Padjadjaran Journal of International Relations (PADJIR)
e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

Diplomasi Siber Indonesia dalam Penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* 2019

Allisa Salsabilla Waskita
Program Studi Hubungan Internasional Universitas Padjadjaran; allisa18001@mail.unpad.ac.id
Hasan Sidik
Program Studi Hubungan Internasional Universitas Padjadjaran; hasan.sidik@unpad.ac.id

Submit: 12-08-2022 | Accept: 06-08-2023 | Publish: 31-08-2023

Keywords
Cyber Diplomacy, Cybersecurity, Cybersecurity Capacity Building.

ABSTRACT
The development of Information and Communication Technology has created new security issues in cyber space with the emergence of various cyber threats and attacks. This article aims to explain cyber diplomacy practices carried out in related workshops and how cyber diplomacy can be optimized. The author uses the concepts of cyber security and cyber diplomacy in conducting the analysis. The author uses a case study qualitative method with data collection instruments in the form of interviews, document-based studies, and internet-based studies. As a result, this study found that cyber diplomacy instruments can be optimized in four areas: human resources, legislation, institutions, and technology. This can be seen from the positive response to the diplomacy carried out by Indonesia towards the International Telecommunication Union (ITU) in the holding of the workshop. Based on this, Indonesia can optimize its cyber diplomacy efforts in the bilateral arena with international and state cyber security organizations; as well as the multilateral arena in the UN and ASEAN forums.

Kata Kunci
Diplomasi Siber, Keamanan Siber, Pengembangan Kapasitas Keamanan Siber.

ABSTRAK
Perkembangan Teknologi Informasi dan Komunikasi telah menimbulkan isu keamanan baru di ruang siber dengan munculnya berbagai ancaman dan serangan siber. Artikel ini bertujuan menjelaskan praktik diplomasi siber yang dilakukan pada penyelenggaraan *workshop* terkait dan bagaimana diplomasi siber bisa dioptimalkan. Penulis menggunakan konsep keamanan siber dan diplomasi siber dalam melakukan analisis. Penulis menggunakan metode kualitatif studi kasus dengan instrumen pengumpulan data berupa wawancara, studi berbasis dokumen, dan studi berbasis internet. Hasilnya, penelitian ini menemukan bahwa instrumen diplomasi siber dapat dioptimalkan di empat area: sumber daya manusia, legislasi, kelembagaan, dan teknologi. Hal ini terlihat dari respon positif atas diplomasi yang dilakukan Indonesia terhadap *International Telecommunication Union* (ITU) di dalam penyelenggaraan *workshop*. Berdasarkan hal tersebut, Indonesia dapat mengoptimalkan upaya diplomasi siber pada arena bilateral kepada organisasi keamanan siber internasional dan negara; serta arena multilateral di forum PBB dan ASEAN.

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

PENDAHULUAN

Perkembangan Teknologi Informasi dan Komunikasi (TIK) yang semakin pesat telah menghadirkan dimensi baru dalam kehidupan manusia, yaitu ruang siber atau umum disebut dengan ruang maya. Perkembangan ini sejatinya telah memberi dampak yang signifikan dalam kehidupan manusia melalui akses informasi yang tak terbatas. Namun, pada perkembangannya, TIK juga dapat digunakan untuk tujuan kejahatan yang menjadi ancaman besar terhadap individu, organisasi, dan masyarakat (Liang & Xue, 2009, hal. 71). Ancaman semacam ini dikenal dengan istilah *cyber threat* (ancaman siber) yang berpotensi menimbulkan *cyber-attack* (serangan siber).

Minimnya regulasi yang mengatur mengenai praktik di ruang siber menyebabkan ancaman serangan siber semakin merajalela. Oleh karena itu, perkembangan TIK yang semakin canggih telah menimbulkan isu keamanan baru di ruang siber, tak terkecuali terhadap negara. Adapun ancaman siber yang dihadapi negara antara lain *cyber-terrorism* yang menargetkan infrastruktur vital negara (Solms & Niekerk, 2013, hal. 4), hingga kemungkinan timbulnya *cyber-war* yang dilakukan pihak tertentu untuk mencapai tujuan politik dalam melawan negara, masyarakat negara, atau ekonomi negara (Sheldon, 2019, hal. 294).

Dengan adanya isu keamanan tersebut, Indonesia, sama seperti negara lainnya, juga memperhitungkan keamanan siber sebagai bagian dari kepentingan nasional yang harus dilindungi. Keamanan siber di Indonesia dikelola oleh sebuah instansi pemerintah non-kementerian bernama Badan Siber dan Sandi Negara (BSSN) yang bertanggungjawab kepada Presiden Republik Indonesia secara langsung. Adapun kepentingan Indonesia di ruang siber meliputi kedaulatan, ketahanan, dan perlindungan siber (BSSN, 2020, hal. 5). Dalam memelihara kepentingan tersebut, tentunya Indonesia membutuhkan sebuah instrumen yang mampu meningkatkan kerja sama dengan negara lain guna mewujudkan keamanan siber.

Diplomasi siber menjadi salah satu instrumen yang dikedepankan oleh Indonesia dalam memenuhi kebutuhan tersebut. Pada 2019, Indonesia melakukan sebuah upaya diplomasi siber melalui penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* di Jakarta bersama *International Telecommunication Union* (ITU) dan beberapa negara di kawasan Asia Pasifik. Adapun agenda yang dibawa dalam penyelenggaraan *workshop* ini adalah pengembangan strategi keamanan siber nasional serta perlindungan data pribadi, mengingat dua hal ini masih menjadi kekurangan bagi keamanan siber Indonesia. Oleh karenanya, Indonesia berharap *workshop* ini dapat meningkatkan pemahaman dan memberikan panduan untuk membangun kerangka kerja strategi keamanan siber nasional serta mendorong adopsi peraturan data pribadi yang lebih luas (Biro Hukum dan Hubungan Masyarakat BSSN, 2019).

Capacity Building on National Cybersecurity Strategy Workshop diselenggarakan sejalan dengan tujuan diplomasi siber Indonesia, yaitu untuk meningkatkan kapasitas dalam hal keamanan siber, khususnya yang berkaitan dengan strategi keamanan siber nasional dan regulasi perlindungan data pribadi. Akan tetapi, jika melihat realita yang ada, Indonesia justru masih menghadapi berbagai tantangan dan permasalahan dalam kedua hal tersebut.

Penelitian yang dilakukan oleh Wisnu Handi Prabowo, Satriya Wibawa, dan Fuad Azmi (2020) menemukan bahwa kasus kebocoran data masih sering terjadi di Indonesia (Prabowo, Wibawa, & Azmi, 2020, hal. 236). Kemudian, laporan BSSN pada 2020 juga menyebut bahwa Indonesia masih menghadapi tantangan keamanan siber dari berbagai serangan siber yang masuk, yaitu serangan *trojan activity* dan *information gathering* (pengumpulan informasi) (Biro Hukum dan Kerjasama BSSN, 2020).

Kondisi tersebut menunjukkan bahwa Indonesia masih belum mencapai tujuan keamanan siber meski upaya diplomasi siber untuk meningkatkan kapasitas terus dilakukan. Oleh karena itu, penelitian ini dilakukan guna mengetahui bagaimana diplomasi siber dapat membantu pengembangan kapasitas

keamanan siber Indonesia berdasarkan studi kasus penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019;* serta mengetahui upaya-upaya diplomasi siber lain yang dapat dioptimalkan di masa depan.

Dalam melakukan penelitian ini, peneliti telah melakukan kajian terhadap studi terdahulu terkait topik atau permasalahan yang sama. *Pertama*, Iskandar Hamonangan dan Zainab Assegaff (2020) menemukan bahwa diplomasi siber menjadi penting untuk mengurangi gesekan, mencegah perang siber terbuka, dan mewujudkan ruang siber yang damai (Hamonangan & Assegaff, 2020). *Kedua*, Hidayat Chusnul Chotimah (2019) menemukan bahwa melalui berbagai kerjasama bilateral maupun multilateral yang telah terjalin, BSSN melakukan diplomasi siber guna menjaga keamanan dan kedaulatan siber Indonesia (Chotimah, Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara, 2019). *Ketiga*, Henike Primawanti dan Sidik Pangestu (2020) menemukan bahwa Indonesia melakukan diplomasi siber melalui *ASEAN Regional Forum* dengan membawa empat agenda: diadakannya kontak poin, dibentuknya *study group* untuk merumuskan kurikulum peningkatan *capacity building*, transisi penggunaan *Internet Protocol version 4* ke *Internet Protocol version 6*, dan pembentukan lembaga khusus siber di masing-masing negara anggota ASEAN (Primawanti & Pangestu, 2020).

Berdasarkan kajian mengenai studi terdahulu tersebut, terdapat keterkaitan dengan penelitian ini, yaitu mengenai upaya Indonesia dalam mencapai keamanan siber melalui diplomasi siber. Penelitian-penelitian sebelumnya lebih banyak membahas mengenai praktik diplomasi siber Indonesia dalam hal aktor dan agenda pembentukan norma. Sementara itu, penelitian ini akan lebih fokus kepada agenda pengembangan kapasitas yang dibawa di dalam praktik diplomasi siber Indonesia, khususnya pada penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*, yaitu kapasitas sumber daya manusia, legislasi, dan kelembagaan.

Dengan demikian, penelitian ini diharapkan dapat memberikan referensi bagi penelitian selanjutnya terkait praktik diplomasi siber Indonesia; memberikan rekomendasi kepada pemangku kebijakan di bidang keamanan siber; dan memberikan sumbangan terhadap perkembangan Studi Hubungan Internasional, khususnya di dalam bidang keamanan kontemporer dan diplomasi siber.

KERANGKA KONSEPTUAL

Keamanan Siber

Konsep mengenai keamanan siber terbilang sebagai konsep baru yang memiliki beragam definisi. Namun, definisi paling umum yang banyak dirujuk adalah definisi keamanan siber yang diungkapkan oleh *International Telecommunication Union* (ITU). Menurut ITU, keamanan siber dimaknai sebagai sekumpulan alat, kebijakan, konsep keamanan, panduan, tindakan, pelatihan, praktik, jaminan, dan teknologi yang dapat digunakan untuk melindungi aset pengguna serta organisasi dan lingkungan siber (ITU-T, 2008, hal. 2). Adapun aset pengguna dan organisasi yang dimaksud mencakup perangkat komputer yang terkoneksi, personil, infrastruktur, aplikasi, jasa, sistem telekomunikasi, dan keseluruhan informasi yang ditransmisikan maupun disimpan di ruang siber.

Keamanan siber sendiri berupaya untuk menjamin pencapaian dan pemeliharaan properti keamanan aset pengguna dan organisasi dari risiko keamanan di lingkungan siber. Adapun tujuan keamanan umum dari keamanan siber mencakup (ITU-T, 2008, hal. 2; Veale & Brown, 2020, hal. 6):

- ketersediaan (*availability*), yang berarti bahwa sistem tidak dijadikan *offline* sehingga tidak dapat digunakan atau tidak berfungsi;
- integritas (*integrity*), yang berarti bahwa sistem tidak diganggu keakuratan, konsistensi, dan kepercayaan informasinya; dan
- kerahasiaan (*confidentiality*), yang berarti bahwa data tidak terekspos kepada aktor yang tidak memiliki wewenang atas data tersebut.

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

Dalam Studi Hubungan Internasional, konsep keamanan siber mulai mendapat banyak perhatian seiring meningkatnya aktivitas sehari-hari, bisnis, hingga pemerintahan yang mulai dijalankan secara *online* sehingga menimbulkan kekhawatiran akan isu keamanan di ruang siber. Terlebih lagi, jumlah serangan siber terus meningkat seiring berjalannya waktu. Hanna Kassab (2014) menyebut perlawanan negara terhadap serangan siber sebagai "perang siber". Hal ini didasarkan pada fakta bahwa serangan-serangan siber merupakan upaya destruktif yang dilakukan untuk menghancurkan sebuah negara dari dalam. Beberapa serangan atau ancaman terhadap keamanan siber yang ditimbulkan dari situasi tersebut di antaranya adalah pencurian data, *bugs* dan *back doors*, kebocoran informasi, *botnet*, serangan otentifikasi, kegagalan protocol, dan serangan eksponensial (Kassab, 2014, hal. 64; Cheswick, Bellovin, & Rubin, 2003, hal. 95-118).

Diplomasi Siber

Konsep diplomasi siber (*cyber-diplomacy*) merupakan konsep baru yang dikembangkan dari konsep diplomasi umum seiring berkembangnya ruang siber sebagai lokus dan fokus baru di dalam hubungan internasional. Hal ini salah satunya ditandai dengan adanya perubahan pada ruang siber yang semula hanya menjadi isu teknis di bidang TIK saja, kini mulai menjadi perhatian aktor-aktor negara dengan masuknya kepentingan politik, norma, dan nilai di ruang tersebut. Selain itu, kemunculan serangan siber, aktivitas peretasan, dan gangguan berbasis jaringan lainnya juga menjadi faktor pendorong munculnya konsep diplomasi siber di dalam praktik hubungan antar negara.

Pada perkembanganya, konsep ini berkembang dengan mengadopsi beberapa istilah yang berbeda. Diplomasi siber dan diplomasi digital menjadi dua istilah yang paling banyak digunakan secara bergantian. Barrinha dan Renard (2017) menyatakan bahwa diplomasi siber lebih merujuk pada aktivitas diplomasi yang membawa agenda kepentingan di ruang siber, seperti keamanan siber suatu negara. Sementara itu, diplomasi digital lebih merujuk pada aktivitas penggunaan teknologi digital dan media sosial oleh diplomat atau menteri luar negeri untuk mendukung aktivitas diplomatik (Barrinha & Renard, 2017, hal. 355-356). Dalam hal ini, penelitian ini fokus pada konsep diplomasi siber tentang bagaimana suatu negara membawa isu keamanan siber di dalam agenda diplomasinya.

Berbicara lebih jauh mengenai diplomasi siber, terdapat beberapa karakteristik yang dimiliki oleh diplomasi siber. *Pertama*, berkaitan dengan aktor, seorang diplomat dapat menjalankan agenda diplomasi siber dengan berbagai aktor, baik aktor negara maupun non-negara, seperti perusahaan internet, perusahaan teknologi, atau organisasi masyarakat. *Kedua*, berkaitan dengan arena, diplomasi siber juga dapat dilakukan melalui berbagai forum internasional, baik yang sifatnya bilateral maupun multilateral (Barrinha & Renard, 2017, hal. 355).

Kemudian, seiring dengan meningkatnya kesadaran akan regulasi dan tata kelola di ruang siber, agenda-agenda diplomasi siber pun mulai banyak dijumpai di berbagai forum internasional. Tiirmaa-Klaar (2013) mengungkapkan adanya lima area kunci dari diplomasi siber yang menjadi landasan dari berbagai agenda diplomasi siber internasional, yaitu (Tiirmaa-Klaar, 2013, hal. 529):

- hak asasi manusia (*human rights*);
- keamanan internasional (*international security*);
- tata kelola internet (*internet governance*);
- kejahatan siber (*cybercrime*); dan
- pengembangan kapasitas (*capacity building*).

Di antara agenda-agenda diplomasi siber yang dikemukakan oleh Tiirmaa-Klaar, peneliti memfokuskan analisis pada agenda pengembangan kapasitas untuk melakukan analisis yang lebih mendalam dan relevan dengan studi kasus yang diteliti. Selain itu, pengembangan kapasitas juga menjadi salah satu area prioritas diplomasi siber internasional guna mencapai ruang siber global yang reliabel. Hal ini salah satunya dinyatakan dalam *Seoul Conference on Cyberspace 2013* bahwa

pengembangkan kapasitas menjadi salah satu cara untuk menyamakan kedudukan di antara negara-negara terkait kesenjangan, kebutuhan, dan kepentingan dalam hal keamanan siber (Kavanagh, 2013, hal. 1). Munculnya prioritas agenda ini juga didasarkan pada fakta bahwa tidak semua negara memiliki kapabilitas yang sama untuk menangani ancaman siber.

Tiirmaa-Klaar menjelaskan lebih jauh bahwa terdapat beberapa isu kunci yang perlu diperhatikan oleh pembuat kebijakan terkait pengembangan kapasitas (Tiirmaa-Klaar, 2013, hal. 523). *Pertama*, pengembangan kapasitas keamanan siber nasional harus dibarengi dengan upaya membangun koneksi dan jaringan komunikasi di seluruh dunia. *Kedua*, negara mengembangkan model dimana lembaga penegak hukum terhubung dengan CERT, penyedia layanan internet, dan jaringan kemitraan publik-swasta untuk melakukan manajemen insiden. *Ketiga*, negara harus memiliki kerangka hukum yang tepat untuk memfasilitasi penyelidikan dan penuntutan terhadap pelanggaran di ruang siber secara tepat waktu.

METODE RISET

Penelitian ini menggunakan metode kualitatif dengan menggunakan studi kasus guna mencapai tujuan penelitian untuk menganalisis dan memahami suatu kasus secara mendalam, dan menarik kesimpulan general yang dapat digunakan pada kasus lainnya. Pemilihan varian penelitian ini dianggap tepat karena peneliti dapat fokus pada objek penelitian, yaitu diplomasi siber, dan mengkaji hubungan antara teori dengan realita yang ada.

Adapun data yang digunakan di dalam penelitian ini didapatkan dengan menggunakan teknik wawancara kepada diplomat Indonesia; studi berbasis dokumen terhadap laporan-laporan resmi lembaga pemerintah dan organisasi internasional; serta studi berbasis internet terhadap jurnal, buku, dan artikel media yang relevan dengan penelitian ini. Data tersebut kemudian dianalisis dengan tahapan berikut (Yin, Qualitative Research from Start to Finish, 2016, hal. 185-187): (1) pengumpulan data, (2) pembongkaran data, (3) penataan ulang data, (4) interpretasi data, dan (5) penarikan kesimpulan. Data yang dihasilkan kemudian divalidasi dengan metode triangulasi.

HASIL DAN PEMBAHASAN

Kapasitas Keamanan Siber Indonesia

Kapasitas keamanan siber Indonesia masih memiliki kekurangan dan kebutuhan yang besar. Khusus berbicara mengenai periode 2018-2019 sebelum *Capacity Building on National Cybersecurity Strategy Workshop* 2019 dilaksanakan, kapasitas keamanan siber Indonesia tergolong rendah. Menurut Laporan Penilaian Keamanan Internet tahun 2018 sesuai dengan *Id-SIRTII Index*, tingkat keamanan internet di Indonesia memiliki nilai indeks yang buruk dengan skor 25 dari skor maksimal 60 (Id-SIRTII/CC, 2018, hal. 39).

Sementara itu, menurut *Global Cybersecurity Index* (GCI) yang dikeluarkan oleh ITU pada 2018, indeks keamanan siber Indonesia menempati peringkat 41 dari 195 di dunia dengan skor 0,776 dari skor maksimal 1,000. Nilai ini didapat dengan mengukur lima buah indikator, yaitu legal, teknikal, organisasional, pengembangan kapasitas, dan kerja sama (ITU, 2018, hal. 63). Meski begitu, laporan GCI pada 2018 tersebut tidak merinci nilai untuk masing-masing indikator, sehingga tidak terlihat aspek mana yang menjadi kelebihan dan masih menjadi kekurangan dari keamanan siber Indonesia.

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

Gambar 1. Hasil GCI tahun 2018

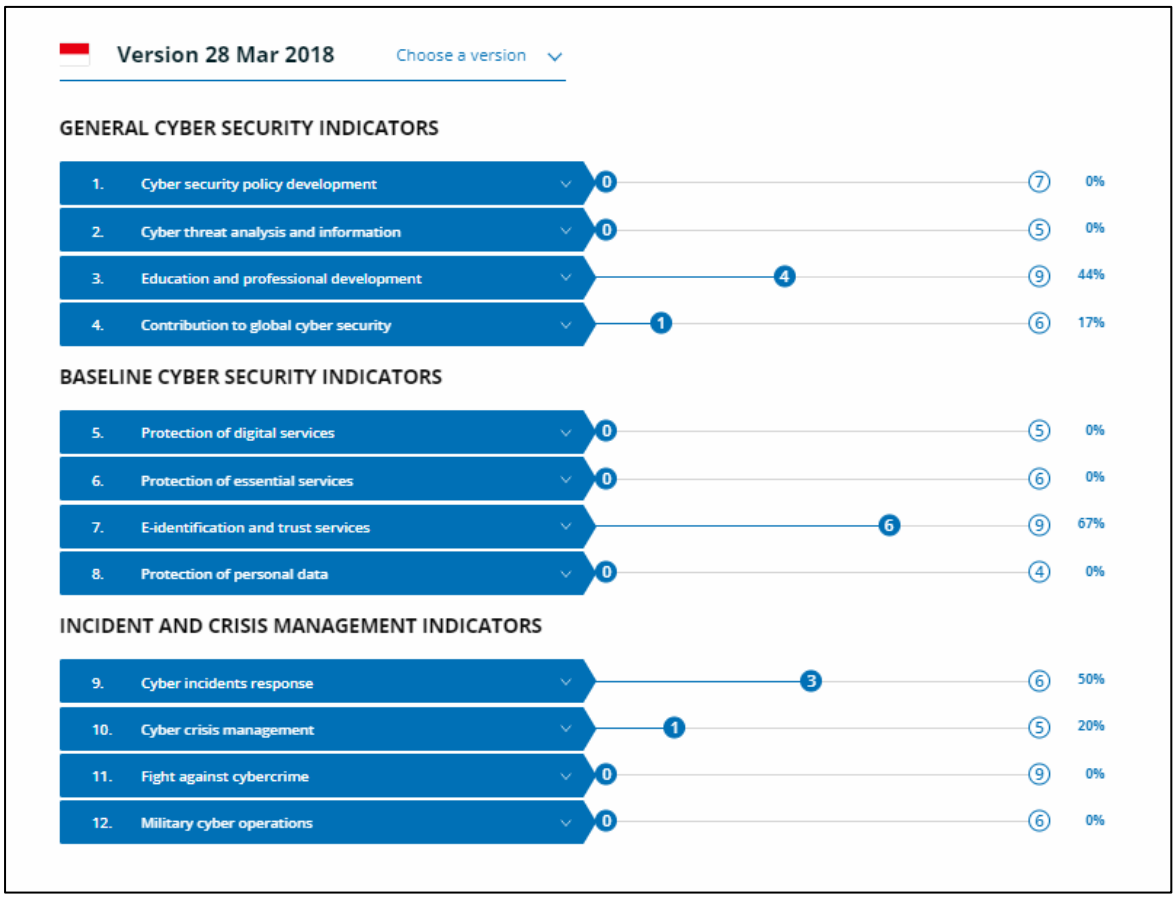
Asia-Pacific region

Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10
Japan	0.880	4	14
Republic of Korea	0.873	5	15
China	0.828	6	27
Thailand	0.796	7	35
New Zealand*	0.789	8	36
Indonesia	0.776	9	41
India	0.719	10	47
Viet Nam	0.693	11	50
Philippines	0.643	12	58
Iran	0.641	13	60

Sumber: ITU, 2018, hal. 58

Selain GCI, terdapat indeks keamanan siber lain yang dapat digunakan untuk mengukur kapasitas keamanan siber Indonesia, yaitu *National Cyber Security Index* (NCIS) yang dikeluarkan oleh organisasi non-profit e-Governance Academy. Menurut laporan NCIS tahun 2018, Indonesia memiliki skor nol untuk indikator pengembangan kebijakan keamanan siber; analisis dan informasi ancaman siber; perlindungan layanan digital; perlindungan layanan esensial; perlindungan data pribadi; perlawanan terhadap kejahatan siber; dan operasi siber militer. Sementara itu, skor tertinggi ada pada indikator layanan identifikasi elektronik dan kepercayaan; serta respon terhadap insiden siber (E-Government Academy, 2018).

Gambar 2. Nilai indikator keamanan siber Indonesia menurut NCIS tahun 2018



Sumber: E-Government Academy, 2018

Dalam dokumen Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019, dinyatakan pula bahwa keamanan siber Indonesia menghadapi banyak tantangan, seperti belum meratanya infrstruktur TIK di Indonesia, regulasi-regulasi yang masih perlu disesuaikan, dan industri teknologi informasi yang masih bergantung pada produk impor. Selain itu, dalam hal sumber daya manusia, Indonesia juga masih membutuhkan profesional di bidang *coding*, *programming*, dan keamanan siber yang mampu mendukung ekonomi digital serta melindungi lingkungan siber Indonesia (BSSN, 2018, hal. 13-14).

Kebutuhan dan tantangan tersebut juga dikonfirmasi oleh Diplomat Harditya (2022) dalam wawancara bersama peneliti. Harditya menyebut bahwa, hingga saat ini, masih terdapat banyak kebutuhan untuk meningkatkan kapasitas keamanan siber Indonesia. Yang *pertama* tentunya adalah kapasitas sumber daya manusia, yaitu e*xpert* di bidang keamanan siber yang menguasai sisi teknis maupun kebijakan. Hal ini juga didukung oleh dokumen Rencana Strategis BSSN Tahun 2018-2019 yang menyatakan bahwa peningkatan jumlah sumber daya manusia di bidang siber dan sandi menjadi salah satu program utama BSSN (BSSN, 2018, hal. 66).

Yang *kedua* adalah kapasitas kelembagaan yang belum memiliki sistem koordinasi yang baik meski BSSN telah dibentuk sebagai koordinator keamanan siber nasional. Menurut Harditya (2022), koordinasi lembaga yang berkaitan dengan keamanan siber masih menjadi tantangan tersendiri. Tantangan yang dimaksud adalah bagaimana para pemangku kepentingan di bidang keamanan siber mengsinkronkan tujuan keamanan siber nasioal, peta jalan kerja sama, dan prioritas keamanan siber yang ingin dicapai (Harditya, 2022). Hal ini juga terbukti salah satunya melalui penelitian yang dilakukan oleh Lebo dan Anwar (2020) bahwa masing-masing pihak yang terlibat di dalam perwujudan keamanan siber Indonesia hanya melakukan pemantauan terhadap infrastruktur informasi kritis masing-

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

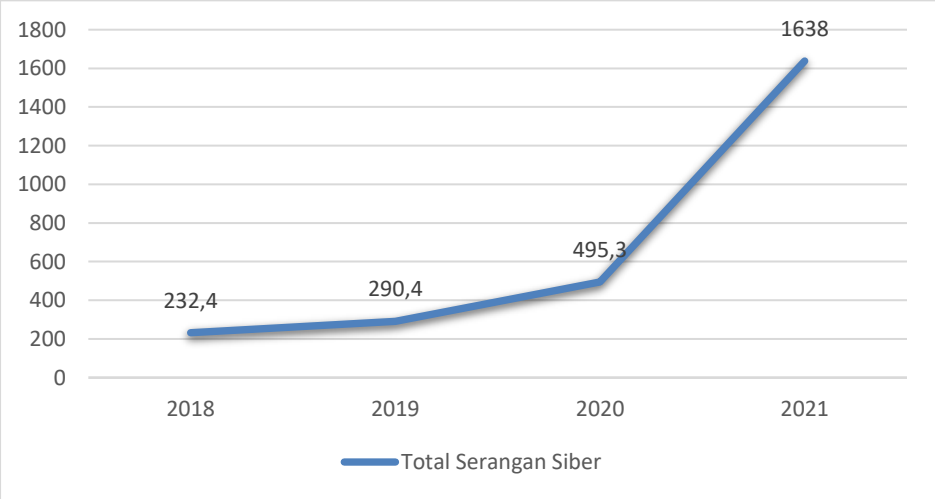
masing tanpa adanya kerja sama dan kolaborasi antar pihak mengenai pelaporan dan pengamatan yang terintegrasi (Lebo & Anwar, 2020, hal. 116).

Yang *ketiga* adalah pengembangan regulasi keamanan siber, karena saat ini, keamanan siber Indonesia masih mengandalkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) saja. Padahal, untuk melindungi keamanan di ruang siber yang kompleks, Indonesia membutuhkan payung hukum yang lebih komprehensif. Beberapa di antaranya adalah strategi keamanan siber yang perlu diperbarui (Harditya, 2022); dan RUU Keamanan dan Ketahanan Siber serta RUU Perlindungan Data Pribadi yang masih belum disahkan untuk menjadi panduan pelaksanaan keamanan di ruang siber (Kominfo, 2019, hal. 24).

Yang *keempat* adalah kapasitas teknologi, di mana saat ini Indonesia masih mengimpor teknologi, terutama *hardware*, yang mendukung perlindungan keamanan siber dan belum menjadi produsen. Beberapa perusahaan asing yang saat ini bekerja sama untuk pengadaan teknologi keamanan siber di Indonesia adalah Huawei, Simons, dan Motorola (Harditya, 2022). Hal ini tentunya menimbulkan risiko dari adanya keterlibatan pihak asing di dalam perwujudan keamanan siber. Salah satunya terlihat di dalam penelitian yang dilakukan oleh Krisna Narindra (2021) bahwa terdapat ancaman dari penyedia teknologi swasta asing yang membawa *bug* (kode atau program khusus) untuk tujuan kepentingan nasional negara asal mereka sendiri (Narindra, 2021, hal. 44). Oleh karenanya, Indonesia juga memiliki tujuan untuk memenuhi kapasitas teknologi dalam hal keamanan siber.

Dengan adanya kekurangan pada kapasitas keamanan siber Indonesia, serangan-serangan siber dapat terus masuk dan menganggu keamanan ruang siber Indonesia. Hal ini terlihat dari meningkatnya serangan siber dan/atau anomali trafik secara signifikan setiap tahunnya. Data terkait dapat dilihat melalui grafik yang diolah peneliti berdasarkan data serangan dan/atau anomali trafik berikut.

Tabel 1. Data serangan dan/atau anomali trafik (dalam juta)



Sumber: Diolah oleh peneliti dari laporan hasil monitoring BSSN tahun 2018-2021

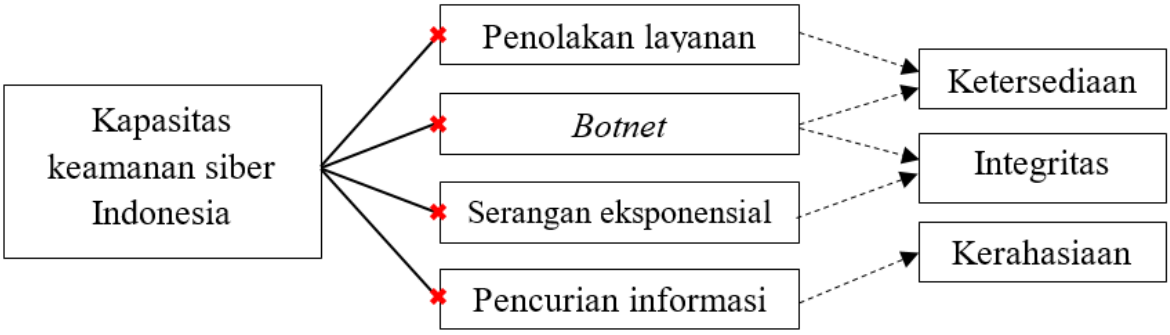
Ancaman terbesar yang masih dihadapi oleh ruang siber Indonesia adalah serangan *malware*, *trojan*, *phising*, kebocoran dan pencurian data, DDoS, *botnet*, serta penyebaran konten negatif seperti informasi palsu dan pencemaran nama baik. Serangan-serangan ini kemudian peneliti kelompokkan berdasarkan jenis serangan siber yang dikemukakan oleh Cheswick, Bellovin, dan Rubin (2003).

Pertama adalah *botnet*, yaitu serangan yang ditujukan untuk menyusupi dan mengendalikan perangkat, serta mencuri informasi tanpa sepengatahuan pengguna. Dalam hal ini yang termasuk ke dalam serangan *botnet* adalah *malware* dan *trojan*. *Kedua* adalah pencurian informasi yang dilakukan melalui pencurian data secara langsung maupun upaya pembocoran data. *Ketiga* adalah serangan eksponensial yang dilakukan dengan menyebarkan virus kepada perangkat pengguna. Dalam hal ini,

serangan *phishing* yang dihadapi oleh Indonesia termasuk ke dalam salah satu upaya serangan ekskponensial karena serangan tersebut mengakibatkan masuknya program atau file berbahaya (virus) ke dalam perangkat pengguna. *Keempat* adalah serangan penolakan layanan (DoS dan DDoS) yang ditujukan untuk mematikan atau menurunkan fungsi sistem tertentu.

Tingginya ancaman siber yang dihadapi dan adanya kebutuhan untuk mengembangkan kapasitas menimbulkan celah di dalam keamanan siber Indonesia. Menurut ITU, keamanan siber idealnya harus memenuhi prinsip ketersediaan, integritas, dan kerahasiaan. Akan tetapi, serangan-serangan siber yang masih dialami oleh Indonesia menunjukkan bahwa keamanan siber Indonesia belum memenuhi prinsip-prinsip tersebut. Celah keamanan siber Indonesia untuk mencapai kondisi yang ideal dapat dilihat dalam ilustrasi bagan berikut.

Bagan 1. Celah keamanan siber Indonesia



Pada prinsip **ketersediaan**, keamanan siber seharusnya dapat menjamin sistem yang ada selalu aktif (*online)* sehingga dapat digunakan atau berfungsi. Dengan adanya serangan berupa penolakan layanan dan *botnet*, akses terhadap sistem yang dimaksud menjadi terhambat. Penolakan layanan (DoS atau DDoS) merupakan serangan siber yang dapat mematikan atau menurunkan fungsi sistem. Sementara itu, *botnet* merupakan serangan yang dapat memungkinkan peretas mengendalikan perangkat tanpa sepengetahuan pengguna. Dengan adanya dua serangan ini, pengguna menjadi kehilangan akses terhadap sistem sehingga sistem tidak dapat digunakan atau berfungsi. Oleh karenanya, ketika masih terdapat serangan berupa penolakan layanan dan *botnet* di ruang siber, keamanan siber Indonesia belum sepenuhnya memenuhi prinsip ketersediaan.

Kemudian, pada prinsip **integritas**, keamanan siber seharusnya dapat menjamin bahwa sistem tidak diganggu keakuratan, konsistensi, dan kepercayaan informasinya. Hal ini berarti bahwa sistem akan tetap memberikan akses dan informasi yang sama di manapun pengguna masuk ke ruang siber. Akan tetapi, dengan adanya jenis serangan berupa *botnet* dan serangan eksponensial, sebuah perangkat dapat disusupi oleh virus atau program tertentu yang dapat menggangu sistem TIK di perangkat pengguna. Selain itu, kedua jenis serangan juga memungkinkan adanya aktivitas spionase oleh para peretas untuk mencuri informasi sensitif, seperti kata sandi, identitas, dsb. Hal ini tentu dapat mengurangi keakuratan dan konsistensi pada sebuah sistem, terutama ketika serangan yang dilakukan dapat mengambil alih dan mengubah data di dalam sebuah perangkat tanpa sepengetahuan pengguna. Dengan masih dihadapinya serangan berupa *botnet* dan serangan eksponensial, keamanan siber Indonesia masih memiliki celah untuk dapat memenuhi prinsip integritas.

Terakhir, berkaitan dengan prinsip **kerahasiaan**, prinsip ini merupakan prinsip penting untuk melindungi privasi pengguna di ruang siber yang tidak mengenal batas geografis, waktu, maupun nilai. Prinsip ini mendorong keamanan siber untuk dapat menjamin bahwa data yang ada di ruang siber tidak terekspos kepada aktor yang tidak memiliki wewenang atas data tersebut. Pada realitanya, serangan berupa pencurian informasi masih sering terjadi di Indonesia hingga melibatkan puluhan juta data pengguna bocor dan diperjualbelikan oleh pihak ketiga yang tidak memiliki wewenang. Hal ini tentunya

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

bertentangan dengan prinsip kerahasiaan pada keamanan siber yang seharusnya dapat melindungi data pengguna. Oleh karenanya, prinsip kerahasiaan juga masih belum terpenuhi didalam perwujudan keamanan siber Indonesia.

Berdasarkan celah-celah yang terdapat pada keamanan siber Indonesia untuk memenuhi prinsip-prinsip keamanan siber, muncul kebutuhan yang besar untuk terus mengembangkan kapasitas Indonesia. Secara menyeluruh, kebutuhan akan strategi keamanan siber nasional menjadi poin utama mengingat pentingnya hal tersebut sebagai acuan keamanan siber bagi para pemangku kepentingan di Indonesia. Selain itu, terdapat pula kebutuhan untuk menyusun legislasi perlindungan data pribadi guna melindungi ratusan juta warga negara Indonesia yang aktif menggunakan internet. Terlebih lagi, serangan pencurian dan pembocoran data terus terjadi dan menimbulkan ancaman tersendiri.

Dengan adanya kebutuhan tersebut, pada 2019, Indonesia berupaya menyelenggarakan *workshop* dengan topik pengembangan strategi keamanan siber nasional dan perlindungan data pribadi guna memberikan pelatihan dan edukasi agar Indonesia dapat mengembangkan strategi yang diperlukan. Hal ini juga dikonfirmasi oleh Harditya (2022) bahwa pada 2019, Indonesia memang tengah menyusun dokumen strategi keamanan siber nasional dan terdapat urgensi untuk mendorong perlindungan warga negara Indonesia di ruang siber. Oleh karenanya, pelaksanaan *workshop* akan sangat bermanfaat untuk mendatangkan *expert* di bidang strategi keamanan siber dan perlindungan data pribadi sehingga dapat membantu Indonesia mengembangkan dan menyusun strategi yang diperlukan. Sebagai hasilnya, Indonesia diharapkan dapat memiliki peta jalan keamanan siber yang lebih terukur dan terarah untuk dapat mewujudkan keamanan siber yang memenuhi prinsip ketersediaan, integritas, dan kerahasiaan

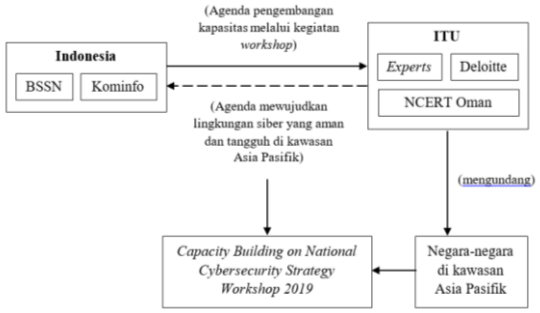
Pelaksanaan Diplomasi Siber Indonesia di dalam Penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* 2019

Dengan adanya kebutuhan untuk mengembangkan kapasitas keamanan siber Indonesia seperti yang telah disampaikan pada bagian sebelumnya, Indonesia memerlukan sebuah referensi dan panduan untuk membangun serta meningkatkan kerangka kerja dalam hal strategi keamanan siber nasional dan perlindungan data pribadi. Oleh karenanya, diselenggarakanlah *Capacity Building on National Cybersecurity Strategy Workshop* 2019 dengan mengundang ITU untuk dapat mendatangkan *expert* yang mampu memberikan pelatihan dan edukasi pada topik terkait. Penyelenggaraan *workshop* ini juga menjadi salah satu contoh bagaimana diplomasi siber dapat membantu Indonesia mewujudkan keamanan siber melalui pengembangan kapasitas pada aspek sumber daya manusia, legislasi, dan kelembagaan.

Harditya (2022) menyatakan bahwa dalam menjalin kerja sama bersama ITU untuk menyelenggarakan sebuah pelatihan, terdapat dua mekanisme yang dapat dilakukan. *Pertama* adalah memberikan undangan kepada ITU untuk melakukan *workshop* atau pelatihan yang diperlukan bersama dengan *expert* yang dimiliki oleh ITU. Jika isu atau topik yang diajukan sesuai dengan agenda ITU, ITU akan menerima undangan tersebut. Lalu, mekanisme yang *kedua* adalah menerima undangan dari ITU atas inisiasi program-program ITU untuk menyelenggarakan pengembangan kapasitas di negara tertentu. Bagi Indonesia, jika agenda program yang dibawa sesuai dengan kebutuhan nasional, maka Indonesia akan menerima undangan tersebut (Harditya, 2022).

Dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* 2019, Indonesia menggunakan mekanisme yang pertama. Indonesia melalui BSSN dan Kemenkominfo mengundang ITU untuk berkolaborasi menyelenggarakan sebuah *workshop* pengembangan kapasitas yang disesuaikan dengan kebutuhan Indonesia akan strategi keamanan siber nasional dan perlindungan data pribadi. Pada tahap inilah praktik diplomasi siber Indonesia dilakukan terhadap ITU guna mewujudkan kepentingan nasional. Proses diplomasi yang dimaksud dapat dilihat melalui ilustrasi bagan berikut.

Bagan 2. Proses diplomasi Indonesia kepada ITU dalam penyelenggaraan *workshop*



Diplomasi merupakan sarana komunikasi yang memungkinkan negara untuk mengamankan kepentingan nasional tanpa menggunakan kekuatan. Hal yang sama dilakukan oleh Indonesia melalui undangan yang disampaikan kepada ITU untuk dapat memenuhi kebutuhan pengembangan kapasitas keamanan siber Indonesia, yaitu kebutuhan atas edukasi dan pelatihan dari para *experts*.

Selain itu, praktik ini juga mencerminkan fungsi utama diplomasi, yaitu negosiasi. Dalam hal ini, baik Indonesia (melalui BSSN dan Kemenkominfo) maupun ITU telah bernegosiasi mengenai topik dan agenda yang akan dibawa dan berhasil mencapai kesepakatan untuk menyelenggarakan *workshop* bersama. Di satu sisi, Indonesia memiliki kebutuhan dan agenda diplomasi siber yang telah ditetapkan untuk mengembangkan kapasitas keamanan siber nasional. Di sisi lain, ITU juga memiliki agenda untuk mengembangkan keamanan siber di kawasan Asia Pasifik, yaitu *ITU Regional Initiative for Asia-Pacific Region* periode 2018-2021. Oleh karenanya, ITU menyetujui undangan Indonesia karena penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* 2019 sejalan dengan *framework* kelima pada program inisiasi tersebut, yaitu berkontribusi untuk mewujudkan lingkungan (siber) yang aman dan tangguh di kawasan Asia-Pasifik (ITU, t.thn.). Hal ini juga dikonfirmasi oleh Harditya (2022) bahwa *workshop* dapat diselenggarakan ketika terdapat kesekapatan mengenai agenda yang dibawa antara Indonesia dan ITU.

Praktik diplomasi siber yang dilakukan dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop* 2019 juga sejalan dengan agenda diplomasi siber yang dikemukakan oleh Tiirmaa-Klaar (2013), yaitu agenda *capacity building* atau pengembangan kapasitas. Agenda ini ditujukan untuk meningkatkan kapabilitas teknis, kesiapsiagaan, dan kerangka legal guna menangani ancaman siber. Hal ini sejalan dengan apa yang sudah menjadi agenda diplomasi siber yang disampaikan oleh Harditya (2022) bahwa Indonesia sangat membutuhkan pengembangan kapasitas, khususnya kapasitas sumber daya manusia, kelembagaan, legislasi, dan teknologi atau infrastruktur. Oleh karenanya, penyelenggaraan *workshop* ini merupakan salah satu perwujudan dari agenda tersebut.

Dari hasil diplomasi siber yang dilakukan, Indonesia berhasil menjalin kolaborasi dengan ITU untuk menyelenggarakan *workshop* berbasis internasional dengan topik pengembangan strategi keamanan siber nasional dan perlindungan data pribadi. *Workshop* yang bertajuk "*Capacity Building on National Cybersecurity Strategy Workshop"* diselenggarakan di Jakarta, Indonesia, pada 26-28 Agustus 2019. Adapun keuntungan yang didapat oleh Indonesia dari penyelenggaraan *workshop* ini adalah edukasi dan pelatihan dari para *expert* yang tergabung dengan organisasi ITU kepada para pemangku kebijakan keamanan siber di Indonesia, baik dari pemerintahan maupun swasta.

Pada penyelenggaraannya, *Capacity Building on National Cybersecurity Strategy Workshop* 2019 sendiri dimulai dengan menyebarkan undangan kepada para partisipan dari berbagai negara. Adapun partisipan yang ditargetkan adalah kementerian, pembuat kebijakan, orang-orang yang bekerja dalam sistem hukum, badan regulator, badan keamanan nasional, divisi militer yang menangani manajemen TIK, badan penegak hukum, penyedia infrastruktur kritis, bank umum dan bank sentral, *telco* dan penyedia jasa layanan internet, serta akademisi. Selain itu, *workshop* ini juga tidak menutup

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

kemungkinan adanya partisipan yang berasal dari badan riset nasional serta industri lokal yang bergerak dalam bidang inisiatif keamanan (ITU, t.thn.).

Pada pelaksanaanya, *Capacity Building on National Cybersecurity Strategy Workshop* 2019 diikuti oleh 35 peserta yang berasal dari berbagai negara dan institusi nasional di Indonesia dengan agenda selama tiga hari yang mencakup pelatihan pengembangan strategi keamanan siber nasional secara komprehensif. Adapun topik-topik yang dipelajari dalam *workshop* ini adalah prinsip umum, siklus (*lifecycle*), tata kelola, implementasi, monitoring dan evaluasi, serta *good practices* di dalam pengembangan strategi keamanan siber nasional. Hal ini bertujuan untuk memberikan pemahaman mendalam serta panduan yang diperlukan bagi para peserta.

Selain itu, masing-masing topik juga disampaikan langsung oleh narasumber yang merupakan *expert* dalam hal keamanan siber dari ITU. Kelima *expert* yang menjadi narasumber dalam *workshop* ini adalah Ismail Shah (Kepala Kantor ITU Jakarta), Marco Obiso (Kepala Divisi Keamanan Siber ITU), Lorenzo Russo dan Orhan Osmani (Programmer ITU), dan Nadher Alsafwani (perwakilan *Oman National Computer Emergency Readiness Team*).

Aktor-Aktor Diplomasi yang Terlibat di dalam Penyelenggaraan *Workshop*

Diplomasi siber dapat melibatkan berbagai aktor, baik aktor negara seperti diplomat dan institusi pemerintah, maupun non-negara seperti perusahaan internet dan perusahaan teknologi. Di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*, pihak yang menjadi aktor utama adalah BSSN dan Kemenkominfo yang berperan sebagai inisiator penyelenggaraan *workshop* tersebut. Hal ini berkaitan dengan agenda *workshop* itu sendiri yang merupakan bagian teknis dari keamanan siber Indonesia, sehingga diplomasi dapat dilakukan oleh institusi pemerintah seperti BSSN dan Kemenkominfo yang langsung menanganinya terhadap ITU.

Di samping itu, praktik diplomasi siber ini tentunya tidak lepas dari koordinasi dengan Kemenlu. Sesuai dengan UU no. 37 tahun 1999 tentang hubungan luar negeri pada pasal 28 (2), Kemenlu memegang peran diplomasi Indonesia sehingga koordinasi di dalam penyelenggaraan hubungan luar negeri dilakukan melalui Kemenlu. Hal yang sama juga berlaku untuk praktik diplomasi siber. Dalam hal ini, Kemenlu berperan untuk memastikan bahwa seluruh upaya yang dilakukan sejalan dengan agenda diplomasi siber Indonesia.

Dalam praktik diplomasi siber di dalam penyelenggaraan *workshop* ini, masing-masing BSSN dan Kemenkominfo memegang elemen keamanan siber yang berbeda. Strategi keamanan siber nasional menjadi ruang lingkup BSSN, sementara perlindungan data pribadi menjadi ruang lingkup Kemenkominfo

Kemudian, selain BSSN, Kemenkominfo, dan Kemenlu yang menjadi aktor diplomasi di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*, ada pula aktor-aktor lain yang terlibat yang merupakan sasaran dari diplomasi siber yang dilakukan. Yang *pertama* tentunya adalah ITU sebagai organisasi internasional yang menyediakan sumber daya yang diperlukan oleh Indonesia untuk memenuhi agenda pengembangan kapasitas keamanan siber. Sumber daya yang dimaksud adalah lima orang *expert* di bidang keamanan siber yang melakukan transfer pengetahuan kepada para peserta *workshop* yang berasal dari para ahli di ITU, lembaga keamanan siber Oman, dan perusahaan teknologi global Deloitte.

Yang *kedua* adalah perwakilan beberapa negara di Asia Pasifik yang turut berpartisipasi di dalam *Capacity Building on National Cybersecurity Strategy Workshop 2019*. Negara-negara tersebut adalah Papua Nugini, Malaysia, dan Brunei Darussalam. Partisipasi ini didasarkan pada kebutuhan yang sama akan pengembangan kapasitas sumber daya manusia, legislasi, dan kelembagaan, khususnya yang berkaitan dengan strategi keamanan siber nasional. Hal ini juga dikonfirmasi oleh Harditya (2022)

bahwa memang banyak negara yang belum memiliki kebijakan, aturan, atau strategi nasional keamanan sibernya sendiri.

Selanjutnya, ada pula berbagai lembaga non-pemerintah yang turut dilibatkan di dalam penyelenggaraan *workshop* ini. Lembaga-lembaga tersebut meliputi perusahaan yang bergerak di sektor-sektor kritis, yaitu perbankan, energi, dan informatika; serta komunitas yang berkaitan dengan tekonologi siber. Keterlibatan ini tidak telepas dari perhatian negara bahwa aktor-aktor non-negara seperti ini merupakan pemilik teknologi itu sendiri yang mengimplementasikan keamanan siber secara langsung, sehingga kolaborasi yang kuat perlu dibangun. Hal ini dilakukan terutama karena *Capacity Building on National Cybersecurity Strategy Workshop 2019* ditujukan untuk memberikan pengetahuan dan panduan dasar yang diperlukan dalam implementasi dua elemen penting keamanan siber, yaitu strategi keamanan siber dan perlindungan data pribadi

Dampak Penyelenggaraan *Workshop* terhadap Keamanan Siber Indonesia

Tujuan dari diselenggarakannya *Capacity Building on National Cybersecurity Strategy Workshop 2019* adalah untuk mengembangkan kapasitas keamanan siber dalam hal strategi keamanan siber nasional dan perlindungan data pribadi dengan memberikan panduan yang kredibel dan membangun kerangka kerja yang diperlukan. Ketercapaian tujuan tersebut melalui diplomasi siber yang dilakukan terhadap ITU dapat dilihat dari disusunnya Strategi Keamanan Siber Nasional oleh BSSN pada 2020 dan dirumuskannya RUU Perlindungan Data Pribadi pada 2019.

Berkaitan dengan startegi keamanan siber nasional, dalam Simposium Strategi Keamanan Siber Nasional, Kepala BSSN Hinsa Siburian mengemukakan bahwa penyusunan Strategi Keamanan Siber Nasional telah melalui proses diskusi dengan banyak pihak dan berhasil menentukan lima komponen utama strategi keamanan siber. Kelima komponen ini ditujukan untuk menciptakan lingkungan siber yang strategis guna mempertahankan dan mewujudkan kepentingan nasional Indonesia di ruang siber. Kelima komponen yang dimaksud adalah visi, misi, landasan pelaksanaan, peran dari tiap-tiap pemangku kepentingan, serta fokus area kerja (Siburian, Simposium Strategi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2020).

Visi dari Strategi Keamanan Siber Nasional Indonesia yang telah ditetapkan adalah "Terwujudnya keamanan dan ketahanan ruang siber nasional guna mendukung Indonesia yang berdaulat, mandiri, dan berkepribadian berdasarkan gotong royong". Adapun **misi** yang ditetapkan guna mewujudkan visi tersebut terdiri dari empat poin, yaitu melindungi sistem pemerintah, infrastruktur informasi kritis, warga negara Indonesia, dan ekosistem ekonomi digital; membina kekuatan dan kemampuan keamanan siber; serta memajukan kepentingan nasional Indonesia di ruang Siber (Siburian, Simposium Strategi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2020).

Penetapan visi dan misi Strategi Keamanan Siber Nasional ini tentunya tidak dilakukan tanpa pondasi yang kuat. **Landasan pelaksanaan** Strategi Keamanan Siber Nasional didasarkan pada tiga poin utama, yaitu (1) sistem hukum nasional, (2) totalitas sumber daya keamanan siber nasional, dan (3) sinergi antar lembaga pemerintah dan kemitraan di antara para pemangku kepentingan. Khusus berbicara mengenai poin ketiga, BSSN menggunakan pendekatan yang disebut *quad helix*, yaitu kolaborasi **peran di antara pemangku kepentingan** yang fokus pada empat kategori, yaitu pemerintah, akademisi, bisnis atau pelaku usaha, serta masyarakat dan komunitas (Siburian, Simposium Strategi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2020).

Terakhir, setelah ditetapkannya visi, misi, landasan pelaksanaan, serta peran bagi masing-masing pemangku kepentingan, BSSN memusatkan upaya perwujudan keamanan siber pada tujuh **fokus area kerja** yang harus diimplementasikan. Ketujuh area tersebut adalah tata kelola; manajemen risiko dalam keamanan siber nasional; kesiapsiagaan dan ketahanan; infrstruktur informasi kritis nasional; pembangunan kapabilitas dan kapasitas keamanan siber; legislasi dan regulasi; serta kerja sama internasional. Meski demikian di dalam simposium strategi keamanan siber yang dilakukan, BSSN

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

tidak menyebutkan secara rinci bagaimana masing-masing fokus area ini akan diimplementasikan oleh masing-masing pemangku kepentingan yang terlibat.

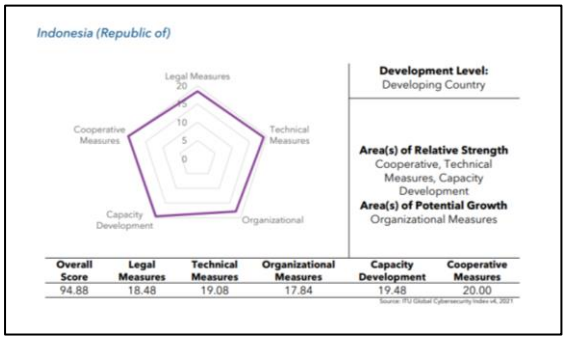
Dalam kegiatan yang berbeda, Hinsa Siburian mengemukakan bahwa Strategi Keamanan Siber Nasional yang telah disusun melalui proses simposium dan koordinasi dengan kementerian terkait ini akan lebih optimal apabila bisa menjadi suatu produk hukum baru berupa peraturan presiden. Dengan adanya peraturan presiden, Indonesia dapat menggunakan sarana dan sumber daya siber yang ada secara maksimal untuk mengamankan ruang siber dan melindungi kepentingan nasional di ruang siber (Siburian, BSSN Menyusun Strategi Keamanan Siber Nasional, 2020).

Kemudian, berkaitan dengan perlindungan data pribadi, Menteri Komunikasi dan Informatika Johnny Plate mengemukakan bahwa penyusunan RUU Perlindungan Data Pribadi akan menjadi landasan hukum yang komprehensif dalam melindungi warga negara Indonesia di manapun mereka berada, termasuk di ruang siber. Upaya perlindungan ini didasarkan pada lima prinsip, yaitu pengumpulan data pribadi secara terbatas dan spesifik; pemrosesan data pribadi sesuai tujuan; pemrosesan data pribadi dengan mempertimbangkan perlindungan keamanan data; melakukan pemberitahuan ketika terjadi masalah keamanan; dan hak penghapusan data pribadi (Plate, 2020).

Selain prinsip-prinsip tersebut, RUU Perlindungan Data Pribadi juga memuat hak pemilik data serta kewajiban pengendali atau pengelola dalam memproses data pengguna di ruang siber. Elemen inilah yang menjadi penting guna mengamankan warga negara Indonesia yang beraktivitas di ruang siber. Hak pemilik data yang dimaksud adalah hak meminta informasi, hak mengubah ketidakakuratan data pribadi, hak menghapus data pribadi, hak menarik persetujuan pemoresan, hak mengajukan keberatan untuk tindakan *profiling*, hak pembatasan pemrosesan, dan hak menuntut ganti rugi. Sementara itu, kewajiban pengendali data pribadi adalah menjaga kerahasiaan, melindungi keamanan data, melakukan pengawasan, melakukan perekaman atas pemrosesan data, dan menjadi akurasi data pribadi (Plate, 2020).

Di samping hadirnya Strategi Keamanan Siber Nasional dan RUU Perlindungan Data Pribadi, luaran diplomasi siber yang dilakukan Indonesia melalui kegiatan *workshop* juga dapat dilihat dari meningkatnya nilai GCI Indonesia pada tahun 2020. Pada periode laporan sebelumnya di tahun 2018, Indonesia menempati urutan 41 secara global dan urutan 9 untuk kawasan Asia Pasifik dalam hal keamanan siber. Lalu pada periode laporan tahun 2020, indeks keamanan siber Indonesia meningkat dengan menempati urutan 24 secara global dan urutan 6 untuk kawasan Asia Pasifik. Nilai tertinggi ada pada aspek *cooperative measure* (20,00 dari 20,00) dan *capacity development* (19,48 dari 20,00).

Gambar 3. Hasil penilaian GCI Indonesia tahun 2020



Sumber: ITU, 2020, hal. 87

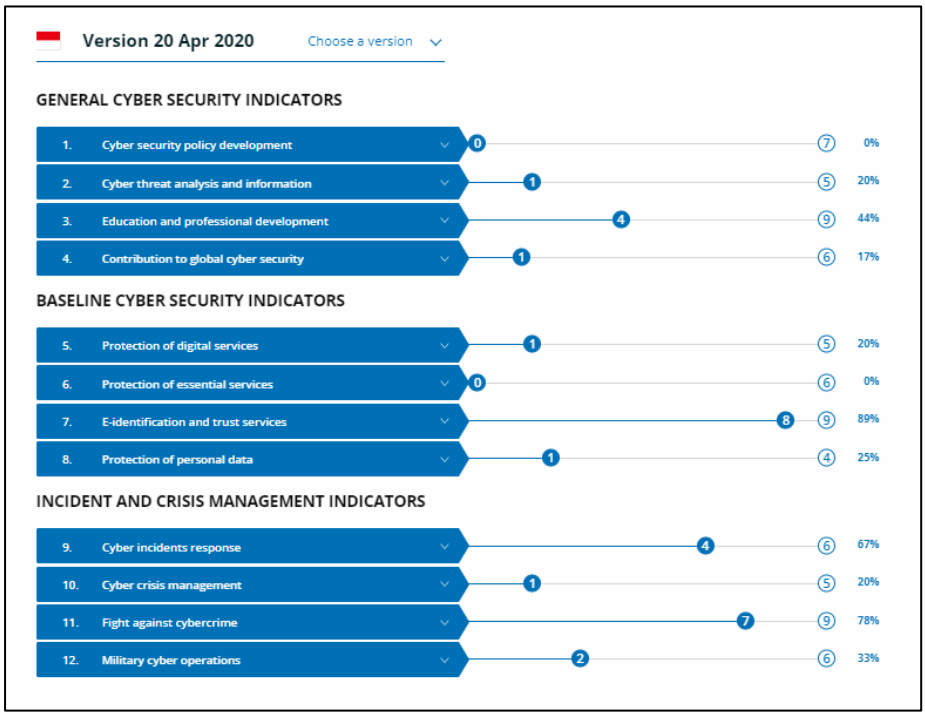
Peningkatan indeks ini memang tidak dapat dijadikan tolak ukur yang pasti untuk melihat luaran diplomasi siber di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*, karena terdapat upaya pengembangan kapasitas lain yang juga mendukung peningkatan indeks tersebut. Akan tetapi, peningkatan indeks ini dapat memberikan gambaran

mengenai peningkatan kapasitas yang dialami oleh Indonesia setelah dilaksankannya *workshop*, khususnya pada aspek *capacity development* yang memiliki nilai 19,48 dari nilai maksimal 20,00.

Aspek *capacity development* sendiri merupakan aspek yang memperhitungkan pendidikan, pelatihan, kampanye kesadaran, dan insentif untuk mengembangkan kapasitas keamanan siber di suatu negara. Salah satu indikatornya adalah ketika pemerintah menyadari adanya kebutuhan program pendidikan dan pelatihan di sektor yang spesifik untuk para profesional keamanan siber (ITU, 2020, hal. 17). Penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019* dapat termasuk ke dalam realisasi dari indikator tersebut, yaitu upaya yang dilakukan pemerintah untuk memberikan pelatihan (*workshop*) kepada profesional keamanan siber di Indonesia. Oleh karenanya, peningkatan indeks keamanan siber Indonesia, khususnya dalam aspek *capacity development*, juga dapat menunjukkan capaian agenda diplomasi siber yang dilakukan pada *Capacity Building on National Cybersecurity Strategy Workshop 2019*.

Selain GCI, NCIS juga mencatat adanya peningkatan indeks keamanan siber Indonesia pada 2020. Terkait dengan upaya pengembangan kapasitas dalam hal strategi keamanan siber nasional dan perlindungan data pribadi, Indonesia menunjukkan peningkatan pada indikator perlindungan layanan digital dan perlindungan data pribadi. Akan tetapi, indikator penting terkait pengembangan kebijakan keamanan siber masih memiliki skor nol. Hal ini terlihat dari penjelasan sebelumnya bahwa Strategi Keamanan Siber Nasional Indonesia dan RUU Perlindungan Data Pribadi masih menjadi rancangan kebijakan dan belum disahkan menjadi produk hukum.

Gambar 4. Nilai indikator keamanan siber Indonesia menurut NCSI tahun 2020



Sumber: E-Government Academy, 2020

Dengan melihat rumusan kebijakan-kebijakan baru yang dikeluarkan oleh BSSN maupun Kemenkominfo serta peningkatan indeks keamanan siber tersebut, peneliti melihat adanya capaian yang dilakukan oleh Indonesia di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*. *Workshop* ini ditujukan untuk menciptakan referensi dan panduan dalam membangun serta meningkatkan kerangka kerja dalam hal strategi keamanan siber nasional dan perlingungan data pribadi. Dengan disusunnya Strategi Keamanan Siber Nasional dan RUU Perlindungan Data Pribadi, serta meningkatkan indeks pengembangan kapasitas dan perlindungan data

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

serta layanan digital, hal tersebut menjadi bukti hasil dari referensi serta panduan yang dimaksud dalam tujuan penyelenggaraan *workshop*.

Meski kedua rumusan kebijakan ini belum diwujudkan dalam bentuk produk hukum mengingat adanya faktor lain di dalam merumuskan kebijakan keamanan siber di Indonesia, capaian ini dapat menjadi gambaran bagaimana instrumen diplomasi siber mampu memenuhi kebutuhan keamanan siber nasional melalui kegiatan pelatihan dan edukasi untuk mengembangkan kapasitas sumber daya manusia, kelembagaan, dan legislasi.

Optimalisasi Diplomasi Siber Indonesia untuk Mengembangkan Kapasitas Keamanan Siber

Berkenaan dengan diplomasi siber, Indonesia memiliki poin keunggulan dalam hal posisi dan rekam jejak diplomasi yang kuat dalam membawa isu-isu keamanan siber di berbagai forum internasional. Selain itu, komitmen Indonesia dalam mewujudkan keamanan siber dan menjalin kerja sama internasional juga sangat tinggi. Hal ini terlihat dari penilaian GCI terbaru di tahun 2020 yang menunjukkan nilai sempurna (20,00 dari 20,00) untuk indikator *cooperative measures*. Kondisi ini tentu dapat Indonesia manfaatkan untuk terus melakukan upaya diplomasi guna menutup celah keamanan siber yang masih ada. Terlebih lagi, upaya diplomasi siber yang dilakukan di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019* menunjukkan adanya respon positif dari negara maupun organisasi internasional serta memberikan luaran bagi kebutuhan keamanan siber Indonesia dalam membentuk referensi strategi keamanan siber nasional dan regulasi perlindungan data pribadi.

Dalam dokumen rencana strategis BSSN terbaru untuk periode 2020-2024, dikemukakan bahwa Indonesia masih menghadapi tantangan terkait perlindungan infrastruktur TIK nasional dan pemenuhan kebutuhan sumber daya manusia yang mumpuni. Adapun tantangan perlindungan infrastruktur TIK yang dimaksud antara lain adalah adanya ancaman kebocoran data dan informasi diplomasi Indonesia melalui kegiatan spionase; serta adanya kemungkinan perusahaan rintisan teknologi besar (*unicorn*) Indonesia dikuasai oleh pihak asing (BSSN, 2020, hal. 24).

Sementara itu, kebutuhan akan sumber daya manusia yang dimaksud antara lain belum optimalnya pemenuhan sumber daya manusia atas kebutuhan sumber daya manusia yang ada dan belum tersedianya standar kompetensi bidang keamanan siber di Indonesia. Sampai dengan 2020, untuk BSSN sendiri, sumber daya manusia yang dimiliki berjumlah 1.149 orang dengan berbagai latar belakang pendidikan. Adapun praktisi yang memiliki gelar doktor (S3) baru berjumlah enam orang. Hal ini menunjukkan tingginya kebutuhan *expert* yang menguasai bidang keamanan siber (BSSN, 2020, hal. 18 & 22).

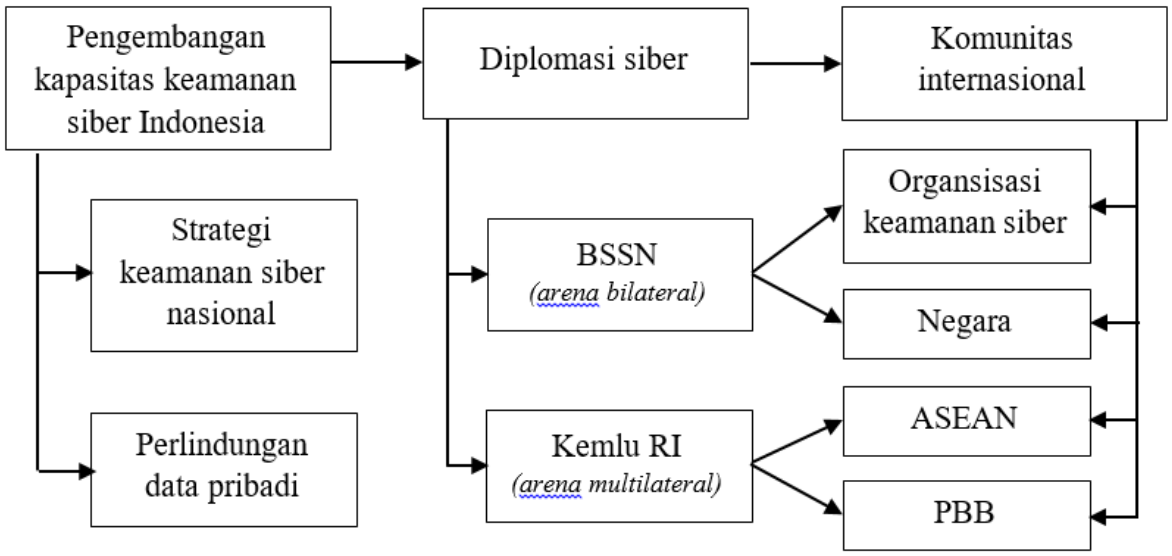
Kebutuhan-kebutuhan di bidang keamanan siber ini sejalan dengan pendapat Harditya mengenai kebutuhan keamanan siber yang telah disampaikan pada bagian sebelumnya. Hingga saat ini, Indonesia masih harus memenuhi kebutuhan keamanan siber dalam empat aspek, yaitu sumber daya manusia, legislasi, kelembagaan, dan teknologi. Hal inilah yang masih menjadi kebutuhan untuk terus mengoptimalkan instrumen diplomasi siber agar dapat menjalin kerja sama internasional guna memenuhi kebutuhan tersebut. Agenda ini juga telah menjadi bagian dari arah kebijakan dan strategi keamanan siber nasional untuk meningkatkan kerja sama internasional (BSSN, 2020, hal. 36).

Guna mewujudkan hal tersebut dan mempertimbangkan luaran diplomasi siber yang dilakukan di dalam penyelenggaraan *Capacity Building on National Cybersecurity Strategy Workshop 2019*, peneliti melihat bahwa Indonesia dapat mengoptimalkan intrumen diplomasi siber untuk mengembangkan kapasitas pada area lainnya. Hal ini dapat dilakukan melalui kegiatan edukasi dan pelatihan, maupun mengeksplorasi topik-topik lain yang dapat mendukung penguatan startegi keamanan siber nasional dan perlindungan data pribadi. Hal ini sejalan dengan prinsip *capacity*

development menurut ITU bahwa pengembangan kapasitas dapat dilakukan melalui kegiatan pelatihan dan edukasi untuk meningkatkan jumlah profesional di bidang keamanan siber yang dapat mendukung perwujudan keamanan siber nasional pada aspek lainnya.

Berangkat dari hal tersebut, BSSN dan Kemlu RI sebagai aktor utama di dalam upaya diplomasi siber Indonesia dapat meoptimalkan upaya masing-masing pada arena bilateral maupun multilateral terhadap forum-forum yang diikuti oleh masing-masing pihak. Upaya ini selaras dengan apa yang disampaikan oleh Barrinha dan Renard (2017) bahwa diplomasi siber dapat dilakukan melalui forum bilateral maupun multilateral terhadap berbagai aktor negara maupun non-negara. Dengan begitu, peneliti melihat diplomasi siber Indonesia dapat dioptimalkan dengan memanfaatkan forum-forum internasional yang ada untuk mendukung strategi keamanan siber nasional dan perlindungai data pribadi sebagaimana peneliti gambarkan melalui ilustrasi bagan berikut.

Bagan 3. Optimalisasi diplomasi siber di berbagai arena



Pada **arena bilateral**, BSSN dapat menjalin hubungan dengan lembaga-lembaga keamanan siber di berbagai negara, melakukan tolak ukur atas upaya mewujudkan keamanan siber yang dilakukan oleh negara maju, dan mewakili Indonesia dalam berbagai forum siber di tingkat internasional yang berkaitan dengan kebutuhan teknis (BSSN, 2018, hal. 12-13). Berdasarkan laporan tahunan keamanan siber tahun 2021, BSSN juga mengakui bahwa diplomasi dan kolaborasi bilateral dapat membantu Indonesia meningkatkan kompetensi dalam menghadapi serangan siber yang dapat dilakukan antara lain dengan (Id-SIRTII/CC, 2021, hal. 193):

a. Meningkatkan hubungan kerja sama dengan berbagai pihak dalam bidang keamanan siber.
b. Memfasilitasi pertukaran informasi, pengalaman, dan teknologi mengenai kode-kode berbahaya dan virus yang dapat menyerang perangkat TIK.
c. Mencegah kejahatan di ruang siber dengan menyelaraskan kebijakan, regulasi, dan peraturan.
d. Membantu lembaga CERT dan CSIRT di berbagai negara untuk meningkatkan tanggap insiden keamanan siber.
e. Memberi rekomendasi dalam mengatasi permasalahan hukum dan respon darurat terkait insiden keamanan siber lintas negara.

Adapun arena bilateral yang dimaksud adalah upaya diplomasi kepada organisasi keamanan siber internasional dan negara-negara yang memiliki hubungan kerja sama siber dengan Indonesia. Untuk organisasi keamanan siber internasional, Indonesia memiliki kontribusi yang kuat pada berbagai

e-ISSN: 2684-8082 Vol. 5 No. 2, Agustus 2023 (142-164) doi: 10.24198/padjirv5i2.41337

organisasi dengan agenda pengembangan kapasitas yang Indonesia bawa. Hal ini tentunya dapat mendorong BSSN untuk menyusun strategi keamanan siber nasional yang lebih baik.

Yang *pertama* tentunya adalah ITU seperti yang telah peneliti jelaskan di dalam studi kasus penelitian ini. Indonesia merupakan anggota ITU yang secara rutin menyumbangkan kontribusi setiap tahunnya. Tentu hal ini mendorong Indonesia untuk dapat memanfaatkan keanggotaan dengan sebaik-baiknya. Salah satunya adalah dengan mengikuti dan mendapatkan kegiatan edukasi serta pelatihan seperti *Capacity Building on National Cybersecurity Strategy Workshop* pada 2019. Hal ini juga dikonfirmasi oleh Harditya (2022) bahwa dengan keanggotaan tersebut, Indonesia memiliki hak suara, hak untuk mengetahui program-program ITU, dan hak untuk mendapatkan timbal balik dari kontribusi berupa dana puluhan ribu dolar Amerika Serikat yang diberikan (Harditya, 2022). Dengan mengoptimalkan keanggotaan Indonesia pada ITU, Indonesia dapat memaksimalkan agenda diplomasi siber untuk mengembangkan kapasitas sumber daya manusia dan melindungi kepentingan nasional.

Yang *kedua* adalah OIC-CERT, yaitu organisasi CERT bagi negara-negara anggota OIC. Indonesia telah menjadi anggota sejak 2008 dan mendapatkan amanat untuk menjadi *deputy chair* mendampingi Oman sebagai *chair* sejak 2018 hingga saat ini. Selama menempati posisi tersebut, Indonesia banyak mendorong agenda pengembangan kapasitas bagi lembaga-lembaga siber di negara anggota OIC bersama Mesir dan Malaysia (Id-SIRTII/CC, 2021, hal. 194). Contohnya adalah Indonesia menginisiasi pelatihan manajemen respon insiden siber selama pandemi Covid-19 dengan membagikan pengalaman Indonesia ketika melakukan hal yang sama; memberikan pelatigan mengenai mitigasi kebocoran data; dan mengadakan *workshop* mengenai analisis trafik *malware*. Tidak hanya sebagai inisiator, Indonesia juga mendapatkan banyak manfaat dari pelaksanaan *drill test* maupun c*yber drill* yang dilaksanakan oleh OIC-CERT untuk terus mengembangkan kapasitas sumber daya manusia dan teknologi keamanan siber Indonesia (OIC-CERT, 2020)..

Yang *ketiga* adalah *Asia Pacific CERT* (APCERT), yaitu organisasi CERT bagi negara-negara di kawasan Asia Pasifik. Indonesia telah menjadi anggota sejak 2009 dan aktif sebagai *operational member* yang memberikan kontribusi dalam program edukasi, pengembangan kapasitas, maupun *working group*. Salah satunya yang terbaru di tahun 2021, Indonesia aktif tergabung di *working group* APCERT untuk merumuskan standar keamanan informasi dan tanggap insiden bagi keamanan *Internet of Things* (IoT), yaitu objek-objek yang dilengkapi perangkat komunikasi, sensor, maupun aktuator yang saling terhubung melalui internet. Hal ini bermanfaat untuk membangun kepercayaan dan menciptakan ekosistem IoT yang aman di kawasan Asia Pasifik, termasuk Indonesia (Id-SIRTII/CC, 2021, hal. 214-216). Keterlibatan seperti itu tentu dapat Indonesia memanfatakan terutama untuk mewujudkan agenda melindungi kepentingan nasional Indonesia di ruang siber, yaitu mendorong ekonomi digital dan pengembangkan kapasitas keamanan siber Indonesia.

Selain organisasi keamanan siber internasional, diplomasi siber di arena bilateral juga bisa dioptimalkan kepada negara-negara maju yang telah memiliki sistem keamanan siber yang lebih baik. Salah satunya adalah Amerika Serikat yang telah lama menjalin hubungan baik dengan Indonesia dalam hal pengembangan kapasitas keamanan siber. Contoh diplomasi yang banyak dijalin adalah dengan Carnegie Mellon University yang memiliki divisi CERT yang terkenal unggul dalam hal keamanan siber dan telah bekerja sama dengan banyak pemerintah, industri, maupun akademisi untuk meningkatkan keamanan dan ketahanan sistem jaringan komputer (CMU, t.thn.).

Bekerja sama dengan Carnegie Mellon University, Indonesia bisa mendapatkan pelatihan, mengembangkan metode, dan alat canggih untuk menangani ancaman siber yang memiliki dampak luas. Hal ini terlihat dari program-program BSSN bersama Carnegie Mellon University yang telah dilakukan, yaitu pengembangan kemampuan sumber daya manusia untuk mengelola CERT; pelatihan deteksi dan identifikasi aktivitas siber berbahaya berdasarkan pengalaman intelejen Amerika Serikat; dan *training on trainer* terkait manajemen CSIRT agar pemerintah pusat, pemerintah daerah, dan sektor

infrastruktur kritis nasional dapat membentuk tim tanggap insiden sendiri (Id-SIRTII/CC, 2021, hal. 206-207).

Selain bersama Carnegie Mellon University, Indonesia juga memiliki hubungan diplomasi yang kuat dengan FBI Amerika Serikat dalam hal pertukaran informasi terkait investigasi insiden keamanan siber. Dengan dua peluang kerja sama yang besar bersama Amerika Serikat tersebut, Indonesia dapat memaksimalkan agenda diplomasi siber untuk mengembangkan kapasitas sumber daya manusia serta teknologi.

Selanjutnya, pada **arena multilateral**, Kemlu RI memainkan peranan yang lebih besar dan telah memiliki rekam jejak yang kuat dalam membawa isu-isu keamanan siber, baik dalam forum PBB maupun ASEAN. Hal ini tak terlepas dari kepentingan nasional Indonesia sebagai salah satu negara dengan pengguna internet tertinggi di dunia. Adapun isu utama yang selalu Indonesia bawa adalah mendorong implementasi 11 norma sukarela mengenai keamanan di ruang siber, karena hingga saat ini, belum terdapat instrumen hukum yang kuat terkait keamanan siber secara internasional. Dengan adanya implmenetasi 11 norma ini, Indonesia akan sangat terbantu untuk mengamankan ruang siber Indonesia, khususnya yang berkaitan dengan perlindungan data pribadi dan pertumbuhan ekonomi digital.

Saat ini, Indonesia memiliki banyak peluang untuk dapat mengoptimalkan diplomasi siber dan mewujudkan agenda-agenda diplomasi siber Indonesia. Yang *pertama* pada forum PBB, Indonesia aktif berpartisipasi dalam berbagai diskusi substantif mengenai norma dan hukum internasional keamanan siber dengan menjadi anggota UNGGE dan UNOEWG.

Indonesia telah tiga kali tergabung dalam UNGGE, yaitu pada periode 2012-2013, periode 2014-2015, dan periode 2019-2021. Dalam hal ini, Indonesia berperan sebagai peace builder, fasilitator, dan/atau negosiator yang menjembatani perbedaan kapasitas keamanan siber di antara negara maju dan berkembang (Ruddyard, 2021). Selain itu, Indonesia juga aktif mendorong implementasi 11 norma keamanan siber oleh negara-negara anggota hingga ke tingkat teknis. Hal ini tentunya dilakukan untuk menunjang kepentingan dan pembangunan nasional, khususnya pembangunan ekonomi, serta melindungi infrastruktur keamanan siber yang Indonesia miliki.

Kemudian pada UNOEWG, Indonesia aktif menjadi salah satu anggota pada periode 2019-2021 dengan agenda untuk mendorong implementasi norma dan hukum internasional mengenai keamanan siber, memastikan *confidence building measures*, dan tentunya mengembangkan kapasitas negara-negara berkembang. Hasil dari upaya tersebut dapat dilihat dalam Laporan Substansi Final UNOEWG (A/AC.290/2021/CRP.2).

Laporan akhir UNOEWG tersebut menjadi landasan kuat untuk mendorong peningkatan kesadaran dan implementasi norma terkait di negara-negara anggota PBB. Dengan kepentingan yang dimiliki Indonesia, peluang ini tentu dapat dimanfaatkan untuk mengoptimalkan agenda diplomasi siber Indonesia dalam meningkatkan peran di tatanan siber global, mengatasi tantangan keamanan siber, dan melindungi kepentingan nasional. Terlebih lagi, diskusi UNOEWG masih berlanjut untuk periode baru di tahun 2021-2025.

Yang *kedua* adalah forum ASEAN. Berdasarkan pertemuan ke-28 *ASEAN Regional Forum* pada 6 Agustus 2021, Indonesia mendapatkan kesempatan untuk menjadi *co-chair* bersama Australia, Rusia, dan Republik Korea untuk memimpin *Inter-sessional Meeting on ICTs Security* untuk periode 2022-2024. *Inter-sessional meeting* ini ditujukan untuk mengeksplorasi solusi kreatif yang dapat memastikan kelanjutan kerja sama negara di bidang-bidang keamanan siber (ASEAN Regional Forum, 2021). Dalam hal ini, Kemlu RI berperan sebagai *co-chair* dan turut didukung oleh BSSN sebagai delegasi. Adapun peluang ini memberikan keuntungan besar bagi Indonesia untuk meningkatkan postur Indonesia dalam mencapai tujuan keamanan siber nasional dan meningkatkan peran Indonesia sebagai aktor utama dalam hal perwujudan keamanan siber. Selain itu, sama seperti agenda Indonesia pada forum PBB, Indonesia juga memiliki agenda untuk mendorong kesadaran dan implementasi norma-

norma keamanan siber di kawasan Asia Tenggara guna melindungi ruang siber dan warga negara Indonesia (Harditya, 2022).

KESIMPULAN

Berdasarkan studi kasus diplomasi siber yang dilakukan oleh Indonesia di dalam penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019, terlihat adanya komitmen dari Indonesia untuk mengembangkan kapasitas keamanan siber, khususnya dalam hal membangun strategi keamanan siber nasional dan regulasi perlindungan data pribadi. Akan tetapi, upaya ini belum secara langsung memberikan dampak untuk mencegah serangan-serangan siber sehingga Indonesia belum dapat memenuhi prinsip keamanan siber yang ideal, yaitu ketersediaan, integritas, dan kerahasiaan. Hal ini terjadi karena Indonesia belum memprioritaskan diplomasi siber sehingga luaran yang didapat dari upaya yang dilakukan belum ditindaklanjuti menjadi sebuat produk hukum yang utuh. Selain itu, Indonesia juga masih memiliki keterbatasan pada aspek sumber daya manusia, regulasi, kelembagaan, dan teknologi. Oleh karenanya, diplomasi siber Indonesia perlu dioptimasi melalui berbagai arena dan forum internasional untuk mendukung pengembangan kapasitas pada aspek-aspek yang masih memiliki kekurangan.

Pada penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019, terlihat bahwa upaya diplomasi siber Indonesia melalui BSSN dan Kemenkominfo terhadap ITU mendapat respon positif hingga akhirnya workshop tersebut dapat terlaksana dengan mendatangkan lima orang experts. Keberhasilan ini tak terlepas dari adanya kesamaan agenda di antara Indonesia dan ITU. Selain itu, penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019 juga memberikan luaran yang memenuhi tujuan diplomasi yang diinginkan, yaitu membentuk referensi dan kerangka kerja yang diperlukan pada topik terkait. Hal ini terlihat dari disusunnya Strategi Keamanan Siber Nasional Indonesia, RUU Perlindungan Data Pribadi, dan meningkatnya indeks keamanan siber Indonesia dalam hal pengembangan kapasitas.

Berdasarkan hal tersebut, peneliti melihat bahwa diplomasi siber dapat dioptimasi karena adanya kesadaran yang tinggi di antara negara dan organisasi internasional dalam memandang keamanan siber sebagai isu bersama, sehingga upaya-upaya yang dilakukan untuk mewujudkan keamanan siber mendapatkan respon yang positif. Indonesia dapat mengoptimasi diplomasi siber dengan memanfaatkan beberapa peluang yang Indonesia miliki saat ini. Yang pertama adalah diplomasi siber oleh BSSN pada arena bilateral kepada organisasi keamanan siber internasional serta negara lain. Diplomasi siber ini dapat dilakukan guna memperkuat strategi keamanan siber nasional Indonesia. Yang kedua adalah diplomasi siber oleh Kemlu RI pada arena multilateral di forum PBB dan ASEAN. Dalam upaya diplomasi siber ini, Indonesia berpeluang untuk mendorong kesadaran dan implementasi norma-norma keamanan siber untuk mendukung upaya perlindungan data pribadi, pertumbuhan ekonomi digital, dan menciptakan ruang siber Indonesia yang aman.

DAFTAR PUSTAKA

Anthony, U. E. (2019). The Effects of Information Technology on Global Economy. *Italienisch, 9*(1), 135-147. Diambil kembali dari http://italienisch.nl/index.php/VerlagSauerlander/article/view/77

ASEAN Regional Forum. (2021, Agustus 6). *Chairman's Statement of the 28th ASEAN Regional Forum 6 August 2021 via videoconference*. Dipetik Juli 31, 2022, dari MOFA of Japan: https://www.mofa.go.jp/files/100220807.pdf

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

Biro Hukum dan Hubungan Masyarakat BSSN. (2019, Agustus 27). *BSSN Gelar Capacity Building on National Cybersecurity Strategy Workshop*. Dipetik Mei 10, 2021, dari Badan Siber dan Sandi

Negara: https://bssn.go.id/bssn-gelar-capacity-building-on-national-cybersecurity-strategy-workshop/

Biro Hukum dan Kerjasama BSSN. (2020, April 20). *Rekap Serangan Siber (Januari – April 2020)*. Dipetik Oktober 10, 2021, dari BSSN: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

BPPK Kementerian Luar Negeri Republik Indonesia. (2017). *Laporan Kinerja (LKJ) Pusat P2K Multilateral 2017*. Jakarta: Kementerian Luar Negeri Republik Indonesia. Diambil kembali dari https://kemlu.go.id/download/L3NpdGVzL3B1c2F0L0RvY3VtZW50cy9MS0olMjBQdXNhdCUyMFAySyUyME11bHRpbGF0ZXJhbCUyMDIwMTcucGRm

BSSN. (2018). *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019*. Jakarta: Badan Siber dan Sandi Negara. Diambil kembali dari https://cloud.bssn.go.id/s/rXg5HZY877xWGrL

BSSN. (2020). *Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024*. Jakarta: Badan Siber dan Sandi Negara. Diambil kembali dari https://jdih.bssn.go.id/wp-content/uploads/2020/07/Peraturan-BSSN-Nomor-5-Tahun-2020_sign.pdf

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking Trust, and Fear Between Nations*. New York: Oxford University Press.

Buletin APJII. (2020, November 9). *Siaran Pers: Pengguna Internet Indonesia Hampir Tembus 200 Juta di 2019 – Q2 2020*. Dipetik Mei 3, 2021, dari Asosiasi Penyelenggara Jasa Internet Indonesia: https://blog.apjii.or.id/index.php/2020/11/09/siaran-pers-pengguna-internet-indonesia-hampir-tembus-200-juta-di-2019-q2-2020/#:~:text=JAKARTA%20%E2%80%93%20Senin%2C%209%20November%202020,(9%2F11)%20siang.&text=Jumlah%20ini%20setara%20196%2C7,9%20juta%20be

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica, 10*(2), 113-128. doi:https://doi.org/10.22212/

CMU. (t.thn.). *The CERT Division*. Dipetik Juli 31, 2022, dari Carnegie Mellon University: https://www.sei.cmu.edu/about/divisions/cert/

E-Government Academy. (2018, Maret 28). *Indonesia*. Dipetik Januari 12, 2022, dari NCIS: https://ncsi.ega.ee/country/id/42/#details

E-Government Academy. (2020, April 20). *Indonesia*. Dipetik Januari 12, 2022, dari NCIS: https://ncsi.ega.ee/country/id/

Hamonangan, I., & Assegaff, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Relations (PADJIR), 1*(3), 311-333. doi:10.24198/padjir.v1i3.26246

Harditya. (2022, April 18). Diplomasi Siber Indonesia. (A. S. Waskita, Pewawancara)

Id-SIRTII/CC. (2018). *Indonesia Cyber Security Monitoring Report*. BSSN, Pusat Operasi Siber Nasional. Jakarta Pusat: Id-SIRTII/CC. Diambil kembali dari https://cloud.bssn.go.id/s/Y9tSycL4Pzci2qW

Id-SIRTII/CC. (2021). *Laporan Tahunan Monitoring Keamanan Siber 2021*. Jakarta Selatan: Direktorat Operasi Keamanan Siber BSSN. Diambil kembali dari https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

ITU. (2018). *Global Cybersecurity Index 2018*. ITU Publications. Diambil kembali dari https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITU. (2020). *Global Cybersecurity Index 2020*. Geneva: International Telecommunication Union. Diambil kembali dari https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (t.thn.). *Regional Capacity Building on National Cyber Security Strategy*. Dipetik Januari 12, 2022, dari ITU: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2019/Aug-NCSS/main.aspx

ITU-T. (2008). *Recommendation ITU-T X. 1205: Overview of Cybersecurity*. ITU, Telecommunication Standarization Sector. International Telecommunication Union. Dipetik Agustus 8, 2021, dari https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Kassab, H. S. (2014). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. Dalam J. F. Kremer, & B. Muller (Penyunt.), *Cyberspace and International Relations* (hal. 59-76). Berlin: Springer. doi:https://doi.org/10.1007/978-3-642-37481-4_4

Kominfo. (2019). *Strategi Implementasi Perlindungan Data Pribadi di Indonesia.* Kementerian Komunikasi dan Informatika, Badan Penelitian dan Pengembangan SDM. Jakarta: Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik. Diambil kembali dari https://balitbangsdm.kominfo.go.id/publikasi_661_3_227

Lebo, D., & Anwar, S. (2020). Pemberdayaan Komunitas Siber oleh Pemerintah Republik Indonesia dari Perspektif Strategi Perang Semesta. *Jurnal Strategi Pertahanan Semesta, 6*(1), 101-127. Diambil kembali dari https://jurnalprodi.idu.ac.id/index.php/SPS/article/view/653

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71-90. doi:https://doi.org/10.2307/20650279

Narindra, K. S. (2021). Keamanan dan Ancaman Cyber Bagi Sektor Privat dan Industry Militer Di Era 4.0. *Jurnal Diplomasi Pertahanan, 7*(1), 36-55. doi:https://doi.org/10.33172/jdp.v7i1.675

OIC-CERT. (2020). *Online Training: 2020*. Dipetik Juli 31, 2022, dari OIC-CERT: https://www.oic-cert.org/en/events/online/2020.html#.YuaJJnZBzrc

Plate, J. (2020, Februari 25). *Penjelasan Pemerintah mengenai Rancangan Undang-Undang tentang Perlindungan Data Pribadi.* Dipetik Juli 25, 2022, dari DPR RI: https://www.dpr.go.id/dokakd/dokumen/RJ5-20200305-121009-3116.pdf

Prabowo, W. H., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations, 1*(3), 218-239. doi:10.24198/padjir.v1i3.26194

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia dalam Meningkatkan Keamanan Siber melalui Association of South East Asian Nations (ASEAN) Regional Forum. *Global Mind, 2*(1), 1-15. Diambil kembali dari https://journal2.unfari.ac.id/index.php/globalmind/article/view/89

Ruddyard, F. A. (2021, Agustus 2). Peran dan Capaian Indonesia Dalam Diplomasi Keamanan Siber. *Zona Inspirasi*. (M. Gandasari, Pewawancara) Kompas TV. Dipetik Juli 11, 2022, dari https://www.youtube.com/watch?v=mjt7TKhgx0A&list=WL&index=13

Sheldon, J. B. (2019). The Rise of Cyberpower. Dalam J. Baylis, J. J. Wirtz, & C. S. Gray (Penyunt.), *Strategy in the Contemporary World* (6 ed., hal. 291-307). Oxford: Oxford University Press.

Siburian, H. (2020, Desember 15). BSSN Menyusun Strategi Keamanan Siber Nasional. *Sapa Indonesia Malam.* (A. Wicaksono, Pewawancara) Kompas TV. Dipetik Juli 25, 2022, dari https://www.youtube.com/watch?v=bUV4VfqMNVg&list=WL&index=7

Siburian, H. (2020, Desember 7). *Simposium Strategi Keamanan Siber Nasional Badan Siber dan Sandi Negara*. Dipetik Juli 25, 2022, dari Badan Siber dan Sandi Negara: https://www.youtube.com/watch?v=9jHLH4WwQLk&list=WL&index=8&t=5760s

Solms, R. v., & Niekerk, J. v. (2013). From Information Security to Cyber Security. *Computers and Security*, 1-6. doi:http://dx.doi.org/10.1016/j.cose.2013.04.004

Svetlakov, A. G., & Glotina, I. (2018). Assessing the Impact of Information Space on Economic Security in the Region. *Ekonomika Regional*(2), 474-484. Diambil kembali dari https://search.proquest.com/openview/fba032de5586b403bdda6e6ff539c473/1?pq-origsite=gscholar&cbl=5002427

Tiirmaa-Klaar, H. (2013). Cyber Diplomacy: Agenda, Challenges and Mission. Dalam K. Ziolkowski (Penyunt.), *Peacetime Regime for State Activities in Cyberspace* (hal. 509-532). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Diambil kembali dari https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf

United Nations. (2021, Maret 10). *Final Substantive Report*. Dipetik Juli 31, 2022, dari United Nations: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

BIOGRAFI

Allisa Salsabilla Waskita merupakan mahasiswa Program Studi Hubungan Internasional Universitas Padjadjaran.

Hasan Sidik merupakan dosen di Program Studi Hubungan Internasional Universitas Padjadjaran.