penyusunan dan juga implementasi mekanisme internasional terkait dengan keamanan siber. Mekanisme internasional biasanya dapat berupa norma, peraturan dan prinsip yang dibentuk dalam organisasi internasional atau forum internasional sehingga menjadi mekanisme yang dapat digunakan untuk implementasi keamanan siber. Keikutsertaan Indonesia dalam mekanisme internasional terkait dengan keamanan siber bisa disebut merujuk pada teori institusionalis, yaitu institusi dimana di dalamnya berisi seperangkat norma, nilai, dan peraturan, yang diciptakan dan disepakati bersama oleh negara-negara karena adanya rasa antisipasi yang muncul terhadap pola-pola tingkah laku yang seringkali dilakukan oleh negara itu sendiri (Keohane & Martin, 1995, p. 46). Dalam hal ini, partisipasi Indonesia dalam bidang keamanan siber merupakan respon dan sikap antisipasi Indonesia sebagai negara berdaulat terhadap keamanan atas ruang sibernya, yang mungkin saja menjadi target ancaman dari negara lain.

Partisipasi Indonesia dalam mekanisme internasional terkait dengan keamanan siber juga dapat dibuktikan dari partisipasi Indonesia sebagai anggota organisasi *International Telecommunication Union* (ITU). ITU merupakan organisasi internasional pertama yang memiliki fokus terhadap pengembangan teknologi informatika dan telekomunikasi dunia. Organisasi ini, berdiri pertama kali tahun 1865 di Prancis dengan nama *International Telegraph Union* yang disepakati oleh 20 negara yang saat itu sedang melakukan konvensi dan menemukan solusi untuk membuat layanan telekomunikasi yang jauh lebih efisien (Anshary, 2016).

ITU sendiri bertujuan untuk membangun keamanan serta keamanan bagi para pengguna layanan telekomunikasi di dunia. Oleh karena itu, ITU mengeluarkan 5 pilar yang disebut sebagai *Global Cybersecurity Index* (GCI) untuk mengukur komitmen negara-negara anggota dalam menjaga keamanan sibernya. Selain itu, keberadaan ITU juga digunakan untuk menjaga perdamaian dan keamanan dunia. Indonesia sendiri tercatat sebagai anggota dalam ITU, sehingga dalam menjalankan misi keamanan sibernya Indonesia mengikuti indikator penilaian dalam pilar-pilar GCI.

Dalam Siaran Pers No. 252/HM/KOMINFO/10/2018 yang dikeluarkan pada tanggal 2 Oktober 2018, Menteri Komunikasi dan Informatika periode pertama pemerintahan Presiden Joko Widodo, Rudiantara menyampaikan bahwa pemerintah Indonesia akan mengajukan menjadi anggota Dewan *International Telecommunication Union* (ITU). Indonesia telah mengajukan proposal kepada ITU untuk menjadi dewan ITU dalam *Plenipotentiary Conference* di Dubai, Uni Emirat Arab pada 29 Oktober-16 November tahun 2018 dengan tujuan melakukan transformasi teknologi ke ITU (Setu, 2018).

Partisipasi Indonesia dalam Resolusi Majelis Umum Perserikatan Bangsa-Bangsa (PBB) juga terhitung sebagai komitmen yang ditunjukkan oleh Indonesia dalam menjaga keamanan ruang sibernya melalui mekanisme-mekanisme yang diputuskan dalam forum. Pada tahun 2018, Majelis Umum PBB mengadopsi dua resolusi yang disponsori oleh Amerika Serikat (A/RES/73/266) dan Rusia (A/RES/73/27), yang merupakan bagian dari *United Nations Open Ended Working Group* (UN OEWG), yang merupakan kelanjutan dari *United Nations Group of Governmental Experts* (UNGGE) yang telah ada sebelumnya. UNGGE *on Advancing Responsible State Behaviour in Cyberspace in The context of International Security* merupakan *working group* atas mandat PBB dalam bidang keamanan informasi yang telah dibentuk sejak tahun 2004. UNGGE beranggotakan 25 negara terpilih.

Kursi konsultasinya terletak pada 6 organisasi internasional, diantaranya adalah *African Union, European Union, Organization of American State, Organization for Security and Co-operation in Europe, ASEAN Regional Forum (ARF)* dan dua diantaranya adalah negara anggota. Tujuan utama dari UNGGE adalah untuk membentuk norma, pertukaran dan prinsip, untuk membentuk *Confidence-building Measures* (CBMs) dan *Capacity Building* serta menjelaskan bagaimana hukum Internasional diaplikasikan pada ruang siber. Indonesia pernah terpilih dan terlibat sebanyak 2 kali diantara 25 negara untuk UNGGE tahun 2013 dan 2015. Pada tahun tersebut, poin-poin yang didapatkan adalah Hukum Internasional termasuk Piagam PBB berlaku pada ruang siber, CBMs, *capacity-building* dan 11 norma yang tidak mengikat atau bersifat sukarela (DiploFoundation, n.d.).

Dalam seminar '*Peran Indonesia dalam Pembentukan Norma Keamanan Siber Dunia'* yang dilaksanakan oleh *Centre for Strategic and International Studies* (CSIS) pada 30 Januari 2020, Grata E. Werdaningtyas selaku Direktur Keamanan Internasional dan Perlucutan Senjata, Kementerian Luar Negeri RI menyebutkan bahwa terdapat 11 norma sukarela dan tidak mengikat dalam ruang siber yang berlaku untuk negara-negara di dunia, termasuk Indonesia. Norma-norma tersebut diantaranya adalah: a) Kerjasama keamanan siber antar negara; b) Mempertimbangkan semua informasi relevan saat insiden siber; c) Cegah penyalahgunaan *Information and Communication Technology* (ICT) di wilayah masing-masing; d) Kerjasama penanggulangan kejahatan siber dan terorisme; e) Penghormatan dan perlindungan HAM di ruang siber; f) Dilarang merusak infrastruktur kritis; g) Perlindungan infrastruktur kritis; h) Respon terhadap permintaan bantuan; i) Memastikan keamanan *supply chain*; j) Pelaporan kerentanan ICT; dan k) Dilarang menyerang tim tanggap darurat/CERT.

Sedangkan *United Nations Open-Ended Working Group* (UN OEWG) merupakan *working group* yang juga dibentuk oleh resolusi PBB pada tahun 2018 sebagai kelanjutan UNGGE. UN OEWG beranggotakan seluruh anggota PBB yang tertarik untuk bergabung dan memiliki tombak konsultasi dengan berbagai pertemuan dengan berbagai pemegang kekuasaan (bisnis, *Non-Govermental Organizations* (NGOs) dan akademisi). Tujuan dari UN OEWG diantaranya adalah pembentukan norma, peraturan dan prinsip yang telah terdaftar dalam resolusi A/RES/73/27 bagian 1, pembentukan CBMs dan *capacity building*, bagaimana hukum internasional diaplikasikan dalam ruang siber, keberadaan akan adanya ancaman, adanya dialog regular dalam Perserikatan Bangsa-Bangsa (PBB), serta relevansi konsep internasional untuk mengamankan sistem teknologi informasi (DiploFoundation, n.d.).

4) Partisipasi Indonesia Dalam Forum Internasional/Asosiasi

Partisipasi Indonesia dalam forum atau asosiasi internasional dalam bidang siber biasanya berupa seminar, *workshop* ataupun forum diskusi untuk membicarakan isu kemanan siber yang ada di dunia. Adanya partisipasi Indonesia dalam forum internasional dapat menjadi ladang ilmu dan informasi bagi Indonesia, karena dalam forum ini banyak negara-negara yang ahli di bidang keamanan siber sehingga dapat memotivasi Indonesia untuk terus berkembang. Partisipasi Indonesia dalam forum maupun asosiasi internasional berkaitan dengan bagaimana peran institusi untuk mengatasi konflik yang mungkin terjadi.

Kerjasama internasional dan keterlibatan dalam forum internasional maupun institusi, penting bagi negara-negara dalam membentuk *mutual trust*. Dalam hal ini, *trust* memungkinkan aktor secara kognitif mengurangi atau menghilangkan secara keseluruhan adanya risiko dan ketidakpastian yang mereka hadapi dalam proses pengambilan keputusan. Adanya *mutual trust* dianggap penting sebagai struktur ideasional intersubjektif yang memungkinkan dua atau lebih aktor untuk mengesampingkan kemungkinan-kemungkinan risiko dan ketidakpastian yang ada pada aktor lainnya dengan asumsi bahwa mereka telah memegang teguh norma yang disepakati bersama dalam forum internasional mupun institusi internasional. Oleh karena itu, layaknya isu keamanan lainnya, keamanan dalam domain siber penting untuk dibicarakan bersama sehingga masing-masing negara yang terlibat dapat membangun kepercayaan bersama untuk tidak menyerang atau mengancam domain siber satu sama lain (Keating & Ruzicka, 2014, p. 755); (Luhmann, 1979, p. 15). Adapun partisipasi yang dilakukan Indonesia dalam forum internasional/asosiasi diantaranya adalah:

- Indonesia yang diwakili oleh Badan Siber dan Sandi Negara (BSSN) juga terlibat dalam kegiatan *18th International Institute for Strategic Studies (IISS) Shangri-La Dialogue* yang berlangsung di Singapura pada tanggal 31 Mei 2019 hingga 2 Juni 2019. Selain Indonesia, terdapat 30 negara lainnya yang menjadi delegasi pada kegiatan tersebut. Salah satu tema yang menjadi isu kajian dalam forum tersebut adalah terkait dengan isu *Cyber-Capability Development : Defence Implications* (Chotimah, 2019). Pada acara ini, BSSN menjadi delegasi Indonesia bersama beberapa instansi lain yaitu Kementerian Pertahanan, Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan Republik Indonesia (Kemenko Polhukam RI), Kementerian Koordinator Bidang Maritim, Markas Besar Tentara Nasional Indonesia

(TNI), Badan Intelijen Nasional (BIN), dan Lembaga Pertahanan Nasional. Kegiatan ini dibuka oleh Perdana Menteri (PM) Singapura, Lee Hsien Loong. BSSN sebagai perwakilan Indonesia menyampaikan *opening comment* selama kurang lebih 3 menit dan BSSN menyampaikan bahwa perkembangan teknologi yang tengah memasuki revolusi industri keempat memiliki risiko.

- Kegiatan ini juga memfasilitasi pertemuan bilateral guna menghasilkan solusi terhadap isu-isu keamanan yang dihadiri oleh Menteri Pertahanan dan didampingi oleh BSSN dengan Kerajaan Inggris Raya (Bagian Komunikasi Publik, 2019). Poin yang dibahas pada kegiatan adalah perkembangan teknologi revolusi industri keempat serta sebagai fasilitator pertemuan bilateral Indonesia dengan Inggris Raya. Ini, menurut penulis, sesuai dengan prinsip liberalisme yang menyebutkan bahwa perlu adanya perkembangan teknologi dan terhubungnya komunikasi yang baik.
- Indonesia juga hadir sebagai delegasi pada pertemuan ASEAN *Political and Security Council* (APSC) ke-18 di Singapura. Menteri Koordinator Bidang Politik, Hukum dan Keamanan sebagai delegasi yang mewakili Indonesia pada saat itu menegaskan bahwa ada tiga hal utama yang dibahas, salah satunya terkait dengan *Cyber Security*. Dalam fokus pembahasan terkait hal tersebut, terdapat *sharing* pengalaman bagaimana negara-negara ASEAN menghadapi terorisme dalam wilayah siber. Indonesia bisa menerima informasi dengan baik terkait dengan keamanan siber dan mampu melakukan pembaharuan terhadap teknologi siber (Aliansyah, 2018). Poin dari kegiatan ini juga sejalan dengan kebutuhan Indonesia untuk membentuk prinsip liberalisme yang baik dalam kerjasama yang dijalaninya. Diantaranya adalah adanya *mutual sharing* yang merujuk pada perkembangan informasi terkait siber, perkembangan teknologi dan pertumbuhan komunikasi yang baik.
- Komitmen Indonesia dalam partisipasi forum internasional juga terbukti dalam Konferensi Bidang Keamanan Internasional *The 10th International Meeting of High Level Responsible for Security Matters.* Konferensi ini merupakan konferensi bidang keamanan yang bersifat tahunan yang diselenggarkan oleh Pemerintah Federasi Rusia. Konferensi ini mengundang para pejabat tinggi setingkat menteri yang menaungi bidang keamanan serta di dalamnya juga terdapat perwakilan PBB di bidang keamanan. Pada tahun 2019, konferensi ini dihadiri oleh 119 negara dengan tema tentang *point of intervention* masing-masing negara. Delegasi Indonesia terdiri dari Kementerian Koordinator Bidang Politik, Hukum dan Keamanan (Kemenkopolhukam), Badan Siber dan Sandi Negara (BSSN), serta Kementerian Luar Negeri. Pada kesempatan ini, ketua delegasi dari Kemenkopolhukam menyampaikan *point of intervention*-nya dengan judul *"Sustainable Development and Security Challenges: Indonesia's Perspective*" yang intinya adalah menyampaikan sejumlah upaya yang dilakukan Pemetintah Indonesia dalam menghadapi ancaman, seperti ancaman keamanan siber dan terorisme (Biro Hukum dan Humas, 2019).

5) Public Private Partnership

Kerjasama instansi publik dan privat merupakan salah satu indikator yang juga dinilai dalam *GCI Guideliness* untuk pilar kerjasama. Kerjasama ini mencakup kerjasama instansi internal dan juga kerjasama instansi internal dengan instansi asing yang bernaung di Indonesia. Kerjasama instansi dan juga perusahaan lokal di Indonesia tentu melibatkan instansi-instansi pemerintah yang menaungi keamanan siber di Indonesia, seperti kerjasama Kementerian Komunikasi dan Informatika dengan *Go-Jek* dan *Tokopedia* sebagai layanan yang menghubungkan banyak orang di dalamnya. Dalam rancangan strategi yang ditulis oleh BSSN, yakni Rancangan Strategi Keamanan Siber Nasional Tahun 2018-2019, disebutkan bahwa BSSN selaku instansi pemerintah yang menaungi keamanan siber perlu untuk merangkul seluruh aktor yang disebut sebagai *quadhelix multistakeholder* untuk menjaga keamanan siber Indonesia, termasuk diantaranya adalah pemerintah, sektor privat, akademisi, komunitas, dan masyarakat sipil.

Urgensi sektor privat, seperti yang disebutkan oleh Saputra, dkk (2019) ialah banyaknya Infrastruktur Informasi Kritikal Nasional (IIKN) yang menjadi tanggung jawab bagi pemerintah

dan juga sektor privat untuk berkolaborasi perihal keamanan siber, diantaranya adalah energi, transportasi, keuangan dan perbankan, Teknologi Informasi dan Komunikasi (TIK), industri pertahanan dan strategis, serta sektor kesehatan. Di masa mendatang, risiko yang muncul dari ancaman siber (serangan siber dan kejahatan siber) memiliki dampak yang besar terhadap sektor swasta. Oleh karena itu, penting bagi sektor privat untuk terlibat dalam keamanan domain siber, yang mana saat ini banyak sektor privat yang telah mengoperasikan jaringan informasi, menyediakan layanan internet, serta menyediakan produk teknologi informasi kepada aktor lainnya, dan juga banyak menyimpan data-data pribadi masyarakat (2019, p. 109).

Go-Jek merupakan aplikasi berbasis transportasi yang telah diunduh oleh banyak pengguna. Terhitung dari tahun 2015 sampai saat ini, *Go-Jek* telah diunduh sebanyak 190 juta kali dengan menghubungkan 2 juta partner *drivers*, 900.000 *GoFood Merchants* dan 2.448 kali peningkatan unduh dari 2015 ke tahun 2020. Oleh karena itu, *Go-Jek* sebagai pelaku bisnis digital bertanggungjawab atas banyak data milik pengguna yang bersifat privat dan vital. Selain itu, *Go-Jek* juga telah bertanggung jawab sebagai aplikasi berbasis teknologi yang menghubungkan banyak orang dengan berbagai macam latar belakang. *Go-Jek* juga tentu telah mempengaruhi pertumbuhan ekonomi digital dan perkembangan komunikasi global. Untuk menjaga keamanan data pengguna itulah, *Go-Jek* menggandeng Kominfo. Kerjasama keduanya dilakukan dengan fokus literasi digital bagi para pengguna dan pemantauan penggunaan aplikasi tersebut. Seperti diketahui, Kominfo merupakan instansi pemerintah yang memiliki fungsi penting dalam pemantauan informasi dalam menjaga keamanan siber.

Kerjasama Kominfo dengan *Tokopedia* juga menjadi bagian penting yang menunjukkan bahwa seluruh lapisan masyarakat, khususnya instansi pemerintah dan penyokong pertumbuhan ekonomi digital juga turut berkomitmen dalam menjaga ruang siber dan memastikan kerahasian data pengguna yang perangkatnya saling terhubung. *Tokopedia* merupakan salah satu aplikasi *e-commerce* terbesar yang berada di Indonesia yang dibentuk untuk melakukan pemerataan ekonomi digital. Dengan adanya misi ini, secara otomatis *Tokopedia* juga bertanggung jawab untuk pertumbuhan ekonomi dan komunikasi global. Dilihat dari event-event *Tokopedia* yang telah menghubungkan banyak pengguna dan mengundang antusiasme dari berbagai negara dan latar belakang, layak jika hal ini menjadikan *Tokopedia* sebagai perusahaan *e-commerce* yang besar dan berpengaruh.

Tokopedia melalui *website* resminya melaporkan bahwa telah terdapat 100 juta lebih pengguna aktif dengan 11 juta penjual dan 86,5% penjual baru. Dengan banyaknya jumlah yang disebutkan, *Tokopedia* juga berdampak pada perekonomian Indonesia yaitu memberdayakan 90% penjual beskala mikro, peningkatan jumlah penjualan yang mencapai 133% hingga adanya kemudahan pengelolaan atau pengoperasian bisnis berbasis aplikasi yang dirasakan kurang lebih 76,4% pengguna *Tokopedia* serta mendorong inklusi keuangan di Indonesia. Saat ini *Tokopedia* dan *Go-Jek* telah melakukan merger perusahaan dengan entitas baru bernama *GoTo* pada akhir Mei 2021 dengan peusahaan induk PT Aplikasi Karya Anak Bangsa (AKAB) yang sebelumnya menaungi Go-Jek. *VP of Corporation Communication Tokopedia*, Nuraini Razak mengungkapkan bahwa *GoTo* akan memanfaatkan potensi ekonomi digital Indonesia yang sangat besar dan paling menarik di Asia Tenggara (Sultan, 2021).

Banyaknya pengguna *Tokopedia* membuat *Tokopedia* juga menjadi target sasaran serangan siber dari aktor kejahatan siber. Tercatat pada tahun 2020 lalu, *Tokopedia* mengalami kejahatan siber yaitu sebanyak 91 data pengguna diperjualbelikan oleh oknum yang tidak bertanggung jawab di *dark web* dengan harga 75 juta. Namun, hal itu berhasil diatasi dengan baik oleh *Tokopedia*. Apalagi, pada tahun 2020 dan 2021, *Tokopedia* semakin melebarkan sayapnya dengan menjadikan *idol* asal Korea Selatan yang sangat ternama yaitu *Bangtan Sonyeondan* (BTS) dan *Blackpink* menjadi *brand ambassador* dari *e-commerce* tersebut untuk meningkatkan *brand reputation* dari *Tokopedia*. Tidak hanya itu, *Tokopedia* secara berkala, tiap bulannya menghadirkan *event* tanggal kembar yang juga mengundang banyak artis lokal dan idola K-Pop besar, seperti TXT, ITZY, NCT *Dream* dan *The Boyz*. Hal tersebut memungkinkan *Tokopedia* tidak hanya diakses secara minor saja, melainkan juga secara mayor yakni banyak masyarakat asing yang juga mengunduh aplikasi *Tokopedia* untuk menonton acara *Waktu Indonesia Belanja*

pISSN : 2460-4208
eISSN : 2549-7685

(WIB). Bahkan sempat tersebar juga *link illegal* dari beberapa oknum. Dengan meluasnya jangkauan pengguna, maka juga akan semakin luas ancaman siber yang dialami Tokopedia.

Untuk itu, sejak tahun 2020 lalu *Tokopedia* menggandeng BSSN dan Kominfo untuk bekerja sama dalam melakukan literasi digital terkait dan keamanan siber kepada para pengguna. Baik BSSN maupun Kominfo, menyarankan agar *Tokopedia* mengambil langkah secepat mungkin terkait dengan masalah ini. Selain itu, kedua lembaga menyarankan agar *Tokopedia* menghimbau kepada para penggunanya untuk melakukan pengecekan kata sandi secara berkala dan kedua lembaga menyarankan untuk menggunakan enkripsi kriptografi secara sistem guna mengamankan kerahasiaan data para pengguna (Luthfi, 2020).

Indikator penilaian dalam GCI juga menuntut negara-negara anggotanya dalam melakukan kerjasama dengan perusahaan-perusahaan asing yang juga berkembang di Indonesia. Salah satunya ialah kolaborasi yang dilakukan BSSN dengan Huawei selaku raksasa teknologi Tiongkok dalam menggarap kapasitas keamanan siber Republik Indonesia. Kemitraan ini berkaitan dengan peningkatan kualitas kapasitas Sumber Daya Manusia (SDM) di bidang keamanan siber, pembangunan kesadaran masyarakat terhadap keamanan siber, serta *knowledge sharing* terhadap ancaman keamanan siber saat ini. Menurut Jacky Chen selaku CEO Huawei Indonesia, kesadaran serta pemahaman masyarakat terhadap keamanan dan pendeteksian dini terhadap ancaman siber penting untuk terus ditingkatkan guna mewujudkan keamanan siber yang semakin solid. Penandatanganan nota kesepahaman tersebut menjadi bukti bahwa BSSN dan Huawei berkomitmen untuk berperan dalam membangun ruang siber yang cerdas dan aman, sekaligus sebagai upaya untuk meningkatkan kepercayaan digital (Indotelko.com, 2019).

6) Kerjasama Inter-Agensi

Kerjasama inter-agensi merupakan kerjasama yang melibatkan antar organisasi atau agensi tertentu yang berbeda dari kedua negara atau lebih. Urgensi dari kerjasama inter-agensi pada dasarnya sama dengan kerjasama yang telah disebutkan pada bagian-bagian sebelumnya. Namun, kerjasama inter-agensi terlihat lebih khusus dan intim apabila dibandingkan dengan kerjasama yang lain. Hal ini dapat terjadi karena kerjasama inter-agensi biasanya hanya merujuk pada agensi-agensi tertentu yang juga bersinggungan dengan keamanan siber.

Komitmen kerjasama inter-agensi dapat dibuktikan melalui kerjasama yang disepakati oleh Kepolisian Republik Indonesia (Polri) dengan *Korea International Cooperation Agency* dan juga Institut Teknologi Bandung (ITB) untuk mengembangkan kapasitas personel Polri dalam bidang forensik siber. Tujuan dari kerjasama ini ialah untuk mengembangkan kapasitas personel Polri supaya personel Polri dapat mengerti dan memahami secara teori dan praktek isu-isu ancaman di dunia maya. Selain itu, untuk memahami langkah yang tepat dalam mengenai rencana aksi ancaman kriminal siber (Bunga, 2019).

Kerjasama inter-agensi juga disepakati oleh pemerintah Belanda dengan Universitas Budi Luhur dari tangggal 17 hingga 21 September 2018. Pemerintah Belanda mengadakan seminar dengan Universitas Budi Luhur sebagai lembaga pendidikan di bidang layanan pendidikan terkait keamanan siber dan *bigdata* melalui Paul Van der Veer selaku kepala perusahaan konsultansi VDC, sebuah perusahaan di bidang *Educational Service* terkait *Cyber Security* dan Big Data. Kerjasama ini menghasilkan Pusat Keamanan Siber (CoE/*Center of Excellence*) yang sangat baik di negara ini. Ini untuk membangun ruang pendidikan bagi para pakar jaringan (R. Samuel, 2018).

Dari uraian di atas, bisa dinyatakan bahwa Indonesia berhasil memenuhi seluruh indikator penilaian yang disediakan oleh GCI dalam sektor kerjasama *public-private* dan juga *inter-agency*. Hal ini bisa dilihat sebagaimana diuraikan pada Tabel 3.

pISSN : 2460-4208
eISSN : 2549-7685

Tabel 3. Indikator Kerjasama *Public-Private* dalam GCI

Indikator yang dinilai		
Apakah pemerintah Indonesia berhubungan dengan *Public-Private Partnership* dengan perusahaan lokal?	**Apakah permerintah Indonesia berhubungan dengan *Public-Private Partnership* dengan perusahaan asing yang ada di Indonesia?**	**Apakah ada kerjasama atau kesepakatan *inter-agency* dari badan pemerintahan yang berbeda terkait dengan keamanan siber?**
a. Kerjasama Kominfo dengan Go-Jek b. Kerjasama antara Tokopedia, Kominfo dan BSSN	• Kerjasama Indonesia dengan perusahaan teknologi asal Tiongkok, Huawei	a. Kerjasama Kepolisian Republik Indonesia dengan *Korea International Cooperation Agency* dan Institut Teknologi Bandung b. Kerjasama Pemerintah Belanda dengan BSSN

(Dari berbagai sumber, data diolah oleh penulis)

C. Keuntungan Dan Kerugian Kerjasama yang Dilakukan Oleh Pemerintah Indonesia

Dalam studi Hubungan Internasional (HI), khususnya yang merujuk pada kerjasama internasional, keterlibatan sebuah negara dalam kerjasama internasional memiliki pertimbangan untung dan rugi atas hasil yang mungkin untuk didapatkan. Berdasarkan penjabaran pada bagian-bagian sebelumnya, penulis berupaya untuk menjabarkan apa saja keuntungan dan kerugian yang mungkin didapatkan oleh Indonesia melalui kerjasama yang terjalin terkait dengan keamanan siber.

Melalui kerjasama yang dilakukan oleh pemerintah Indonesia, keuntungan yang didapatkan oleh Indonesia adalah: (1) Informasi; (2) Peningkatan Kualitas dan Kuantitas SDM; (3) Pengetahuan terkait Hukum dan Kejahatan Siber; (4) Komitmen Indonesia dalam Keamanan Siber Terjamin; (5) Pengemabangan Teknologi; (6) Adanya Penurunan Grafik Serangan Siber dari Beberapa Negara. Melihat fakta yang ada, beberapa negara yang bekerja sama dengan Indonesia berhasil mencegah kejahatan siber dari negaranya untuk masuk ke Indonesia. Meskipun tidak sepenuhnya berhasil, tetapi terlihat adanya penurunan pada grafik serangan siber dari beberapa negara.

Dalam laporan yang disediakan oleh Badan Siber dan Sandi Negara (BSSN), pada tahun 2018, Rusia menjadi negara yang menduduki posisi pertama sumber serangan siber yang masuk ke Indonesia dengan jumlah serangan 2.597.256. Kemudian pada tahun 2019, Rusia menjadi negara dengan posisi ketujuh sumber serangan siber yang masuk ke Indonesia dengan jumlah serangan 1.589.326 dan pada tahun 2020, Rusia masih menempati posisi 7 namun dengan jumlah serangan yang lebih besar yaitu 12.413.645. Hal itu tentu bukan tanpa alasan, mengingat jumlah serangan yang masuk juga cukup besar karena adanya pandemi.

Grafik yang konsisten juga ditunjukkan oleh Australia. Selama dua tahun berturut-turut (2018-2019), Australia tidak tergabung dalam 10 besar negara yang menjadi sumber serangan siber ke Indonesia. Hanya saja, pada tahun 2020 negara tersebut masuk sebagai urutan ke-enam dengan jumlah serangan 14.743.994. Oleh karena itu, kedua negara (Indonesia-Australia) kembali membahas kerjasama mereka dalam bidang siber ini.

Sementara itu, karena Indonesia masih terbilang baru dalam meningkatkan keamanan sibernya, maka ada beberapa kekurangan yang mungkin didapat, diantaranya adalah:

(1) Tidak semua kelebihan yang didapat berhasil dilaksanakan dengan baik oleh Indonesia. Seperti diketahui, bahwa masih banyak masyarakat Indonesia yang belum sadar akan pentingnya teknologi atau masih banyak juga distribusi teknologi yang kurang memadai. Oleh karena itu, banyak hal yang belum bisa diselesaikan secara maksimal. Masih banyak masyarakat Indonesia yang memiliki ketertarikan minim terhadap seminar atau *campaign* bertemakan keamanan siber. Sehingga sulit untuk merealisasikan kesepakatan yang telah dibuat. Selain itu, untuk meningkatkan kualitas SDM di Indonesia perlu adanya sumber daya

teknologi dan pendidikan yang memadai. Namun, beberapa ahli IT menjadi tidak terkendali arahnya karena tidak memiliki teknologi yang memadai dan pendidikan yang layak;

(2) Ketergantungan.
Selagi Indonesia masih belum bisa menopang sebagian besar keamanan sibernya dengan baik, maka kemungkinan terburuknya ialah ketergantungan. Apalagi negara-negara *partner* kerjasama Indonesia dikenal sebagai negara yang maju, baik dari segi keamanan siber, politik, ekonomi dan juga militer. Apabila Indonesia tidak dapat menyeimbangi dengan baik maka Indonesia akan ketergantungan dengan kerjasama tersebut sehingga sulit unuk mengembangkan keamanan sibernya sendiri.

SIMPULAN

Ruang siber atau domain siber merupakan bentuk domain baru yang saat ini menjadi sama pentingnya dengan domain lainnya, yakni darat, laut, udara, dan juga ruang angkasa. Urgensi ruang siber dalam studi hubungan internasional terletak pada bagaimana ruang siber juga menjadi hal yang vital bagi keamanan dan kedaulatan sebuah negara. Saat ini, setelah munculnya revolusi digital dan perkembangan teknologi, ruang siber menjadi domain yang menghubungkan satu domain dengan domain lainnya dengan koneksi jaringan internet dalam dunia maya. Berkaitan dengan hal itu, setiap negara pada akhirnya berkeinginan untuk menjaga ruang sibernya dengan sebaik mungkin sehingga mengurangi atau bahkan meretas seluruh kemungkinan ancaman yang masuk ke dalam ruang siber.

Indonesia sebagai salah satu negara yang berdaulat telah sejak lama berkomitmen dalam organisasi telekomunikasi internasional atau ITU untuk menjaga keamanan ruang sibernya. Dengan berlandaskan 5 (lima) pilar *Global Cybersecurity Index* (GCI), Indonesia terus berupaya untuk menjaga konsistensinya dalam hal keamanan siber. Hingga saat ini, Indonesia berhasil memperoleh poin maksimal (20.00) dari salah satu pilar GCI, yakni pilar kerjasama. Kerjasama dalam pilar GCI pada dasarnya merujuk pada kolaborasi antar aktor, baik secara internal maupun eksternal untuk terus berkontribusi dalam menjaga ruang siber.

Kerjasama, yang seringkali dibicarakan dalam studi hubungan internasional, biasanya terjadi untuk membentuk kepercayaan bersama dan mereduksi berbagai ketidakpastian yang ada dalam menjalin hubungan. Kerjasama juga berfungsi untuk mengukur bagaimana tindakan yang mungkin dilakukan oleh aktor lain terhadap diri sendiri. Berkaitan dengan keamanan siber, kerjasama penting dilakukan untuk membentuk kepercayaan bersama dalam menjaga ruang siber satu sama lain, sehingga ancaman siber bisa terus direduksi. Namun, berdasarkan hasil yang penulis temui, dari poin-poin indikator yang ada masih banyak poin yang nampaknya belum secara jelas dijabarkan pada urgensi kerjasama yang dilakukan. Selain itu, masih banyak negara-negara yang belum berkomitmen dengan baik untuk mereduksi ancamannya terhadap negara lain.

DAFTAR PUSTAKA

Aliansyah, M. A. (2018). *RI Dorong Penguatan Keamanan Siber & Kerjasama Intelijen Antisipasi Terorisme.* Jakarta: merdeka.com.

Anshary, A. D. (2016). Peran International Telecommunication Union Dalam Mengatasi Cyber Crime di Indonesia Tahun 2011-2013. *Journal of International Relations*, 91-103.

Bagian Komunikasi Publik. (2019, Juni 20). *ASEAN-JAPAN Online Cyber Exercise.* Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/asean-japan-online-cyber-exercise/

Bagian Komunikasi Publik. (2019, Juni 2019). *BSSN sebagai Pembicara dalam Forum Strategis Keamanan Global Asia-Pasifik (Shangri-La Dialogue).* Retrieved from Badan Siber dan Sandi Negara : https://bssn.go.id/bssn-sebagai-pembicara-dalam-forum-strategis-keamanan-global-asia-pasifik-shangri-la-dialogue/

Biro Hukum dan Humas BSSN. (2018, Agustus 14). *BSSN Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber Dengan Pemerintah Inggris Raya*. Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/

Biro Hukum dan Hubungan Masyarakat. (2018, Agustus 31). *PRESS RELEASE INDONESIA DAN AUSTRALIA SEPAKAT JALIN KERJASAMA DI BIDANG SIBER*. Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/press-release-indonesia-dan-australia-sepakat-jalin-kerjasama-di-bidang-siber/

Biro Hukum dan Humas. (2018, Juli 3). *PENANDATANGAN LETTER OF INTENT KERJASAMA BIDANG KEAMANAN SIBER KEPALA BSSN DENGAN MENLU BELANDA*. Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/penandatangan-letter-of-intent-kerjasama-bidang-keamanan-siber-kepala-bssn-dengan-menlu-belanda/

Biro Hukum dan Humas. (2019, July 5). *Peran Indonesia dalam Konferensi Bidang Keamanan Internasional*. Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/peran-indonesia-dalam-konferensi-bidang-keamanan-internasional/

Biro Informasi dan Hukum Kemenko Kemaritiman dan Tim Komunikasi Pemerintah Kemkominfo. (2021, Januari 21). *Tingkatkan Kerjasama Bilateral, BSSN Gelar The 1st Cybersecurity Dialogue Indonesia-Belanda*. Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/tingkatkan-kerjasama-bilateral-bssn-gelar-the-1st-cybersecurity-dialogue-indonesia-belanda/

Bryman, A. (2012). *Social Research Method.* Great Clarendon Street, Oxford: Oxford University Press.

(2019). *BSSN gaet Huawei untuk tingkatkan kemampuan di bidang keamanan siber*. Jakarta: indotelko.com.

Bunga, H. (2019). *Penanganan Kejahatan Siber, Polri Kerjasama dengan ITB dan Korea.* Jakarta: Tempo.co.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica*, 113-128.

DiploFoundation. (n.d.). *UN GGE and OEWG*. Retrieved from Geneva Internet Platform DigWatch: https://dig.watch/processes/un-gge

Direktorat Deteksi Ancaman BSSN. (2018). Laporan Tahunan 2018 Honeynet Project BSSN-IHP. *ISSN 2655-8467*, 1-50.

Direktorat Deteksi Ancaman BSSN. (2019). Laporan Tahunan 2019 Honeynet Project BSSN-IHP. *ISSN 2655-8467*, 1-56.

Hakim, L. (2017). *Kemenlu : diplomasi siber mutlak diperlukan.* Yogyakarta: AntaraYogya.

ID-SIRTII/CC. (2018). *Indonesia Cyber Security Monitoring Report 2019.* Jakarta: ID-SIRTII/CC.

Irawan, A. W., Yusufianto, A., Agustina, D., Dean, R., & etc. (2020). *Laporan Survei Internet APJII 2019-2020 (Q2).* Jakarta: Indonesia Survey Center.

ITU. (2019). *Global Cybersecurity Index (GCI) 2018.* ITU Publications.

ITU. (2021). *Global Cybersecurity Index 2020.* ITUPublications.

Keating, V. C., & Ruzicka, J. (2014). Trusting relationship in international politics: No need to hedge. *Review of International Studies*, 753-770.

Keohane, R. O., & Martin, L. L. (1995). The Promise of Institutionalist Theory. *International Security*, 39-51.

Koran Sindo. (2019, Maret 27). *BSSN Beberkan 10 Sektor yang Rentan Serangan Siber*. Retrieved from SINDONEWS.com: https://tekno.sindonews.com/berita/1390355/122/bssn-beberkan-10-sektor-yang-rentan-serangan-siber

Luhmann, N. (1979). *Trust and Power.* New York: John Wiley & Sons.

Luthfi, A. (2020). *Investigasi, Tokopedia Kerjasama dengan Kominfo dan BSSN.* Jakarta: okezone.com.

Media Indonesia. (2020, Desember 16). *Terjadi Peningkatan Jumlah Serangan Siber pada Tahun 2020*. Retrieved from mediaindonesia.com: https://mediaindonesia.com/politik-dan-hukum/369457/terjadi-peningkatan-jumlah-serangan-siber-pada-tahun-2020

Nursaid, F. A. (2022, Maret 8). *Waspada Serangan Siber, Ini Pesan BSSN Kepada Masyarakat*. Retrieved from Komite.Id: https://www.komite.id/2022/03/08/waspada-serangan-siber-ini-pesan-bssn-kepada-masyarakat/

Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara. (2019). *Indonesia Cyber Security Monitoring Report 2019.* Badan SIber dan Sandi Negara.

R. Samuel. (2018). *Kerjasama Indonesia Belanda Bangun Centre of Excellence Cyber Security & Big Data dengan Universitas Budi Luhur.* Jakarta: komite.id.

Ristianto, C. (2019, 05 24). *BSSN Raih Peringkat ke-41 dalam Global Cyber Security Index*. Retrieved from Kompas.com: https://nasional.kompas.com/read/2019/05/24/16374011/bssn-raih-peringkat-ke-41-dalam-global-cyber-security-index

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International and Security Studies (CEJISS)*, 104-120.

Setu, F. (2018, 10 02). *Ajukan Jadi Anggota Dewan ITU, Indonesia Siap Lakukan Transformasi Teknologi*. Retrieved from KOMINFO: https://kominfo.go.id/content/detail/14805/siaran-pers-no-252hmkominfo102018-tentang-ajukan-jadi-anggota-dewan-itu-indonesia-siap-lakukan-transformasi-teknologi/0/siaran_pers

Siburian, H. (2020, 12 22). Strategi Keamanan Siber dan Pertumbuhan Ekonomi Digital. (C. Mae, Interviewer)

Sultan, R. (2021). *Gojek dan Tokopedia merger menjadi GoTo, ini kata idEA.* Jakarta: Kontan.co.id.

Umah, A. (2019, October 01). *Rudiantara: RI Masuk 2 Besar Negara Target Serangan Siber*. Retrieved from CNBC Indonesia: https://www.cnbcindonesia.com/tech/20191001160328-37-103579/rudiantara-ri-masuk-2-besar-negara-target-serangan-siber