BAB V

KERJASAMA SIBER INDONESIA MELALUI BADAN SIBER DAN SANDI NEGARA (BSSN) DI ASIA TENGGARA TAHUN 2018-2020

5.1 BSSN Dalam Upaya Memperkuat Keamanan Dalam Negeri

5.1.1 Strategi Keamanan Siber Nasional

Keamanan siber telah menjadi isu prioritas nasional bagi seluruh negara di dunia, termasuk di Indonesia. Hal ini dikarenakan tingkat pemanfaatan IPTEK yang makin meningkat dalam berbagai aspek kehidupan bermasyarakat dalam berbagai aspek baik hukum, sosial, ekonomi, kesehatan, pendidikan, budaya, keamanan, pertahanan dan lainnya. Disandingkan secara langsung dengan tingkat pemanfaatan IPTEK , tingkat ancaman yang dapat terjadi juga lebih tinggi dan lebih kompleks.

Dalam menanggapi hal tersebut, untuk mendukung dan menciptakan lingkungan siber strategis serta mewujudkan sistem elektronik nasional yang aman, andal, terpercaya, serta dapat mendorong dan menumbuhkan ekonomi digital dengan meningkatkan daya saing dan inovasi siber, serta membangun kesadaran dan kepekaan terhadap keamanan dan ketahanan nasional dalam ruang siber yang baik. Pemerintah Indonesia melalui Peraturan Presiden Nomor 53 Tahun 2017 dan perubahan nomor 133 Tahun 2017 tentang BSSN membentuk BSSN dengan peran utamanya adalah menyelenggarakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan memantapkan seluruh unsur yang terkait dengan keamanan siber nasional. Dalam rangka memberikan acuan strategis kebijakan keamanan siber, BSSN menyusun Strategi Keamanan Siber Indonesia.

Strategi Keamanan Siber Indonesia telah disusun menjadi 5 prinsip: Kedaulatan, Kemandirian, Keamanan, Kebersamaan dan Adaptif. Berdasarkan asas tersebut diharapkan dapat tercapai Sasaran Strategis Ketahanan Siber, Keamanan Pelayanan Publik, Penegakan Hukum Siber, Budaya Keamanan Siber dan Keamanan Siber dalam Ekonomi Digital guna mewujudkan Visi Strategi Keamanan Siber: Membangun dan menjaga keamanan siber nasional dengan mensinergikan berbagai pemangku kepentingan untuk ikut serta mewujudkan ketahanan nasional dan meningkatkan pertumbuhan ekonomi nasional.

Tujuan dari Strategi Keamanan Siber Indonesia adalah untuk mencapai budaya keamanan siber dan keamanan siber dalam ekonomi digital, keamanan layanan publik, penegakan hukum siber, dan tentunya ketahanan siber. Strategi Keamanan Informasi Indonesia diharapkan dapat menjadi salah satu tumpuan kepercayaan dunia terhadap Indonesia di berbagai forum keamanan siber internasional. Strategi Keamanan Siber Indonesia merupakan sumbangsih bangsa Indonesia dalam mendorong perdamaian dunia.

5.1.2 Gov-CSIRT

Gov-CSIRT menyelenggarakan layanan terhadap insiden siber yang terjadi dalam sektor pemerintahan. Insiden yang dapat ditangani antaralain adalah *data breach, ransomware, phising, malware, denial of service* dan *distributed denial of service, web defacement,* serta pencurian data yang berdampak gangguan pada berjalannya layanan sistem elektronik pada minimal dua organisasi dan maksimal setengah jumlah organisasi dalam satu sektor pemerintah.

Visi

Visi Gov-CSIRT Indonesia adalah terwujudnya ketahanan siber pada sektor pemerintah yang andal dan profesional.

Misi

Misi dari Gov-CSIRT Indonesia, yaitu:

1. membangun kapasitas sumber daya keamanan siber pada sector pemerintah
2. mengkoordinasikan serta mengolaborasikan tanggap insiden siber pada sector pemerintah
3. mengkoordinasikan serta mengolaborasikan layanan keamanan siber pada sektor pemerintah;

Gov-CSIRT Indonesia memiliki otoritas untuk menangani insiden yaitu:

1. *Web Defacement*;
2. *Distributed Denial of Service dan Denial of Service*;
3. *Malware*;
4. *Phishing*;

5. *Ransomware*;
6. *Data Breach*;
7. Pencurian Data;
8. Insiden siber lainnya yang mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada paling sedikit 2 (dua) organisasi dan paling banyak setengah jumlah organisasi di 1 (satu) sektor pemerintah.

Dukungan layangan yang diberikan oleh Gov-CSIRT Indonesia kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden. Layanan tersebut yaitu antaralain :

1. Layanan Utama

Layanan utama dari Gov-CSIRT Indonesia yaitu :

– Pemberian Peringatan Insiden Keamanan Siber

Layanan ini berupa pemberian peringatan adanya indikasi insiden siber kepada pemilik sistem elektronik.

– Layanan Tanggap Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka tanggap Insiden Siber.

2. Layanan Tambahan

– Layanan Forensik Digital : Layanan ini berupa pemberian dukungan dalam mengidentifikasi, mengoleksi, menganalisis dan menguji bukti-bukti digital system terdampak.
– Pemberitahuan Imbauan Keamanan : Gov-CSIRT Indonesia memberikan layanan pemberitahuan imbauan keamanan.
– Konsultasi Penanganan Insiden Siber : Layanan ini diberikan Gov-CSIRT Indonesia berupa kegiatan konseling yang dilakukan dengan tujuan memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan Insiden Siber.

- Pembangunan kesadaran dan kepedulian terhadap keamanan siber : Gov-CSIRT Indonesia menyediakan forum dalam upaya pembangunan kesadaran dan kepedulian terhadap keamanan siber.
- Peningkatan kapabilitas dan kompetensi : Gov-CSIRT Indonesia memberikan layanan peningkatan kapabilitas dan kompetensi konstituen dalam hal penanganan insiden berupa pelaksanaan table top exercise, drill test, dan workshop.
- Asistensi Pembentukan CSIRT Pemerintah : Asistensi pembentukan CSIRT Pemerintah diberikan kepada konstituen Gov-CSIRT yang membentuk CSIRT.
- Pendaftaran CSIRT Pemerintah : Pendaftaran CSIRT Pemerintah diberikan kepada konstituen Gov- CSIRT yang akan mendaftar CSIRT

5.2 Implementasi Kerjasama dan Kebijakan Dalam Negeri

Berdasarkan hasil wawancara penulis dengan narasumber dari BSSN, dapat diketahui bentuk implementasi dari kerja sama ataupun kebijakan yang sudah dibentuk pemerintah bersama BSSN tersebut yang bisa dirasakan langsung oleh masyarakat yaitu (Sulistyo, 2022)

5.2.1 CSIRT di Sektor Pemerintah

Pembentukan CSIRT di sektor pemerintah (pusat dan daerah) dan badan usaha negara dan swasta, CSIRT yang sudah terbentuk adalah sebanyak 142 tim.

5.2.2 Sertifikat Elektronik

Pemanfaatan Sertifikat Elektronik untuk meningkatkan keamanan transaksi elektronik; pengamanan teknologi informasi dan komunikasi; peningkatan dan pengembangan sumber daya manusia; dan pertukaran informasi kepada organisasi pemerintah dan swasta.

5.2.3 Budaya Keamanan Siber

BSSN berupaya membangun budaya keamanan siber sebagai tatanan nilai budaya yang melekat dan mendorong tumbuhnya budaya penggunaan ruang siber yang aman dan nyaman sehingga BSSN melakukan literasi dan edukasi budaya keamanan siber kepada setiap warga negara Indonesia melalui bentuk lokakarya, seminar, penerbitan dokumen tertulis, dan sebagainya.

5.3 Pembentukan Kerjasama Antara BSSN dengan Negara-Negara di Kawasan Asia Tenggara

Kejahatan siber sering kali melibatkan aktor kejahatan lintas negara. Khusus di Asia Tenggara, tingkat resiliensi antar negara terhadap kejahatan siber masih tergolong rendah. Setidaknya dari banyak kasus yang terjadi di beberapa negara, hal itu diakibatkan karena lemahnya sumber daya manusia yang terampil di bidang keamanan siber, lemahnya tata kelola keamanan data & teknologi, belum terbentuknya pola pikir sistematis bagi keamanan siber, dan terbatasnya teknologi di tengah perkembangan globalisasi yang semakin dinamis (Chang, 2017). Untuk menjawab permasalahan tersebut dalam konteks hubungan internasional, maka diperlukannya kerjasama dan diplomasi. Indonesia melalui BSSN pun sadar akan kemampuan diri dan kesempatan untuk mengembangkan kerjasama dengan negara-negara lain melalui bentuk kerjasama regional maupun bilateral. Berikut ini adalah bentuk kerjasama antara BSSN dalam mekanisme regional maupun bilateral (Sulistyo, 2022)

5.3.1 Kerjasama Regional (ASEAN)

1. **ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies (ARF-ISM on ICT)**

Secara umum pada dasarnya pelaksanaan kerjasama maupun diplomasi siber Indonesia melalui BSSN di tingkat ASEAN dilaksanakan melalui forum *ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies* (ARF-ISM on ICT) dengan dasar dari pilar *ASEAN Political-Security Community* (APSC) (Sulistyo, 2022). Rancangan terkait ARF-ISM on ICT ini pertama kali dibentuk pada 12 Juli 2012 di Phnom Penh, Kamboja saat pelaksanaan *ARF Ministerial Meeting* ke-19. Secara resmi pertama kali dibentuk pada tahun 2017. Adapun tujuan dari dibentuknya forum ini yakni sebagai forum dialog yang terfokus pada penggunaan dan keamanan teknologi, serta untuk peningkatan kapasitas sumber daya negara-negara yang tergabung di ARF (ASEAN Regional Forum, 2012).

Sejak tahun 2018 hingga tahun 2020 setidaknya ada beberapa agenda kegiatan kerjasama di tingkat ARF ini yang diikuti & telah dibangun secara konsensus oleh Pemerintah RI melalui BSSN (mulai tahun 2017) bersama anggota ARF-ISM on ICT:

1. Pembentukan *ARF Points of Contact (POC) Directory on Security of and in the Use of ICTs*. Adapun hasilnya yakni dibentuknya kerangka atau mekanisme direktori komunikasi antara anggota ARF untuk mengurangi ketegangan dan risiko konflik yang timbul dari kesalahan interpretasi insiden siber.
2. Mengikuti sesi *Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations*. Bertujuan untuk mengurangi kesalahpahaman, kesalahan perhitungan serta mencegah kemungkinan konflik dengan meningkatkan transparansi melalui sesi berbagi informasi dari sistem masing-masing negara anggota ARF.
3. Mengikuti sesi Sesi *Protection of Critical Infrastructures and Consultations Mechanism.* Dengan tujuan menjadi agenda yang akan berfungsi sebagai jalan praktis untuk konsultasi dan berbagi informasi di antara anggota ARF tentang langkah-langkah untuk melindungi infrastruktur penting dari tindakan siber yang berbahaya.
4. Mendorong adanya sesi Peningkatan Kesadaran dan Berbagi Informasi tentang Tanggap Darurat terhadap Insiden Keamanan dalam Penggunaan Teknologi Siber. Bertujuan untuk meningkatkan pembangunan kapasitas kawasan dalam menangani insiden terkait teknologi dan siber, serta memastikan respon yang ada tepat dan sesuai. Para anggota ARF menyepakati agar adanya penegakan hukum dalam suatu *Concept Note ARF-ISM on ICT*.
5. Mengikuti *ARF Workshop on Principles of Building Security of and in the Use of ICTs in the National Context.* Bertujuan untuk membahas berbagai pendekatan dan strategi terhadap pembentukan konsep & pengembangan strategi keamanan dalam penggunaan teknologi siber yang paling sesuai dengan kebutuhan negara anggota ARF.

Pada umumnya sesi-sesi maupun kerjasama yang diimplementasikan oleh ARF-ISM on ICTs disesuaikan dengan kondisi-kondisi keamanan maupun teknologi yang terjadi di kawasan maupun internal masing-masing anggota ARF, yang kemudian didiskusikan melalui forum ARF tersebut. Komitmen Indonesia bersama anggota-anggota ARF dalam forum ini memiliki tujuan yang besar yakni untuk mempermudah proses diplomasi siber dalam menangani suatu masalah siber yang terjadi berbasis pada transparansi kontak poin (Setyawan & Sumari, 2016). Selain kegiatan-kegiatan ARF ISC on ICT sebagai basis kerjasama regional Pemerintah RI melalui BSSN di tingkat regional, melalui wawancara dengan BSSN, BSSN menyebutkan bahwa ada kerjasama-kerjasama lainnya seperti ASEAN Cyber CC, ADGSOM – ANSAC, ASEAN – Japan CSWG, AMCC/ SICW, APEC-TEL WG SPSG, SOMTC/ AMMTC, ADMM Plus, ACCEC, ASEAN-US, ASEAN-Rusia, dan ASEAN-India. Kerjasama antara ASEAN yang dimana Indonesia melalui BSSN ada di dalamnya, disesuaikan dengan poin kritis yang ingin dibahas dengan negara-negara mitra ASEAN tersebut.

Di tingkat ASEAN, BSSN berkolaborasi dengan kementerian/lembaga terkait di bidang siber terutama dengan Kementerian Komunikasi dan Informatika karena tata kelola siber di Indonesia masih dipengaruhi kuat oleh para pejabat di kementerian tersebut, mengingat sebelum BSSN dibentuk, Kemenkomifo yang berperan kuat dalam keamanan siber tersebut (Rai, Heryadi, & N, 2022). Contohnya melalui *ASEAN Telecommunications and IT Ministers Meeting* (TELMIN) pembahasan yang terkait dengan keamanan siber tetap dibahas di tingkat kementerian. Keamanan siber bersifat *cross-sectors*. Kejahatan di sektor IT atau siber seringkali dikombinasikan dengan kejahatan transnasionalisme lainnya. Seperti *cyber-terrorism*, *cryptojacking*, investasi bodong dan sebagainya yang sangat umum di Asia Tenggara memerlukan kolaborasi antar kementerian/lembaga sebelum dibahas di tingkat regional ASEAN. Oleh karena itu, untuk menyatukan persepsi di tingkat nasional koordinasi dan komunikasi antar K/L menjadi yang utama, sebelum pada akhirnya di tingkat ASEAN persepsinya dapat disamakan antar negara. Perkembangan terakhir Indonesia merupakan *co-chair* dari ARF-ISM of ICT untuk tahun 2021-2024. Hal ini

diharapkan dapat menjadi landasan diplomasi siber BSSN agar lebih aktif di tingkat regional maupun multilateral.

2. *ASEAN Ministerial Conference on Cybersecurity* (AMCC)

Dalam acara *Singapore International Cyber Week* yang digelar pada Oktober 2020, ada satu rangkaian acara yang bertajuk "*ASEAN Ministerial Conference on Cybersecurity* (AMCC)". AMCC sendiri adalah Konferensi Tingkat Menteri ASEAN yang membicarakan terkait *cybersecurity* di kawasan ASEAN. Dalam acara ini Kepala BSSN, Hinsa Siburian turut hadir secara daring. Konferensi ini memiliki tujuan untuk meminta serta mengajak seluruh negara anggota ASEAN untuk memperkuat kolaborasi penyelenggaraan keamanan siber melalui berbagai kerja sama di tingkat regional maupun internasional. (BSSN, 2020) Dalam acara tersebut, Kepala BSSN menyampaikan bahwa Indonesia akan turut serta berkolaborasi dan bekerjasama dengan negara-negara di kawasan Asia Tenggara untuk menjaga keamanan siber.

Gambar 1 Kepala BSSN, Hinsa Siburian, secara daring menghadiri ASEAN Ministerial Conference on Cybersecurity (AMCC)

Sumber : BSSN

5.3.2 Kerjasama Bilateral

Setiap negara memiliki kapabilitasnya masing-masing dalam menjaga keamanan teknologinya dari ancaman kejahatan siber. Dengan menyadari adanya beberapa kekurangan dari segi keamanan siber Indonesia, BSSN melakukan kerjasama secara bilateral dengan negara-negara lain yang tentu dapat memberikan pembelajaran dan peningkatan akan kapasitas keamanan siber di Indonesia yang mumpuni dan aman. Khususnya dengan negara-negara yang maju secara teknologi, Indonesia diharapkan dapat mampu menarik ilmu-ilmu yang berguna bagi peningkatan sumber daya manusia di bidang keamanan siber. Selain itu, adanya kerjasama bilateral yang dilakukan oleh BSSN diharapkan dapat menjadi media ataupun sarana dalam melakukan pertukaran informasi, ketika pelaku kejahatan siber ditemukan melalui alamat IP berada di lintas negara.

Berikut ini merupakan kerjasama-kerjasama yang pernah dilakukan oleh BSSN dengan negara-negara di Asia Tenggara dalam rangka meningkatkan kemampuan keamanan siber di Indonesia:

1. Rencana Kerjasama Siber dengan Singapura

Perlu diketahui Singapura merupakan pemeringkat pertama negara dengan keamanan siber terbaik di ASEAN. Adapun keunggulan dari Singapura di bidang keamanan siber yakni berada di rapihnya tata kelola secara tugas, pokok dan fungsi dari badan keamanan siber-nya dan sistem sertifikasi yang terkoordinir dan terkoneksi (Putra, 2019). Pada gelaran *Shangri-la Dialogue* yang dilakukan di Singapura tahun 2018, Kepala BSSN, Djoko Setiadi melakukan penjajakan kemungkinan kerjasama di bidang siber dengan Cyber Security Agency (CSA) Singapura. Tupoksi dan regulasi yang jelas dapat memberikan panduan maupun arah dari suatu sistem keamanan siber. Melalui pertemuan singkat tersebut, rencana kerjasama siber dengan Cyber Security Agent (CSA) Singapura masih dirundingkan untuk pendalaman lebih lanjut.

Namun, hingga tahun 2020 belum ada kerjasama konkrit melalui nota kesepahaman antara kedua negara yang diinformasikan. Sebagai informasi tambahan, Singapura merupakan mitra konsultasi pemerintah Indonesia ketika ingin membentuk Badan Siber dan Sandi Negara.

Gambar 2 . Pertemuan Kepala BSSN & Kepala CSA Singapura, 2018

Sumber: BSSN

2. *Joint-Webinar* dalam Meningkatkan Kepedulian Publik dengan Keamanan Siber dengan Singapura, Malaysia, dan Brunei

Pada perayaan *Safer Internet Day* tepatnya pada 17 Maret 2022, *CyberSecurity Malaysia* (CSM) bekerjasama dengan Badan Siber dan Sandi Negara Indonesia (BSSN), *Cyber Security Agency of Singapore* (CSA), dan *Cyber Security Brunei* (CSB) menyelenggarakan *joint-webinar* yang bertajuk 'Webinar Kita Siber Serumpun'. Webinar ini memiliki tujuan bagi negara-negara serumpun Melayu untuk mensosialisasikan kepada publik apa arti dari keharmonisan ruang digital, bagaimana caranya membangun koneksi positif di daring, dan perilaku etis ketika berada di dunia siber (Cyber Security Brunei, 2022). Dalam webinar tersebut, delegasi Indonesia yang diwakili oleh Adi Nugroho dari Badan Siber & Sandi Negara (BSSN) menjelaskan aktivitas serangan siber khususnya malware & pencurian data yang meningkat di masa pandemi melalui transaksi *online*. Selain itu di aspek sosial, berita bohong menjadi momok yang sangat meningkat di masa pandemi yang perlu dikurasi dan dikontrol oleh BSSN.

Gambar 3 Joint Webinar Indonesia, Brunei, Malaysia, Filipina Tahun 2022

Sumber: CSB Brunei

Selain pertemuan bilateral kerjasama di atas antara Indonesia melalui BSSN dengan negara-negara di Asia Tenggara, belum ditemukan lagi pasca pandemi COVID-19 kerjasama bilateral yang direncanakan maupun direalisasikan. Dengan negara-negara di Asia Tenggara, BSSN masih merasa cukup kerjasama di lakukan melalui ekosistem bentuk kerjasama regional yaitu ASEAN. Penulis melihat bahwa masih terlingkupinya dan setaranya kemampuan antara negara-negara di Asia Tenggara dapat diselesaikan secara solutif di tingkat ASEAN maupun ASEAN Regional Forum. Selain itu secara bilateral, kedepannya kemungkinan besar akan menjajaki kerjasama-kerjasama tersebut secara *G-to-G* mengingat Indonesia baru saja pulih dari pandemi dan BSSN masih tergolong baru dibentuk pada tahun 2017. Perlunya penguatan dan *transfer of knowledge* & *technology* dari negara-negara maju di bidang keamanan siber di Asia Tenggara menjadi urgensi bagi BSSN di tengah meningkatnya ancaman siber yang muncul secara transnasional dari negara-negara di Asia Tenggara.

3. Komitmen Jaga Ruang Digital Indonesia – Malaysia

H.E. Tan Sri Annuar Haji Musa, Menteri Komunikasi dan Multimedia Malaysia melaksanakan kunjungan bilateral ke Indonesia untuk bertemu dengan

Johnny G. Plate yaitu Menteri Komunikasi dan Informatika Republik Indonesia. Tujuan dari pertemuan ini sendiri disampaikan oleh Menteri Johnny guna agar *cyberspace* Indonesia, Malaysia, serta Asia Tenggara selalu aman serta membawa manfaat untuk seluruh masyarakat baik Indonesia, Malaysia ataupun Kawasan Asia Tenggara. Dalam pertemuan ini kedua menteri membahas terkait kerjasama untuk penjagaan *cyberspace* atau ruang digital. Dalam pertemuan ini hal-hal yang di diskusikan antaralain terkait tata kelola ruang digital, infrastruktur hilir digital, dan infrastruktur hulu digital, dan hampir semua pekerjaan digital (Kementerian Kominfo, 2022)

Gambar 4 Diskusi Indonesia-Malaysia Terkait Jaga Ruang Digital

Sumber : Kementerian Kominfo

Kementerian Komunikasi dan Informatika (Kominfo) juga menerbitkan, pada tanggal yang sama, pernyataannya tentang peningkatan kerja sama, yang mencatat bahwa Indonesia perlu mengintegrasikan teknologi baru di dalam negeri terkait satelit, telekomunikasi, keamanan siber, dan ruang digital secara lebih luas (OneTrust , 2022)

Menteri Annuar Haji Musa dalam pertemuan tersebut juga menyampaikan bahwa pertemuan ini merupakan momen yang membanggakan dimana menunjukan

betapa eratnya hubungan kedua negara serta adanya tujuan yang sama terkait bidang siber dan telekomunikasi. Kerjasama *cyberspace* ini diharapkan oleh kedua negara agar tetap terus berjalan sehingga segala urusan terkait ruang digital baik itu penggunaan teknologi atau penyediaan infrastruktur dan lainnya dapat terselenggara dengan baik di kedua negara. Serta dinyatakan pula bahwa para pemimpin dan lembaga terkait dari kedua negara akan memperkuat manajemen keamanan siber mereka dan mengembangkan hubungan yang lebih erat di forum internasional, seperti International Telecommunications Union ('ITU') (OneTrust , 2022)