DIPLOMASI SIBER INDONESIA DALAM MENINGKATKAN KEAMANAN SIBER MELALUI *ASSOCIATION OF SOUTH EAST ASIAN NATION* (ASEAN) REGIONAL FORUM

Henike Primawanti

henikeprimawanti22@gmail.com

Sidik Pangestu

pangestu.sidik2@gmail.com

ABSTRAK

Teknologi merupakan sebuah anugerah tetapi juga merupakan sebuah ancaman yang nyata. Dunia maya dan teknologi internet misalnya, dunia maya maupun internet yang mampu menghubungkan jutaan orang, telah diakui sangat berguna dan mendukung hampir setiap bidang kehidupan. Maka dari itu penelitian ini bertujuan untuk mengetahui bagaimana Indonesia dalam berdiplomasi demi meningkatkan keamanan siber melalui ASEAN regional Forum. Penelitian ini menjelaskan latar belakang negara indonesia ikut serta dalam ASEAN *Regional Forum* serta seperti apa diplomasi yang dilakukan oleh negara Indonesia dalam upaya meningkatkan keamanan siber negara.

Hasil penelitian ini menunjukkan bahwa alasan yang melatarbelakangi Indonesia dalam ASEAN *regional Forum* adalah karena keadaan *Cybersecurity* indonesia yang masih memiliki banyak celah, kepentingan nasional berupa kebutuhan keamanan yang bersifat mutlak dan ancaman-ancaman yang berasal dari ruang siber. Dalam melakukan diplomasi di ASEAN *Regional Forum,* Indonesia mengusulkan empat poin khusus yaitu adanya kontak poin, dibentuknya *study group* untuk perumusan kurikulum dalam peningkatan *capacity building,* transisi penggunaan *Internet Protocol version 4* (IPv4) ke IPv6, pembentukan badan atau lembaga khusus terkait *cyber* di negara masing-masing.

Indonesia menginisiasi negara-negara ASEAN untuk menjalankan usulan tersebut. Dua poin diantaranya berhasil di terima dan dituangkan dalam ASEAN *Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies (Ict's).* Dalam upaya pembangunan dan peningkatan keamanan siber diperlukan adanya keselarasan antara hukum, teknis dan tindakan prosedural, struktur organisasi, *capacity building,* dan kerja sama internasional.

Kata Kunci: Cybersecurity, Cyber Crime, ASEAN Regional Forum, Diplomasi

1. Latar Belakang

Pada saat ini seluruh bidang dan aspek kehidupan sebuah negara mengalami berbagai macam perubahan dan pengembangan. Hal ini tentunya di iringi pula dengan kecanggihan teknologi yang semakin mempermudah kehidupan manusia. Namun dibalik kemilau teknologi yang mampu memberikan kita akses ke seluruh dunia. Terdapat sisi gelap yang mengintai stabilitas dan keamanan suatu negara.

Teknologi merupakan sebuah anugerah tetapi juga merupakan sebuah ancaman yang nyata. Dunia maya dan teknologi internet misalnya, dunia maya maupun internet yang mampu menghubungkan jutaan orang, telah diakui sangat berguna dan mendukung hampir setiap bidang kehidupan. Media sosial yang di gaungi kaum muda, kemudahan bertransaksi online, pendidikan, pembangunan dalam ekonomi, akulturasi budaya merupakan bentuk-bentuk nyata atas manfaat dari keberadaan dunia maya dan internet. Tetapi juga tidak dapat dipungkiri bahwa keberadaan teknologi seperti ini juga membawa dampak atau efek buruk dengan munculnya berbagai Kejahatan di bidang siber.

2. Kejahatan Siber (*Cyber Crime*)

Internet telah menjadi sebuah ruang informasi dan komunikasi yang dapat menembus batas-batas negara serta mempercepat penyebaran dan pertukaran ilmu maupun gagasan dikalangan ilmuwan dan cendikiawan diseluruh dunia. *Internet* membawa manusia pada suatu ruang atau dunia baru yang tercipta dan dinamakan *cyberspace* (Samaun Samadikun, 2000 hal. 4) Ruang Siber (*cyberspace*) merupakan ruang dimana komunitas saling terhubung melalui jaringan (salah satunya internet) untuk melakukan berbagai kegiatan. (Kemenhan, 2014 hal.5) *Cyberspace* sendiri merupakan sebuah dunia komunikasi berbasis computer dengan realitas yang cukup unik, realitas yang dimaksud ialah realitas virtual. Perkembangan pada bidang ini membawa perubahan yang sangat besar dan mendasar khususnya pada tatanan sosial dan budaya dalam skala global. Perkembangan tentang *cyberspace* mengubah pengertian tentang interaksi sosial, masyarakat, komunikasi, komunitas, dan budaya.(Samaun Samadikun, 2000 hal. 91)

Ruang siber tentu memiliki efek negatif. Kemudahan akses pada kecanggihan teknologi seperti internet mengundang pelaku-pelaku yang tidak bertanggung jawab dalam pemanfaatan ruang siber. Ruang siber digunakan sebagai media dalam melakukan tindakan

menyimpang dan melanggar hukum-hukum yang berlaku. Hal ini juga berdampak pada kerugian-kerugian yang harus ditanggung pihak lain. Tindakan-tindakan tersebut memunculkan bentuk-bentuk baru dan berbeda dari tindak kejahatan yang ada. Kejahatan yang berasal atau terjadi di ruang siber inilah disebut dengan kejahatan dunia maya atau *cybercrime.*

Meningkatnya konektivitas di dunia maya dan ketergantungan akan siber juga meningkatkan kemungkinan kejahatan transnasional yang berbasis siber. (James Andrew Lewis, 2013 hal. 1) Heinl mengemukakan ancaman siber paling banyak dialami oleh negara-negara di ASEAN sejak tahun 2012 – 2013 khususnya penyerangan pada *website* atau situs resmi milik pemerintahan (Heinl, C. H., 2013 hal. 137) Data dan informasi menjadi sasaran utama karena merupakan entitas yang paling bernilai tinggi dalam suatu sistem informasi korporasi. (Richardus Eko Indrajit, 2011, hal 12)

Dampak yang mungkin dialami akibat dari serangan siber ialah berupa : Penyalahgunaan informasi, pengendalian sistem secara *remote*, kerusuhan, ketakutan, kekerasan, kekacauan, konflik, gangguan fungsional ataupun kondisi merugikan lain nya, hingga mungkin dapat mengakibatkan kehancuran. (Kemenhan, 2014 hal.14). Ancaman-ancaman yang berasal ruang siber sangatlah berbahaya karena mengintai di segala penjuru serta setiap celah yang mampu dimanfaatkan untuk melakukan kejahatan. Kejahatan siber memiliki cangkupan yang luas serta dampak yang luas pula pada suatu negara, kawasan bahkan dunia.

Kejahatan siber sendiri memiliki berbagai macam bentuk dan jenis yang berbeda. Secara umum kita dapat mengkategorikan beberapa potensi ancaman kejahatan siber sebagai berikut: *illegal content,cyber espionage, data forgery, carding, cracking,unauthorized access to computer system and service, offense against intellectual property, cyber stalking, cyber terrorism and cybersquatting, infringements of privacy,* (I Nyoman & Wayan, 2018:5) dan masih terdapat banyak lagi.

3. Keamanan Siber (*Cyber Security*)

Ancaman-ancaman dan kejahatan tersebut perlu diantisipasi, Salah satunya melalui Kemanan siber atau *cyber security*. Keamanan Siber atau *cybersecurity* dapat dikatakan sebagai sebuah rangkaian aktifitas ataupun pengukuran yang dimaksudkan untuk melindungi dari disrupsi, serangan, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* baik *software, hardware, computer network.* (Fischer, 2009).

Dapat dikatakan bahwa keamanan siber merupakan segala upaya yang dilakukan baik perorangan atau kelompok secara mandiri ataupun kolektif dengan melakukan tindakan-

tindakan atau upaya untuk mengamankan, menjaga, mengantisipasi ataupun meminimalisir dampak-dampak yang berkaitan dengan ruang siber. Fungsi dari keamanan Siber sendiri dapat dijabarkan sebagai berikut :(Kemenhan, 2014 hal.14).

1. Menjamin tercapainya sinergi kebijakan pertahanan siber.
2. Membangun organisasi dan tata kelola sistem penanganan keamanan siber.
3. Membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan siber.
4. Membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber.
5. Mewujudkan kesadaran keamanan siber.
6. Meningkatkan keamanan sistem siber sektor pertahanan.
7. Mewujudkan riset dan pengembangan untuk mendukung pembinaan dan pengembangan kemampuan Pertahanan Siber.
8. Menyelenggarakan kerjasama nasional dan internasional guna pembinaan dan pengembangan kemampuan Pertahanan Siber.

Keamanan siber atau *cyber security* sangat diperlukan untuk menjaga dan mengantisipasi ancaman-ancaman yang berasal dari ruang siber. *Cybersecurity* semestinya adalah sebuah ekosistem dimana hukum *(laws),* organisasi *(organizations),* kemampuan *(skills),* kerjasama *(cooperation),* dan *technical implementation* berjalan secara selaras untuk dapat menjadi efektif (ITU, 2017). *International Telecommunication Union* (ITU) melakukan survey dalam mengukur komitmen negara-negara anggota terhadap keamanan siber melalui *Global Cybersecurity Index* (GCI).(Maulia, 2017:139) *Global cyber-security indexs atau* indeks keamanan siber dunia berguna supaya negara dapat melakukan proyeksi dan peninjauan kembali pada bidang keamanan siber masing-masing negara. Berdasarkan GCI keamanan siber dapat ditinjau atau dibangun di atas lima bidang kerja yaitu : (Maulia, 2017:140)

1. *Legal (hukum)*, diukur melalui keberadaan institusi legal atau framework keamanan siber
2. *Technical*, diukur melalui keberadaan institusi teknis dan penerapan teknologi
3. *Organizational*, diukur melalui koordinasi pembuat kebijakan serta pengembangan strategi keamanan siber
4. *Capacity Building*, diukur melalui pendidikan dan program pelatihan, penelitian dan pengembangan profesional dan aparatur yang tersertifikasi
5. *Cooperation*, diukur melalui adanya partnership, kerangka kerjasama atau *information sharing network.*

Beragam cara dapat dilakukan dalam meningkatkan atau membangun kemanan siber oleh suatu negara seperti peningkatan kapasitas siber dalam negeri, kerjasama dengan negara lain atau bahkan organisasi-organisasi internasional.

Di Indonesia sendiri tentunya telah digalakkan berbagai kebijakan dan usaha-usaha dalam membangun kemanan siber. Salah satu bentuk peningkatan kapasitas siber dalam

negeri ialah adanya Keamanan Siber Nasional (*National Cyber Security*) oleh Kemenhan. *National Cyber Security* merupakan segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional dan bersifat lintas sektor.(Kemenhan, 2014 hal.5) Kemhan/TNI juga telah merancang pedoman pertahanan siber berdasarkan Permenhan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber.(Kemenhan, 2014:5) Salah satu bentuk kerja sama dalam upaya peningkatan keamanan siber melalui lingkungan eksternal ialah melalui ASEAN *Regional Forum* (ARF).

4. ASEAN Regional Forum (ARF)

ASEAN Regional Forum merupakan satu dari sekian forum ASEAN dalam membahas isu internasional. ARF merupakan salah satu badan sektoral yang berada di bawah koordinasi Dewan Masyarakat Politik dan Keamanan ASEAN (ASEAN *Political-Security Community*). Peserta ARF berasal dari 26 negara dan 1 entitas Uni Eropa (total 27), terdiri dari sepuluh negara anggota ASEAN (Brunei Darussalam, Kamboja, Indonesia, Laos, Myanmar, Malaysia, Filipina, Singapura, Thailand dan Viet Nam), sepuluh Mitra Wicara ASEAN (Amerika Serikat, Australia, Kanada, RRT, India, Jepang, Selandia Baru, Rusia, Korea Selatan, dan Uni Eropa), dan 7 negara lain di kawasan (Bangladesh, Korea Utara, Mongolia, Pakistan, Papua Nugini, Sri Lanka, Timor Leste). Penyebutan keanggotaan dalam ARF adalah peserta (participant). Tujuan ASEAN Regional Forum diuraikan dalam Pernyataan Ketua ARF Pertama (1994).

Pembentukan ARF ditujukan untuk beberapa hal berikut:

1. Mendorong dialog dan konsultasi yang konstruktif atas isu-isu politik dan keamanan yang menjadi perhatian bersama di kawasan;(Kemlu.go.id diakses 19 Mei 2019)
2. Memberikan kontribusi nyata bagi upayaupaya pembangunan rasa saling percaya (confidence-building) dan diplomasi preventif (preventive diplomacy) di kawasan Asia Pasifik; dan(Kemlu.go.id diakses 19 Mei 2019)
3. Mendorong kerjasama yang dapat menumbuhkembangkan budaya damai, toleransi, saling memahami dan beradab. ARF diharapkan dapat mendukung upaya penciptaan lingkungan yang kondusif bagi pembangunan yang berkelanjutan dan bagi kemajuan lainnya yang bermanfaat bagi kehidupan manusia.

Kerjasama ARF dilakukan melalui 3 tahapan yaitu *Promotion of Confidence Building Measures (CBM), Development of Preventive Diplomacy mechanisms (PD), dan Development of Conflict Resolution mechanisms*.(Kemlu.go.id diakses 19 Mei 2019) Dalam

kegiatannya ARF juga melibatkan peran akademisi untuk membantu mengidentifikasi dan mengkaji permasalahan politik dan keamanan di kawasan.

ARF juga mengadakan dialog mengenai isu-isu militer, pertahanan, dan keamanan secara rutin melalui mekanisme *ARF Defence Officials' Dialogue, ARF Security Policy Conference, ARF Heads of Defence Universities/Colleges/Institutions Meeting*, baik di antara pejabat pertahanan maupun universitas atau institusi pertahanan. Area prioritas kerja sama yang dibahas dalam ARF terdiri dari 4 bidang besar, yaitu:

1. Penanggulangan bencana (*disaster relief*);
2. Kontra-terorisme dan kejahatan lintas negara (*counter-terrorism and transnational crime*);
3. Keamanan Maritim (*maritime security*);
4. Non-proliferasi dan perlucutan senjata (*non-proliferation and disarmament*); dan
5. Teknologi Informasi dan Komunikasi (i*nformation and communication technologies).*

Tiap area kerja sama diatas memiliki *Work Plan* yang berlaku selama 2 atau 3 tahun yang berisikan mengenai agenda, kegiatan dan hal yang harus dilakukan selama kurun waktu tersebut. Kegiatan seperti workshop, seminar, symposium atau training juga dilakukan untuk berbagi infomasi, meningkatkan pemahaman, membangun jejaring yang di harapkan dapat membantu membangun kapasitas pejabat pemerintah dalam menangani isu-isu keamanan

Mempertimbangkan komposisi peserta dan kerja sama yang dilakukan, kita dapat menyimpulkan bahwa memiliki 3 potensi berikut, yaitu:

1. *Investment in the habit of dialog and cooperation*. Bagi Indonesia, forum ini merupakan wadah untuk menumbuh-kembangkan budaya dialog dan kerja sama dalam menangani perbedaan atau konflik di kawasan. Indonesia juga menegaskan bahwa penggunaan use of force atau threat of use of force bukan merupakan opsi dalam menyelesaikan masalah antarnegara.
2. *Early Warning System.* Menjadikan Forum ini sebagai sistem peringatan dini atas *emerging security issues* yang belum atau perlu mendapatkan perhatian lebih dari pemerintah RI.
3. *Test the Water***.** Menjadikan Forum ini sebagai kesempatan untuk mengarusutamakan isu-isu yang menjadi kepentingan RI yang belum menjadi perhatian kawasan guna mendorong Peserta ARF lainnya untuk bekerja sama dalam penanganan isu tersebut.

5. Kepentingan Nasional Indonesia

Ancaman siber ataupun serangan siber seringkali mengincar objek-objek vital suatu negara sehingga menyebabkan kerugian besar yang harus ditanggung oleh berbagai pihak. Padahal ruang siber secara langsung dapat meningkatkan perekonomian negara baik secara makro maupun mikro. Salah satu nya melalui keberadaan usaha-usaha "*unicorn*" yang semakin berkembang serta keberadaan mangsa pasar yang tidak lagi terbatas pada skala nasional namun pada skala dunia. Selain itu kini digalakkan pula revolusi industri 4.0 dimana kemananan siber merupakan hal yang sangat penting bagi sebuah industri nantinya. Untuk itu keamanan siber sangat lah dibutuhkan demi menjaga objek-objek vital negara sekaligus mendorong peningkatan perekonomian suatu negara.

Dengan adanya peningkatan keamanan siber melalui kerja sama negara internasional ataupun pemanfaatan organisasi internasional (ASEAN) sebagai wadah nya. Maka Indonesia telah menunjukan eksistensi nya dalam berkomitmen, serta menunjukan kemampuan negara dalam menyelesaikan sebuah isu permasalahan. Kerja sama seperti ini juga menjadi media dalam memperlihatkan kontribusi atau sumbangsih Indonesia dalam menjaga dan mempertahankan kedamaian dunia.

Tindakan Indonesia dalam mengamankan objek vital negara, memperbaiki perekonomian serta mewujudkan perdamaian dunia sejalan dengan apa yang dikemukakan oleh K.J Holsti (1988) yang mengidentifikasi kepentingan nasional berdasarkan 3 klasifikasi yaitu:

1. *Core values* atau sesuatu yang dianggap paling vital bagi negara dan menyangkut eksistensi suatu negara.
2. *Middle-range objectives*, biasanya menyangkut kebutuhan memperbaiki derajat perekonomian.
3. *Long-range goals*, merupakan sesuatu yang bersifat ideal, misalnya keinginan mewujudkan perdamaian dan ketertiban dunia.

Keikutsertaan Indonesia dalam ARF menggambarkan upaya Indonesia dalam mencapai kepentingan nasional melalui lingkungan Eksternal. Tindakan ini merupakan salah satu bentuk contoh bahwa lingkungan eksternal merupakan salah satu faktor yang dapat berpengaruh pada kondisi domestik negara. Kepentingan nasional terbentuk dari asumsi bersama suatu bangsa terhadap suatu kondisi tertentu yang mengharuskan suatu negara menjadikannya perhatian mendasar. (Jackson & Sorensen, 2013) Maka ikut serta nya Indonesia dalam ASEAN *Regional Forum* telah menegaskan bahwa bangsa Indonesia memandang ancaman *cyber* sebagai suatu situasi yang memerlukan perhatian khusus karena dapat mengancam kondisi keamanan nasional negara. (David & Arwin, 2016:17) Ancaman yang berasal dari ruang *cyber* dapat mengakibatkan gangguan pada sektor ekonomi, politik,

dan sosial bahkan mengganggu keamanan dan pertahanan negara. Maka dari itu *cybersecurity* merupakan sebuah kepentingan nasional yang sifatnya mutlak karena berhubungan dengan optimalisasi fungsi pertahanan negara dalam menjaga dan melindungi kedaulatan serta keutuhan Indonesia. Terlebih menyangkut keselamatan rakyat dan bangsa indonesia. Hal ini juga sesuai dengan pendapat Andrew Heywood dalam bukunya *Global Politics,* bahwa kepentingan nasional merupakan tujuan kebijakan luar negeri atau preferensi kebijakan yang menguntungkan bagi masyarakat secara keseluruhan.(Andrew Heywood, 2011) Terjaga nya keamanan suatu negara tentu menguntungkan masyarakat secara keseluruhan.

Perlu dipahami bahwa *cyberspace* memiliki cangkupan yang sangat luas dimana penggunaannya telah menyentuh berbagai aspek kehidupan bangsa dan negara seperti penyebaran informasi dan promosi pendidikan, percepatan transaksi ekonomi, bahkan teknologi militer. Kini jelas kemanan di bidang siber dibutuhkan demi keberlanjutan pembangunan nasional, stabilitas regional dan perdamaian dunia.

Dihadapkan pada kepentingan nasional tersebut, sangat perlu untuk mengukur, mengantisipasi, memahami, mengkaji, dan menyiapkan tindakan yang dibutuhkan dalam menangani kondisi-kondisi di bidang siber. Oleh karena itu diperlukan penyusunan suatu pedoman pertahanan siber sebagai acuan yang digunakan untuk persiapan, pembangunan, pengembangan dan penerapan pertahanan siber. Kementerian Pertahanan dan Tentara Nasional Indonesia sendiri memiliki dua kepentingan dalam pertahanan siber. Pertama untuk mengamankan semua sistem elektronik maupun jaringan informasi. Kedua mendukung koordinasi pengamanan siber di sektor-sektor lain sesuai kebutuhan.

6. Diplomasi Siber Indonesia

Deputi bidang proteksi infrastruktur informasi kritikal BSSN, Agung Nugraha dalam seminar nasional yang dilakukan tahun 2018 di kota Bandung, telah memaparkan bahwa diplomasi siber berbeda dengan diplomasi publik. Diplomasi siber merupakan diplomasi dimana hal-hal terkait bidang siber menjadi instrumen utama dalam melakukan negosiasi serta menjalin suatu hubungan dengan negara lain. Berdasarkan wawancara pribadi yang dilakukan dalam jurnal David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, Direktorat Kerjasama Internasional Kementerian Pertahanan mengemukakan bahwa

> Kondisi saat ini berada pada titik dimana lingkungan strategis semakin tidak pasti dan tidak dapat diprediksi. Oleh karenanya, pemerintah Indonesia perlu menerapkan strategi yang mampu beradaptasi dan meningkatkan peran diplomasi yang dilakukan dalam mencegah konflik yang dapat mengganggu stabilitas kawasan serta kepentingan nasional. (David & Arwin, 2016)

Oleh karena nya upaya dalam membangun *cybersecurity* , bukanlah sesuatu yang dapat diperjuangkan sendirian oleh suatu negara. Diperlukan berbagai dukungan dan kerjasama serta keselarasan dari berbagai pihak dalam pembangunan keamanan siber. Pemerintah Indonesia sangat menyadari gagasan bahwa lingkungan keamanan siber tidak dapat dibangun seorang diri melainkan lebih efektif apabila dilakukan bersama-sama. Berangkat dari gagasan tersebut Indonesia melakukan upaya kerja sama dengan negara dan organisasi internasional. Contoh nya ialah keikutsertaan ASEAN *Regional Forum* di tingkat regional atau kawasan.

Di forum multilateral seperti ARF, Indonesia menggunakan diplomasi sebagai instrumen dalam mencapai kepentingan nasional sekaligus membangun hubungan baik dengan negara lain. Indonesia sadar bahwa situasi eksternal dan stabilitas keamanan di kawasan dapat mempengaruhi keamanan nasional nya. Jadi melalui diplomasi tersebut Indonesia dapat mengamankan wilayahnya sekaligus berkontribusi pada stabilitas keamanan di kawasan. Melalui diplomasi nya, Indonesia menginisisasi beberapa hal di forum ARF diantaranya:

1. Kontak Point

Salah satu capaian diplomasi Indonesia ialah diperolehnya kontak poin (*point of contacts)* dari perwakilan negara-negara ASEAN maupun negara-negara di kawasan regional yang juga menghadapi masalah *cybersecurity.*(David & Arwin, 2016:11) kontak poin diusulkan untuk memudahkan komunikasi antar negara ketika terjadi suatu serangan *cyber*. Kontak poin yang diperoleh akan memudahkan Indonesia dalam melakukan proses diplomasi, baik berupa diplomasi dalam penanganan insiden *cyber,* maupun hal-hal lain terkait dengan pencapaian tujuan bersama. Perlu diketahui bahwa kontak poin yang diperoleh tidak hanya sebatas nama instansi atau nomor telpon instansi tersebut, tetapi juga nomor pribadi serta email pribadi pejabat yang memiliki kewenangan. Ini merupakan sebuah kesempatan bagi pemerintah Indonesia supaya mendapatkan hasil yang lebih maksimal karena proses diplomasi dan komunikasi dapat berjalan lebih mudah.

Kontak poin yang berhasil diperoleh berasal dari seluruh negara anggota ASEAN dan negara-negara non anggota ASEAN seperti AS, China, Belanda, Australia dan Rusia. Usulan mengenai adanya kontak poin tersebut merupakan gagasan murni yang berasal dari pemerintah Indonesia. (David & Arwin, 2016:11) Gagasan ini diterima dan disepakati lalu dituangkan dalam dokumen ASEAN *Regional Forum Workplan on Security of and in the Use of Information and Communications Technologies* (ICT's).

Kontak poin juga digunakan dalam upaya memudahkan identifikasi pelaku kejahatan siber. Dengan teridentifikasinya pelaku kejahatan siber tentu akan memberi kemudahan bagi pemerintah Indonesia dalam mengambil suatu tindakan.

Misal, jika terjadi serangan *cyber* dan teridentifikasi berasal dari singapura, pemerintah tentu harus mengetahui apakah serangan tersebut berasal dan dilakukan oleh suatu kelompok tertentu atau bahkan merupakan ulah *state aktor*. Dengan adanya kontak poin pemerintah dapat melakukan klarifikasi melalui kontak poin negara bersangkutan. Setelah itu negara dapat memutuskan tindakan lanjutan yang paling efektif atau bahkan melakukan serangan balasan. Jika serangan tersebut teridentifikasi sebagai ulah suatu negara, maka kita dapat membalas dengan kapasitas sebagai sebuah negara. Namun, apabila serangan tersebut dilakukan oleh suatu kelompok *non state aktor* maka merupakan suatu tindakan yang cukup berlebihan dan tidak efektif apabila kita merespon serangan tersebut dengan kapasitas sebagai sebuah negara.

Kasus serupa pernah dialami bangsa Indonesia, tepatnya ketika pemerintah Indonesia hendak mengeksekusi mati dua orang pelaku tindak kejahatan pengedaran narkoba berkewarganegaraan Australia. Sebagai bentuk keberatan atas vonis hukuman mati yang di berikan, serangan siber *(cyber attack)* dilancarkan pada beberapa situs resmi milik pemerintah Indonesia. Hal ini berlanjut pada serangan balik terhadap situs-situs resmi milik pemerintah Australia. Peristiwa ini hampir mengakibatkan terjadinya perang *cyber (cyber warfare)* antar negara, namun dapat dicegah dengan melakukan konfirmasi serta klarifikasi oleh masing-masing negara melalui kontak poin yang ada. Hasil dari koordinasi tersebut ialah bahwa masing-masing pihak saling menjaga sisi *cyber* di wilayahnya untuk menahan diri dan tidak saling menyerang.(David & Arwin, 2016:12)

2. Membentuk Suatu Kurikulum Untuk Meningkatkan *Capacity Building* Melalui *Study Group*

Pada tingkat kawasan seperti Asia Tenggara, belum ada kebijakan regional khusus mengenai *cybersecurity*. Ini merupakan peluang bagi pemerintah Indonesia dalam mempromosikan kebutuhan keamanan *cyber* di tingkat regional. Indonesia melalui ASEAN *Regional Forum* menyarankan untuk menyusun suatu kurikulum khusus terkait siber. Indonesia juga mengusulkan pembentukan *study group* untuk mengkaji, menyusun ataupun merumuskan kurikulum tersebut. Dengan terlibat nya Indonesia dalam perumusan kurikulum maka Indonesia dapat menyelipkan nilai-nilai kepentingan nasional di dalamnya. Kurikulum yang dimaksud dapat berupa sebuah prosedur ataupun protokol khusus untuk menangani hal-hal terkait siber.

Study group ini tidak hanya berfokus pada pembentukan kurikulum tetapi juga mencangkup diadakannya workshop, seminar dan pelatihan di tingkat regional mengenai penanganan siber sekaligus berbagi pengetahuan mengenai *cybersecurity.* Pada salah satu *study group* yang telah diadakan, Indonesia memaparkan berbagai bentuk penanganan tentang menyikapi serangan *cyber.* Dalam *study group* tersebut, pemerintah Indonesia bersama dengan delegasi Rusia membentuk suatu simulasi mengenai penanganan insiden *cyber.* (David & Arwin, 2016:17)

Salah satu tujuan diadakannya *study grup* ini ialah agar pemerintah Indonesia dapat membentuk suatu kurikulum untuk meningkatkan *capacity building* bersama dengan negara-negara ASEAN lainnya. Gagasan mengenai adanya *study group* ini merupakan satu dari dua usul pemerintah Indonesia yang diterima dan di tetapkan dalam ASEAN regional forum *work plan on Ict's*

3. *Internet Protocol Version 4* (Ipv4) *Upgrade* Ipv6

Melalui *ASEAN Regional Forum*, pemerintah Indonesia juga mengusulkan pada seluruh negara-negara ASEAN untuk melakukan transisi atau *upgrade* pada penggunaan *Internet Protocol version 4* (IPv4) ke *Internet Protocol version 6* (IPv6). Ini merupakan salah satu solusi konkret dan efektif dalam upaya peningkatkan sistem keamanan internet. Usulan perubahan penggunaan IPv4 ke IPv6 merupakan suatu solusi dalam meningkatkan kapabilitas pertahanan dan keamanan jaringan internet di ASEAN, mengingat bahwa IPv6 memiliki sistem keamanan yang lebih baik dan dapat diubah sesuai kebutuhan. Namun usul tersebut mendapat respon yang tidak memuaskan. Hal ini terjadi karena seringkali delegasi yang dikirim adalah seseorang yang tidak menguasi bidang *cyber*.(David & Arwin, 2016:12)

Kendala lain yang harus dihadapi ialah kenyataan bahwa beberapa negara ASEAN memang belum memenuhi persyaratan keamanan. Sebagai contoh, dalam hal *Domain Name Server* (DNS) *security*, Indonesia berada pada *grade* A di dunia namun masih banyak negara-negara ASEAN yang berada dibawah grade tersebut. Tidak semua negara ASEAN memiliki standar keamanan yang dimaksud. Hanya Pemerintah Indonesia melalui Kemenkopolhukam dan Pemerintah Korea Selatan yang telah mampu memenuhi semua kriteria yang ada. (David & Arwin, 2016:13) Kurangnya kemampuan sumber daya dan kondisi-kondisi diatas merupakan salah satu kendala dalam proses diplomasi di ASEAN *Regional Forum.*

4. Pembentukan Badan Atau Lembaga Yang Bertanggung Jawab Mengenai *Cybersecurity* Masing-Masing Negara

Kondisi dimana tidak adanya dukungan dari kebijakan dalam negeri yang mengatur mengenai *cyberspace* secara komprehensif, tentu akan menyebabkan usaha-usaha yang telah

dilakukan di tingkat regional tidak lagi efektif. Pemerintah Indonesia mengusulkan agar masing-masing negara segara membentuk suatu badan atau suatu lembaga yang bertanggung jawab secara khusus mengenai *cybersecurity*. (David & Arwin, 2016:13) Hal ini dilakukan bukan tanpa alasan, pada faktanya masih terdapat beberapa negara ASEAN yang belum memiliki badan khusus untuk menangani bidang *cybersecurity.* Hal ini tentu berdampak pada peningkatan *capacity building* di tingkat regional terhambat dan menyebabkan beberapa kontak poin yang diterima Indonesia dari negara lain bersifat informal. Dengan adanya badan resmi yang bersifat khusus tentu akan mempermudah proses diplomasi dalam pencapaian kepentingan nasional di bidang *cybersecurity*. Selain itu Pemerintah Indonesia dapat memetakan jaringan serangan, melakukan klarifikasi, dan mengambil tindakan yang efektif bersama dengan negara lain dan menghindari adanya kesalahpahaman ataupun hal-hal lain terkait *cyber* diplomasi.

Indonesia sendiri telah membentuk badan resmi dan bersifat khusus dalam penanganan terkait bidang siber. Lembaga yang dimaksud ialah Badan Sandi dan Siber Negara atau disingkat BSSN. BSSN sendiri memiliki lingkup kegiatan seperti teknis di bidang deteksi, identifikasi, proteksi, pemantauan, penanggulangan, pemulihan, evaluasi, pengendalian proteksi e-ommerce, penapisan, persandian, diplomasi siber, sentra informasi, pusat manajemen krisis siber, pusat kontak siber, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan serangan siber

Dari keempat poin yang diusulkan oleh Indonesia di ARF, dua diantaranya disetujui dan disepakati. Kedua poin tersebut kemudian dituangkan dalam *ASEAN Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies (Ict's)*.

7. Kesimpulan

Mengingat ruang siber menjadi celah untuk berbagai tindak kejahatan yang dapat mengancam stabilitas dan keamanan nasional suatu negara. Diperlukan tindakan pengamanan untuk mencegah dan mengantisipasi ancaman-ancaman yang berasal dari ruang siber sekaligus menjaga kemananan nasional negara. Menjaga keamanan nasional suatu negara merupakan kepentingan nasional yang bersifat mutlak. Diperlukan adanya lingkungan yang mendukung terbentuknya keamanan siber secara efektif. Yaitu keselerasan antara hukum, struktur organisasi yang jelas, *capacity building*, teknis dan prosedural, dan kerja sama internasional. Indonesia menyadari bahwa pembangunan keamanan siber tidak dapat dilakukan sendiri dan akan lebih efektif apabila dilakukan bersama dengan

Indonesia aktif dalam keikutsertaan di ASEAN *Regional Forum*. Pada forum yang dilaksanakan tahun 2015 Indonesia mengusulkan empat hal. Pertama, Indonesia menginisisasi negara-negara ASEAN untuk membentuk suatu kurikulum demi meningkatkan capacity building melalui study group, karena belum adanya kurikulum atau protokol khusus dalam menghadapi ancaman siber di tingkat regional seperti Asia Tenggara. Kedua mengajak negara-negara anggota ASEAN melakukan transisi atau upgrade pada penggunaan *Internet Protocol version 4* (IPv4) ke *Internet Protocol version 6* (IPv6) sebagai solusi konkrit dan efektif dalam upaya peningkatkan sistem keamanan internet. Ketiga, pemerintah Indonesia juga mengusulkan agar masing-masing negara segara membentuk badan atau lembaga yang bertanggung jawab mengenai cybersecurity , mengingat masih banyak negara-negara ASEAN yang belum memiliki badan atau lembaga khusus dalam menangani isu siber, Keempat ialah adanya kontak poin (*point of contact*) dari masing- masing negara untuk memudahkan pemerintah Indonesia dalam melakukan proses diplomasi, baik berupa diplomasi dalam penanganan insiden cyber, maupun hal-hal lain terkait dengan pencapaian tujuan bersama. Dua poin diantaranya di terima dan dituangkan dalam dalam *ASEAN Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies* (Ict's).

Daftar Pustaka

Fischer, E. A. 2009. *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options.* New York: Nova Science Publishers, Inc.

Heywood, Andrew. 2011. *Global Politics*. New York: Palgrave Macmillan

Holsti, K. J. 1998. *Politik Internasional: suatu kerangka Analisis Jilid I.* Jakarta: Erlangga

ID-SIRTII. 2017. *Tren Serangan Siber Nasional 2016 dan Prediksi 2017*. ID-SIRTII.

ITU. 2017. *Global Cybersecurity Index 2017*. International Telecommunication Unit.

Jackson, R., & Sorensen, G. 2013. *Introduction to International Relations*. United Kingdom: Oxford University Press.

KEMENHAN 2014. RI, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber*. Kementrian Pertahanan

Lewis, James Andrew. 2013. *Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia*. Lowy Institute MacArthur

Richardus Eko Indrajit. 2011. *Pengantar konsep keamanan informasi di dunia siber*. Aptikom

Samadikun, Samaun. 2000. *Pengaruh Perpaduan Teknologi Komputer, Telekomunikasi dan Informasi*. Jakarta: Kompas

Jurnal :

Setyawan, David Putra & Arwin Datumaya Wahyudi Sumari. 2016. Jurnal *Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives*. Universitas Pertahanan Indonesia

Maulia, Jayantina Islami. 2017. *Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index* Jurnal Masyarakat Telematika dan Informasi Volume: 8 No. 2

Heinl, Caitriona. H. 2013. *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. asia policy*. Singapore: S.Rajaratnam School of International Studies

Sukayasa, I Nyoman & Wayan Suryath. 2018. *Law Implementation of Cybercrime in Indonesia Department of Business Administration.* Politeknik Negeri Bali

Website :

Kementrian luar negeri, Forum regional ASEAN dalam https://kemlu.go.id/portal/id/read/126/halaman_list_lainnya/forum-regional-asean-arf#! Diakses pada 19 Mei 2019