PEMBANGUNAN KAPASITAS *CYBER SECURITY* DI NEGARA ASEAN: ANALISIS KOMPARATIF TERHADAP BRUNEI DAN INDONESIA

CYBER SECURITY CAPACITY BUILDING IN ASEAN COUNTRIES: A COMPARATIVE ANALYSIS OF BRUNEI AND INDONESIA

I Wayan Midhio[1]; Yono Reksoprodjo[2]; Hamzah Zaelani[3]
Universitas Pertahanan
(midhio_2003_iwayan@yahoo.com; yono@sintesagroup.com; zaylen28@gmail.com)

Abstrak – Memasuki era teknologi informasi yang berperanan penting bagi semua aspek kehidupan baik individu, organisasi, ataupun suatu Negara membuat masyarakat seakan memperoleh sebuah dunia baru yang kemudian dinamakan *cyber space*. Kehadiran *cyber space* memunculkan dampak negative yang tentu memerlukan perhatian serta keseriusan seluruh pihak dalam membangun kapasitas *cyber security* suatu Negara sebagai upaya dalam memberikan keamanan di dunia siber. Oleh karena itu, hal ini kemudian membuat setiap Negara berupaya secara maksimal dalam membangun kapasitas *cyber security* secara nasional. Tulisan ini akan membahas mengenai pembangunan kapasitas *cyber security* di Negara ASEAN dengan melakukan analisis komparatif terhadap Brunei Darussalam dan Indonesia. Metode yang digunakan dalam penelitian ini ialah kualitatif dengan pendekatan deskriptif. Hasil penelitian ini menggambarkan perbandingan pembangunan kapasitas *cyber security* antara Brunei Darussalam dan Indonesia sehingga dapat menjadi masukan dalam mengembangkan kapasitas *cyber security* Indonesia kedepannya.
Kata Kunci: *cyber security*, pembangunan, Brunei, Indonesia, keamanan siber

Abstract *-- Encountering the era of information technology that plays an important role in all aspects of life whether an individuals, an organizations, or a State made the communities as if acquiring a new world which called cyber space. The presence of cyber space raises negative impact that would require an attention and a seriousness from all the parties in building the cyber security capacity of a State as an effort in providing security in the cyber space. Therefore, this makes every State have to put a maximum effort in building national cyber security capacity. This paper will discuss the development of cyber security capacity in ASEAN countries by conducting comparative analysis on Brunei Darussalam and Indonesia. The method used in this research is qualitative with descriptive approach. The results of this study illustrate the comparison of cyber security capacity building between Brunei Darussalam and Indonesia. Then, it can be an input in developing the capacity of Indonesian cyber security in the future.*
Key Words: cyber security, development, Brunei, Indonesia

[1] Dosen di Universitas Pertahanan.
[2] Dosen di Universitas Pertahanan.
[3] Mahasiswa Prodi Peperangan Asimetris Co.5 Universitas Pertahanan

Pendahuluan

Dewasa ini, dunia tengah memasuki era teknologi informasi yang memiliki peranan penting bagi semua aspek kehidupan baik individu, organisasi, ataupun suatu Negara. Salah satu hal yang kemudian memberikan pengaruh besar bagi masyarakat ialah hadirnya internet. Seiring dengan penggunaan jaringan system computer yang menggunakan infrastruktur system telekomunikasi, pada akhirnya masyarakat seakan memperoleh sebuah dunia baru yang kemudian dinamakan *cyber space*.[4] *Cyber space* ialah sebuah tempat maya dimana komunikasi antar pengguna terjadi. Istilah ini pada awalnya diperkenalkan oleh seorang novelis sains fiksi bernama William Gibson pada buku *Neuromancer*, dimana saat itu ia melihat semacam integrasi antara komputer dengan manusia.[5]

Kehadiran *cyber space* mengakibatkan masyarakat cukup sulit untuk melepaskan dirinya dari arus komunikasi dan informasi, sehingga pada akhirnya selain memberikan kemudahan bagi masyarakat untuk memperoleh informasi, internet juga memberikan dampak negatif bagi kehidupan manusia.[6] Dampak negative ini tentu menjadi ancaman bagi setiap pengguna *cyber space*. Ancaman tersebut dapat muncul dari individu, organisasi, pengusaha, atau pemerintah, baik disengaja ataupun tidak disengaja.[7] Munculnya dampak negative dari kehadiran *cyber space* tentu memerlukan perhatian serta keseriusan seluruh pihak dalam membangun kapasitas *cyber security* suatu Negara sebagai upaya dalam memberikan keamanan di dunia siber.

Berdasarkan data United Nations Institute for Disarmament Research (UNIDIR) pada tahun 2011 ada 68 dari 193 negara anggota PBB yang memiliki *cyber security programmes* dimana 32 negara diantaranya memasukan juga *cyberwarfare* dalam organisasi dan perencanaan militer. Kemudian pada tahun 2012 terjadi peningkatan jumlah menjadi 114 dari 193 negara anggota PBB yang memiliki *cyber security*

[4] M. Arsyad Sanusi, Hukum Teknologi dan Informasi, (Bandung: Tim Kemas Buku, 2005), hlm. 93

[5] John Vivian, Teori Komunikasi Massa, (Jakarta: Kencana, 2008), hlm. 264

[6] Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, (Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007), hlm. 3

[7] M. Smith, *Research Handbook on International Law and Cyberspace*, (Massachusetts: Edwar Elgar Publishing Limited, 2015), hlm. 1

programmes.[8] Upaya yang dilakukan Negara – Negara tersebut dalam membangun kapasitas siber kebanyakan melibatkan langkah yang paling mendasar, seperti melalui undang – undang *cybercrime*, meningkatkan kemampuan penegakan hukum, atau menciptakan tim tanggap darurat yang biasa disebut *Computer Emergency Response Team (CERT)*. Pada Negara maju, pembangunan kapasitas *cyber security* juga telah dikembangkan strategi untuk melakukan perlindungan terhadap infrastruktur kritis serta dengan membentuk organisasi yang secara khusus bertanggung jawab terhadap permasalahan *cyber security*.

Pada lingkup regional, Negara – Negara anggota ASEAN juga melakukan pembangunan kapasitas *cyber security* karena menganggap hal ini cukup mendesak. Hal ini terbukti dengan dilakukannya pembahasan mengenai *cyber security* dalam berbagai macam diskusi dalam salah satu forum kerjasama politik dan keamanan bernama *Associattion of South East Asian Nation Regional Forum (ARF)*. Salah satu contoh Negara ASEAN yang sudah sejak lama memberikan perhatian terhadap persoalan *cyber security* ialah Brunei Darussalam.

Sejak tahun 1992, Pemerintah Brunei Darussalam telah merumuskan kerangka perencanaan strategi teknologi informasinya yang kemudian mulai dijalankan di akhir tahun 2000. Penerapan teknologi informasi oleh Pemerintah Brunei Darussalam dituangkan pada tiga hal, yaitu *e-government, e-business* dan *e-Brunei* yang pada awalnya diberi nama "*IT 2000 and Beyond"* sebagai *national strategic IT plan* Brunei Darussalam.[9] Penerapan strategi tersebut tentu saja menimbulkan ancaman *cyber* bagi Brunei. Dalam rangka memberikan keamanan siber bagi Brunei, maka pada tahun 2004 dibentuk *Brunei Computer Emergency Response Team (BruCERT)* dibawah *Information Technology Protective Security Services (ITPSS)*, sebuah perusahaan yang bekerjasama dengan Kementrian Komunikasi Pemerintah Brunei Darussalam.[10] Sebagai sebuah tim yang bertugas untuk melakukan pengamanan terhadap ancaman siber, BruCERT memiliki lima kemampuan,

[8] Center for Strategic and International Studies, The Cyber Index: International Security Trends and Realities, (UNIDIR, 2013) hlm. 13

[9] Richardus E. Indrajit, Strategi Brunei Menuju Masyarakat Berbasis Elektronik, (Jakarta: 2013), hlm. 1

[10] Center for Strategic and International Studies, *op.cit*., hlm. 58

antara lain ialah *incident response, managed security services, network security analysis, log security analysis,* serta *malware analysis*.[11]

Indonesia sebagai salah satu Negara anggota ASEAN juga telah cukup lama melakukan berbagai macam upaya untuk membangun kapasitas *cyber security*. Hal ini salah satunya didorong karena besarnya jumlah pengguna internet Indonesia yang pada tahun 2017 sudah mencapai angka 132,7 juta.[12] Selain itu, maraknya berbagai ancaman *cyber* di Indonesia membuat Pemerintah merumuskan berbagai macam kebijakan dalam rangka mengatasi permasalahan tersebut. Bahkan, sebuah fakta yang mengejutkan hadir dari sebuah perusahaan *monitoring internet* Akamai yang menyatakan bahwa terjadi peningkatan kejahatan internet di Indonesia yang kemudian menempatkan Indonesia di peringkat pertama sebagai Negara yang berpotensi menjadi target *hacker* dengan kontribusi sebesar 38% dari total sasaran *traffic hacking* di internet.[13] Salah satu upaya yang dilakukan oleh Indonesia dalam membangun kapasitas *cyber security* dilakukan sejak tahun 2007 melalui Peraturan Menteri Komunikasi dan Informatika No. 26 mengenai pengamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet yang kemudian dilakukan revisi dengan Peraturan Menteri Komunikasi dan Informatika No. 29 tahun 2010. Salah satu hal yang diatur dalam peraturan tersebut ialah mengenai pembentukan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII).[14]

Perbedaan langkah di setiap Negara anggota ASEAN, khususnya Brunei Darussalam dan Indonesia dalam membangun kapasitas *cyber security* masing – masing yang kemudian melatarbelakangi penulis untuk membahas secara lebih mendalam mengenai pembangunan kapasitas *cyber security* di Negara ASEAN dengan melakukan analisis komparatif terhadap Brunei Darussalam dan Indonesia.

[11] Penjelasan BruCERT pada kegiatan Kuliah Kerja Luar Negeri Mahasiswa Peperangan Asimetris di kantor ITPSS, Brunei Darussalam pada tahun 2017

[12] Laporan hasil survey Asosiasi Penyedia Jasa Internet Indonesia (APJII), http://www.apjii.or.id/survei diakses 12 April 2017 pukul 17.00 WIB.

[13] Indonesian Attack Traffic Tops List, https://blogs.akamai.com/2013/10/indonesia-attack-traffic-tops-list-port-445-no-longer-main-launching-pad.html diakses 12 April 2017 pukul 18.30 WIB.

[14] Handrini Ardiyanti, Cyber Security dan Tantangan Pengembangannya di Indonesia, https://jurnal.dpr.go.id/index.php/politica/article/view/336 , 2014, hlm. 99.

Sehingga diharapkan melalui tulisan ini Indonesia dapat melakukan studi komparatif dalam pembangunan kapasitas *cyber security*.

Metodologi

Metode yang digunakan dalam tulisan ini menggunakan metode kualitatif deskriptif yang disajikan dengan data – data yang dikaji melalui pendekatan wawancara, studi literature, studi pustaka, dan *online research*. Data primer yang digunakan dalam penelitian ini diperoleh melalui wawancara selama pelaksanaan Kuliah Kerja Luar Negeri Program Studi Peperangan Asimetris di Brunei Darussalam yang diberikan oleh lembaga – lembaga di Brunei seperti ITPSS. Selain itu, digunakan pula data sekunder yang penulis peroleh dari berbagai sumber informasi relevan mengenai pembangunan kapasitas *cyber security* di Brunei Darussalam dan Indonesia.

Kapasitas Siber

Cyber security terdiri dari berbagai macam aspek, seperti kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman pelaksanaan, pendekatan manajemen resiko, tindakan, serta pelatihan yang kemudian digunakan untuk melindungi ruang siber. Organisasi dan asset pengguna dalam *cyber security* termasuk pada perangkat, personil, infrastruktur, aplikasi, layanan, serta system telekomunikasi pada dunia maya. Pada dasarnya, *cyber security* dibangun diatas lima bidang kerja, yaitu kepastian hukum, tindakan procedural, struktur organisasi, *capacity building*, dan kerjasama internasional.[15]

Sementara *Cyber security* lebih lanjut dipahami sebagai bagian dari mekanisme yang dilaksanakan untuk melindungi dan meminimalisir gangguan terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), serta ketersediaan (*availability*) informasi. Mekanisme ini kemudian harus mampu melakukan perlindungan dari serangan fisik ataupun serangan siber. Adapun elemen – elemen pokok dari *cyber security* antara lain:

a. Dokumen *security policy* yang merupakan dokumen standar sebagai acuan dalam menjalankan proses pengamanan terhadap informasi.
b. *Information infrastructure* yang merupakan media yang berperan dalam kelangsungan penyebaran informasi, baik berupa perangkat keras ataupun perangkat lunak.
c. *Perimeter defense* sebagai media yang menjadi komponen pertahanan pada

[15] Handrini Ardiyanti, *op.cit*., hlm. 98

infrastruktur informasi, seperti IDS, IPS, serta *firewall*.

d. *Network Monitoring System* ialah media yang berperan untuk melakukan pengawasan kelayakan, utilisasi serta *performance* infrastruktur informasi.
e. *System Information and Event Management* ialah media yang berperan dalam melakukan pengawasan terhadap berbagai macam kejadian pada jaringan.
f. *Network Security Assesment* merupakan elemen dari *cyber security* yang memiliki peran dalam melakukan mekanisme control dan memberikan *measurement level* keamanan informasi.
g. *Human resource* dan *security awareness* yang berkaitan dengan sumber daya manusia serta kewaspadaannya terhadap keamanan informasi.

Selain persoalan *cyber security*, kelangsungan proses operasi informasi juga bergantung pada *physical security* yang tentunya memiliki hubungan dengan berbagai macam elemen fisik seperti bangunan *data center, disaster recovery system* serta media transmisi.[16]

Pembangunan Kapasitas *Cyber Security* Brunei Darussalam

Dalam aspek kepastian hukum guna menangani *cyber security* di Brunei Darussalam, *legal measures* dibagi menjadi dua hal, yaitu *criminal legislation* serta *regulation and compliance*. Beberapa instrument peraturan dalam *criminal legislation* antara lain ialah *Computer Misuse Act* yang sudah dibuat sejak tahun 2000 dan diperbaharui pada tahun 2007, *Penal Code* yang diperbaharui pada tahun 2014, serta *Copyright Order* sejak tahun 1999. Adapun instrument peraturan yang masuk pada bagian *regulation and compliance* antara lain ialah *Broadcasting (Class License) Notification* sejak tahun 2000, *Internet Code of Practice* sejak tahun 2001, serta *Electronic Transaction Act* sejak tahun 2008.[17]

Struktur organisasi Brunei Darussalam dalam penerapan *cyber security* sudah cukup baik. Upaya ini sudah dilakukan sejak tahun 2000 ketika Pemerintah Brunei Darussalam mencangkan kebijakan *e-government, e-brunei* dan *e-business* yang diberi nama "*IT 2000 and Beyond*". Sejak tahun 2000, Brunei membentuk sebuah badan untuk mengarahkan dan memfasilitasi pengembangan strategis dan penyebaran

[16] Handrini Ardiyanti, *op.cit*., hlm. 99

[17] Index Law of Brunei Darussalam, http://www.agc.gov.bn/AGC%20Site%20Pages/Legislation.aspx diakses 13 April 2017 pukul 14.00 WIB.

teknologi informasi dan komunikasi kepada masyarakat yang diberi nama *Brunei Darussalam Technology (BIT) Council*. Untuk mencapai tujuannya, badan ini menetapkan sepuluh tujuan yang mencakup berbagai area seperti *leadership, needs, IT Literacy, manpower, applications, Research & Development, links, economy, business* dan *relevance*.

Selain BIT *Council*, Brunei juga membentuk sebuah badan dibawah Menteri Keuangan yang bertugas untuk mengatur beberapa bidang seperti *good governance,* pengembangan berkelanjutan serta layanan elektronis dengan nama *Information Technology and States Stores Department (ITSSD)*. Pada dasarnya, ITSSD ialah badan secretariat dari BIT *Council*, sehingga memiliki tugas untuk mendukung aktifitas BIT *Council* , mengawasi implementasi dari *National IT Strategic Plan*, menjadi ujung tombak dalam memformulasikan serta mengimplementasikan berbagai kebijakan dan perencanaan teknologi informasi nasional, mengadakan hubungan dengan lembaga lain, serta mengatur komunikasi dan publikasi. Brunei Darussalam juga memiliki badan independen yang memiliki tugas untuk membuat regulasi dan mengembangkan industry teknologi informasi dan komunikasi yang diberi nama *Authority of Infocommunications Technology Industry (AITI)*.[18]

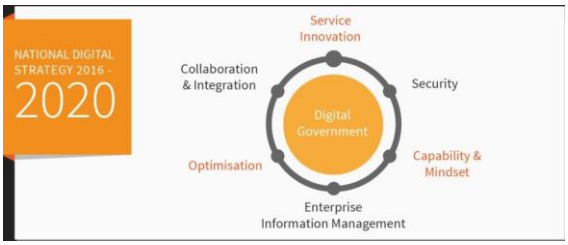
Dalam rangka memberikan keamanan siber bagi Brunei, maka pada tahun 2004 dibentuk *Brunei Computer Emergency Response Team (BruCERT)* dibawah *Information Technology Protective Security Services (ITPSS)*, sebuah perusahaan yang bekerjasama dengan Kementrian Komunikasi Pemerintah Brunei Darussalam. Sebagai sebuah tim yang bertugas untuk melakukan pengamanan terhadap ancaman siber, BruCERT memiliki lima kemampuan, antara lain ialah *incident response, managed security services, network security analysis, log security analysis,* serta *malware analysis*.[19]

Pada dasarnya, Pemerintah Brunei Darussalam sudah menetapkan sebuah strategi nasional dalam aspek *cyber* yang diberi nama *National Digital Strategy 2016 – 2020*. Strategi ini memiliki enam program utama yang terdiri dari *advancing digital services, implementing universal access for government systems, strengthening security, enhancing*

[18] Richardus E. Indrajit, *op.cit*., hlm. 3

[19] Penjelasan BruCERT pada kegiatan Kuliah Kerja Luar Negeri Mahasiswa Peperangan Asimetris di kantor ITPSS, Brunei Darussalam pada tahun 2017.

stakeholder engagement, optimizing digital assets, serta *developing enterprise information management capability*.[20]



Gambar 1. National Digital Strategy 2016 – 2020
Sumber: Slide Presentasi BruCERT, 2016

Dalam menjalankan pengamanan terhadap aspek *cyber*, hingga saat ini Pemerintah Brunei Darussalam masih melakukan pengembangan untuk membuat sebuah *framework* yang rencananya akan diberi nama *Brunei National Cyber Security Framework*. Ada berbagai lembaga yang berkerjasama dalam proses penyusunan kerangka tersebut. ITPSS sebagai perusahaan yang dipercaya oleh Pemerintah dalam *cyber security* juga termasuk dalam tim kerja tersebut. Kerangka kerja ini akan terdiri dari beberapa hal, yaitu standar operasional secara nasional dalam melakukan koordinasi, eskalasi serta menanggulangi insiden dalam *cyber security* di Brunei Darussalam. Dalam membangun kerangka kerja tersebut, ditetapkan delapan aspek yang menjadi infrastruktur kritis secara nasional, antara lain ialah *defense, government, E-Government, Banking & Finance, Energy, Health Services, Telecommunication,* serta *Transportation.*

Gambar 2. Proses Pembangunan *Brunei National Cyber Security Framework*
Sumber: Slide Presentasi BruCERT, 2016.

Dalam aspek *capacity building*, Brunei Darussalam melalui *Ministry of Education* telah memasukan *cyber security awareness* kedalam kurikulum pendidikan. Pada tahun ke 3, terdapat sebuah silabus pendidikan yang menjelaskan mengenai *risk, danger, responsible internet* serta *email safety rules*. Selain itu, BruCERT juga melakukan pembinaan dan pendidikan kepada masyarakat sejak tahun 2005 melalui berbagai program, seperti *Awareness Outreach Programs for Schools*. Selain itu, seminar – seminar juga dilakukan oleh ITPSS, salah satunya ialah seminar *Cybersecurity Threats & Risks in The Government Sectors* pada tahun 2015 yang bekerjasama dengan *Microsoft*. Upaya dalam meningkatkan *awareness* masyarakat terhadap *cyber security* juga

[20] Penjelasan ITPSS mengenai Brunei National Cyber Security Framework pada kegiatan Kuliah Kerja Luar Negeri Mahasiswa Peperangan Asimetris di kantor ITPSS, Brunei Darussalam pada tahun 2017.

dilakukan dengan penyebaran informasi melalui majalah, *e-book*, siaran radio serta informasi pada website khusus yang dibuat dalam meningkatkan *awareness* yaitu www.secureverifyconnect.info.

Tentunya, dalam membangun kapasitas *cyber security* dibutuhkan kerjasama internasional dengan Negara – Negara lain. Hal ini juga dilakukan oleh Pemerintah Brunei Darussalam melalui berbagai forum kerjasama internasional, anatara lain ialah *ASEAN Network Security Action Council, International Telecommunication Union (ITU), Asia Pacific Computer Emergency Response Team (APCERT), Forum of Incident Response and Security (FIRST)*, serta *OIC-CERT*. Brunei juga merupakan anggota dari *ITU-IMPACT* serta berpartisipasi dalam *ASEAN-Japan Information Security Meetings* sejak 2009.[21]

Pembangunan kapasitas *Cyber Security* Indonesia

Kebijakan dalam *cyber security* yang dilakukan oleh Pemerintah Indonesia sudah diinisiasi pada tahun 2007 dengan memberikan kepastian hukum melalui Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Peraturan ini kemudian beberapa kali mengalami proses revisi pada tahun 2010 sehingga muncul Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.Kominfo/12/2010. Dalam peraturan tersebut salah satunya diatur mengenai pembentukan ID-SIRTII sebagai tim yang diberikan tugas oleh Menteri Komunikasi dan Informatika untuk membantu melakukan pengawasan keamanan jaringan telekomunikasi berbasis protocol internet.

ID-SIRTII memiliki tugas serta fungsi untuk melakukan pemantauan, deteksi dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, koordinasi dengan pihak lain dalam melakukan pengamanan jaringan, pemeliharaan serta pengembangan system *database* ID-SIRTII, penyusunan catalog dan silabus mengenai pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan jaringan, menjadi *contact point* dengan lembaga lain dalam pengamanan jaringan, serta menyusun program kerja dalam rangka melaksanakan pengamanan

[21] International Telecommunication Union (ITU), Cyberwellness Profile Brunei, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx diakses pada 13 April 2017 pukul 15.05 WIB

jaringan telekomunikasi berbasis protocol internet.[22]

Indonesia membangun kerangka hukum *cyber security* berdasarkan kepada Undang – undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008 yang kemudian direvisi menjadi Undang – undang No. 19 Tahun 2016, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, serta peraturan menteri dan surat edaran menteri. Upaya – upaya yang dilakukan dalam menjamin kepastian hukum terkait pengembangan *cyber security* juga telah dilakukan antara lain melalui serangkaian program seperti penyusunan undang – undang serta peraturan lainnya dan juga penyusunan kerangka nasional *cyber security*.

Menurut Hasyim Gautama, secara nasional masih terdapat sejumlah permasalahan mengenai pembangunan *cyber security* di Indonesia, antara lain ialah:

a. Lemahnya pemahaman penyelenggara Negara terhadap *cyber security* yang pada dasarnya membutuhkan pembatasan dalam penggunaan layanan yang servernya berada di luar negeri sehingga diperlukan adanya penggunaan *secured system*.
b. Legalitas dalam proses penanganan penyerangan siber.
c. Cepatnya pola kejadian serangan siber sehingga cukup sulit untuk ditangani.
d. Tata kelola dalam kelembagaan *cyber security* secara nasional.
e. Masih rendahnya *awareness* terhadap ancaman *cyber* yang pada dasarnya mampu melumpuhkan infrastruktur penting suatu Negara.
f. Masih lemahnya industry Indonesia dalam melakukan produksi dan pengembangan *hardware* terkait teknologi informasi yang dapat menjadi celah dalam *cyber security*.[23]

Elemen selanjutnya dalam pembangunan kapasitas *cyber security* di Indonesia ialah mengenai struktur organisasi. Penanganan *cyber security* hingga saat ini masih bersifat sektoral serta belum terkoordinasi secara terpadu. Di Indonesia hingga saat ini sebetulnya ada berbagai lembaga yang menangani permasalahan *cyber security*, seperti Kementerian Komunikasi dan Informatika, Lembaga Sandi Negara, Kementerian Pertahanan, TNI, Polri,

[22] Pasal 9 Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.Kominfo/12/2010 tentang pengamanan jaringan telekomunikasi berbasis protocol internet.

[23] Hasyim Gautama, Penerapan Cyber Security, http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf , diakses 12 April 2017 pukul 21.05 WIB

Badan Intelejen Negara, dan lain – lain. Sebagai upaya untuk mengkoordinasikan lembaga – lembaga tersebut, Pemerintah Indonesia sedang merencanakan pembentukan suatu badan yang diberi nama Badan Siber Nasional dibawah koordinasi Kementerian Politik Hukum dan Keamanan.[24]

Selain aspek struktur organisasi, hal lain yang penting dalam membangun kapasitas *cyber security* ialah aspek *capacity building*. Program pelatihan dan peningkatan keahlian sumber daya manusia dalam mengatasi *cyber security* perlu dilakukan dengan baik. Selain itu, pembinaan serta kampanye kepada masyarakat mengenai arti pentingnya *cyber security* guna meningkatkan pemahaman dalam langkah – langkah *preventive* dalam menangkal segala ancaman siber. Di Indonesia, ada berbagai macam upaya yang juga dilakukan dalam meningkatkan keahlian serta memberikan pemahaman mengenai pentingnya *cyber security*. Contohnya seperti kegiatan *Cyber Train* yang dilaksanakan oleh ID-SIRTII pada tahun 2016 sebagai upaya dalam meningkatkan wawasan, kepedulian, dan pendidikan bagi masyarakat terhadap keamanan infrastruktur teknologi informasi.[25] Selain itu, dalam rangka menumbuhkan kesadaran masyarakat akan pentingnya keamanan informasi, ID-SIRTII juga menginisiasi kegiatan yang diberi nama *National Security Awareness Program (NSAP)*.[26]

Elemen terakhir dalam membangun kapasitas *cyber security* ialah melakukan kerjasama internasional dengan Negara – Negara lain. Hingga saat ini Indonesia telah melakukan kerjasama baik pada tingkat regional maupun internasional. Beberapa forum kerjasama internasional yang diikuti oleh Indonesia antara lain, *ASEAN Network Security Action Council, International Telecommunication Union (ITU), Asia Pacific Computer Emergency Response Team (APCERT),* serta *Forum of Incident Response and Security (FIRST)*. Selain itu Indonesia juga seringkali melakukan kerjasama bilateral di bidang *cyber security* dengan Negara – Negara lain, seperti Jepang, Inggris, dan lain – lain.[27]

Pembahasan

[24]https://news.detik.com/berita/d-3389060/wiranto-peran-basinas-memayungi-badan-siber-yang-sudah-ada diakses 13 April 2017 pukul 08.00 WIB

[25]http://www.idsirtii.or.id/training/index.html diakses 13 April 2017 pukul 10.25 WIB

[26] http://nsap.idsirtii.or.id/ diakses 13 April 2017 pukul 10.45 WIB

[27] Handrini Ardiyanti, *op.cit.,* hlm. 102

Seperti dijelaskan diawal, bahwa *cyber security* dibangun diatas lima bidang kerja, yaitu kepastian hukum, tindakan procedural, struktur organisasi, *capacity building*, dan kerjasama internasional. Sehingga dalam melakukan perbandingan pembangunan kapasitas *cyber security* antara Brunei dan Indonesia juga perlu dilihat dari masing – masing aspek pada pembahasan diatas.

Dalam aspek kepastian hukum, dapat dilihat bahwa Brunei Darussalam lebih awal *concern* terhadap *cyber security* jika dibandingkan dengan Indonesia. Sejak tahun 2000, Pemerintah Brunei Darussalam telah merumuskan berbagai aturan mengenai *cyber security* dalam rangka pengamanan ruang sibernya. Berbeda dengan Indonesia yang baru merumuskan peraturan pada tahun 2008. Hal ini tentu berakibat pada keterlambatan pembangunan kapasitas *cyber security* Indonesia jika dibandingkan dengan Brunei Darussalam.

Aspek selanjutnya dalam pembangunan kapasitas *cyber security* ialah tindakan procedural yang didalamnya terdiri dari kerangka kerja serta strategi mengenai *cyber security*. Jika melihat pada aspek ini, ada kesamaan antara Brunei Darussalam dan Indonesia dimana hingga saat ini masih merumuskan strategi dan kebijakan dalam *cyber security*. Hal ini mengakibatkan upaya koordinasi dan integrasi setiap lembaga menjadi kurang baik dalam melakukan pengamanan siber. Akan tetapi, Brunei Darussalam agaknya sedikit lebih diuntungkan dalam aspek ini. Hal ini karena secara keseluruhan, Pemerintah Brunei Darussalam memberikan tanggung jawab kepada BruCERT sebagai tim yang bertugas untuk melakukan pengamanan jaringan siber di Brunei Darussalam.

Dalam aspek struktur organisasi, Brunei Darussalam memiliki lembaga yang terstruktur dengan baik dalam masalah *cyber security*. Hal ini dapat dilihat dengan pembentukan BIT *Council* sebagai lembaga yang secara keseluruhan bertugas untuk mengkoordinasikan lembaga – lembaga lain dalam masalah *cyber*. Walaupun, hingga saat ini prosedur standar dalam koordinasi setiap lembaga masih dirumuskan bersamaan dengan perumusan *Brunei National Cyber Security Framework*. Berbeda dengan Indonesia yang hingga saat ini permasalahan *cyber security* masih ditanggulangi oleh masing – masing lembaga. Sehingga koordinasi antar lembaga masing kurang baik akibat dari belum adanya badan yang bertugas

untuk mengkoordinasikan lembaga – lembaga lainnya.

Dalam aspek *capacity building*, perhatian dan keseriusan Pemerintah Brunei Darussalam dapat terlihat dengan jelas melalui kebijakannya untuk memasukan *cyber security awareness* kedalam kurikulum pendidikan di Brunei Darussalam. Hal ini membuat masyarakat akan memahami dan sadar sejak dini terhadap persoalan *cyber security*. Selain itu, program pelatihan yang dilakukan oleh BruCERT ke setiap sekolah memberikan manfaat dalam meningkatkan kemampuan pelajar dalam masalah *cyber security*. Indonesia melalui ID-SIRTII juga telah melakukan upaya – upaya dalam meningkatkan *capacity building*. Akan tetapi, program – program tersebut masih dalam bentuk himbauan yang tidak mengikat. Hal ini mengakibatkan kesadaran dan pemahaman masyarakat dalam *cyber security* tergantung kepada keinginan setiap individu untuk ikut serta dalam program – program tersebut.

Dalam aspek kerjasama internasional mengenai *cyber security*, Brunei juga terlihat lebih aktif apabila dibandingkan dengan Indonesia. Tercatat bahwa Pemerintah Brunei Darussalam aktif dalam lima forum kerjasama internasional. Lebih banyak jika dibandingkan dengan Indonesia yang mengikuti empat forum kerjasama internasional yang membahas mengenai *cyber security*.

Secara keseluruhan, berdasarkan kepada lima aspek dalam pembangunan kapasitas *cyber security* maka dapat terlihat bahwa Brunei Darussalam lebih baik jika dibandingkan dengan Indonesia. Hal ini perlu menjadi perhatian serius bagi Pemerintah Indonesia, apalagi jika merujuk kepada data yang disajikan di awal bahwa Indonesia berada pada tingkat teratas sebagai Negara yang seringkali menjadi target serangan *hacker*.

Kesimpulan

Berdasarkan pembahasan dan analisa yang dilakukan dalam penelitian ini, maka dapat disimpulkan bahwa hingga saat ini, Indonesia masih lemah dalam masalah *cyber security*. Terkait dengan kepastian hukum misalnya, pengembangan dan penguatan kebijakan *cyber security* di Indonesia seharusnya terpadu dalam strategi nasional sebagai upaya dalam membangun kapasitas *cyber security* secara nasional. Selain itu, dalam strategi nasional tersebut juga dapat meliputi landasan hukum, teknis procedural, penataan keorganisasian dalam

penanganan *cyber*, *capacity building*, serta peningkatan kerjasama internasional.

Dalam teknis procedural atau standar operasional, ada banyak hal yang harus menjadi perhatian Pemerintah Indonesia. pertama misalnya ialah pengadaan satelit khusus dalam rangka pertahanan dan keamanan. Hal ini mutlak diperlukan akibat dari telah dimilikinya sejumlah *provider* telekomunikasi oleh pemilik modal asing.

Melalui gambar diatas, maka dapat dilihat bahwa satelit khusus sangat diperlukan dalam sector pertahanan, seperti pengawalan Presiden/Wakil Presiden, pengawalan tamu Negara, konflik akibat separatism, pengamanan perbatasan, penanganan terorisme, dan lain – lain. Membangun kapasitas *cyber security* diperlukan keseriusan, khususnya dalam aspek infrastruktur sebagai penunjang pengamanan siber.

Sifat dari ancaman *cyber* yang multidimensional juga membuat penanganannya bukan hanya tanggung jawab TNI/Polri, Kemhan ataupun Kemenkominfo saja. Ancaman siber yang termasuk dalam ancaman asimetris dalam penanganannya membutuhkan pendekatan komprehensif. Sehingga dalam penanganannya tidak dibebankan kepada satu kementerian saja, melainkan seluruh elemen di Pemerintahan.

Oleh karena itu, diperlukan suatu kebijakan *cyber security* yang dalam implementasinya membutuhkan suatu badan koordinasi. Sehingga diharapkan dengan pembentukan badan tersebut akan meningkatkan kemampuan dalam pengaturan dan penataan lembaga secara terintegrasi. Badan Siber Nasional yang hendak dibentuk oleh Pemerintah Indonesia diharapkan mampu menyelesaikan permasalahan koordinasi antara lembaga yang memiliki kemampuan dalam *cyber security* di Indonesia.

Pengembangan strategi nasional dalam membangun kapasitas *cyber security* di Indonesia juga perlu memperhatikan kualitas sumber daya manusia yang dimiliki. Dalam *cyber security*, kesadaran masyarakat sangat diperlukan. Hal ini mengingat masyarakat sebagai pengguna *cyber* ialah bagian yang penting dalam keamanan informasi. Pelatihan, seminar, penyebaran informasi dalam rangka meningkatkan pemahaman dan kesadaran masyarakat harus dilakukan secara massif oleh Pemerintah guna membangun kapasitas *cyber security* Indonesia.

Dalam kerjasama internasional, permasalahan yang saat ini belum selesai ialah belum adanya sebuah kesepakatan bersama secara internasional mengenai *cyber security*. Indonesia, seharusnya dapat aktif dalam forum – forum kerjasama internasional bahkan diharapkan dapat memberikan kontribusi dalam terbentuknya kesepakatan internasional tersebut.

Kerjasama internasional lainnya terkait dengan pengembangan *cyber security* adalah dalam rangka meningkatkan kapasitas kemampuan *cyber security* baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan SDM dalam bidang *cyber security* baik bilateral antar dua negara maupun regional ataupun internasional. Peningkatan kerja sama teknologi informasi dan *cyber security* selain itu juga diharapkan mampu membuka peluang bagi pengembangan industri media baru terkait dengan IT di Indonesia sebagai salah satu bagian dari pengembangan industri strategis.

Terkait dengan pengembangan kerjasama internasional dalam rangka pengembangan *cyber security* Indonesia perlu meningkatkan peran aktif mendorong berbagai kesepakatan bersama yang sepakati bersama dalam ITU yang merupakan organisasi terdepan dalam menciptakan ruang siber yang aman bagi negara, pemerintah, masyarakat maupun dunia usaha. Selain itu Indonesia juga dapat mengembangkan kerjasama dengan negara-negara anggota ITU lainnya yang memiliki kemampuan IT lebih baik dari Indonesia untuk memberikan asistensi dalam upaya peningkatan sumber daya manusia, memberikan perlindungan kepada penguna dari ancaman *cyber* dan meningkatkan kebermanfaatan internet untuk masyarakat informasi. Di samping itu juga Indonesia perlu terus meningkatkan peran aktifnya dalam program *Global Cyber security Agenda (GSA).*

Daftar Pustaka

Buku

Badan Pengkajian dan Penerapan Teknologi (BPPT). (2007). *Kajian Konvergensi Teknologi Informasi dan Komunikasi*. Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT

Center for Strategic and International Studies. (2013). *The Cyber Index: International Security Trends and Realities*. UNIDIR

Indrajit, Richardus E. (2013). *Strategi Brunei Menuju Masyarakat Berbasis Elektronik*.

Sanusi, M. Arsyad. (2005). *Hukum Teknologi dan Informasi*. Bandung: Tim Kemas Buku

Smith, M. (2015). *Research Handbook on International Law and Cyberspace*. Massachusetts: Edwar Elgar Publishing Limited

Vivian, John. (2008). *Teori Komunikasi Massa*. Jakarta: Kencana

Jurnal

Ardiyanti, Handrini. (2014). *Cyber Security dan Tantangan Pengembangannya di Indonesia*. https://jurnal.dpr.go.id/index.php/politica/article/view/336

Gautama, Hasyim. (2011) Penerapan Cyber Security. http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf

Peraturan Perundangan

Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.Kominfo/12/2010 tentang pengamanan jaringan telekomunikasi berbasis protocol internet

Website

Indonesian Attack Traffic Tops List, https://blogs.akamai.com/2013/10/indonesia-attack-traffic-tops-list-port-445-no-longer-main-launching-pad.html

Index Law of Brunei Darussalam, http://www.agc.gov.bn/AGC%20Site%20Pages/Legislation.aspx

International Telecommunication Union (ITU), Cyberwellness Profile Brunei, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx

Laporan hasil survey Asosiasi Penyedia Jasa Internet Indonesia (APJII), http://www.apjii.or.id/survei

Pernyataan Menkopolhukam Mengenai Badan Siber Nasional. https://news.detik.com/berita/d-3389060/wiranto-peran-basinas-memayungi-badan-siber-yang-sudah-ada

Website ID-SIRTII http://www.idsirtii.or.id/training/index.html

Website Program Kesadaran Nasional *Cyber Security* ID-SIRTII http://nsap.idsirtii.or.id/