Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara

Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency

Hidayat Chusnul Chotimah
Ilmu Hubungan Internasional, Universitas Teknologi Yogyakarta
email: hidayat.chusnul@gmail.com

Riwayat Artikel

Diterima 3 Juli 2019
Direvisi 12 September 2019
Disetujui 7 Oktober 2019

doi: https://doi.org/10.22212/jp.v10i1.1447

Abstract

The virtual world is one territory that is now taken into account in a national security state, in addition to land, sea and air territories. As one of the largest internet user countries in the world, Indonesia is vulnerable to cyber threats. In response to the said threat, the Indonesian government established the National Cyber and Encryption Agency (BSSN) as a national cyber institution mandated with the responsibility to maintain cyber security and sovereignty. This paper uses a qualitative approach to interpret concepts, definitions, characteristics, metaphors, symbols, and descriptions of things through library research. It elaborates further on the role of BSSN in the management of cyber security in Indonesia as well as in the implementation of Indonesian cyber diplomacy both through bilateral and multilateral cooperation.

Keywords: Cyber Security; Cyber Diplomacy; Institutional; BSSN; Indonesia.

Abstrak

Dunia maya merupakan salah satu aspek yang saat ini ikut diperhitungkan dalam sebuah keamanan nasional suatu negara, di samping ranah darat, laut dan udara. Sebagai salah satu negara pengguna internet terbesar di dunia, telah menjadikan Indonesia rentan atau tidak luput dari ancaman siber. Oleh sebab itu, untuk merespons ancaman tersebut, pemerintah Indonesia kemudian membentuk Badan Siber dan Sandi Negara (BSSN) sebagai institusi siber nasional yang berfungsi menjaga keamanan dan kedaulatan siber. Pendekatan yang digunakan dalam tulisan ini menggunakan pendekatan kualitatif untuk menginterpretasikan konsep, definisi, karakteristik, metafora, simbol, dan deskripsi dari suatu hal melalui studi pustaka. Tulisan ini akan memaparkan lebih jauh mengenai peran BSSN dalam tata kelola keamanan siber di Indonesia sekaligus dalam pelaksanaan diplomasi siber Indonesia baik yang dilakukan melalui kerjasama bilateral maupun multilateral.

Kata Kunci: Keamanan Siber; Diplomasi Siber; Kelembagaan; BSSN; Indonesia.

Pendahuluan

Pada awal abad kedua puluh satu, ancaman berbasis siber menambahkan dimensi baru dalam memahami ancaman keamanan dari abad sebelumnya. Kemajuan teknologi informasi dan komunikasi (TIK) khususnya yang berbasis pada internet, telah menggiring hampir semua orang untuk memanfaatkan dan menggunakannya dengan berbagai cara. Artinya, berbagai aktor, baik negara maupun *non-state*, memiliki potensi ancaman untuk mengganggu jaringan karena sulitnya mengidentifikasi pelaku di dunia maya (siber) atas tindakan tertentu dan tindakan di suatu tempat yang memiliki efek atau dampak di seluruh belahan dunia.[1] Oleh sebab itu, internet telah menjadi bagian tak terpisahkan dari masyarakat modern dewasa ini, terlebih bagi generasi yang lahir setelah tahun 1995.

Munculnya gelombang transformasi teknologi informasi dan komunikasi ini juga telah menjadikan seluruh warga dunia terhubung dalam satu wadah yang disebut sebagai 'desa global' (*global village*). Perpaduan teknologi telekomunikasi, internet, dan penyiaran, telah mendorong munculnya infrastruktur jaringan pita lebar yang juga mendorong lahirnya ekonomi baru. Jaringan pita lebar tersebut di satu sisi memberikan manfaat bagi peningkatan kualitas kehidupan sosial dan ekonomi yaitu adanya globalisasi ekonomi digital. Namun, di sisi lain, keterhubungan jaringan pita lebar global (*global broadband*), juga memunculkan ancaman terhadap seluruh aset negara. Keterhubungan global ini membentuk dunia siber (*cyber-world*) dengan ciri interaksi daring yang memberi banyak kemudahan, sekaligus menghadirkan kerentanan dan ancaman baru, termasuk ancaman kedaulatan siber sebuah negara.[2]

Perlu diingat bahwa, interaksi masyarakat digital dalam menggunakan internet akan sangat bergantung pada ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi di ruang siber. Hal ini menjadi pendorong perlunya perlindungan terhadap sarana dan prasarana infrastruktur negara dalam pemanfaatan teknologi informatika. Dengan demikian, ancaman keamanan siber tidak lagi dipandang pada masalah teknis keamanan komputer semata, melainkan mencakup aspek ideologi, politik, ekonomi, sosial, budaya dan keamanan nasional.[3] Sementara di tingkat internasional, baik negara maupun masyarakat internasional harus mengembangkan strategi kooperatif dalam menanggapi perkembangan di dunia maya yang meluas secara internasional. Misalnya dengan membuat norma internasional yang menyangkut permasalahan dan ancaman siber.[4]

Jika menelaah tentang keamanan siber di Indonesia, ada beberapa serangan siber maupun perang siber yang pernah terjadi dengan pihak lain. Misalnya pada tahun 1998 di mana kerusuhan rasial di dunia siber atau dunia maya yaitu Indonesia berperang dengan para *hacker* yang diduga dari China dan Taiwan. Kemudian melalui penelitian dari Symantec, yaitu produsen Antivirus Norton, pada Agustus 2010, Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan *worm* Stuxnet. Tidak hanya itu saja, melalui laporan dari *Sydney Morning Herald* 31 Oktober 2013, Australia telah melakukan penyadapan terhadap pemerintah Indonesia melalui gedung perwakilan diplomatiknya di Jakarta.[5]

1 Nazli Coucri dan Daniel Goldsmith, "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security", *Buletin of the Atomic Scientists* 68, No. 2 (2012):70.

2 Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019*.

3 Hidayat Chusnul Chotimah, "Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia," *Jurnal Diplomasi*, Volume 7 No. 4, (Desember 2015):109.

4 Choucri dan Goldsmith, "Lost in Cyberspace," 72.

5 Nur Khalimatus Sa'diyah dan Ria Tri Vinata, "Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara," *Perspektif,* Volume XXI No. 3 (September 2016): 169.

Lebih jauh, jika dilihat dari aspek kejahatan di ranah media sosial, Indonesia masuk peringkat 13 di wilayah Asia Pasifik dan Jepang, dan sebanyak 72,87 persen dari penipuan dalam ranah media sosial tersebut, ternyata disebarkan sendiri oleh pengguna tanpa sadar.[6] Sementara, laporan dari Kantor Berita Radio Nasional (KBRN), menyebutkan bahwa pada kuartal kedua 2013, Indonesia adalah negara terbesar pertama sebagai asal serangan siber dunia dan negara dengan risiko siber tertinggi (38%), diikuti oleh China di urutan kedua (33%) dan Amerika Serikat di posisi ketiga (6,9%).[7]

Dalam kasus ancaman siber, berdasarkan analisis data sistem *monitoring traffic* ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*) tercatat bahwa insiden serangan di dalam dunia maya di Indonesia mencapai satu juta insiden dan akan cenderung mengalami peningkatan setiap harinya akibat kelemahan sistem dan aplikasi yang tidak diketahui. Dalam hal ini, institusi pemerintah juga tidak luput dari serangan siber di mana dalam kurun waktu 1998 - 2009 sebanyak 2.138 serangan telah dialamatkan terhadap *website domain* milik pemerintah. Serangan *Distributed Denial of Service* pada sistem *Domain Name Service* (DNS) CCTLD-ID yaitu domain .id terutama .co.id. Kasus lain juga menyangkut penyebaran *malware* dan *malicious code* yang disisipkan di dalam *file* dan *web site* serta *phising site*, spionase industri dan penyanderaan sumber daya informasi kritis, maupun *black campaign* partai politik atau penistaan keyakinan dan penyebaran kabar bohong (*hoax*) untuk tujuan provokasi politis serta rekayasa ekonomi. Akibat keterbatasan sumber daya dan akses terkait pemeriksaan oleh penegak hukum Indonesia kepada penyelenggara layanan asing di luar negeri, beberapa kasus tersebut belum dapat diatasi walaupun Undang-Undang ITE telah mengaturnya.[8]

Sementara dalam konteks global, intensitas serangan siber yang semakin tinggi, bisa dilihat dari serangkaian serangan siber seperti yang dilaporkan dari *The Telegraph UK*, di mana pada bulan Mei 2017 telah terjadi serangan *cyber WanaCrypt0r 2.0* atau yang biasa disebut sebagai virus *WannaCry* menyebar dengan cepat dalam skala masif sepanjang sejarah di tingkat global. Virus tersebut pada awalnya menyebar di Ukraina yang kemudian merembet ke 10 negara lainnya hanya dalam waktu kurang dari dua jam, termasuk Indonesia.[9] Bahkan virus ini kemudian meluas ke 99 negara di dunia.[10] Jika melihat *trend* global, negara-negara seperti Brazil, Rusia, India, China sudah meningkatkan keamanan *cyber security* mereka. Bahkan perang siber sudah banyak terjadi, sehingga sebagai sebuah negara, termasuk dalam hal ini Indonesia, juga perlu memelihara kedaulatan di ranah siber mengingat bahwa kekerahasiaan, komunikasi antara pejabat publik sekarang pun memasuki dunia digital.[11]

Hal ini menandakan bahwa kondisi dunia yang dihadapkan pada perang generasi keempat dan kelima ini pada akhirnya membutuhkan strategi penangkalan yang berbeda dari penanganan terhadap ancaman-

6 "Indonesia Butuh Badan Cyber Nasional", diakses 12 Maret 2018, http://www.majalahict.com/indonesia-butuh-badan-cyber-nasional/

7 CATRA, "Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional", *Majalah Setjen Wantannas*, Edisi VI (September 2016):16.

8 Ahmad Budi Setiawan, "Peran Government Chief Information Officer (GCIO) dalam Tata Kelola Keamanan Informasi Nasional", *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Indonesia*, Volume 2 No. 4 (2011): 395-442.

9 Sabrina Burhanuddin,"Membangun Strategi Pertahanan Cyber di ASEAN", *Majalah Masyarakat ASEAN*, Edisi 16 (September 2017):34.

10 Susetyo Dwi Prihadi, "Dihantam Ransomware, Indonesia Butuh Badan Siber Nasional". *CNN Indonesia*, diakses 12 Maret 2018, https://www.cnnindonesia.com/teknologi/20170515073309-185-214802/dihantam-ransomware-indonesia-butuh-badan-siber-nasional.

11 Iris Gera, "LIPI: Dibutuhkan Badan Cyber Nasional Indonesia", *VoA Indonesia*, diakses 12 Maret 2018, https://www.voaindonesia.com/a/lipi-dibutuhkan-badan-cyber-nasional-di-indonesia-/2591870.html

ancaman sebelumnya. Jika, konsep perang generasi sebelumnya bersifat konvensional dan lebih banyak melibatkan kontak fisik, maka konsep perang generasi keempat berada pada masyarakat yang saling terhubungkan (*networked*), bersifat lintas negara, dan berbasis informasi.[12]

Dalam rangka merespon berbagai peristiwa tersebut Indonesia kemudian membentuk Badan Siber dan Sandi Negara (BSSN) sebagai model institusi *cyber security* nasional. Terlebih mengingat bahwa identitas Indonesia sebagai salah satu negara berkembang yang memiliki tingkat populasi penduduk terbesar di dunia dan menjadi salah satu negara pengguna internet terbesar di dunia. Perkembangan jumlah pengguna internet meningkat pesat di mana pada periode Juni 2017 sebanyak 132,700,000 menjadi 143,260,000 pada 31 Maret 2019, atau mengalami pertumbuhan internet dari tahun 2000-2019 sebesar 7,063.[13]

Di Indonesia penerapan pertahanan siber sudah dilaksanakan pada masing-masing institusi atau lembaga nasional maupun swasta untuk melindungi sistem jaringan yang menopang infrastruktur kritis mereka. Namun, perlindungan secara nasional dalam kerangka kebijakan siber nasional belum diamanatkan dalam sebuah regulasi dalam bentuk perundang-undangan. Padahal beberapa negara telah menerapkan undang-undang terkait *cyber security* mengingat ketergantungan mereka akan teknologi informatika. Meskipun Indonesia telah mengeluarkan regulasi dan kebijakan tentang keamanan informasi melalui Undang-Undang ITE, untuk membangun pertahanan negara melalui *cyber security* tidak cukup dilaksanakan jika hanya berlandaskan pada undang-undang tersebut. Salah satu penyebabnya adalah pembagian fungsional pada masalah kewenangan dan otoritas yang berkewajiban dalam menanggulangi ancaman *cyber* seperti *cybercrime*, *cyberterrorism*, *cyber hacktivism* maupun *cyber warfare* yang masih belum jelas. Oleh sebab itu, Penulis di sini ingin mengetahui bagaimana tata kelola pembentukan kelembagaan Badan Siber dan Sandi Negara (BSSN) sebagai institusi pelaksana diplomasi siber yang menanganai permasalahan keamanan siber di Indonesia.

Perumusan Masalah

Tulisan ini akan menganalisis tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara (BSSN) melalui perumusan pertanyaan berikut:

1. Mengapa pemerintah Indonesia berinisiatif untuk membentuk Badan Siber dan Sandi Negara (BSSN) sebagai model institusi *cyber security* di Indonesia?
2. Bagaimana peran BSSN dalam menjaga keamanan siber di Indonesia?
3. Bagaimana peran Badan Siber dan Sandi Negara (BSSN) sebagai lembaga pelaksana diplomasi siber di Indonesia?

Metode Penelitian

Tulisan ini menggunakan pendekatan kualitatif yang mengacu pada makna, konsep, definisi, karakteristik, metafora, simbol, dan deskripsi dari suatu hal.[14] Penelitian kualitatif dilakukan melalui pencarian sebuah jawaban dengan memeriksa berbagai pengaturan sosial dan kelompok atau individu di suatu *setting* sosial. Dalam hal ini, penelitian kualitatif memahami lingkungan yang diteliti melalui simbol, ritual, struktur sosial, peran sosial, dan sebagainya.[15] Menurut Berg dkk., teknik kualitatif di sini memungkinkan

12 David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, "Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives", *Jurnal Penelitian Politik*, Volume 13 No. 1 (Juni 2016): 2.

13 Internet Wolr Stats, "Top 20 Countries with The Highest Number of Internet Users, diakses 8 Mei 2019, https://www.internetworldstats.com/top20.htm.

14 B.L. Berg, H. Lune, *Qualitative Research methods for The Social Sciences, ninth edition*, (England, Essex: Pearson Education Limited, 2017), 12.

15 Berg, dkk., *Qualitative Research methods*, 15.

peneliti untuk berbagi dalam pemahaman dan persepsi orang lain dan mengeksplorasi bagaimana orang menyusun dan memberi makna pada kehidupan sehari-hari.[16] Dalam teknik pengumpulan data di sini, penulis hanya menggunakan studi pustaka atau telaah pustaka dengan metode deskriptif dari sumber-sumber penelitian sebelumnya maupun data sekunder lainnya. Pustaka-pustaka tersebut berasal dari laporan tahunan maupun kajian yang dilakukan instansi pemerintah dan non-pemerintah, dokumen perjanjian internasional, majalah pemerintah, maupun berita-berita *online* yang masih relevan dengan masalah keamanan siber dan diplomasi siber, maupun peran dari BSSN sebagai institusi siber di Indonesia.

Kerangka Pemikiran

Teori Kelembagaan (Institutional Theory)

Menurut Scott *Institutional theory* ditujukan untuk memperdalam struktur sosial yang didasarkan pada proses yang terstruktur, termasuk skema, aturan, norma, dan rutinitas sebagai pedoman otoritatif untuk perilaku sosial. Akar teori ini telah memperkaya studi ilmu-ilmu sosial dan menggabungkan wawasan kreatif mulai dari Marx dan Weber, Cooley dan Mead, hingga Veblen dan Commons. Banyak dari karya ini, muncul pada akhir abad kesembilan belas dan awal abad kedua puluh, seperti munculnya teori neoklasik di bidang ekonomi, behavioralisme dalam ilmu politik, dan positivisme dalam sosiologi pada masa tersebut.[17]

Institusi merupakan aturan permainan dalam masyarakat atau, lebih formalnya, adalah kendala-kendala yang dirancang secara manusiawi yang membentuk interaksi manusia. Tujuan dari institusi adalah untuk menentukan cara permainan dimainkan, pada saat tujuan pemain atau organisasi adalah untuk memenangkan permainan melalui kombinasi keterampilan, strategi, dan koordinasi.[18]

Teori kelembagaan atau institusional menurut Nee dan Swedberg dapat dikonseptualisasikan sebagai sistem dominan yang meliputi elemen informal dan formal yaitu kebiasaan, keyakinan bersama, norma, dan aturan di mana terdapat aktor yang mengarahkan tindakan mereka ketika mereka mengejar kepentingan tertentu. Berdasarkan konsteks tersebut, institusi atau lembaga-lembaga adalah struktur sosial yang dominan yang menyediakan saluran untuk aksi sosial dan aksi kolektif dengan memfasilitasi dan melakukan penataan kepentingan aktor dan menegakkan hubungan agen utama. Nee dan Swedberg juga menjelaskan bahwa perubahan kelembagaan tidak hanya memperbaharui aturan formal, tetapi membutuhkan penataan kembali kepentingan, norma dan kekuasaan.[19]

Konsep Keamanan Siber (Cybersecurity)

Pada dekade kedua abad kedua puluh satu, prefix "*cyber*" telah melekat pada konsep-konsep seperti "*cyberculture*", "*cybersex*", dan"*cyberwar*", yang semuanya terkait dengan ranah media digital, *virtual reality*, dan internet. Dalam budaya populer, awalan dan imbuan berbagai kata terlihat samar-samar, seperti halnya dengan gerakan sastra "*cyberpunk*". Demikian pula, sejak munculnya internet, kata "*network*" telah menjadi metafora menonjol dan telah mengambil perhatian di hampir setiap disiplin ilmu kontemporer dan institusi besar. Seperti pada tahun 1948, prefix "*cyber*" ditemukan dalam istilah "*cybernetics*" yang digambarkan

16 Berg, dkk., *Qualitative Research methods*, 16.

17 W. Richard Scott, "Institutional Theory: Contributing to a Theoretical Research Program", dalam Ken G. Smith and Michael A. Hitt (eds), *Great Minds in Management: The Process of Theory Development*, (Oxford University Press, Oxford, 2004).

18 D.C. North, *Institutions, Institutional Change and Economic Performance*, (Cambridge University Press, Cambridge, 1990).

19 Victor Nee dan Richard Swedberg, "Economic Sociology and New Institutional Economics", dalam C. M´enard dan M. M. Shirley (eds.), *Handbook of New Institutional Economics*, pp. 789–818, (Netherland: Springer, 2005), 798.

sebagai "studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat". Namun, pada dasarnya, tujuan *cybernetics* adalah untuk mengembangkan bahasa dan teknik menyerang terkait dengan masalah kontrol dan komunikasi pada umumnya dan kemudian menjadi dasar untuk komputasi setelah Perang Dunia II. Seperti halnya istilah "*cyber*", istilah "*network*" sejak pertengahan abad kedua puluh juga telah ada, dan dalam era globalisasi di mana orang di seluruh dunia saling berhubungan melalui infrastruktur transportasi dan komunikasi, *network* atau jaringan merupakan sebuah material dan realitas metafora.[20]

Sementara itu, sejarah *cybersecurity* sebagai konsep sekuritisasi dimulai dengan disiplin Ilmu Komputer dan Informasi di mana yang pertama kali menggunakan *cybersecurity* adalah dalam laporan *Computer Science and Telecommunications Board (CSTB)* pada tahun 1991, di mana keamanan di era informasi dalam istilah "*security*" didefinisikan sebagai perlindungan terhadap pengungkapan yang tidak diinginkan, modifikasi, atau kerusakan data dalam suatu sistem dan juga untuk pengamanan sistem itu sendiri. Dalam hal ini ancaman dalam *cybersecurity* tidak hanya diakibatkan oleh agen atau aktor tertentu tetapi juga oleh sistem itu sendiri sehingga kemudian muncul istilah "*computer security*". Nissenbaum menunjukkan bahwa mayoritas ilmuwan komputer mengadopsi wacana teknis yang difokuskan pada pengembangan program yang baik dengan sejumlah *bug* dan sistem yang sulit ditembus oleh penyerang luar sehingga "*computer security*" bergeser ke "*cybersecurity*" di mana *cybersecurity* dapat dilihat sebagai "keamanan komputer" dan "sekuritisasi".[21]

Konsep *cybersecurity* ini kemudian berkembang di mana menurut Saco dan Deibert ancaman dari *cybersecurity* juga telah melanggar batas-batas negara sehingga mengancam secara internasional. Hal ini disebabkan oleh, adanya interaksi masyarakat melalui dunia maya yang semakin tinggi akibat kemajuan teknologi dan era informasi. Berbeda halnya pendapat dari Deibert yang menjelaskan bahwa *cybersecurity* didasari melalui empat wacana terpisah dengan benda rujukan, ancaman, pilihan kebijakan, dan perintah yang berbeda yaitu mencakup keamanan nasional, keamanan negara (terdiri ancaman eksternal terhadap kedaulatan negara serta ancaman internal terhadap keamanan rezim), keamanan swasta, dan keamanan jaringan. Pendapat tersebut didukung oleh Hansen dan Nissenbaum di mana dalam kasus keamanan siber mencakup hubungan antara "jaringan" dan "individu" serta objek *referen* kolektif manusia sehingga tidak ada wacana tentang keamanan swasta yang merupakan keamanan individu sebagai objek rujukan, melainkan bahwa wacana keamanan individu terkait dengan rujukan sosial dan politik.[22]

Konsep Diplomasi Siber

Seiring dengan adanya perkembangan zaman, Barrinha dan Renard menyebutkan bahwa diplomasi bukan hanya aktivitas yang melibatkan hubungan antar negara semata, tetapi juga melibatkan sejumlah aktor seperti *regional* dan *international organisation*, perusahaan multinasional, *sub-national actors*, *advocacy networks*, maupun individu yang berpengaruh. Lebih jauh, Barrinha dan Renard juga menyebutkan bahwa konsep diplomasi meluas pada kebijakan baru yang kemudian masuk ke area politik yang belum dipetakan seperti negosiasi iklim hingga meluas ke dalam isu-isu siber.[23]

20 Patrick Jagoda, "Speculative Security", Dalam Reveron, Derek S., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (eds), (Washington, D.C.: Georgetown University Press, 2012), 22.

21 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol. 53, No. 4 (2009): 1160.

22 Hansen dan Nissenbaum, "Digital Disaster," 1163.

23 Barrinha A, Renard T. Cyber-diplomacy: the making of an International society in the digital age. *Global Affairs*; (2017): 1-12. https://doi.org/10.1080/23340460.2017.1414924, Retrieved from http://www.tandfonline.

Menurut Barrinha dan Renard, diplomasi siber (*cyber diplomacy*) merupakan diplomasi yang dilakukan di ranah atau domain siber di mana sumber daya diplomatik dan kinerja fungsi diplomatik digunakan untuk mengamankan kepentingan nasional terkait dengan dunia maya yang dilakukan dalam format bilateral maupun multilateral. Dalam hal ini, agenda diplomatik yang menjadi isu utamanya mencakup isu *cyber security*, *cyber crime*, *confidence-building*, *internet freedom*, dan *internet governance*.

Diplomasi siber sendiri telah berkembang pesat dalam mendefinisikan dan merangkum upaya yang terus-menerus dilakukan untuk menyelesaikan jenis konflik baru yang terjadi di dunia maya. Dialog yang dijalankan antar aktor dalam kegiatan diplomasi merupakan salah satu jalan untuk meraih sebuah keuntungan bersama, begitu pula dengan peran utama diplomasi dunia maya yaitu menghasilkan keuntungan melalui dialog tentang masalah keamanan siber.[24]

Inisiatif Pembentukan Badan Siber dan Sandi Negara (BSSN) sebagai Model Institusi *Cybersecurity* di Indonesia

Adanya pola interaksi masyarakat digital dalam dunia maya, termasuk di dalamnya ada aktor individu, dunia usaha/swasta, pemerintah/representasi negara, kelompok-kelompok tertentu, telah melahirkan budaya digital di mana mereka seringkali bebas berkomunikasi dan berinteraksi. Tentu saja hal ini dapat memicu adanya gesekan kepentingan yang pada akhirnya akan menimbulkan konflik bahkan perang antar negara di ruang maya atau siber tersebut. Oleh sebab itu, di Indonesia sendiri lahir Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Di dalamnya telah diatur bagaimana mengoperasikan sistem elektronik yang disediakan baik oleh pihak swasta maupun pemerintah agar dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronis.

Di samping Undang-Undang ITE, selama ini *cyber security* Indonesia juga diawasi oleh *Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII)*, *Indonesia Computer Emergency Response Team (ID-CERT)*, dan Sub Direktorat *Cyber Crime* Direktorat Tingkat Pidana Ekonomi dan Khusus (Dittipideksus) Bareskrim Polri. Meski kebijakan tentang keamanan siber telah diatur melalui UU ITE, Indonesia juga menghadapi masalah pembagian kewenangan dan otoritas mana yang berkewajiban dalam menanggulangi *cyber crime*, *cyber terrorism*, *cyber hacktivism* maupun *cyber warfare*.

Dengan demikian, keberadaan BSSN sebagai lembaga baru pun menjadi penting untuk mengkoordinasikan tugas-tugas dari berbagai lembaga, khususnya yang menangani insiden siber tersebut. Mengingat bahwa dampak dari serangan siber (*cyber attack*) yang begitu luas, tidak hanya masalah kerugian ekonomi semata, tetapi juga hak individu sampai pada keutuhan dan kedaulatan negara, maka pembangunan pertahanan dan keamanan siber adalah sebuah kebutuhan dan keharusan guna menjaga keamanan nasional di Indonesia.[25]

Salah satu payung hukum yang menaungi Lembaga Sandi Negara sebagai cikal bakal dari pembentukan BSSN diatur dalam Keppres No. 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen (LPND) dengan tugasnya yaitu melaksanakan tugas pemerintahan di bidang persandian sesuai dengan ketentuan peraturan

com/loi/rgaf20.

24 Carmen Elena CÎRNU, "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy", *No. 17* (May-Jun, 2019), http://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/.

25 *CATRA*, "Dari Desk Cyberspace Nasional ",16.

perundang-undangan yang berlaku.[26] Sebelum dibentuknya Badan Siber Nasional yang berada di bawah Badan Inteligen Negara (BIN), melalui Setjen (Sekretariat Jenderal) Dewan Ketahanan Nasional (Wantannas) pada 30 Oktober 2013, dibentuklah Desk Keamanan Siber Nasional (*Desk* KSN) dan tertuang dalam Kajian Setjen Wantannas Nomor K-102/ Sesjen/X/2013 tentang Antisipasi dan Solusi Ancaman Terhadap Keamanan Siber dalam rangka memantapkan stabilitas nasional. Selanjutnya oleh Kemenko Polhukam usulan tersebut ditindaklanjuti dengan pembentukan *Desk* Ketahanan dan Keamanan Informasi *Cyber* Nasional (DK2ICN) pada 2014 berdasarkan Keputusan Menkopolhukam Nomor 24 Tahun 2014 tanggal 8 April 2014 tentang *Desk* Ketahanan dan Keamanan Informasi *Cyber* Nasional Tahun 2014.

DK2ICN diketuai oleh Deputi Bidang Koordinasi Komunikasi, Informasi, dan Aparatur Kemenko Polhukam RI Marsda TNI Agus Ruchyan Barnas dengan masa kerja selama dua belas bulan. Anggota DK2ICN melibatkan *multistakeholder* yang berasal dari Kementerian/Lembaga, praktisi, akademisi, lembaga swadaya masyarakat yang cinta tanah air, pakar, TNI, dan Polri. DK2ICN juga bekerja sama dengan Institut Teknologi Bandung (ITB) karena dianggap memiliki laboratorium yang mumpuni untuk mengkaji permasalahan *cyber*. DK2ICN adalah badan yang tidak terikat dengan kelompok mana pun. DK2ICN ini disiapkan sebagai embrio dari Badan *Cyber* Nasional (BCN). Selanjutnya, pada 2016, DK2ICN berubah nama menjadi *Desk Cyberspace* Nasional (DCN) dengan tujuan untuk mengantisipasi pembentukan BCN. Masa kerja DCN pun hanya dua belas bulan seperti DK2ICN dan berkedudukan di bawah Kemenko Bidang Polhukam RI. Tugasnya adalah menyelenggarakan koordinasi, sinkronisasi, dan pengendalian urusan kementerian dalam penyelenggaraan pemerintahan yang terkait dengan upaya membangun ketahanan dan keamanan *cyberspace* nasional sesuai ketentuan perundang-undangan.[27]

Namun demikian, TNI di bawah Kementerian Pertahanan Indonesia, pada 2016 juga berinisiatif membentuk Badan *Cyber* TNI untuk mengamankan aset militer seperti pengamanan misil dan pemantauan kapal asing yang masuk wilayah Indonesia tanpa izin melalui satelit. Tugas dan fungsi Badan *Cyber* TNI ini berbeda dari yang akan dibentuk polhukam.[28] Dalam rangka menghadapi ancaman pertahanan yang memanfaatkan perkembangan teknologi informasi, TNI meresmikan terbentuknya Satuan Siber (Satsiber) TNI. Berdasarkan Peraturan Presiden (Perpres) No.62 Tahun 2016 tentang Perubahan atas Perpres No. 10 Tahun 2010 tentang Susunan Organisasi TNI, Sat siber TNI dipimpin Komandan Satsiber TNI atau Dansatsiber TNI yang berkedudukan dan bertanggung jawab kepada Panglima TNI.

Di dunia militer, keberadaan tentara siber sudah menjadi kebutuhan. Hal ini bisa dilihat dari tentara siber negara lain yang sudah memiliki lembaga antara lain Korea Utara yang mendirikan Biro 121, Tentara Pembebasan Rakyat (PLA) China dengan Unit 61398, Singapura yang membentuk Organisasi Siber Pertahanan (DCO) dengan melibatkan 2.600 tentara khusus, serta Australia yang membentuk Unit Perang Siber. Satsiber TNI dituntut untuk mampu menjamin terwujudnya ketahanan siber TNI dalam rangka mendukung pelaksanaan tugas pokok TNI. Salah satunya adalah untuk melindungi sumberdaya informasi di lingkungan TNI dari gangguan dan penyalahgunaan maupun

26 Ahmad Budiman, "Optimalisasi Peran Badan Siber dan Sandi Nasional", *Majalah Info Singkat Pemerintahan Dalam Negeri*, Vol. IX, No. 12, 2 (Juni 2017): 18.

27 *CATRA*, "Dari Desk Cyberspace Nasional," 17.

28 "TNI Pastikan Tetap Membentuk Badan Cyber", *CISSREC*, diakses 12 Maret 2018, https://www.cissrec.org/publications/detail/42/TNI-Pastikan-Tetap-Membentuk-Badan-Cyber.html

pemanfaatan oleh pihak-pihak lain. Beragam perubahan sebagai akibat perkembangan teknologi informasi dan komunikasi mengharuskan TNI memiliki kemampuan pertahanan siber untuk peningkatan daya tangkal dan pencegahan perang atau serangan siber terhadap TNI. Indonesia sebagai salah satu negara yang terdampak akibat serangan "teroris siber" belum lama ini. Komisi I DPR merespons positif terbentuknya Satsiber TNI. Pasalnya saat ini tengah berlangsung perang yang bertujuan membuat orang Indonesia lebih pro-asing ketimbang bangsa sendiri. Pelurunya berupa opini dan neo-propaganda yang dilancarkan di berbagai media sosial. TNI sebagai salah satu alat negara dituntut mampu melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Keberadaan Satsiber TNI berbeda dengan Badan Siber dan Sandi Negara (BSSN) yang berada di bawah Kemenko Polhukam. Satsiber TNI secara umum akan melakukan tugas pengamanan melalui ruang siber seperti mengamankan aset militer dari ancaman misil dan pemantauan kapal asing yang masuk wilayah Indonesia tanpa izin melalui satelit.[29]

Dengan adanya permasalahan terhadap penanganan *cyber-security* dalam kerangka pertahanan negara yang masih bersifat sektoral dan belum terkoodinasi serta belum terpadu, pada akhirnya, mendorong pemerintah untuk membentuk Badan Siber dan Sandi Negara pada 19 Mei 2017 melalui Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN). Beberapa lembaga lain yang memiliki kepentingan dalam area pertahanan kemanan nasional termasuk lingkup *cyber* disinergikan di bawah BSSN ini. Kementerian Pertahanan, TNI, Polri, BIN, Kemenkominfo, Lembaga Sandi Negara, dan berbagai instansi terkait lainnya adalah lembaga-lembaga pemerintah yang perlu disinergikan untuk menangkis, menangkal, dan mencegah serangan *cyber* baik yang dilakukan oleh *state* maupun *non-state actor* yang berasal dari dalam negeri maupun negara lain.

Tata Kelola Keamanan Siber Indonesia di Bawah Kelembagaan BSSN

Pembentukan BSSN yang sebelumnya merupakan Lembaga Sandi Negara, membutuhkan proses transformasi sehingga menjadi sebuah lembaga yang kredibel dan sebagai pilar keamanan siber di Indonesia. Proses transformasi ini tertuang dalam Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019 yang terdiri dari 7 tahapan tema, yaitu:[30]

a. Tahap tema yang pertama yaitu Integrasi Organisasi (*Organization Integration*) yang ditujukan untuk menghadapi tantangan terkait integrasi, internalisasi, dan harmonisasi organisasi dalam rangka membentuk fondasi organisasi yang kuat.
b. Tahapan tema yang kedua yaitu Sistem dan Pengembangan Standar (*system and standard development*) sebagai *roadmap* dalam mengembangkan keamanan siber pemerintahan (*secured cyber government*) dan keamanan siber negara (*secured cyber nation*).
c. Tahapan tema yang ketiga yaitu Akuisisi Kemampuan (*Capabilities Acquisition*) sehingga menciptakan SDM siber yang berkualifikasi dan tersertifikasi secara internasional, di samping juga melakukan akuisisi dan pembaharuan infrastruktur, sarana, prasarana, fasilitas, dan teknologi di bidang keamanan siber.
d. Tahapan tema yang keempat yaitu Penerimaan dan Operasional (*Acceptance and Operational*) dalam rangka menciptakan kesadaran penerimaan di seluruh

29 Bentuk Satuan Siber, TNI siap Hadapi Serangan di Dunia Maya", *Koran Sindo*, diakses 12 Maret 2018, https://nasional.sindonews.com/read/1248299/14/bentuk-satuan-siber-tni-siap-hadapi-serangan-di-dunia-maya-1507966324

30 Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019*, 6-8.

Kementerian/Lembaga Pemerintah Non Kementerian dan sektor swasta (*private sector*) tentang perlunya keamanan siber di Indonesia serta terbentuknya protokol keamanan siber yang tersinergi dan terkoordinasi sehingga operasi berjalan dengan lancar.

e. Tahapan tema yang kelima yaitu Pencapaian Skala Nasional (*Nation-Wide Achievement*) yaitu dengan menambah dan memperbaharui infrastruktur dan keamanan siber dan sandi daerah serta melakukan implementasi keamanan siber dan sandi di provinsi dan kabupaten/kota.
f. Tahapan tema yang keenam yaitu Keamanan Siber Nasional (*Secured Cyber Nation*) dalam artian memberikan pemahaman kepada masyarakat sehingga tercipta kesadaran yang tinggi tentang keamanan siber.
g. Tahapan tema yang ketujuh yaitu Tolak Ukur dan Praktek Terbaik (*Best Practices and Benchmark*) yaitu dengan menjalankan praktek-praktek terbaik di bidang keamanan siber di lingkup ASEAN, Asia, dan global.

Hadirnya BSSN sebagai institusi siber nasional di sini berperan dalam menjalin koordinasi dan kerjasama antara institusi dan pemangku kepentingan di bidang siber di Indonesia, yang meliputi Kepolisian Republik Indonesia (*cyber crime*), TNI/Kementerian Pertahanan (*cyber defense*), Kementerian Luar Negeri (*cyber diplomacy*) dan Kementerian Komunikasi dan Informatika, serta lembaga-lembaga lainnya.[31]

Kelembagaan Badan Siber dan Sandi Negara dapat dilihat dalam struktur organisasi yang menjalankan fungsi berikut:

1. *The Strategyc Apex* yang berfungsi untuk menyusun visi, misi, tujuan dan rencana strategis di level organisasi, yang terdiri dari Kepala BSSN, Wakil Kepala BSSN, Sekretaris Utama, Deputi Bidang Identifikasi dan Deteksi, Deputi Bidang Proteksi, Deputi Bidang Penanggulangan dan Pemulihan, dan Deputi Bidang Pemantauan dan Pengendalian.
2. *The Middle Line* yaitu sebagai penghubung antara strategis manajemen terkait dengan visi, misi, tujuan dan rencana strategis organisasi.
3. *The Techno Structure* yang berfungsi untuk memberikan dukungan teknis terkait dengan visi, misi, tujuan dan rencana strategis organisasi.
4. *The Operating Core* yang berfungsi melaksanakan tugas inti guna mencapai visi, misi, tujuan dan rencana strategis organisasi.
5. *The Supporting Staff* yang memberikan jasa pendukung tidak langsung kepada organisasi.

Secara umum, tugas BSSN yaitu melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Untuk mewujudkan tugas tersebut, dalam hal ini BSSN memiliki beberapa fungsi yaitu:[32]

- menyusun kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber;
- melaksanakan kebijakan teknis yang telah disusun;
- melakukan pemantauan dan evaluasi terhadap kebijakan teknis yang telah disusun;

31 Badan Siber dan Sandi Negara, *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019*, 11.

32 "Tugas dan Fungsi BSSN", *BSSN*, diakses 26 Juni 2019, https://bssn.go.id/tugas-dan-fungsi-bssn/.

- mengoordinasikan kegiatan fungsional dalam pelaksanaan tugas BSSN dan sebagai wadah koordinasi bagi semua pemangku kepentingan;
- melaksanakan pembinaan dan pemberian dukungan administrasi kepada seluruh unit organisasi di lingkungan BSSN;
- melakukan pengawasan atas pelaksanaan tugas BSSN;
- melaksanakan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN; dan
- melaksanakan kerjasama nasional, regional, dan internasional dalam urusan keamanan siber

Selama ini BSSN telah menjalankan fungsi yaitu melakukan pembinaan terhadap komunitas keamanan siber. Hal ini diwujudkan pada kegiatan *Community Building and Information Sharing* Sektor Ekonomi Digital yang dihadiri oleh Pejabat Tinggi dari BSSN, Bais TNI, Bareskrim Polri, Bainstranas Kemhan, BIN, serta komunitas keamanan siber.[33] Kegiatan tersebut merupakan salah satu bentuk pelaksanaan fungsi BSSN dalam mengoordinasikan kegiatan fungsional dalam upaya kolaborasi, koordinasi, sinergi, dan *sharing* informasi.

Pelaksanaan Diplomasi Siber di Indonesia melalui Peran Badan Siber dan Sandi Negara (BSSN)

Sifat dunia maya yang asimetris dan transnasional, menjadi bagian penting dari diplomasi dan konflik militer antar negara karena dapat menimbulkan ketidaksepakatan diplomatik akibat adanya kepentingan nasional dan posisi politik negara yang saling berbenturan.[34] Dalam hal ini, internet telah membawa dimensi baru pada keamanan informasi dan siber, yang pada akhirnya memberikan implikasi terhadap hubungan internasional, di mana apa pun yang dikirim melalui internet, berpotensi untuk dapat disebarluaskan dengan bebas.[35] Dengan demikian, Perkembangan TIK memberi tekanan yang signifikan pada negara dalam mengembangkan kapasitas yang kuat untuk memahami potensi teknologi digital serta merancang strategi pengarusutamaan maupun menyesuaikannya dengan tujuan kebijakan jangka pendek dan jangka panjang.[36]

Salah satu lembaga di Indonesia yang berperan sebagai lembaga pelaksana diplomasi siber, disamping oleh Kementerian Luar Negeri adalah Badan Siber dan Sandi Negara (BSSN). Fungsi sebagai pelaksana diplomasi siber itu sendiri melekat pada Deputi II bidang Proteksi yang mempunyai tanggung jawab yaitu di bidang tata kelola keamanan informasi dari peralatan, alat pendukung, manajemen kunci, frekuensi, jaringan intra, serta audit keamanan informasi dilakukan serta fungsi diplomasi siber dan *focal point* kerjasama.[37]

Mengutip pendapat dari Indra Rosandry bahwa diplomasi siber di Indonesia dapat berjalan efektif dengan adanya beberapa aspek berikut.[38] ***Pertama***, adanya ancaman siber yang memiliki kompleksitas dan lintas negara, membutuhkan sebuah kemitraan atau kerjasama internasional dengan negara lain karena posisi

33 Biro Hukum dan Humas BSSN, "BSSN Selenggarakan Community Building and Information Sharing Sektor Ekonomi Digital", 30 April 2019, diakses 26 Juni 2019, https://bssn.go.id/bssn-selenggarakan-community-building-and-information-sharing-sektor-ekonomi-digital/.

34 Chotimah, "Membangun Pertahanan dan Keamanan Nasional," 118.

35 Nicholas Westcott, Digital Diplomacy: The Impact of the Internet on International Relations. *Research Report 16*, (July 2008):14.

36 Corneliu Bjola, "Trends and Counter-Trends in Digital Diplomacy," *Working Paper Project*, "Diplomacy in the 21st Century", No. 18, (September 2017): 8.

37 Satriyo wibowo,"BSSN dan Peta Keamanan Siber Indonesia", Senin, 5 Maret 2018, diakses pada 26 Juni 2019, https://inet.detik.com/cyberlife/d-3899799/bssn-dan-peta-keamanan-siber-indonesia.

38 Indra Rosandry, "Merajut Diplomasi Siber Indonesia", Kamis, 22 November 2018, diakses pada 26 Juni 2019, https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia.

strategis Indonesia sebagai salah satu negara pengguna internet terbesar di dunia menjadi penarik bagi negara *major powers* di bidang siber. ***Kedua***, kerjasama tidak hanya dilakukan dengan negara lain semata, tetapi juga perlu melibatkan berbagai unsur di tingkat nasional baik dari kalangan masyarakat maupun swasta. ***Ketiga***, dalam rangka menegaskan orientasi politik luar negeri dan diplomasi Indonesia, strategi di bidang siber memiliki peranan yang sangat vital. Dalam hal ini, dengan dibentuknya BSSN sebagai pelaksana fungsi diplomasi siber maupun keamanan siber menjadi catatan positif dalam upaya mencapai ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber, dan keamanan siber pada ekonomi digital. Selain itu, hal ini juga menjadi modal dalam menyikapi 'adu kekuatan' antara negara-negara besar di bidang *global cyber governance*.

Diplomasi Siber Indonesia dalam Kerangka Kerjasama Bilateral

Pemerintah Indonesia melalui Badan Siber dan Sandi Negara (BSSN) telah membentuk kesepakatan bilateral dalam ranah siber dengan Kementerian Luar Negeri Kerajaan Belanda pada 3 Juli 2018. Sebelumnya Indonesia pada bulan Agustus 2018 juga telah menandatangani kerjasama dengan Australia dan Kerajaan Inggris Raya dalam bidang siber. Kerjasama bilateral yang dilakukan dengan Australia tidak hanya menyangkut tentang keamanan siber semata tetapi juga masalah ekonomi digital. Sementara cakupan kerjasama dengan Belanda diantaranya adalah berbagi informasi dalam bidang hukum, perundang-undangan, kebijakan nasional, dan strategi kebijakan manajemen yang terkait dengan ranah siber; penguatan kapasitas dan perbantuan kelembagaan serta pengembangan teknologi di bidang keamanan siber melalui jejaring dan program pelatihan dan pendidikan, pertukaran kunjungan pejabat tinggi, analis dan pelaksana lapangan, seminar dan konferensi; elaborasi upaya bersama dalam membangun ketahanan terhadap serangan siber dan perlindungan terhadap aset vital di ranah siber.

Selain menjalin kerjasama bilateral dengan beberapa negara yang disebutkan di atas, pemerintah Indonesia juga menjalin kerjasama dengan pemerintah Amerika Serikat pada 28 September 2018 dengan tujuan untuk memajukan kerjasama dan pembangunan kapasistas di ruang siber dalam bidang-bidang seperti dikusi tentang pengembangan strategi ruang siber nasional; kemampuan manajemen insiden nasional; kapasitas dan kerjasama penanggulangan kejahatan siber; kemitraan dengan banyak pemangku kepentingan; penggalakan kesadaran akan keamanan siber dan kerjasama di berbagai forum kawasan sesuai kebutuhan.

Diplomasi Siber Indonesia dalam Kerangka Kerjasama Multilateral

Pada dasarnya pelaksanaan diplomasi siber Indonesia dalam kerangka kerjasama multilateral dapat dilihat dalam *ASEAN Regional Forum* (ARF) melalui *ASEAN Political-Security Community* (APSC) dalam Sub Bab B.4.1. Bab tersebut berisi tentang kesepakatan peningkatan kerjasama dalam hal ancaman non tradisional, lebih khususnya lagi menyangkut persoalan kejahatan transnasional dan lintas batas. Sementara pembahasan mengenai kejahatan siber dijelaskan dalam Pasal XVII. Dalam hal ini, pada tahun 2006 ARF membentuk ARF *on cybersecurity initiatives* terkait pembahasan kejahatan siber di ASEAN yang kemudian dituangkan dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime*. Komitmen dalam menjaga keamanan siber di kawasan ini terlihat pada beberapa pertemuan seperti *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC), *ASEAN Telecommunications Regulators Council* (ATRC), *ASEAN Senior Officials Meeting on Transnational Crime*

(SOMTC), dan *Senior Officials Meeting on Social Welfare and Development* (SOMSWD).[39]

Pelaksanaan diplomasi siber Indonesia melalui ARF *on cybersecurity initiatives* salah satunya adalah dengan diperolehnya *point of contacts* (kontak poin) perwakilan negara-negara ASEAN dan beberapa negara di kawasan regional yang menangani masalah *cybersecurity* seperti Tiongkok, Belanda, Rusia, AS, dan Australia. Kontak poin ini dituangkan dalam dokumen *ASEAN Regional Forum* (ARF) *Workplan on Security of and in the Use of Information and Communications Technologies* (ICT's). Tujuannya adalah mempermudah pemerintah Indonesia untuk melakukan proses diplomasi siber termasuk dalam penanganan insiden siber, maupun hal lain yang terkait pencapaian tujuan bersama. Lebih lanjut, kontak poin yang didapatkan bukan sebatas nama instansi atau nomor telpon instansi, namun juga nomor pribadi maupun email pribadi pejabat berwenang.[40]

Kontak poin yang dituangkan dalam ARF tersebut dapat dimanfaatkan oleh pemerintah Indonesia dalam mengidentifikasi aktor dibalik kejahatan siber sehingga tindakan dan keputusan yang diambil pun tepat. Misalnya apabila terjadi serangan siber di Indonesia oleh Malaysia maka yang perlu dilakukan pemerintah adalah mengidentifikasi siapa aktor atau pelaku utama dari peristiwa tersebut dengan mengklarifikasi melalui kontak poin yang ada, apakah dilakukan oleh individu, kelompok terorganisir atau bahkan negara. Tujuannya adalah adanya koordinasi dengan negara lain untuk menghindari kesalahan fatal dalam merespons serangan-serangan siber tersebut, sehingga masing-masing pihak dapat menahan diri dan tidak saling menyerang.[41]

Selain kegiatan-kegiatan di atas, Indonesia bersama dengan Anggota ASEAN lainnya yaitu Brunei Darussalam, Myanmar, Kamboja, Laos, Filipina, Singapura, Malaysia, Vietnam dan Thailand juga tergabung dalam ASEAN Cyber Capacity Program (ACCP) yang diresmikan pada April 2017. Rezim ini terbentuk atas dasar kesadaran bersama negara-negara ASEAN dalam menghadapi berbagai ancaman siber mengingat bahwa Asia Tenggara merupakan salah satu kawasan yang sedang mengalami pertumbuhan ekonomi digital yang cukup siginifikan sehingga menjadi sasaran serangan siber. ACCP sendiri bertujuan untuk meningkatkan kesadaran dan sebagai wadah forum diskusi regional mengenai norma siber, peningkatan koordinasi regional mengenai kemampuan dan respons insiden siber, membangun kemampuan regional dalam pengembangan strategi dan legislasi siber, serta berkontribusi terhadap upaya global untuk mengembangkan serangkaian standar keamanan siber untuk *Internet of Things* (IoT).[42]

Sementara itu, Indonesia melaui BSSN, juga berkontribusi dalam menggelar ASEAN-JAPAN *Cyber Exercise* secara *online* serentak di 10 negara ASEAN dan Jepang. Kegiatan tersebut merupakan perwujudan kolaborasi bersama negara-negara ASEAN dan Jepang dalam menghadapi berbagai isu di ranah siber seperti penanganan insiden, *capacity building*, *sharing* informasi, dan membangun kesadaran keamanan informasi dari masing-masing negara anggota ASEAN dan Jepang.[43]

Kerjasama di bidang multilateral juga tercermin dari peran serta BSSN yang menjadi delegasi Indonesia bersama beberapa intansi lain dalam kegiatan *18th International Institute for Strategic Studies (IISS) Shangri-La Dialogue* yang berlangsung di Singapura pada tanggal

39 David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, "Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives", *Jurnal Penelitian Politik*, Volume 13 No. 1 (Juni 2016): 4-5.

40 Setyawan dan Sumari, "Diplomasi Pertahanan Indonesia", 11.

41 Setyawan dan Sumari, "Diplomasi Pertahanan Indonesia",12.

42 Strategi, Kebijakan, dan Praktik Siber", diakses 19 Agustus 2019, http://apdf-magazine.com/id/strategi-kebijakan-dan-praktik-siber/

43 "ASEAN-JAPAN Online Cyber Exercise", (20 Juni 2019), diakses 26 Juni 2019, https://bssn.go.id/asean-japan-online-cyber-exercise/.

31 Mei 2019 hingga 2 Juni 2019. Forum dialog tersebut juga dihadiri oleh perwakilan delegasi dari 30 negara. Salah satu tema yang menjadi isu kajian forum ini membahas mengenai isu *Cyber-Capability Development: Defence Implications*.[44]

Penutup

Menelaah kembali posisi strategis Indonesia bagi negara-negara *major power* di bidang siber, menjadikan kebutuhan perlunya kelembagaan siber yang membidangi aspek keamanan siber maupun diplomasi siber. Oleh sebab itu, tidak salah Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) yang merupakan transformasi dari Lembaga Sandi Negara. BSSN berperan dalam menjalin koordinasi dan kerjasama antara institusi dan pemangku kepentingan di bidang siber baik lingkup nasional maupun internasional. Dalam konteks ini, BSSN sebagai salah satu lembaga pelaksana diplomasi siber Indonesia telah menjalin kerjasama secara bilateral dengan beberapa negara seperti Australia, Kerajaan Inggris Raya, Kerajaan Belanda maupun Amerika Serikat. Sementara di tingkat regional, Indonesia juga ikut terlibat dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime* dan ASEAN Cyber Capacity Program (ACCP). Upaya-upaya diplomasi tersebut dilakukan untuk menjaga keamanan dan kedaulatan siber Indonesia dengan melibatkan peran serta dari BSSN sebagai institusi siber nasional.

44 "BSSN sebagai Pembicara dalam Forum Strategis Keamanan Global Asia Pasifik (Shangri-La Dialogue)", (20 Juni 2019), diakses 26 Juni 2019, https://bssn.go.id/bssn-sebagai-pembicara-dalam-forum-strategis-keamanan-global-asia-pasifik-shangri-la-dialogue/.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019.

Barrinha A, Renard T. "Cyber-diplomacy: the making of an International society in the digital age". *Global Affairs*, (2017). https://doi.org/10.1080/23340460.2017.1414924, Retrieved from http://www.tandfonline.com/loi/rgaf20.

"Bentuk Satuan Siber, TNI siap Hadapi Serangan di Dunia Maya". *Koran Sindo*. Diakses 12 Maret. 2018https://nasional.sindonews.com/read/1248299/14/bentuk-satuan-siber-tni-siap-hadapi-serangan-di-dunia-maya-1507966324.

Berg, B.L. dan H. Lune, *Qualitative Research methods for The Social Sciences, ninth edition*, England, Essex: Pearson Education Limited, 2017.

Biro Hukum dan Humas BSSN. "BSSN Selenggarakan Community Building and Information Sharing Sektor Ekonomi Digital". Diakses 26 Juni 2019. https://bssn.go.id/bssn-selenggarakan-community-building-and-information-sharing-sektor-ekonomi-digital/.

Bjola, Corneliu. "Trends and Counter-Trends in Digital Diplomacy". *Working Paper Project*, "Diplomacy in the 21st Century", No. 18 (September 2017).

Budiman, Ahmad. "Optimalisasi Peran Badan Siber dan Sandi Nasional". *Majalah Info Singkat Pemerintahan Dalam Negeri*, Vol. IX, No. 12/II, Puslit, Juni 2017.

Burhanuddin, Sabrina. "Membangun Strategi Pertahanan Cyber di ASEAN". *Majalah Masyarakat ASEAN*, Edisi 16 September 2017.

CATRA. "Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional". *Majalah Setjen Wantannas*, Edisi VI September 2016.

Chotimah, Hidayat Chusnul. "Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia". *Jurnal Diplomasi*, Volume 7 No. 4 (Desember, 2015).

Choucri, Nazli dan Daniel Goldsmith. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security". *Buletin of the Atomic Scientists*, 68, No. 2 (2012).

CÎRNU, Carmen Elena. "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy", *No. 17* (May-Jun, 2019), http://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/.

Gera, Iris. "LIPI: Dibutuhkan Badan Cyber Nasional Indonesia". *VoA Indonesia*. Diakses 12 Maret 2018. https://www.voaindonesia.com/a/lipi-dibutuhkan-badan-cyber-nasional-di-indonesia-/2591870.html

Hansen, Lene dan Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*, Vol. 53, No. 4 (2009).

Jagoda, Patrick. "Speculative Security". Dalam Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (eds). Washington, D.C.: Georgetown University Press, 2012.

Nee, Victor dan Richard Swedberg. "Economic Sociology and New Institutional Economics". Dalam C. M´enard dan M. M. Shirley (eds.), *Handbook of New Institutional Economics*. Netherland: Springer, 2005.

North, D.C. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990.

Prihadi, Susetyo Dwi. "Dihantam Ransomware, Indonesia Butuh Badan Siber Nasional". *CNN Indonesia*. Diakses 12 Maret 2018. https://www.cnnindonesia.com/teknologi/20170515073309-185-214802/dihantam-ransomware-indonesia-butuh-badan-siber-nasional.

Rosandry, Indra. "Merajut Diplomasi Siber Indonesia". Kamis, 22 November 2018. Diakses pada 26 Juni 2019. https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia.

Sa'diyah, Nur Khalimatus dan Ria Tri Vinata. "Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara". *Perspektif*, Volume XXI No. 3 (September 2016).

Scott, W. Richard,. "Institutional Theory: Contributing to a Theoretical Research Program". Dalam Ken G. Smith and Michael A. Hitt (eds), *Great Minds in Management: The Process of Theory Development*. Oxford: Oxford University Press, 2004.

Setiawan, Ahmad Budi. "Peran Government Chief Information Officer (GCIO) dalam Tata Kelola Keamanan Informasi Nasional". *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Indonesia*, Volume 2, No. 4 (2011).

Setyawan, David Putra dan Arwin Datumaya Wahyudi Sumari. "Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives". *Jurnal Penelitian Politik*, Volume 13 No. 1 (Juni 2016).

"Indonesia Butuh Badan Cyber Nasional". *Majalah ICT*. Diakses 12 Maret 2018. http://www.majalahict.com/indonesia-butuh-badan-cyber-nasional/.

"TNI Pastikan Tetap Membentuk Badan Cyber". *CISSREC*. Diakses 12 Maret 2018. https://www.cissrec.org/publications/detail/42/TNI-Pastikan-Tetap-Membentuk-Badan-Cyber.html.

Westcott, Nicholas. "Digital Diplomacy: The Impact of the Internet on International Relations". *Research Report 16*, (July 2008).

Wibowo, Satriyo. "BSSN dan Peta Keamanan Siber Indonesia". 5 Maret 2018. Diakses 26 Juni 2019. https://inet.detik.com/cyberlife/d-3899799/bssn-dan-peta-keamanan-siber-indonesia.

"Tugas dan Fungsi BSSN". *BSSN*. 20 Juni 2019. Diakses 26 Juni 2019. https://bssn.go.id/tugas-dan-fungsi-bssn/

"Strategi, Kebijakan, dan Praktik Siber", 20 Juni 2019. Diakses 19 Agustus 2019, http://apdf-magazine.com/id/strategi-kebijakan-dan-praktik-siber/

"ASEAN-JAPAN Online Cyber Exercise", 20 Juni 2019, diakses 26 Juni 2019, https://bssn.go.id/asean-japan-online-cyber-exercise/

"BSSN sebagai Pembicara dalam Forum Strategis Keamanan Global Asia Pasifik (Shangri-La Dialogue)", 20 Juni 2019, diakses 26 Juni 2019, https://bssn.go.id/bssn-sebagai-pembicara-dalam-forum-strategis-keamanan-global-asia-pasifik-shangri-la-dialogue/.