INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 5 Tahun 2023 Page 8917-8931
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Diplomasi Indonesia Masa Pemerintahan Presiden Joko Widodo di Isu Siber

Yustika Citra Mahendra[1✉]
Hubungan Internasional, Fakultas Ilmu sosial dan Ilmu Politik,
Universitas Brawijaya, Malang, Indonesia
Email: masmahe@ub.ac.id[1✉]

Abstrak

Penelitian ini memaparkan salah satu praktek diplomasi kontemporer yang dilakukan oleh negara dengan isu siber. Penelitian ini diawali dengan memaparkan konteks siber sebagai salah satu fenomena yang terkait dengan perkembangan teknologi informasi internet yang mempengaruhi keamanan yang memungkinkan terdapatnya ancaman kejahatan berbasis siber atau disebut juga *Cybercrime* dalam permasalahan ini peran diplomasi sebuah negara menjadi salah satu hal yang perlu dilakukan mengingat isu Cyber menjadi masalah Global. Permasalahan siber menjadi salah satu hirauan penting bagi sebuah negara mengingat aktivitas manusia saat ini erat kaitannya dengan dunia digital Pada data tim Indonesia Security Incident Responses on the Internet Infrastructure Coordinator Center mendapati kasus serangan siber sebanyak 205 juta serangan cyber pada tahun 2017. Penelitian ini mencoba mengulas praktek diplomasi siber yang dilakukan oleh Indonesia sebagai upaya peningkatan kapabilitas inptek dan inovasi di era pemerintahan Joko Widodo dengan memberikan gambaran komperhensif mengenai beberapa aspek seperti kepentingan nasional indonesia dalam isu siber, hal yang dilakukan pada agenda siber secara umum dan juga para aktor diplomasi yang melakukan aktivitas diplomasi ditulis dengan melakukan penjabaran dengan temuan pemetaan konteks siber dalam kepentingan negara Khususnya Indonesia di era Presiden Joko Widodo melalui aktivitas diplomasi dalam isu Cyber.

Kata Kunci : *Cyber Diplomacy, Cyber Issues, National Interest*

Abstract

This research describes one of the contemporary diplomatic practices carried out by countries with cyber issues. This research begins by explaining the context of cyber as one of the phenomena related to the development of internet information technology which affects security which allows the threat of cyber-based crime or also called cybercrime. In this problem the role of a country's diplomacy is one of the things that needs to be done considering that cyber issues are Global problems. Cyber problems have become an important concern for a country considering that human activities are currently closely related to the digital world. Data from the Indonesian Security Incident Responses on the Internet Infrastructure Coordinator Center team found that there were 205 million cyber attacks in 2017. This research tries to review cyber diplomacy practices carried out by Indonesia as an effort to increase technological and innovation capabilities in the Joko Widodo government era by providing a comprehensive overview of several aspects such as Indonesia's national interests in cyber issues, things being done on the cyber agenda in general and also diplomatic actors carrying out activities Diplomacy is written by elaborating on the findings of mapping the cyber context in the interests of the state, especially Indonesia in the era of President Joko Widodo through diplomatic activities on cyber issues.

Keywords: *Cyber Diplomacy, Cyber Issues, National Interest*

PENDAHULUAN

Laju perkembangan globalisasi yang semakin cepat setiap harinya berdampak pada berbagai sektor dalam dan luar negeri. Kemudahan akses, percepatan informasi serta efektifitas waktu merupakan beberapa contoh dari buah manis peningkatan teknologi (Primawanti & Pangestu. 2020:1-15)

Namun tidak hanya membawa dampak baik, teknologi juga dapat menjadi sebuah ancaman yang nyata. Penggunaan teknologi informasi yang masif tidak menutup kemungkinan datangnya ancaman kejahatan berbasis siber (*cybercrime*). *Cybercrime* ini tidak hanya mengancam bagian-bagian utama dari negara seperti pemerintah, namun juga mengancam pihak swasta bahkan hingga pada level individu. Tim Indonesia *Security Incident Response on the Internet Infrastructure Coordinator Center* mencatat bahwa selama tahun 2017 Indonesia mengalami sekitar 205 juta serangan *cyber*. Sementara itu, data Kementerian Komunikasi dan Informatika menunjukkan bahwa lembaga kesehatan, keuangan, pendidikan, dan pemerintahan adalah yang paling banyak rentan menjadi sasaran serangan *cyber*. Disinilah isu *cybersecurity* mulai menjadi perhatian baik bagi pihak individu, swasta hingga negara. PBB melalui ITU (*International Telecommunication Union*) merilis indikator-indikator yang menentukan sejauh mana komitmen negara perihal *cybersecurity*. Indeks yang disebut *Global Cybersecurity Index* (GCI) ini memiliki lima pilar

indikator.

1. *Legal*: Mengukur hukum dan regulasi negara terkait *cybercrime* dan *cybersecurity*
2. *Technical*: Mengukur implementasi kemampuan teknis melalui agen nasional dan sektor spesifik.
3. *Organizational*: Mengukur strategi nasional dan organisasi yang mengimplementasikan *cybersecurity*
4. *Capacity Development*: Mengukur kampanye *awareness*, pelatihan dan pendidikan untuk pengembangan kapasitas *cybersecurity*.
5. *Cooperation*: Mengukur capaian kerja sama antara swasta dan negara dalam hal *cybersecurity*.

Dalam laporan yang dikeluarkan 2 tahun sekali oleh ITU-*Development* itu, Indonesia menempati peringkat 24 di dunia dan peringkat 6 dalam regional Asia-Pasifik degan skor 94,88. *Cybersecurity Index* Indonesia mengalami peningkatan dari tahun 2018 yang awalnya hanya berada di peringkat 41. Hal ini membuktikan bahwa Indonesia telah memiliki kepedulian terhadap isu *cybersecurity*.

Kepedulian terhadap isu ini ditunjukkan pada periode kedua pemerintahan Presiden Jokowi, dimana disusun Rencana Pembangunan Jangka Menengah (RPJM) Nasional tahun 2020-2024 yang dapat dilihat dalam bentuk lima poin besar yaitu pembangunan Sumber Daya Manusia, pembangunan infrastruktur, penyederhanaan regulasi, penyederhanaan birokrasi, serta transformasi ekonomi. Pada periode RPJM ini negara berupaya untuk meningkatkan kapabilitas Iptek dan penciptaan inovasi, yang diantaranya terdapat cita-cita untuk meningkatkan penguasaan teknologi dalam bidang-bidang strategis termasuk *cybersecurity*. Peningkatan kapabilitas Iptek ini merupakan turunan dari Prioritas Nasional 3 tentang "Meningkatkan Sumber Daya Manusia Berkualitas dan Berdaya Saing" (BPPN 2020: 313)

Data seputar *cybersecurity* menjadi perhatian dalam indikator Prioritas Nasional 7 yaitu "Menguatnya Stabilitas Polhukhankam dan Terlaksananya Transformasi Pelayanan Publik". Dalam indikator tersebut disajikan data dimana pada tahun 2018 skor *Global Cyber Security Index* Indonesia berada pada angka 0,776, yang ditargetkan pada tahun 2024 mengalami peningkatan hingga ke angka 0,838[7]. Namun seperti yang dapat dilihat, pada tahun 2020 Indonesia telah mengalami peningkatan signifikan dengan menempati peringkat 24 dunia dengan capaian skor 94,88 (terdapat perbedaan jumlah indikator dan metode *scoring* dibandingkan dengan tahun 2018 sehingga satuan skor berbeda).

Menanggapi adanya potensi ancaman terhadap *cybersecurity* di dalam negeri, Indonesia melakukan berbagai diplomasi dan kerjasama regional, bilateral dan multilateral

dengan negaranegara di dunia. Dalam upaya pembangunan dan peningkatan *cybersecurity,* diperlukan adanya keselarasan antara hukum, teknis dan tindakan prosedural, struktur organisasi, *capacity building*, dan kerja sama internasional. Di Indonesia sendiri tentunya telah digalakkan berbagai kebijakan dan usaha-usaha dalam membangun *cybersecurity*. Salah satu bentuk peningkatan kapasitas *cyber* dalam negeri ialah adanya Keamanan Siber Nasional (*National Cyber Security*) oleh Kemenhan yang bertujuan untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional dan bersifat lintas sektor. Kemhan/TNI juga telah merancang pedoman pertahanan *cyber* berdasarkan Permenhan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber (BPPN 2020: 313)

Di internal Indonesia, penanganan *cybersecurity* masih bersifat sektoral karena setiap kementerian memiliki upaya penanganan masing-masing sehingga terjadi tumpang tindih kewenangan. Sebagai contoh, mengenai penyensoran konten negatif di dunia *cyber* menjadi tugas Kementerian Komunikasi dan Informatika. Perburuan pelaku kejahatan digital (*cybercriminals*) yang dilakukan oleh Unit *Cyber Crime* Mabes Polri dari sisi pertahanan akan bersinggungan dengan Kementerian Pertahanan yang telah *memiliki Cyber Operation Center* (COC). Ada beberapa pekerjaan penanganan insiden keamanan informasi oleh Kementerian Luar Negeri, Penanganan penipuan *e-commerce* dengan Kementerian Perindustrian, Kementerian Perdagangan, dan Kementerian Komunikasi dan Informatika. Kemudian, penanggulangan terorisme oleh Badan Nasional Penanggulangan Terorisme (BNPT), operasi *cyber* cerdas dengan Badan Intelijen Negara (BIN), kejahatan keuangan, dan ekonomi digital oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dan Komisi Pemberantasan Korupsi (KPK).

Di Indonesia saat ini melalui Kemhan RI sendiri telah membentuk suatu lembaga yang terkait dengan pertahanan *cyber* yaitu Pusat Pertahanan Siber (*Pushansiber*), sebagai unsur pelaksana tugas dan fungsi badan instalasi Pertahanan Strategis Kemhan yang memiliki tugas menyelenggarakan pemerintahan, kerjasama, operasional, dan dunia maya jaminan keamanan pertahanan. Sebagaimana tertuang dalam Peraturan Menteri Pertahanan (Permenhan) 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan, tugas pokok pertahanan *cyber* adalah menanggulangi *cyberattack* yang menyebabkan gangguan terhadap administrasi negara. Peraturan ini digunakan sebagai pedoman atau acuan dalam penyusunan, pengembangan, dan penerapan pertahanan siber di lingkungan Kementerian Pertahanan.

Sementara itu di ranah regional negara-negara anggota ASEAN juga melakukan *capacity building* keamanan *cyber* di lingkup regional karena dinilai cukup mendesak. Hal

ini dibuktikan dengan dilakukannya pembahasan mengenai keamanan *cyber* dalam berbagai diskusi di salah satu forum kerja sama politik dan keamanan yaitu *Association of Southeast Asian Nation Regional Forum* (ARF) dan *Expert Working Group pada ASEAN Defense Ministry Meeting* (ADMM) Plus. ADMM *Plus* merupakan pertemuan pejabat tinggi dalam hal ini, menteri pertahanan negara-negara ASEAN dan negara-negara terkait, untuk membahas isu-isu keamanan di kawasan ASEAN. Tidak hanya pada ranah regional, kerja sama *cyber* juga dilakukan di level global. Pada Desember 2019 dilakukan pertemuan diwakili diplomat dari Direktorat Keamanan Internasional dan Perlucutan Senjata, Kementerian Luar Negeri, yang menegosiasikan bagaimana pengaturan ranah siber yang mulai dipersenjatai. Indonesia terpilih sebagai satu dari 25 negara yang duduk dalam pertemuan PBB untuk Kelompok Ahli Pemerintah di bidang perkembangan informasi dan telekomunikasi dalam konteks keamanan internasional atau *United Nations Group of Governmental Experts on Information Security* (UNGGE).

UNGGE merupakan wadah bagi negara-negara anggota PBB dalam menjaga keamanan informasi. Upaya yang dilakukan ini merupakan salah satu perwujudan dari adanya *cyber diplomacy. Cyber diplomacy* terjadi di ruang *cyber*. Oleh karena itu, penting untuk memahami tentang ruang *cyber*. Menurut Buck (1998), ruang *cyber* memiliki karakteristik yang membingkai keterlibatan diplomatik di antara para pemangku kepentingan. Lebih lanjut ia menjelaskan bahwa ruang *cyber* merupakan domain global yang menghubungkan berbagai negara dan masyarakat di seluruh dunia dalam berbagai cara, sehingga dapat terjadi interaksi dan juga gesekan di antara negara dan masyarakat. Ruang *cyber* juga seringkali dianggap sebagai global *common*. Ruang *cyber* dapat dibandingkan dengan sumber daya global lainnya, seperti laut lepas, wilayah udara, dan luar angkasa.

Dengan demikian, ruang *cyber* membutuhkan serangkaian peraturan dan regulasi untuk memastikan akses bagi semua dalam menghindari konflik yang berpotensi. Hal ini dapat dicapai dengan negosiasi diplomatik (Di & Malaka. 2020: 311-322). Karakteristik-karakteristik ruang *cyber* menjadikan hubungan ruang *cyber* internasional dan tata kelola ruang *cyber* sangat kompleks dan rapuh, tetapi di saat yang bersamaan menjadikan diplomasi semakin diperlukan, terutama dalam mekanisme pembangunan kepercayaan serta pengembangan norma dan nilai internasional. Merupakan hal yang urgen bagi pemerintah Indonesia melalui berbagai lembaganya untuk melaksanakan pertahanan terhadap ancaman *cybercrime* dengan upaya diplomasi bersama negara- negara kawasan maupun global.

Hal ini menentukan posisi dan strategi diplomasi pertahanan Indonesia di ASEAN serta meningkatkan peran Indonesia dalam konstelasi dunia global sebagai aksi nyata melindungi kepentingan nasional dan membangun pertahanan Indonesia. Berangkat dari konteks tersebut tersebut, riset mengenai diplomasi di isu siber merupakan bagian dari upaya pemerintah dalam merespon dampak dari era digital dalam bentuk tata kelola pemerintahan yang berkaitan dengan kehidupan individu dan kolektif. Jika merujuk pada RIP UB 2021-2025 maka tema besarnya adalah digitalisasi tatakelola pemerintahan. Mengingat tantangan yang dihadapi oleh pemerintah Indonesia dalam era digital, perlu kiranya untuk memastikan upaya diplomasi pemerintah Indonesia di isu siber guna terwujudnya tatakelola pemerintahan di sektor digital lebih baik.

TINJAUAN PUSTAKA

Konsep Cyber Diplomacy

Dalam kajian diplomasi, praktek diplomasi siber terbilang cukup baru mengingat isu siber di era saat ini dimana perkembangan teknologi informasi menjadi perhatian banyak negara. Konteks dunia siber (dunia maya) cukup berbeda dengan konteks digital, yang kemudian menjadi pembeda dalam praktek diplomasi. Jika diplomasi digital selama ini dikenal sebagai salah satu praktek diplomasi yang menyorot strategi penggunaan teknologi komunikasi internet (*Internet communication technologies/ ICTs*) dalam prakteknya sedangkan diplomasi siber lebih berfokus pada isunya terlebih isu keamanan. Penggunaan media sosial dalam praktek diplomasi menjadi salah contoh bagaimana praktek diplomasi digital dilakukan oleh aktor internasional. Maka tidak mengherankan jika kita melihat perkembangan dewasa ini, para pemimpin negara, figur-figur internasional hingga pemimpin organisasi internasional memanfaatkan media sosial sebagai sarana melakukan diplomasi kontemporer. Sangat wajar jika kemudian praktek diplomasi digital erat dikaitkan dengan diplomasi publik dalam derajat tertentu. Pemakanaan ini pula yang kemudian erat dengan penamaan lainnnya yaitu, e-diplomacy.

E-diplomacy secara ringkas dapat dimaknai sebagai metode baru dalam menjalankan praktek diplomasi dan hubungan internasional dengan menggunakan teknologi informasi dan internet (Bjola & Holmes. 2015) *E- diplomacy* dapat dianggap sebagai *sub-set-e governance* termasuk didalamnya *cyber diplomacy dan digital diplomacy*. Berangkat dari penjelasan ini aktivitas diplomasi siber bergeser secara signifikan antara masyarakat internasional dan dunia, itulah mengapa kita akan melihat tidak hanya dalam tataran konsep saja tetapi juga prakteknya. Beberapa pengkaji diplomasi melihat *cyber diplomasi* merupakan salah satu bentuk evolusi dari diplomasi publik di era digital yang berfokus pada

transformasi digital yang lebih luas, sehingga tidak mengherankan jika mereka tidak terlalu membahas proses diplomatik yang diperlukan untuk menangani aspek-aspek yang muncul dari permasalahan siber (Kleiner. 2018: 321-349) Pandangan lain seperti Potter melihat diplomasi siber juga untuk menggambarkan dampak internet dan teknologi dalam praktek diplomasi (Potter 2002).

Menurut Andre Barrinha, *cyber diplomacy* didefinisikan sebagai bentuk diplomasi dalam isu siber atau dengan kata lain penggunaan sumber daya diplomatik dan kinerja fungsi diplomatik untuk mengamankan kepentingan nasional yang berkaitan dengan dunia maya (siber). (Barinha & Ronard. 2017:353-364). Kepentingan semacam ini umumnya diidentifikasi dalam dunia maya nasional atau strategi keamanan siber yang seringkali mencakup referensi ke agenda diplomatik. Dalam prakteknya, diplomasi siber dilakukan secara keseluruhan atau sebagian oleh para diplomat dalam pertemuan baik secara bilateral atau multilateral. Selain melaksanakan fungsi diplomasi tradisional (G to G), para diplomat juga seringkali berinteraksi dengan aktor-aktor non negara seperti pemimpin perusahaan internet, perusahaan teknologi bahkan organisasi masyarakat sipil.

Definisi menurut Barrinha menjadi landasan penting dalam memahami konteks diplomasi siber. Meskipun dalam penjelasan tersebut menyisakan ruang abu-abu dalam memaknai apa itu diplomasi siber, setidaknya Barrinha memberi peluang lebar dalam mengeksplor praktek diplomasi siber di era kontemporer. Hal ini dapat kita lihat tidak hanya dalam praktek diplomasinya semata tetapi juga pada varibel-variabel lainnya, yang dijelaskan melalui komponen *cyber diplomacy.*

Komponen Cyber Diplomacy

Barinha dan Renrad menjelaskan cyber diplomacy dalam beberapa komponen, yaitu *diplomat activity, national interest, cyber issue, and diplomat. Diplomat activity* adalah merujuk kepada aktivitas yang dilakukan dalam sebuah negara. Aktivitas diplomasi tersebut dianalogikan sebagai wadah komunikasi yang dapat memelihara hubungan di dunia siber antar kedua negara. Beberapa bentuk dari aktivitas ini diataranya adalah pertemuan diplomatic antar negara yang merundingkan sebuah kesepakatan dan pertemuan yang mendiskusikan atau menandatangani sebuah komitmen dibidang siber. Aktivitas diplomasi siber ini juga tidak hanya seputar negosiasi seputar isu siber tetapi juga melalui aktivitas ini dapat mengembangkan alat dan sistem teknologi yang dapat dimanfaatkan untuk meningkatkan keamanan siber di sebuah negara.

National interest, dalam konteks ini adalah merujuk pada kepentingan sebuah negara dalam isu siber. Dalam hal ini kita akan melihat strategi yang dimiliki oleh negara, baik itu

melalui arah kebijaan negara dalam rancangan pembangunannya hingga keterlibatan negara dalam fora internasional dalam isu siber. Berangkat dari konteks tersebut setidaknya kita dapat menakar kepentingan nasional suatu negara. Komponen *ketiga* adalah *cyber issue* yaitu apa saja yang berkaitan seputar dunia siber. Dalam dunia siber kita dihadapkan pada ancaman di dunia siber (*cyber threats*) yang kemudian dapat menjadi perhatian dalam isu keamanan siber (*cyber security*). Karena permasalahan keamanan siber dapat mengancam siapa saja, itulah kemudian diangkat menjadi agenda global (*cyber agenda*). Salah satu harapannya adalah negara-negara dapat berpartisipasi dalam menghadapi ancaman siber dengan mengaplikasikan kedalam hukum internasional maupun membangun norma perilaku bersama dalam ranah *cyber space.* Dalam hal ini pembahasan isu siber kemudian dapat dilakukan melalui aktivitas diplomatik. Beberapa agenda dalam diplomasi siber yang terkait dengan isu siber diantaranya adalah *cyber security, cybercrime, confidencebuilding, internet freedom,* dan *internet governance.*

Komponen keempat adalah *cyber diplomacy actor,* yang merupakan representasi resmi suatu negara atau yang bisa dikenal sebagai diplomat. Sebagai pelaksana diplomasi suatu negara, diplomat disini tentu bermakna membawa agenda politik serta sebagai penangggun jawab dalam aktivitas diplomasi. Dalam permasalahan diplomasi siber ini, diplomat memiliki peran kunci sebagai pelopor diplomasi siber karena akan membawahi kementerian dan instansi terkait dalam penanganan isu siber.

METODE PENELITIAN

Penelitian ini merupakan peneltian deskriptif eksploratif dengan pendekatan kualitatif dimana penulis berupaya menggambarkan dan menjelaskan secara mendalam mengenai praktek diplomasi Indonesia di era presiden Joko Widodo di isu siber. Penelitian deskriptif eksploratif menurut Bhattacherjee sering kali dilakukan untuk ranah penelitian yang baru, di mana tujuan penelitian adalah: (1) untuk mengetahui besaran atau luasnya fenomena, masalah, atau perilaku tertentu, (2) untuk menghasilkan beberapa gagasan awal (atau "firasat") tentang fenomena tersebut, atau (3) untuk menguji kelayakan untuk melakukan studi yang lebih luas tentang fenomena tersebut (Bhattacherjee 2012). Menurut King, Keohane dan Verba, penelitian dengan pendekatan kualitatif banyak digunakan dalam penelitian-penelitian ilmu sosial dan fokus pada fenomena-fenomena sosial, kebijakan-kebijakan, Lembaga-lembaga atau organisasi, permasalahan sosial atau undangundang yang berlaku di masyarakat.

Rancangan penelitan dalam studi ini mengambil empat komponen dalam penelitian sosial yang saintifik yaitu pertanyaan penelitian, kerangka konsep, pengumpulan data dan

analisa data (Garry, Keohane & verba 1994). Penelitian ini disusun untuk menjawab pertanyaan bagaimana diplomasi Indonesia di masa Pemerintahan Joko Widodo dalam isu siber. Dari rumusan permasalahan tersebut, peneliti mencoba menggunakan konsep *cyber diplomacy* milik Andre Barrinha. Rancangan penelitian disusun melalui beberapa tahapan seperti, pengumpulan data, penggunaan teori/ model atau konse serta melakukan analisa data.

HASIL DAN PEMBAHASAN

Dalam konteks ini Indonesia saat ini telah memiliki Lembaga khusus yang mengurusi permasalahan siber yaitu Badan Siber dan Sandi Negara (BSSN), yang berdiri sejak tahun 2017. Lembaga tersebut diharapkan menjadi ujung tombak dalam menagani isu seputar dunia siber di Indonesia. Meskipun demikian dalam aktivitasnya tentu BSSN menggandeng beberapa lembaga lainnya seperti kepolisian, tni dan juga beberapa kementerian, salah satunya adalah kementerian luar negeri. Kementerian Luar Negeri digandeng terkait salah satu fungsi utamanya yaitu diplomasi.

Perkembangan Isu Siber di Indonesia

Dalam konteks keamanan siber, awal mula hukum Indonesia yang bergerak di bidang keamanan teknologi dan informasi (IT) bisa dilacak dengan diberlakukannya UU Telekomunikasi No.36/1999 dan UU Informasi dan Transaksi Elektronik (ITE) No.11/2008. Kedua UU ini dihitung sebagai bentuk kebijakan dari pemerintah Indonesia mengenai keamanan jalur komunikasi teknologi pada umumnya di Indonesia. Ditandatangani oleh Presiden RI Bacharuddin Jusuf Habibie dan Menteri Sekretaris Negara Muladi, UU Telekomunikasi merupakan salah satu contoh pertama dari dibentuknya sebuah kebijakan khusus tentang kegiatan telekomunikasi di Indonesia (UU RI 1999). UU ini membahas semua bentuk komunikasi yang menggunakan teknologi komunikasi pada masanya seperti televisi, radio, telepon, dan lain sebagainya.

Selain UU Telekomunikasi, UU lain yang seringkali menjadi rujukan dalam mengamankan jaringan teknologi dan informasi di Indonesia adalah UU ITE No.11/2008. Sebagai sebuah UU yang sudah lebih mengakui keberadaan internet sebagai sarana komunikasi di Indonesia dibanding dengan UU Telekomunikasi, UU ITE secara eksplisit membahas tentang konsep internet sendiri sebagai sarana komunikasi. Sesuai dengan judulnya, UU ITE membahas tentang informasi elektronik yang bisa didefinisikan sebagai sekumpulan data elektronik yang bisa berbentuk tulisan, gambar, atau lainnya. Lebih rinci lagi, UU ITE turut membahas tentang konsep transaksi elektronik dan dokumen elektronik yang penggunaannya meluas semenjak akses internet di Indonesia menjadi semakin luas.

Meskipun begitu, kedua UU ini dianggap tidak mencukupi dalam beberapa hal untuk bisa secara signifikan menegakkan keamanan siber di Indonesia (Nugraha & Putri). Contohnya, UU Telekomunikasi tidak menyebutkan jaringan internet sebagai sebuah media komunikasi yang telah digunakan di Indonesia. Meskipun internet sudah memasuki Indonesia beberapa tahun sebelum diberlakukannya UU

Di sisi lain, UU ITE yang dibentuk pada tahun 2008 masih membutuhkan beberapa UU lain untuk bisa bekerja secara efektif. Beberapa UU seperti UU Perlindungan Konsumen No.8/1999, UU Hak Cipta No.19/2002 dan UU Pornografi No.44/2008 merupakan beberapa jenis UU yang digunakan untuk menindak para pelaku cybercrime di Indonesia. Ini menimbulkan kesan bahwa UU ITE masih belum memiliki cakupan yang mencukupi mengenai aturan persekusi dari pihak berwenang terhadap para pelaku cybercrime. Belum lagi, di mana UU tentang keamanan siber negara lain telah membahas aturan penindakan hukum terhadap para pelaku cybercrime secara lengkap, UU ITE masih tidak bisa berdiri sendiri tanpa melibatkan UU lain. Ini menandakan bahwa UU ITE tidak memiliki cakupan yang cukup tentang definisi dan hukuman terhadap tindakan cybercrime secara spesifik di Indonesia.

Di tengah kurangnya cakupan beberapa UU di Indonesia tentang cybersecurity secara spesifik, pemerintah Indonesia telah melakukan beberapa tindakan untuk menegakkan cybersecurity sejak era 2000-an. Pada tahun 2007, Kementerian Komunikasi dan Informasi (Kemkominfo) memberlakukan Peraturan Menteri Komunikasi dan Informasi No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Internet. Peraturan ini membahas tentang pembentukan lembaga keamanan yang relevan untuk menangani masalah cybersecurity di Indonesia, dengan contohnya adalah *Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII).*

Kepentingan Indonesia dalam isu Siber

Dalam upaya pemerintah Indonesia untuk membangun awareness tentang penegakan keamanan siber, pendidikan tentang keamanan siber secara spesifik juga belum dilaksanakan di Indonesia dengan mencukupi. Meskipun beberapa universitas ternama di Indonesia seperti Universitas Indonesia, Universitas Gunadarma, dan Sekolah Tinggi Sandi Nasional (STSN) menyediakan pendidikan tentang keamanan siber sampai tingkatan tertentu (terutama bagi STSN), tidak banyak sekolah tinggi yang menyediakan pendidikan tentang keamanan siber yang mumpuni dan merata di berbagai daerah di Indonesia. Walaupun begitu, perkembangan sebuah lembaga khusus di bidang keamanan siber di Indonesia pun terus dilanjutkan yang berujung dengan dibentuknya Badan Siber dan Sandi

Negara (BSSN) pada tahun 2017.

BSSN dibentuk pada tahun 2017 berdasarkan dari Peraturan Presiden No.53/2017. Sebagai sebuah lembaga pemerintah non-kementerian yang berada di bawah naungan presiden secara langsung, BSSN merupakan kelanjutan dari lembaga pemerintah sebelumnya seperti Lembaga Sandi Negara (LSN) yang bertanggung jawab atas urusan keamanan sandi Indonesia. Hampir mirip seperti ID-SIRTII, BSSN berfungsi untuk melaksanakan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan dan pemantauan keamanan siber di Indonesia.

Selain BSSN, berbagai lembaga pemerintah lain di Indonesia turut memiliki ketertarikan yang sama mengenai konsep keamanan siber dan implikasinya bagi Indonesia. Polri, Kementerian Pertahanan (Kemhan), Badan Intelijen Negara (BIN) dan Tentara Nasional Indonesia masing- masing memiliki ketertarikan sendiri mengenai implementasi keamanan siber. Dari pihak Kemhan, peran keamanan siber sendiri diakui sebelum peresmian BSSN dalam Peraturan Menteri Pertahanan Republik Indonesia No.82/2014 tentang Pedoman Pertahanan Siber. Diresmikannya peraturan ini merupakan bentuk kelanjutan dari berbagai UU sebelumnya yang menegaskan pada pertahanan nasional Indonesia baik dari aspek militer maupun non-militer. Karena cybercrime sendiri merupakan bentuk cyber threat yang bisa mempengaruhi Indonesia dalam berbagai bidang, pemerintah Indonesia tetap mengakui pentingnya penegakan keamanan siber di tengah semua kendala yang ada.

Mengingat bahwa secara turun temurun konsep keamanan di Indonesia masih diartikan sebagai keamanan negara dan bukan keamanan individu, keluputan ini berujung pula dengan bagaimana belum adanya sebuah strategi cybsersecurity yang komprehensif di Indonesia. Menurut Deputi Direktur Riset ELSAM Wahyudi Djafar, perlindungan hak-hak individu di ranah cyberspace sangatlah penting dalam penegakan cybersecurity sebuah negara. Karena para pelaku cybercrime sama sekali tidak terikat dengan sebuah lokasi geografis, maka penanganan cyber threats membutuhkan perhatian ekstra. Meski kondisi ini telah diakui oleh berbagai pihak di Indonesia, belum adanya lagi UU tentang keamanan siber di Indonesia menjadikan penegakan keamanan ini sulit untuk dilakukan.

Pengembangan UU tentang keamanan siber sendiri pun juga menemui halangan. RUU Keamanan dan Ketahanan Siber (KKS) di Indonesia yang diharapkan akan menjadi UU pertama tentang keamanan siber di Indonesia dinyatakan gagal kelanjutannya pada tahun 2019. Menurut Ketua Panitia Khusus (Pansus) RUU Keamanan dan Ketahanan Siber (RUU KKS) Bambang Wuryanto, RUU ini tidak memenuhi mekanisme tata beracara dalam pembuatan legislasi. Tidak adanya kesepakatan mengenai definisi cybercrime dan konten-konten internet yang dianggap sebagai ancaman bagi masyarakat Indonesia turut

mempersulit peresmian RUU tersebut. Belum lagi, tidak hadirnya Menteri Komunikasi dan Informatika Rudiantara, Menteri HAM Yasonna H. Laoly dan Menteri PAN-RB Syafruddin dalam pembahasan RUU ini menandakan halangan bagi peresmian RUU tersebut.

Dari perkembangan di atas, bisa dilihat bahwa pemerintah Indonesia berhasil membentuk beberapa lembaga yang relevan untuk menangani masalah keamanan siber di Indonesia secara spesifik. Pembentukan BSSN pada tahun 2017 dipandang sebagai sebuah babak baru bagi upaya penegakan keamanan siber di Indonesia karena peran dan fungsi yang diemban oleh BSSN. Walaupun begitu, masalah dari aspek legal dan sumber daya tetap menjadi beberapa penghalang besar bagi penegakan keamanan ini. Pembahasan RUU KKS yang dibatalkan pada tahun 2019 juga menghalangi pemerintah Indonesia untuk bisa memiliki UU tentang keamanan siber yang bisa menjadi landasan hukum semua bentuk penegakan keamanan siber di Indonesia.

Aktor Diplomasi Siber Indonesia

Dalam praktek diplomasi, kementerian luar negeri merupakan garda terdepan dalam melakukan kerjasama internasional. Jika melihat konteks isu siber sendiri merupakan ranah BSSN sebagai Lembaga yang menaungi isu tersebut, tetapi dalam praktek diplomasi tentu akan melibatkan kementerian luar negeri sebagai pembuka jalan dalam melakukan negosiasi. Dalam beberapa praktek diplomasi terkait isu siber yang pernah dilakukan oleh Indonesia, beberapa Lembaga dan kementerian lain juga terlibat seperti Kementerian Komunikasi dan Informatika, Kementerian Koordinator Bidang Politik, Hukum dan Keamanan serta Kepolisian Negara Republik Indonesia.

Keterlibatan beberapa kementerian tersebut menjadi perhatian tersendiri dalam kajian diplomasi, khususnya agenda diplomasi siber. Jika merujuk isu yang diangkat, agenda diplomasi siber melingkupi beberapa isu yang lain seperti keamanan siber, kejahatan siber, *confidence building,* kebebasan dalam menggunakan internet serta tata kelola internet. Selain aktor yang berasal dari pemerintah, keterlibatan aktor non pemerintah juga ada seperti perusahan teknologi komunikasi dan internet dan organisasi masyarakat sipil. Aktor-aktor ini mungkin tidak terlibat secara langsung dalam praktek diplomasi antar negara, tetapi mereka berkontribusi menjadi *sharing partner* bagi pemerintah Indonesia.

Diplomasi Siber Indonesia

Salah satu contoh praktek diplomasi siber yang telah dilakukan Indonesia adalah dengan Australia. Beberapa agenda yang pernah dilakukan oleh Indonesia adalah dialog bilateral dalam kerangka kerjasama siber (*Australia-Indonesia Cyber Policy Dialogue*). *Joint*

Statement of 26 February 2017 menjadi penanda antara kedua negara untuk berkomitmen dalam *cyberspace: open, free, and secure internet* sebagai prinsip-prinsip yang disepakati sebagai pendukung pertumbuhan ekonomi dan inovasi serta memperdalam kerjasama dalam menghadapi ancaman *cyberspace.* Pada dialog berikutnya Indonesia dan Australia menegaskan kembali komitmen mereka untuk mempromosikan stabilitas cyberspace internasional berdasarkan hukum internasional yang ada, norma-norma perilaku bertanggung jawab yang sukarela dan tidak mengikat (voluntary and non- binding norms of responsible behavior), practical confidence building measures, dan pembangunan kapasitas kerjasama (Departement of Foreign Affair and Trade, 2018). Dialog ini juga membahas laporan UNGGE tahun 2013 dan 2015 tentang perkembangan di bidang informasi dan telekomunikasi dalam konteks keamanan internasional (Departement of Foreign Affair and Trade, 2018).

Australia dan Indonesia menegaskan kembali bahwa hukum internasional tentang cyberspace yang ada berlaku pada aktivitas negara-negara didunia (Departement of Foreign Affair and Trade, 2018). Tak hanya itu, kedua negara sepakat untuk terus mempromosikan seperangkat common voluntary and non-binding norms of responsible state behavior yang direkomendasikan dalam laporan UNGGE 2015, dan berkomitmen untuk bertindak sesuai dengan norma-norma tersebut (Departement of Foreign Affair and Trade, 2018). Mereka mencatat bahwa aktivitas kerjasama antar negara dan dengan mitra regional lainnya adalah kebutuhan mendesak sebagai upaya untuk mengurangi risiko adanya cyberspace (Departement of Foreign Affair and Trade, 2018).

Beberapa putaran dialog tersebut merupakan bentuk diplomasi kedua negara dalam merespon isu siber. Salah satu hasil dari diplomasi tersebut, pada tahun 2018 Indonesia dan Australia menghasilkan kesepakatan MoU dalam Cyber Cooperation yang ditandatangani oleh Presidan Joko Widodo dan PM Scott Morrison. Dalam kunjungan PM Australia tersebut kedua negara bersepakat berkomitmen untuk mempromosikan stabilitas *cyberspace* berdasarkan; hukum internasional yang ada, *voluntary and non-binding norms of responsible behaviour, practical confidence building measures, and capacity building.*

Menilik ke tahun-tahun sebelumnya Pemerintah Indonesia di era Jokowi telah melakukan beberapa kali upaya yang berkaitan dengan diplomasi siber. Indonesia aktif dalam kelompok kerja yang dibentuk UNODC dalam Menyusun pedoman mengatasi kejahatan dengan lingkup pencegahan, kerjasama internasional dan pengembangan kapasitas. Tahun 2015 Pernyataan Bersama antara Indonesia dengan AS untuk bekerjasama di bidang *cyberspace* serta kerjasama di bidang keamanan siber bersama Cina. Sejak tahun 2016, kerjasama antara Indonesia dan Rusia dalam mengatasi keamanan siber juga telah

dilakukan. Tahun 2017, pengadopsian ASEAN Declaration to *Prevent and Combat Cybercrime* juga merupakan bentuk penguatan isu siber dalam konteks kawasan.

SIMPULAN

Akhirnya, penelitian ini menyimpulkan bahwa perkembangan isu siber di Indonesia telah mengalami evolusi seiring waktu, dimulai dari regulasi awal seperti UU Telekomunikasi No.36/1999 dan UU ITE No.11/2008. Meskipun ada upaya untuk meningkatkan keamanan siber, masih ada beberapa tantangan yang perlu diatasi. Salah satu kendala utama adalah kurangnya cakupan hukum yang memadai untuk menangani tindakan cybercrime. UU Telekomunikasi tidak mencakup internet sebagai media komunikasi, sementara UU ITE masih memerlukan dukungan dari undang-undang lain untuk efektif menangani cybercrime. Selain itu, pembahasan RUU Keamanan dan Ketahanan Siber (KKS) pada tahun 2019 juga tidak berhasil, menghambat upaya untuk memiliki UU keamanan siber yang komprehensif. Pemerintah Indonesia telah mendirikan beberapa lembaga, seperti Badan Siber dan Sandi Negara (BSSN), untuk menangani masalah keamanan siber secara lebih efektif. Namun, tantangan dalam aspek hukum dan sumber daya tetap ada. Diplomasi siber juga menjadi perhatian penting bagi pemerintah Indonesia, dengan kerjasama internasional dalam upaya mempromosikan keamanan siber, kebebasan berinternet, dan kerjasama antar-negara. Beberapa dialog dan perjanjian dengan negara lain, seperti Australia, mencerminkan upaya diplomasi dalam merespons isu siber. Meskipun langkah-langkah telah diambil untuk meningkatkan keamanan siber di Indonesia, masih ada pekerjaan yang perlu dilakukan, terutama dalam pengembangan hukum yang lebih komprehensif dan dalam membangun kesadaran serta pendidikan yang lebih luas tentang keamanan siber di seluruh negeri.

DAFTAR PUSTAKA

Freudenthal, H. 1991. *Revisiting Mathematics Education*. Dordrecht: Kluwer Academic Publishers.

Ary, D., Jacobs, L.C., & Razavieh, A. 1976. *Pengantar Penelitian Pendidikan*. Terjemahan oleh Arief Furchan. 1982. Surabaya: Usaha Nasional

Prahmana, R.C.I. 2012. *Pendesainan Pembelajaran Operasi Bilangan Menggunakan Permainan Tradisional Tepuk Bergambar Untuk Siswa Kelas III Sekolah Dasar (SD)*. Unpublished Thesis. Palembang: Sriwijaya University.

Zulkardi. 2002. *Developing A Learning Environment on Realistic Mathematics Education for Indonesian Student Teachers*. Published Dissertation. Enschede: University of Twente.

Cobb, P. 1994. *Theories of Mathematical Learning and Constructivism: A Personal View*. Paper presented at the Symposium on trends and perspectives in mathematics education, Institute for mathematics, University of Klagenfurt, Austria.

Stacey, K. 2010. *The View of Mathematical Literacy in Indonesia*. Journal on Mathematics Education (IndoMS-JME), 2 (2), 1-24. Palembang: IndoMS.

Pitunov, B. 13 December 2002. *Sekolah Unggulan ataukah Sekolah Pengunggulan?.* Majapahit Pos, page 4 & 11.

Pusat Pembinaan dan Pengembangan Bahasa. 1978. *Pedoman Penulisan Laporan Penelitian*. Jakarta: Depdikbud

Hitchcock, S., Carr, L., & Hall, W. 1996. A Survey of STM Online Journals, 1990-1995: The Calm before the Storm, (Online), (http://journal.ecs.soton.ac.uk/survey/survey.html), diakses 12 Juni 1996

Kumaidi. 1998. Pengukuran Bekal Awal Belajar dan Pengembangan Tesnya. Jurnal Ilmu Pendidikan. (Online), Jilid 5, No. 4, (http://www.malang.ac.id), diakses 20 Januari 2000