Padjadjaran Journal of International Relations (PADJIR)
e-ISSN: 2684-8082 Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam *Singapore International Cyber Week*

Muhammad Fikry Anshori
Program Studi Hubungan Internasional FISIP Universitas Padjadjaran, Indonesia;
email: muhammad15205@mail.unpad.ac.id
Rizki Ananda Ramadhan
Departemen Studi Hubungan Internasional FISIP Universitas Padjadjaran, Indonesia;
Email: rizki.ramadhan@unpad.ac.id

Dikirim: 10 April 2019 | Direvisi: 10 Mei 2019 | Diterima: 25 Mei 2019 | Dipublikasikan: 31 Mei 2019

Keywords
cybersecurity, interest, Singapore International Cyber Week

ABSTRACT
This article describes the interest of Singapore in the cybersecurity of Southeast Asia by organizing Singapore International Cyber Week. This article uses the concept of interest based on constructivism. This article uses interpretive qualitative method. This article finds that Singapore interprets itself as "smart nation" and "cyberattack target" in Southeast Asia; Singapore's objective interests are capacity building, awareness building, and norm formation on cybersecurity of Southeast Asia; and Singapore's subjective interest is involving Southeast Asia nations in cybersecurity issue by organizing ASEAN Ministerial Conference on Cybersecurity, launching ASEAN Cyber Capacity Program, and initiating ASEAN-Singapore Cybersecurity Center of Excellence.

Kata Kunci
keamanan siber, kepentingan, *Singapore International Cyber Week*

ABSTRAK
Artikel ini bertujuan mendeskripsikan kepentingan yang dihadirkan oleh Singapura pada keamanan siber di Asia Tenggara dengan menyelenggarakan *Singapore International Cyber Week*. Konsep yang digunakan adalah kepentingan berdasarkan konstruktivisme. Metode yang digunakan adalah kualitatif interpretatif. Artikel ini menemukan Singapura memaknai kondisi dirinya sebagai "*smart nation*" dan "target serangan siber" di Asia Tenggara; Singapura memiliki kepentingan objektif berupa pembangunan kapasitas, pembentukan kesadaran, dan pembentukan norma pada keamanan siber di Asia Tenggara; serta Singapura memiliki kepentingan subjektif berupa melibatkan negara-negara di Asia Tenggara dalam isu keamanan siber dengan penyelenggaraan *ASEAN Ministerial Conference on Cybersecurity*, peluncuran *ASEAN Cyber Capacity Programme*, dan penggagasan *ASEAN-Singapore Cybersecurity Centre of Excellence*.

PENDAHULUAN

Asia Tenggara merupakan kawasan yang menempati peringkat ketiga di dunia dalam hal penetrasi internet pada tahun 2017. Posisi Asia Tenggara tersebut didasarkan pada jumlah pengguna internet di Asia Tenggara yang sudah mencapai 380 juta pengguna internet. Jumlah tersebut setara dengan 58% dari total jumlah populasi yang ada di Asia Tenggara. Kemudian, presentase tersebut lebih tinggi dibandingkan presentase rata-rata dari penetrasi internet di dunia yaitu sebesar 53% (We Are Social, 2018). Lebih lanjut, jika kondisi penetrasi internet di Asia Tenggara pada tahun 2017 dibandingkan dengan kondisi penetrasi internet di Asia Tenggara pada tahun

2016 maka di Asia Tenggara mengalami peningkatan pengguna internet sebanyak 41 juta pengguna internet yang dengan kata lain mengalami peningkatan sebesar 5% (We Are Social, 2017).

Dengan kondisi penetrasi internet demikian, Asia Tenggara merupakan salah satu kawasan yang memiliki kerentanan terhadap berbagai macam serangan siber. Dari total jumlah pengguna internet yang ada di Asia Tenggara, 29% pengguna internet di Asia Tenggara pernah mengalami serangan siber. Kemudian, pada umumnya serangan siber yang terjadi di Asia Tenggara berupa *malware* dan *ransomware* (FireEye & Singtel, 2015)[i]. Contoh dari *malware* dan *ransomware* tersebut di antaranya adalah Lecna, Gh0STRAT, dan juga LV (aka NJRT). Selanjutnya, di Asia Tenggara sendiri terdapat beberapa sektor dengan layanan berbasis internet yang menjadi sektor yang paling rentan terhadap ancaman serangan siber. Sektor tersebut antara lain adalah pada sektor energi, sektor telekomunikasi, sektor perbankan, serta pada transportasi (FireEye & Singtel, 2015).

Singapura merupakan salah satu negara di Asia Tenggara yang berdasarkan pada *Global Security Index* yang dirilis oleh International Telecommunications Union di tahun 2017 dikategorikan sebagai negara dengan posisi pertama pada keamanan siber dibandingkan dengan negara lainnya yang ada di dunia. Kondisi yang demikian pada hal keamanan siber tersebut juga membuat Singapura menjadi negara yang terdepan juga di kawasan sekitarnya (ITU, 2017). Lebih lanjut, Singapura menjadi negara pada posisi terdepan dalam keamanan siber dengan Singapura menempati peringkat pertama di dunia sebagai negara yang mempunyai komitmen yang baik pada keamanan siber di tahun 2017 berdasarkan Global Security Index yang dirilis oleh International Telecommunications Union. Kemudian, jika dibandingkan antara *Global Security Index* pada tahun 2015 dengan *Global Security Index* pada tahun 2017 maka Singapura mengalami peningkatan dalam peringkat komitmen pada keamanan siber di dunia yaitu yang awalnya peringkat keenam menjadi peringkat pertama (ITU, 2015).

Singapura sampai saat ini sudah melakukan berbagai macam upaya terkait dengan keamanan siber (Cyber Security Agency, 2016). Upaya tersebut dimulai pada tahun 2005 melalui peluncuran perencanaan berupa *Cyber Security Masterplan*. Lalu dilanjutkan dengan peluncuran perencanaan lainnya yang berupa *Infocom Security Masterplan* pada tahun 2007. Pada tahun 2013, Singapura meluncurkan perencanaan lainnya yang berupa *National Cyber Security Masterplan* serta bersamaan juga dengan dibentuknya *National Cyber Security Research and Development Program*. Di tahun yang sama juga, Singapura merintis pembentukan *National Cyber Security Center* (Cyber Security Agency, 2016). Perkembangan selanjutnya terjadi di tahun 2015, Singapura membentuk *Cyber Security Agency* sebagai badan dalam Pemerintah Singapura yang didedikasikan untuk berurusan dengan isu keamanan siber. Kemudian, Singapura pada bidang keamanan siber menyelenggarakan kegiatan yang bernama *Singapore International Cyber Week* (FTI Consulting, 2017).

Singapore International Cyber Week merupakan kegiatan yang diselenggarakan Singapura pada keamanan siber yang ditujukan untuk berfokus pada kawasan Asia Tenggara. *Singapore International Cyber Week* ini pertama kali diselenggarakan pada tahun 2016 yang kemudian selanjutnya diadakan secara tahunan termasuk pada tahun 2018 (SICW, 2018). Di dalam penyelenggaraan *Singapore International Cyber Week* tersebut, Singapura melibatkan aktor negara yang ada di Asia Tenggara seperti Indonesia, Malaysia, Brunei, Filipina, Thailand, Laos, Vietnam, Kamboja, dan Myanmar serta juga aktor non-negara berupa perusahaan multinasional pada keamanan siber atau *think tank* pada keamanan siber yang ada di Asia Tenggara untuk saling bertemu untuk melakukan pembahasan terhadap berbagai macam isu keamanan siber di Asia Tenggara berdasarkan tema tertentu di tiap tahunnya

e-issn: 2684-8082; Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

(SICW, 2018). *Singapore International Cyber Week* dinyatakan sebagai kegiatan pada keamanan siber, pengembangan ekosistem keamanan siber, dan inovasi keamanan siber yang terus berkembang yang menekankan dan mengutamakan kerjasama di antara aktor yang ada di kawasan Asia Tenggara khususnya maupun juga internasional secara umum (SICW, 2018).

Singapura merupakan negara yang menjadi penyelenggara dari *Singapore International Cyber Week.* Penyelenggaraan *Singapore International Cyber Week* melibatkan berbagai macam aktor asing pada keamanan siber di Asia Tenggara. Singapura sebagai aktor negara merupakan aktor yang memiliki kepentingan yang dihadirkan dalam penyelenggaraan *Singapore International Cyber Week* Kepentingan yang dihadirkan tersebut merupakan kepentingan Singapura pada keamanan siber di Asia Tenggara. Dengan hal tersebut, artikel ini bertujuan untuk mendeskripsikan kepentingan Singapura yang dihadirkan pada keamanan siber di Asia Tenggara dalam penyelenggaraan *Singapore International Cyber Week*.

Pemaparan artikel ini disusun dalam beberapa bagian, yaitu pendahuluan, pemaparan konsep terkait yaitu keamanan siber dan *interest,* dan penjelasan singkat mengenai metode riset yang digunakan. Pada bagian pembahasan, artikel ini akan mengaplikasikan konsep *interest* untuk menemukan kepentingan keamanan siber Singapura di Asia Tenggara dalam *Singapore International Cyber Week*. Terakhir, artikel ini ditutup dengan simpulan.

KERANGKA KONSEPTUAL

Ruang Siber dan Keamanan Siber

Ruang siber (*cyberspace*) merupakan arena yang dibuat melalui inovasi teknologi dan keberadaan arena tersebut memungkinkan pengguna di dalamnya untuk terlibat dalam berbagai macam aktivitas yang dilakukan secara elektronik dan melampaui berbagai macam halangan domain ruang yang tradisional berdasarkan teritori (Choucri, 2012, hal. 6). Ruang siber secara sistematis dapat dimodelkan menjadi ruang yang dibentuk oleh empat lapisan yaitu fisik, logika, informasi, dan aktor. Lapisan pertama yaitu lapisan fisik merupakan fondasi atau infrastruktur yang memungkinkan ruang siber terbentuk. Kemudian, lapisan logika merupakan blok yang memungkinkan agar lapisan fisik dapat menghadirkan berbagai macam layanan. Selanjutnya yaitu lapisan informasi merupakan berbagai macam konten yang disimpan, dikirimkan, atau juga ditransformasikan. Terakhir, lapisan aktor merupakan entitas atau pengguna yang memiliki berbagai macam kepentingan dan terlibat atau berpartisipasi dalam dalam ruang siber dengan peran tertentu (Clark dalam Choucri, 2012, hal. 8).

Keberadaan ruang siber dengan segala karakteristiknya memunculkan perhatian pada keamanan di ruang siber (Hughes, 2016). Terdapat beberapa istilah yang berkaitan dengan hal tersebut di antaranya yaitu keamanan siber (*cybersecurity*), serangan siber (*cyberattack*), pertahanan siber (*cyber defense*), deterens siber (*cyber deterrence*), dan kuasa siber (*cyberpower*) (Hughes, 2016, hal. 203). Keamanan siber dapat didefinisikan sebagai berbagai macam tindakan perlindungan yang berkaitan dengan kerahasiaan, ketersediaan, dan keutuhan informasi yang diproses, disimpan, dan dikomunikasikan secara elektronik melalui jaringan komputer. Kemudian untuk serangan siber merupakan tindakan yang bersifat ofensif yang menjadikan sistem informasi komputer atau jaringan komputer sebagai targetnya (Hughes, 2016, hal. 203). Selanjutnya, pertahanan siber dapat didefinisikan sebagai tindakan perlindungan untuk mengantisipasi keberadaan terjadinya serangan yang dilakukan terhadap jaringan komputer atau sistem informasi komputer. Lalu untuk deterens siber merupakan tindakan yang dilakukan dengan tujuan untuk menciptakan atau mendorong terciptanya kondisi atau persepsi bahwa serangan siber tidak terlalu

berguna untuk dilakukan. Terakhir, kuasa siber merupakan kemampuan dalam menggunakan ruang siber untuk membuat kelebihan dan pengaruh dalam cakupan lingkungan operasional dari ruang siber (Hughes, 2016, hal. 203).

Hirauan terhadap keamanan siber sebagai suatu isu tidak lepas begitu saja dari hadirnya juga berbagai macam perdebatan terkait dengan kemanan siber itu sendiri. Perdebatan yang terjadi berpusat pada mempermasalahkan pendekatan yang tepat untuk dapat digunakan terhadap isu keamanan siber karena keamanan siber ini terjadi pada ruang yang berbeda (Hughes, 2016, hal. 202). Terdapat pendapat yang menyatakan bahwa keberadaan ruang siber dan isu keamanan yang ada padanya hanya merupakan bentuk lain dari politik yang berakar pada sifat alamiah manusia sehingga keamanan siber tidak terlepas dari kondisi anarki yang mengutamakan untuk membantu diri sendiri dalam pemenuhan kebutuhan atas kekuatan secara material. Kemudian juga ada yang menyatakan bahwa keberadaan isu keamanan siber menekankan kembali pentingnya keberadaan institusi yang dapat menghadirkan kemungkinan untuk melakukan kerjasama di antara berbagai macam aktor dan juga mendukung tercapainya kerjasama berbagai macam aktor dalam ruang siber yang menghasilkan ekspektasi terhadap keamanan siber sehingga keamanan pada ruang siber itu dapat dijaga (Hughes, 2016, hal. 202).

Kepentingan menurut Konstruktivisme dalam Hubungan Internasional

Konstruktivisme merupakan teori yang berfokus pada konstruksi sosial dari subjektivitas berupa berbagai macam makna (Onuf dalam Wendt, 1992, hal. 393). Asumsi mendasar dari konstruktivisme adalah seseorang bertindak pada suatu objek, termasuk juga terhadap aktor yang lainnya, berdasarkan pada makna yang dimiliki oleh objek atau aktor lainnya yang dihadirkan kepada dirinya (Blumer dalam Wendt, 1992, hal. 396-397). Dalam konstruktivisme makna hadir dari berbagai interaksi yang di dalamnya terdapat tindakan yang terorganisasi (Blumer dalam Wendt, 1992, hal. 403). Teori Konstruktivisme dalam Hubungan Internasional memiliki dua klaim utama pada fenomena hubungan internasional yaitu (1) sturktur mendasar dari politik internasional utamanya adalah sosial dibandingkan dengan material dan (2) struktur sosial utamanya membentuk identitas dan kepentingan aktor dibandingkan hanya perilakunya (Wendt, 1995, hal. 71-72). Kemudian, Teori Konstruktivisme dalam Hubungan International menyatakan juga dua hal, yaitu (1) struktur sosial dari aktor ditentukan utamanya oleh ide bersama di antara aktor dibandingkan dengan kekuatan material serta (2) identitas dan kepentingan pada aktor merupakan konstruksi dari identitas bersama tersebut (Wendt, 1999, hal. 1).

Kepentingan merupakan hal yang diinginkan oleh agen (Wendt, 1999, hal. 231). Agen pada dasarnya tidak memiliki rekam jejak kepentingan yang secara independen dibawa oleh agen tersebut pada berbagai macam konteks sosial (Wendt, 1992 hal. 398). Namun, agen mendefinisikan kepentingan ketika dalam proses pendefinisian situasi yang dialami oleh agen tersebut (Wendt, 1992, hal. 398). Kepentingan merupakan bagian penting yang dikonstruksikan dalam sistem tempat agen berada (Wendt, 1995, hal. 72). Agen perlu mendefinisikan situasi pada suatu kondisi berdasarkan pemahaman mereka yang kemudian sesuai juga dengan tindakan yang dilakukan oleh agen tersebut. Walaupun begitu, situasi tersebut tidak dapat dipahami dengan mudah oleh agen terutama ketika melampaui pengalaman dari agen tersebut. Sehingga, agen tersebut perlu untuk mengkonstruksikan makna pada situasi tersebut sehingga dapat menjadi dasar bagi kepentingan agen tersebut (Wendt, 1992, hal. 398). Oleh karena itu, kepentingan dapat merujuk kepada berbagai macam keinginan yang dapat membantu untuk mendeskripsikan perilaku atau tindakan dari agen dalam sistem internasional (Wendt, 1999, hal. 231).

e-issn: 2684-8082; Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

Kepentingan merupakan hal yang bergantung pada identitas (Wendt, 1994, hal. 385). Identitas merupakan pemahaman mandiri agen terhadap kualitas dirinya sendiri. Identitas dapat dibagi menjadi empat yaitu *corporate identity*, *type identity*, *role identity*, dan *collective identity*. *Corporate identity* dibentuk oleh tata kelola mandiri yang membuat agen tersebut menjadi entitas yang berbeda (Wendt, 1999, hal 224-225). *Type identity* adalah kategori atau label secara sosial yang dilekatkan kepada agen yang membagikan berbagai macam karakteristik tertentu (Wendt, 1999, hal. 225). *Role identity* merupakan identitas agen yang hadir dari ekspektasi bersama dari agen lainnya (Wendt, 1999, hal. 227). *Collective identity* merupakan identitas yang menyatukan berbagai agen yang memiliki identitas tipe dan peran yang berbeda (Wendt, 1999, hal. 229).

Identitas merupakan dasar dari kepentingan bagi agen (Wendt, 1992, hal. 398). Agen tidak akan mengetahui hal yang diinginkan tanpa mengetahui diri agen sendiri (Wendt, 1999, hal. 231). Walaupun begitu, identitas tidak dapat menjelaskan tindakan dari agen karena menjadi suatu agen bukan berarti sama saja dengan menginginkan sesuatu (Wendt, 1999, hal. 231). Tindakan dari agen adalah gabungan dari identitas dan kepentingan dari agen (Wendt, 1999, hal. 231). Identitas merupakan kepercayaan agen terkait dengan dirinya sendiri dan kepentingan merupakan sisi keinginan agen pada suatu hal (Wendt, 1999, hal. 231).

Teori Konstruktivisme menyatakan terdapat dua jenis kepentingan yaitu *kepentingan objektif* dan *kepentingan subjektif* (Wendt, 1999, hal. 231). Kepentingan objektif adalah kebutuhan atau keperluan secara fungsional yang harus dipenuhi oleh suatu agen jika identitas dari agen tersebut tetap hendak direproduksi (Wendt, 1999, hal. 232). Pada kepentingan objektif, agen perlu untuk dapat memahami kebutuhan yang perlu dipenuhi dan bertindak berdasarkan kepada pemahaman tersebut sebagai suatu bentuk untuk memastikan tercapainya upaya dalam mereproduksi identitas (Wendt, 1999, hal. 232). Sehingga, agen tersebut dapat terhindar dari kepentingan yang bertolak belakang dengan kebutuhan mereka yang sebenarnya. Kemudian kepentingan subjektif merujuk kepada sekumpulan kepercayaan yang agen miliki terkait dengan cara untuk dapat memenuhi kebutuhan identitasnya. Hal ini juga dapat dikatakan sebagai motivasi dari perilaku suatu agen (Wendt, 1999, hal. 232). Lebih lanjut, kepentingan subjektif merupakan preferensi agen terhadap suatu hasil perilaku dan bukan perilaku itu sendiri. Pembedaan tersebut merupakan hal yang penting karena perilaku terjadi tidak hanya oleh keinginan dari aktor saja tetapi juga hal yang oleh aktor pikir dimungkinkan untuk didapat (Wendt, 1999, hal. 232).

Dari tinjauan konsep keamanan siber dan kepentingan dalam konstruktivisme di atas maka dapat disusun alur pemikiran sebagai berikut. Keamanan siber di Asia Tenggara merupakan sebuah struktur yang di dalamnya terdapat berbagai macam agen yang berupa negara yang ada di Asia Tenggara. Salah satu dari agen tersebut adalah Singapura. Singapura merupakan agen yang memaknai situasi yang dialaminya dalam hal keamanan siber berdasarkan pada keamanan siber di Asia Tenggara sebagai struktur yang ditempatinya. Dari pemaknaan situasi yang dilakukan Singapura pada keamanan siber di Asia Tenggara tersebut, Singapura menghadirkan kepentingannya pada keamanan siber di Asia Tenggara. Terdapat dua jenis kepentingan yaitu kepentingan objektif yang merupakan kebutuhan yang selayaknya perlu dipenuhi oleh Singapura dalam hal keamanan siber di Asia Tenggara sesuai dengan konteks pemaknaan kondisinya serta kepentingan subjektif yang merupakan kepercayaan yang dimiliki oleh Singapura terkait dengan cara yang digunakan untuk dapat memenuhi kepentingan objektif Singapura pada keamanan siber di Asia Tenggara. Kepentingan-kepentingan tersebut dihadirkan

oleh Singapura di dalam penyelenggaraan *Singapore International Cyber Week*.

METODE RISET

Metode yang digunakan dalam riset ini adalah kualitatif interpretatif. Teknik pengumpulan data yang digunakan adalah studi berbasis internet, studi berbasis pustaka, wawancara, dan observasi. Teknik pengumpulan data tersebut digunakan untuk memperoleh data yang diperlukan untuk mendeskripsikan kepentingan Singapura pada keamanan siber di Asia Tenggara dalam *Singapore International Cyber Week*. Data tersebut berupa keamanan siber di Asia Tenggara dan Singapura, *Singapore International Cyber Week*, serta pemaknaan situasi dan kepentingan Singapura pada keamanan siber. Data yang diperoleh lalu divalidasi dengan cara triangulasi. Lalu untuk menganalisis data yang sudah diperoleh dan valid menggunakan teknik analisis data yang berupa analisis wacana.

KEPENTINGAN KEAMANAN SIBER SINGAPURA DI ASIA TENGGARA DALAM *SINGAPORE INTERNATIONAL CYBER WEEK*

Pemaknaan Singapura pada Situasi Keamanan Siber di Asia Tenggara

Perdana Menteri Singapura, Lee Hsien Loong, menyatakan dalam *Singapore International Cyber Week* 2016 bahwa teknologi siber tersebut membantu perkembangan Singapura dari negara berkembang menjadi negara maju, membuat ekonomi Singapura yang berbasis pengetahuan, meningkatkan produktivitas kerja warga Singapura, dan memperbaiki kehidupan warga Singapura. Keberadaan teknologi informasi dan komunikasi merupakan hal yang penting untuk masa depan Singapura untuk menjadi *"smart nation"*. *Smart Nation* didefinisikan Singapura sebagai negara yang kemampuannya dapat dimungkinkan dengan infrastruktur dan teknologi digital yang terpercaya. Pada *Singapore International Cyber Week* 2017, Wakil Perdana Menteri Singapura, Teo Chee Hean, menyatakan bahwa Singapura merupakan negara yang sangat terhubung dalam jaringan internet.

Singapura sebagai *"smart nation"* merupakan pemahaman mandiri dari Singapura sebagai agen terkait dengan keberadaan teknologi informasi dan komunikasi berupa internet. Definisi *"smart nation"* yang disusun oleh Singapura itu sendiri merupakan subjektivitas Singapura dalam memaknai dirinya sendiri yang dimuat dalam *Singapore Cybersecurity Strategy*. *"Smart nation"* sebagai pendefinisan diri Singapura membentuk rasa menyatukan Singapura sebagai agen yang berbeda dengan agen yang lainnya terutama terlihat dari definisi *"smart nation"* itu sendiri yang intinya menyatakan berbagai bagian dari Singapura yaitu warga negara, perusahaan, dan pemerintah tidak lepas dengan keberadaan teknologi informasi dan komunikasi. Lebih lanjut, Singapura sebagai *"smart nation"* merupakan hal yang didasarkan juga pada pengalaman dari Singapura itu sendiri terutama dengan penggunaan dan keterbukaan pada teknologi informasi dapat membuat Singapura memiliki karakteristik sebagai negara maju yang terhubung dengan jaringan internet.

Lee Hsien Loong dalam pembukaan *Singapore International Cyber Week* 2016 menyatakan bahwa Singapura merupakan pihak yang menjadi target ancaman dan serangan siber. Kemudian dinyatakan juga jaringan internet pemerintah Singapura secara rutin diserang. Teo Chee Hean menyatakan dalam *Singapore International Cyber Week* 2017 bahwa Singapura merupakan negara yang paling terpapar serangan siber dibandingkan dengan negara lainnya. Beberapa serangan siber yang dicontohkan adalah *Advanced Persistent Threat* yang menyerang jaringan universitas di Singapura dan pencurian data personil dari jaringan Kementerian Pertahanan Singapura[ii]. Dalam salah satu sesi *Singapore International Cyber Week 2018*, Menteri Informasi dan Komunikasi Singapura sejak 2018, S. Iswaran,

e-issn: 2684-8082; Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

menekankan bahwa serangan siber menimpa berbagai negara dan mencontohkan pengalaman Singapura terkena serangan siber pada tahun 2018 yaitu serangan terhadap sistem teknologi informasi dari layanan kesehatan masyarakat.

Pendefinisan Singapura sebagai "target serangan siber" adalah pemahaman mandiri dari Singapura sebagai agen terhadap dirinya sendiri serta pemahaman Singapura terahadap agen yang lain yaitu negara anggota ASEAN terkait dengan keberadaan ancaman dan kerentanan pada keamanan siber di Asia Tenggara. Singapura dalam hal adanya ancaman dan kerentanan pada keamanan siber di Asia Tenggara mendefinisikan diri sebagai negara yang terkena serangan siber secara rutin dan memberikan konsekuensi tersendiri baginya. Kemudian tidak hanya berhenti pada pendefinsian diri sendiri saja tetapi Singapura sebagai agen mendefinisikan juga negara anggota ASEAN lainnya sebagai negara yang menjadi "target serangan siber" sama seperti Singapura juga. Di sini maka dapat dikatakan bahwa Singapura sebagai agen menekankan adanya kesamaan nasib di antara negara-negara anggota ASEAN pada keamanan siber di Asia Tenggara. Lebih lanjut dengan Singapura menyatakan hal yang demikian maka Singapura membentuk identitas kolektif di antara Singapura dengan negara anggota ASEAN lainnya yang membuat tidak adanya perbedaan antara Singapura dan negara anggota ASEAN lainnya dalam hal keamanan siber di Asia Tenggara karena sama-sama rentan dengan adanya ancaman dan serangan siber di kawasan Asia Tenggara.

Kepentingan Objektf Singapura pada Keamanan Siber di Asia Tenggara

Secara umum bagi Singapura, ancaman siber merupakan hal yang tidak mengenal batas negara dan tidak ada negara yang dapat berurusan dengan ancaman yang berevolusi secara cepat secara sendirian. Singapura menyatakan kekukuhan komitmennya untuk membangun kapasitas keamanan siber. Sithuraj Ponraj yang merupakan Direktur *International Cyber Policy Office* dari *Cyber Security Agency of Singapura* menyatakan dalam salah satu seminar yang diadakan CSIS bahwa pembangunana kapasitas yang multisipliner merupakan hal yang penting bagi keamanan siber di Asia Tenggara. Pembangunan kapasitas mulitisipliner berarti pembangunan kapasitas yang dilakukan bukan hanya tentang keahlian teknis tetapi juga membangun kapasitas berupa kepakaran di kawasan dalam memahami isu keamanan siber. Pemahaman terhadap isu keamanan siber di Asia Tenggara oleh negara-negara di Asia Tenggara merupakan hal yang penting agar terdapat representasi dari kawasan Asia Tenggara untuk dapat menjelaskan perspektif dari negara anggota ASEAN tersendiri kepada masyarakat internasional. Berdasarkan pada *Singapore Cybersecurity Strategy*, Singapura menyatakan keinginannya dalam pembangunan kapasitas pada keamanan siber yang melibatkan berbagai pihak untuk menjadi mitranya. Pembangunan kapasitas dengan melibatkan negara lain menjadi kepentingan yang perlu dicapai terutama karena tidak terlepas dari ancaman siber yang tidak mengenal batas negara. Singapura mengajak negara-negara ASEAN untuk menjadi mitra dalam pembangunan kapasitas keamanan siber agar dapat meminimalkan adanya resiko serangan siber yang terjadi di antara negara anggota ASEAN.

Menteri Komunikasi dan Informasi Singapura, Yacoob Ibrahim, menyatakan di pembukaan ASEAN *Ministerial Conference on Cybersecurity* 2016 bahwa negara anggota ASEAN memerlukan kesadaran situasi yang lebih baik terkait dengan lingkungan ruang siber secara keseluruhan. Menurutnya, hal ini merupakan kunci untuk dapat memperbaiki higienitas ruang siber terutama dengan lebih baik mengarahkan upaya pencegahan ketika sudah mengetahui adanya kerentanan dan aktivitas ruang siber yang mencurigakan. Kemudian dengan kesadaran situasional pada keamanan siber maka suatu negara dapat

mengambil langkah pencegahan yang tepat dalam mengahdapi ancaman dan kerentanan siber potensial pada masa yang akan datang. Berkaitan dengan kesadaran pada keamanan siber, Sithuraj Ponraj menyatakan pembentukan kesadaran merupakan upaya yang melibatkan berbagai pemangku kepentingan di Asia Tenggara. Ekosistem dari ruang siber itu sendiri memiliki cakupan yang sangat luas melebihi pemerintah dari suatu negara dan dengan hal tersebut perlu mengundang berbagai pihak yang lain.

Dengan kesadaran di antara negara anggota ASEAN pada keamanan siber di Asia Tenggara mendorong adanya keterlibatan dari berbagai pihak agar terdapat munculnya berbagai macam pilihan dalam mendukung keberlangsungan setiap negara pada keamanan siber. Kepentingan Singapura pada keamanan siber di Asia Tenggara berupa pembentukan kesadaran pada keamanan siber mendorong agar negara anggota ASEAN lainnya dapat menentukan langkah tepat yang dapat diambil sesuai dengan konteks keamanan siber yang disadari. Sehingga terlepas dari perbedaan yang ada, dengan kesadaran pada keamanan siber dapat mengarahkan pada berbagai pilihan dalam menanggulangi ancaman dan kerentanan siber yang ada. Selanjutnya dari pembentukan kesadaran di antara negara anggota ASEAN dalam menekankan pentingnya keberadaan keamanan siber maka dapat mendukung negara anggota ASEAN pada hal lainnya terkait ruang siber yaitu ekonomi digital. Dengan kata lain, pilihan untuk pengembangan ekonomi digital di antara negara anggota ASEAN ini dapat dijamin dengan pembentukan kesadaran pada keamanan siber di Asia Tenggara.

Secara umum, mengacu pada *Singapore Cybersecurity Strategy*, maka Singapura menyatakan bahwa konsensus dan kesepakatan di antara berbagai negara merupakan kunci untuk memastikan keberhasilan kerjasama pada keamanan siber. Keberadaan serangan siber yang tidak menghormati yurisdiksi negara membuat Singapura memerlukan kerjasama dengan negara lainnya untuk merespon ancaman siber tersebut. Lee Hsien Loong menyatakan negara anggota ASEAN perlu lebih bekerja sama untuk mempromosikan konsensus pada norma siber agar memperkuat keterikatan operasional dan membentuk kapabilitas siber. Norma pada keamananan siber bagi Singapura bukan merupakan hal yang berupa aturan yang mengikat.

Sithuraj Ponraj menyatakan norma merupakan perilaku yang dapat diterima atau dengan kata lain norma merupakan hal yang semua sepakat untuk dilakukan atau tidak untuk dilakukan. Kemudian terdapat norma yang membatasi yaitu norma mengenai hal yang harus dilakukan dan tidak harus dilakukan serta terdapat norma yang positif yaitu norma yang dapat dilakukan. Bagi Singapura, norma pada keamanan siber merupakan hal yang penting untuknya dengan negara anggota ASEAN lainnya. Komitmen pada norma yaitu ketika Singapura dengan negara anggota ASEAN lainnya sepakat mengenai cara berperilaku maka dapat mendorong predikitabilitas dan stabilitas dalam ruang siber.

Kepentingan Subjektif Singapura pada Keamanan Siber di Asia Tenggara

Dalam memfasilitasi diskusi dan dialog di antara negara anggota ASEAN pada keamanan siber di Asia Tenggara, Singapura mengadakan *ASEAN Ministerial Conference on Cybersecurity* dalam *Singapore International Cyber Week*. Yacoob Ibrahim menyatakan bahwa diskusi dan dialog adalah hal yang krusial pada isu siber. Singapura percaya dengan *ASEAN Ministerial Conference on Cybersecurity* dapat membawa seluruh anggota ASEAN mencapai ruang siber yang berketahanan dan terpercaya. Dari hasil ASEAN *Ministerial Conference on Cybersecurity* 2016, negara anggota ASEAN menyepakati kerjasama yang lebih erat pada keamanan siber, koordinasi yang lebih kuat pada inisiatif pembangunan kapasitas keamanan siber kawasan, dan mendiskusikan fokus yang spesifik pada keamanan siber di

e-issn: 2684-8082; Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

tingkat menteri dan *senior official* (Government of Singapore, 2016c). Selanjutnya, negara anggota ASEAN mengakui nilai dari kegiatan berkumpul seperti ASEAN *Ministerial Conference on Cybersecurity* yang membawa berbagai pihak yang relevan dari kawasan Asia Tenggara. Lebih lanjut, negara anggota ASEAN menyetujui pembentukan sekumpulan norma perilaku keamanan siber yang praktis di ASEAN untuk mendukung teknologi digital agar mencapai pertumbuhan ekonomi dan memperbaiki kelayakan hidup kawasan Asia tenggara (Government of Singapore, 2016c).

Dalam pembukaan ASEAN *Ministerial Conference on Cybersecurity* 2018, S. Iswaran menyatakan apresiasinya pada negara anggota ASEAN untuk komitmen dalam mendukung dan berkontribusi dalam hal kerjasama pada keamanan siber. Kemudian dikutip dari hasil ASEAN *Ministerial Conference on Cybersecurity* 2018 dinyatakan bahwa negara anggota ASEAN menyepakati adanya kebutuhan untuk mekanisme formal keamanan siber ASEAN yang dipertimbangkan dan diputuskan pada hal yang berkaitan dengan isu kebijakan dan operasional. Mekanisme tersebut diajukan memiliki fleksibilitas dan mencakup berbagai dimensi terutama ekonomi (Government of Singapore, 2018d). Selain itu, berkaitan dengan norma siber maka negara anggota ASEAN menyatakan kembali pentingnya ruang siber yang berbasiskan aturan sebagai pendukung kemajuan ekonomi dan standa kehidupan yang lebih baik serta menyepakati pada prinsipnya bahwa hukum internasional, norma perilaku negara yang sukarela dan tidak mengikat, dan *confidence building measure* yang praktis adalah hal yang penting untuk ruang siber yang stabil (Government of Singapore, 2018d).

Kepercayaan Singapura untuk menyelenggarakan ASEAN *Ministerial Conference on Cybersecurity* merupakan hal yang dapat mendukung Singapura juga dalam mencapai kepentingan objektifnya yaitu pembangunan kapasitas, pembentukan kesadaran, dan pembentukan norma pada keamanan siber di Asia Tenggara. Hal tersebut dapat terlihat dengan berbagai hasil dari ASEAN *Ministerial Conference on Cybersecurity* menyatakan bahwa adanya inisiatif untuk pembangunan kapasitas, kemudian adanya pengakuan dari negara anggota ASEAN lainnya bahwa keamanan siber itu penting, disepakatinya mengadopsi norma yang mereferensikan pada *2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

Pada ASEAN *Ministerial Conference on Cybersecurity*, Singapura juga melucurkan ASEAN *Cyber Capacity Programme*. Tujuan dari ASEAN *Cyber Capacity Programme* adalah untuk membantu pembiayaan berbagai upaya dalam kapasitas siber di antara negara anggota ASEAN. Biaya untuk program tersebut adalah $10 juta (Government of Singapore, 2016b; Government of Singapore, 2016e). Dengan dana tersebut dapat membiayai sumber daya, ahli, dan pelatihan sehingga di setiap negara anggota ASEAN secara khususnya dapat mengarahkan agenda keamanan sibernya sendiri. Secara spesifik, ASEAN *Cyber Capacity Programme* akan memberikan sumber daya untuk memperluas cakupan aktivitas pembangunan kapasitas dan keahlian teknis yang lebih baik dalam menangani serangan siber. Lebih lanjut, ASEAN *Cyber Capacity Programme* dapat mendukung diskusi dan konsultasi dalam hal pembentukan badan keamanan siber nasional, perumusan strategi keamanan siber, dan legislasi keamanan siber.

Pada Mei 2017, Singapura berhasil mengadakan ASEAN *Cyber Norms Workshop* yang merupakan bagian dari ASEAN *Cyber Capacity Programme* (Government of Singapore, 2017b; Government of Singapore, 2017e). Kegiatan tersebut untuk mendukung diskusi norma siber di kawasan Asia Tenggara. Yacoob Ibrahim menyatakan apresiasinya pada partisipasi negara anggota

ASEAN yang sangat mendukung dan antusias dalam kegiatan tersebut. Kemudian, Singapura memiliki komitmen pada memelihara hubungan dekat dengan negara anggota ASEAN lainnya untuk membangun kapasitas siber kawasan. Oleh karena itu Singapura mengumumkan penambahan dana sebesar $ 1,5 juta untuk ASEAN *Cyber Capacity Programme* untuk membangun kapasitas teknis dalam meresepon insiden serangan siber (Government of Singapore, 2017b; Government of Singapore, 2017e).

Pada pembukaan *Singapore International Cyber Week* 2018, Teo Chee Hean menyatakan bahwa untuk dapat melakukan hal lebih dalam upaya pembangunan kapasitas keamanan siber di Asia Tenggara maka Singapura meluncurkan *ASEAN-Singapore Cybersecurity Centre of Excellence*. Keberadaan *ASEAN-Singapore Cybersecurity Centre of Excellence* memiliki tiga tujuan umum yaitu (1) memperkuat pengembangan strategi, legislasi, dan kapabilitas penelitian pada keamanan siber di antara negara anggota ASEAN; (2) melatih *Computer Emergency Response Team* yang ada pada tingkat nasional di negara anggota ASEAN pada hal berupa keahlian teknis dan respon insiden serangan siber; dan (3) mempromosikan saling berbagai informasi terkait keamanan siber di antara *Computer Emergency Response Team* dari masing- masing negara (Government of Singapore, 2018b; Government of Singapore, 2018e)[iii]. Teo Chee Hean menyatakan bahwa *ASEAN-Singapore Cybersecurity Centre of Excellence* akan terbuka dan inklusif dalam mendukung dan memperkuat inisiatif kerjasama pada keamanan siber. Kemudian negara anggota ASEAN dapat terlibat lebih dekat di dalamnya.

Iswaran menyatakan dalam ASEAN *Ministerial Conference on Cybersecurity* 2018 bahwa cakupan dari *ASEAN-Singapore Cybersecurity Centre of Excellence* adalah kebijakan, strategi, legislasi, dan operasi pada keamanan siber. Keberadaan *ASEAN-Singapore Cybersecurity Centre of Excellence* merefleksikan kesadaran dalam pentingnya menyelaraskan upaya pada keamanan siber di Asia Tenggara dengan isu operasionalnya. Kemudian dinyatakan bahwa keselarasan pada hal tersebut akan memfasilitasi koordinasi yang menuju kesamaan perspektif di antara negara anggota ASEAN sehingga dapat secara lebih baik mengamankan kepentingan kolektif kawasan pada tingkat internasional. Lebih lanjut, *ASEAN-Singapore Cybersecurity Centre of Excellence* mengeksplorasi dapat berfungsi sebagai pusat untuk mempertahankan dan menyelaraskan upaya pembangunan kapasitas kawasan pada keamanan siber.

KESIMPULAN

Dalam penyelenggaraan *Singapore International Cyber Week*, Singapura memaknai kondisi dirinya pada situasi keamanan siber di Asia Tenggara sebagai *"smart nation"* dan "target serangan siber". Singapura juga menyatakan ide berupa negara di Asia Tenggara lainnya secara kolektif memiliki nasib yang sama dengannya sebagai negara yang terancam dan rentan dalam keamanan siber. Dengan pemaknaannya, Singapura memiliki kepentingan yang ingin dicapainya dalam *Singapore International Cyber Week* berupa pembangunan kapasitas, pembentukan kesadaran, dan pembentukan norma pada keamanan siber di Asia Tenggara. Cara yang dipercayai oleh Singapura untuk dapat mencapai kepentingannya tersebut adalah melibatkan negara di Asia Tenggara lainnya dengan menyelenggarakan *ASEAN Ministerial Conference on Cybersecurity*, meluncurkan *ASEAN Cyber Capacity Programme*, dan menggagas *ASEAN-Singapore Cybersecurity Centre of Excellence* dalam penyelenggaraan *Singapore International Cyber Week*.

DAFTAR PUSTAKA

ASEAN. (2016). Cyber Security and Cybercrime in ASEAN. International Symposium on "*ASEAN Cyber Security and Cyber Crime Center: Possibility and Way Forward*".

e-issn: 2684-8082; Vol. 1 No. 1, Mei 2019 (39-52) doi: 10.24198/padjir.v1i1.21591

ATKearney. (2018). *Cybersecurity in ASEAN: An Urgent Call for Action*. Dipetik 4 Maret 2019 dari https://www.atkearney.com/documents/20152/989824/Cybersecurity+in+ASEAN.pdf/2e0fb55c-8a50-b1e3-4954-2c5c573dd121.

Carr A. & Wallis, J. (2016). An Introduction to Asia-Pacific Security. J. Wallis & A. Carr (eds) *Asia-Pacific Security: An Introduction*. Washington, DC: Georgetown University Press.

Channel News Asia. (2018). *Singapore to pump in $30m for new regional cybersecurity*. Dipetik 4 Maret 2019 dari https://www.channelnewsasia.com/news/singapore/singapore-to-pump-in-s-30m-for-new-regional-cybersecurity-10735308.

Choucri, N. (2012). Cyberpolitics in International Relations. Cambridge: MIT Press.

Ciolan, I. M. (2014). *Defining Cybersecurity as The Security Issue of The Twenty First Century: A Constructivist Approach.* The Public Administration and Social Policies Review VI 1(12) hal. 120-136.

Cyber Security Agency. (2016). *Singapore's Cybersecurity Strategy*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf.

Cyber Security Agency. (2016a). *Singapore Cyber Landscape 2016*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape.pdf.

Cyber Security Agency. (2017). *Singapore Cyber Landscape 2017*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape2017.pdf.

FireEye & Singtel. (2015). *Southeast Asia: An Evolving Cyber Threat Landscape.* Dipetik 4 Maret 2019 dari https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf.

FTI Consulting. (2017). *Singapore's Approach to Cyber Security*. Dipetik 4 Maret 2019 dari https://www.fticonsulting-asia.com/~/media/Files/apac-files/insights/white-papers/singapore-cybersecurity.pdf.

Government of Singapore. (2016). *Key Partnerships Established at the Inaugural Singapore International Cyber Week 2016*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-releases/key-partnerships-established-at-the-inaugural-sicw-2016.

Government of Singapore. (2016a). *Speech by Prime Minister Lee Hsien Loong at the Singapore International Cyber Week 2016.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/singapore-international-cyber-week-2016-opening-ceremony.

Government of Singapore. (2016b). *Opening Speech by Dr Yaacob Ibrahim, Minister for Communications and Information and Minister-In-Charge of Cyber Security, at the Asean Ministerial Conference on Cybersecurity*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2016.

Government of Singapore. (11 Oktober 2016c). *ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean.

Government of Singapore (10 Oktober 2016d). *PM Lee Hsien Loong at the Singapore International Cyber Week Opening Ceremony*. Dipetik 4 Maret 2019 dari https://www.pmo.gov.sg/Newsroom/pm-lee-hsien-loong-singapore-international-cyber-week-opening-ceremony.

Government of Singapore. (2016e). *The ASEAN Ministerial Conference on Cybersecurity*. Dipetik 4 Maret 2019 dari https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2016/10/the-asean-ministerial-conference-on-cybersecurity.

Government of Singapore. (2017). *Key Collaborations Affirm Singapore International Cyber Week as a Premier Platform for Cyber Capacity Building and International Partnerships.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-

releases/key-collaborations-at-singapore-international-cyber-week-2017.

Government of Singapore. (2017a). *Speech by Mr Teo Chee Hean, Deputy Prime Minister and Coordinating Minister for National Security at the 2nd Singapore International Cyber Week.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/singapore-international-cyber-week-2017-opening-ceremony.

Government of Singapore. (2017b). *Opening Speech by Dr Yaacob Ibrahim, Minister for Communications and Information and Minister-In-Charge of Cyber Security, at the Asean Ministerial Conference on Cybersecurity.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2017.

Government of Singapore. (2017c). *ASEAN Member States Affirm Importance of Closer Coordination of Cybersecurity Efforts in ASEAN*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-releases/amcc-2017.

Government of Singapore. (2017d). *DPM Teo Chee Hean at the 2nd Singapore International Cyber Week Opening Ceremony*. Dipetik 4 Maret 2019 dari https://www.pmo.gov.sg/Newsroom/dpm-teo-chee-hean-2nd-singapore-international-cyber-week-opening-ceremony.

Government of Singapore. (2017e). *Speech by Dr Yaacob Ibrahim, Minister for Communications and Information at the opening ceremony of ASEAN Ministerial Conference on Cybersecurity on 18 September 2017, at 9am, at St Regis, John Jacob Ballroom 1*. Dipetik 4 Maret 2019 dari https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/9/the-opening-ceremony-of-asean-ministerial-conference-on-cybersecurity.

Government of Singapore. (2017f). *Joint Call on Acting Prime Minister Teo Chee Hean by Participants of the 2nd ASEAN Ministerial Conference on Cybersecurity*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-releases/joint-call-on-acting-prime-minister-teo-chee-hean.

Government of Singapore. (2018). *Our Organisation.* Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/about-us/our-organisation.

Government of Singapore. (2018a). *Singapore International Cyber Week 2018 - Highlights and Testimonials*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/press-releases/sicw-2018---highlights-and-testimonials.

Government of Singapore. (2018b). *Speech by DPM Teo Chee Hean At The Opening Of The Third Singapore International Cyber Week*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/singapore-international-cyber-week-2018-opening-ceremony.

Government of Singapore. (2018c). *Opening Speech by Mr S Iswaran, Minister for Communications and Information, At The ASEAN Ministerial Conference on Cybersecurity*. Dipetik 4 Maret 2019 dari https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2018

Government of Singapore. (2018d). *ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts*. Dipetik 4 Maret 2019 dari: https://www.csa.gov.sg/news/press-releases/amcc-2018.

Government of Singapore. (2018e). *DPM Teo Chee Hean at the Opening of the 3rd Singapore International Cyber Week*. Dipetik 4 Maret 2019 dari https://www.pmo.gov.sg/Newsroom/dpm-teo-chee-hean-opening-3rd-singapore-international-cyber-week.

Government of Singapore. (2018f). *Opening Remarks by Mr S Iswaran, Minister for Communications and Information, At The ASEAN Ministerial Conference on Cybersecurity, on 19 September 2018.* Dipetik 4 Maret 2019 dari https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity.

Hadiwinata, B. S. (2017). *Studi dan Teori Hubungan Internasional: Arus Utama, Alternatif, dan Reflektivis*. Jakarta: Pustaka OBOR.

Hardy, C. et al. (2004). Discourse Analysis and Content Analysis: Two Solitudes?. *Qualitative Methods* 2(1) hal. 19-22.

Hughes, R. B. (2016). How is the Cyber

Revolution Changing Asia-Pacific National Security Concerns?. J. Wallis & A. Carr (eds) *Asia-Pacific Security: An Introduction.* Washington, DC: Georgetown University Press.

Hogeveen., B. (2019). Wawancara Peneliti dengan Bart Hogeveen, Analyst Cyber Policy Centre, Australian Strategic Policy Institute (ASPI) melalui Surel pada 4 Februari hingga 15 Februari 2019.

Hogeveen, B. (2019a). Pemaparan dari Bart Hogeveen, Analyst Cyber Policy Centre, Australian Strategic Policy Institute (ASPI). Public Seminar ASEAN Cyber Norms: National Impact and Way Forward. Centre for Strategic and International Studies (CSIS) Auditorium. 31 Januari 2019

ICT4Peace Foundation. (2017*). Promoting Norms of Responsible Behaviour in Cyberspace in Singapore.* Dipetik 4 Maret 2019 dari https://ict4peace.org/activities/promoting-norms-of-responsible-behaviour-in-cyberspace/

IGI Global. (2018). *What is intrusion attack.* Dipetik 4 Maret 2019 dari https://www.igi-global.com/dictionary/intrusion-attack/15624.

ITU. (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Dipetik 4 Maret 2019 dari https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

ITU. (2017). *Global Security Index 2017*. Dipetik 4 Maret 2019 dari https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

KnowBe4. (2018). *What is Phishing?* Dipetik 4 Maret 2019 dari https://www.phishing.org/what-is-phishing.

Koh, D. (2017). *CSA Singapore setting up academy to train cybersecurity professionals, starting with government and CII sectors.* Dipetik 4 Maret 2019 dari https://www.opengovasia.com/csa-singapore-setting-up-academy-to-train-cybersecurity-professionals-starting-with-government-and-cii-sectors/

Lamont, C. (2015). *Research Methods in International Relations*. London: SAGE.

Liang, L. Y. (2016). *Singapore's weapon: cyber diplomacy.* Dipetik 4 Maret 2019 dari https://www.straitstimes.com/singapore/spores-weapon-cyber-diplomacy.

Moir, R. (2009). *Defining Malware: FAQ.* Dipetik 4 Maret 2019 dari https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10).

Ng. (2019). Wawancara Peneliti dengan Ng Hoo Ming, Deputy Chief Executive Operations, Singapore Cyber Security Agency (CSA) melalui Surel pada 30 Januari hingga 15 Februari 2019.

Parameswaram, P. (2018). *What's Next for the New ASEAN-Singapore Cyber Center? A closer look at the future prospects of the new body.* Dipetik 4 Maret 2019 dari https://thediplomat.com/2018/09/whats-next-for-the-new-asean-singapore-cyber-center/

Perwita, A. A. B. & Yani, Y. M. (2017). *Pengantar Ilmu Hubungan Internasional*. Bandung: Remaja Rosdakarya.

Ponraj, S. (2019). Pemaparan dari Sithuraj Ponraj, Direktur International Cyber Policy Office, Singapore Cyber Security Agency (CSA). Public Seminar ASEAN Cyber Norms: National Impact and Way Forward. Centre for Strategic and International Studies (CSIS) Auditorium. 31 Januari 2019.

Rahardjo., B. (2019). Wawancara Peneliti dengan Budi Rahardjo, Pakar Keamanan Siber, Indonesia Computer Emergency Response Team (ID-CERT) bertempat di BLOCK71 pada 14 Februari 2019.

Reveron, D. S. (2012). An Introduction to National Security and Cyberspace. D. S. Reveron (eds.). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington D. C.: Georgetown University Press.

SICW. (2016). *About Singapore International Cyber Week (SICW).* Dipetik 4 Maret 2019 dari https://www.sicw.sg/2017/about-event.html.

SICW. (2018). *About Singapore International Cyber Week (SICW).* Dipetik 4 Maret 2019 dari https://www.sicw.sg/about-event.html.

Techopedia. (2018). *Computer Emergency Response Team (CERT).* Dipetik 4 Maret 2019 dari https://www.techopedia.com/definition/310

03/computer-emergency-response-team-cert.

TechTarget. (2018). *Advanced Persistent Threat (APT)*. Dipetik 4 Maret 2019 dari https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

Trend Micro. (2015). *Ransomware*. Dipetik 4 Maret 2019 dari https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

Vu, C. (2019). Wawancara Peneliti dengan Dr Cung Vu, Visiting Senior Fellow, Rajaratnam School of International Studies (RSIS) melalui Surel pada 28 Januari hingga 7 Februari 2019.

We Are Social. (2017). *Digital in 2017: Global Overview*. Dipetik 4 Maret 2019 dari https://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview.

We Are Social. (2018). *Digital in 2018: Global Overview*. Dipetik 4 Maret 2019 dari https://digitalreport.wearesocial.com/report_download.

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International Organization 46(2)* hal. 391–426.

Wendt, A. (1994). Collective Identity Formation and the International State. *The American Political Science Review 88(2)* hal. 384-396.

Wendt, A. (1995). Constructing International Politics. *International Security 20(1)* hal. 71-81. Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

BIOGRAFI

Muhammad Fikry Anshori merupakan mahasiswa Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran angkatan 2015 yang tertarik mengkaji tentang keamanan Siber maupun Studi Keamanan pada umumnya.

Rizki Ananda Ramadhan merupakan dosen pada Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran yang tertarik mengkaji tentang studi keamanan, Diplomasi dan kajian studi kawasan, khususnya perkembangan hubungan internasional di Asia Pasifik.

[i] *Malware* (*malicious software*) adalah istilah yang digunakan untuk merujuk kepada segala perangkat lunak yang didesain untuk merusak komputer atau jaringan komputer (Moir, 2009). *Ransomware* merupakan salah satu jenis *malware* yang mencegah atau membatasi pengguna untuk mengakses komputer dengan cara mengunci sistem komputer tersebut dan pengguna komputer diharuskan membayar kepada pembuat *ransomware* agar komputer tersebut dapat diakses kembali (Trend Micro, 2015).

[ii] *Advanced Persistent Threat* adalah serangan siber yang terjadi pada suatu jaringan komputer yang tidak terdeteksi keberadaanya dalam jangka waktu yang panjang (TechTarget, 2018).

[iii] *Computer Emegency Response Team* (CERT) merupakan istilah untuk sekelompok pakar yang dapat merespon terjadinya insiden dalam keamanan siber (Techpedia, 2018).