PENINGKATAN KEAMANAN SIBER ASEAN MELALUI KERJA SAMA KEAMANAN SIBER DENGAN AUSTRALIA

OLEH : SOFIA TRISNI, RIKA ISNARTI DAN ABDUL HALIM

PUSAT STUDI ASEAN UNIVERSITAS ANDALAS

ABSTRAKSI

Serangan siber termasuk kepada isu keamanan non tradisional, yang dampaknya dapat merusak semua aktivitas yang menggunakan sistem komputer. ASEAN saat ini telah merumuskan berbagai macam dokumen mengenai penanganan kejahatan siber, akan tetapi belum ada upaya kongkrit yang dilaksanakan. Pengembangan siber ASEAN sejauh ini berfokus kepada sektor militer dan masih kurang memperhatikan sektor publik yang merupakan sektor dengan pengguna komputer dalam jumlah terbanyak. Tulisan ini bertujuan untuk memberikan saran kepada ASEAN untuk membangun kerjasama siber dengan salah satu negara mitra wicara ASEAN, yaitu Australia. Australia merupakan negara yang mengembangkan sibernya secara serius dan Australia juga merupakan negara tetangga terdekat ASEAN yang memprioritaskan kerjasama dengan ASEAN, sehingga kerjasama dengan ASEAN dirasa merupakan rekomendasi yang baik bagi ASEAN. Dengan bekerjasama dengan Australia diharapkan ASEAN akan mendapatkan keuntungan yaitu peningkatan keamanan siber di kawasan.

Kata Kunci : ASEAN, Ancaman siber, kerjasama, Australia

A. PENDAHULUAN

Saat ini isu keamanan non tradisional menjadi isu penting karena dampak yang ditimbulkannyatidak kalah dahsyat dari ancaman pada isu keamanan tradisional. Salah satu isu dalam keamanan non tradisional adalah ancaman siber yang berkaitan erat dengan teknologi komputer dan internet. Perkembangan pesat teknologi komputer dan internet telah menciptakan ketergantungan yang sangat besar terhadap keduanya. Setiap aktivitas yang biasanya diawasi dengan mengandalkan tenaga manusia perlahan dialih tugaskan kepada komputer. Tidak hanya itu, internet telah mempermudah kehidupan manusia karena segala informasi dapat diakses dengan mudah hanya dari belakang meja. Ketergantungan kepada komputer dan internet ini kemudian terganggu dengan adanya serangan siber. Contohnya adalah serangan siber yang terjadi di Ukraina pada tanggal 27 Juni 2017 lalu yang menyebabkan lumpuhnya seluruh ATM di negara ini dan lumpuhnya sistem komputer yang bertugas mengawasi Cernobyl, sehingga pengawasan harus dilakukan secara manual.[1] Serangan siber ini tidak hanya melanda Ukraina dan negara Eropa dan Amerika saja, tetapi juga telah mengenai negara-negara ASEAN. Bulan Mei 2017 yang lalu, dilaporkan

[1] N. Perlroth, M Scott and S. Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally", *The New York Times*, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html, 29 Juni 2017

bahwa Indonesia, Malaysia, Thailand dan Vietnam telah diserang oleh ransomware[2], walaupun belum memberikan dampak kelumpuhan yang fatal.

Menilik bahaya kelumpuhan komputer yang dapat ditimbulkan oleh serangan siber, tulisan ini bertujuan untuk memberikan saran agar ASEAN membangun kerjasama dengan salah satu mitra wicaranya yaitu Australia dalam mengantisipasi serangan siber ini. Australia dipilih sebagai negara tujuan kerjasama karena negara ini merupakan negara yang serius dalam memperkuat keamanan negaranya dari bahaya serangan siber dan juga karena fokus pengembangan siber Australia yang merupakan sektor kekurangan ASEAN, sehingga ASEAN akan mendapatkan keuntungan yang besar dari kerjasama ini.

Untuk mencapai tujuan diatas, tulisan ini dibagi menjadi tiga bagian. Bagian pertama menjelaskan mengenai pentingnya keamanan siber,bagian kedua merupakan bagian analisis mengenai kerjasama siber dengan Australia dan bagian ketiga merupakan saran dan rekomendasi.

B. PENTINGNYA KEAMANAN SIBER

Sebelum memetakan keuntungan yang bisa didapatkan oleh ASEAN, penting untuk melihat mengapa ASEAN merupakan kawasan yang rentan akan ancaman siber. Ada beberapa alasan untuk kerentanan ini;pertama, sebagian besar pengguna internet di dunia merupakan masyarakat ASEAN. Pada saat ini, dari 2.1 miliar pengguna internet, 922 juta pengguna berasal dari kawasan ASEAN dan diperkirakan jumlah ini akan terus meningkat setiap tahunnya.[3]Kedua, ASEAN merupakan organisasi kawasan terbesar di Asia Pasifik, artinya interaksi ekonomi dan pasar juga besar dikawasan ini, sebagian besar interaksi ekonomi pada saat ini berlangsung di dunia siber yang juga berarti bagi kawasan ASEAN, sebagian besar interaksi ekonomi siber berada di ASEAN. Selanjutnya, menurut Heinl ASEAN merupakan kawasan yang sedang membangun.[4] Banyak infrasturuktur yang dibangun dengan sistem ICT seperti jaringan transportasi, pertambangan, energi, perbankan serta meningkatkan cakupan dan luasan jaringan telepon genggam menuju wilayah-wilayah

[2]The Straits Times Asia,Cyber attack: Ransomware cases reported in Asia, http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia, 29 Juni 2017
[3]European Commission, “Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level ofNetwork and Information Security across the Union,” Commission StafforkingDocument, February 7, 2013.
[4]Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *asia policy*(18), 131-159. p.135

terpencil. Beberapa fakta ini memperlihatkan bahwa ASEAN merupakan kawasan dengan interaksi siber yang tinggi.

Meningkatnya konektivitas di dunia maya dan ketergantungan akan siber juga meningkatkan kemungkinan kejahatan transnasional yang berbasis siber.[5] Salah satu ancaman siber yang paling banyak dialami oleh negara-negara di ASEAN sejak tahun 2012 – 2013 menurut Heinl adalah penyerangan pada website pemerintahan.[6] Menurutnya, meskipun sebagian negara ASEAN merupakan negara yang masih berkembang, namun tidak luput dari penyerangan dan ancaman siber yang dibuktikan dengan seluruh negara di ASEAN pernah merasakan penyerangan pada website-website pemerintahan mereka.[7]

Untuk menangani ancaman siber di ASEAN, pada level bilateral dan regional telah banyak aksi yang dilakukan oleh ASEAN diantarannya,*ASEAN ICT Masterplan 2015, The ASEAN Cyber Capacity Programme, Mactan Cebu Declaration Connected ASEAN: EnablingAspirations* dan berbagai dokumen lainnya. Namun, sejauh ini aksi yang dilakukan oleh ASEAN dalam menanggulangi ancaman siber masih dalam sebatas pembuatan legal dokumen dan peningkatan kerjasama dalam penegakan hukum. ASEAN masih memerlukan upaya yang lebih komprehensif dan usaha yang lebih nyata dalam menanggulagi ancaman siber dibandingkan hanya sebatas pembuatan dokumen.[8]

Sebagai sebuah kawasan besar dengan interaksi siber yang tinggi, ada beberapa permasalahan siber yang penting diperhatikan oleh ASEAN untuk mencapai integrasi keamanan siber yang lebih baik. Pertama, ASEAN belum memiliki rangking dan prioritas kerentanan sektor infrastruktur pada setiap negara. Sejauh ini, negara-negara di ASEAN masih disibukkan dengan fenomena siber yang merupakan sebuah fenomena yang mengandung ancaman selain memiliki manfaat, namun ASEAN masih belum memiliki kesadaran akan ancaman dan pada sektor apa acaman itu akan terjadi. Penting bagi setiap negara di ASEAN untuk membuat rangking dan prioritas kerentanan akan sektor infrastrukturnya. Hal ini berguna untuk menjaga keberlanjutan akan pembangunan yang dilakukan oleh ASEAN.

[5]James Lewis, “Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia,” prepared for the Lowy Institute MacArthur Asia Security Project, March 7, 2013
[6]Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *asia policy*(18), 131-159. P.137
[7]UN Official on Drugs and Crime, “Comprehensive Study on Cybercrime” (draft February 2013),xvii, xxi, 4–7
[8]James Lewis, “Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia,” prepared for the Lowy Institute MacArthur Asia Security Project, March 7, 2013

Kedua, menurut Heinl dan Kurlanzick , dokumen-dokumen ASEAN mengenai ancaman siber masih ambigu dan susah untuk dipahami.[9] Dokumen-dokumen yang dibuat belum menggambarkan solusi praktis yang harus diambil oleh ASEAN ketika munculnya ancaman siber. Sehingga, dokumen yang dibuat oleh ASEAN mengenai siber masih sebatas gambaran umum mengenai siber dan terkesan hanya sebagai bentuk kesadaran semu ASEAN agar terlihat memiliki kesadaran yang sama seperti institusi regional lainnya.[10] Lemahnya tindakan ASEAN dalam hal ini membuat kaburnya mekanisme yang harus dilakukan oleh ASEAN ketika mengalami ancaman ataupun serangan siber karena tidak ada unit kerja yang jelas serta prosedur yang harus diambil pada saat terjadi serangan begitupun juga prosedur untuk peningkatan keamanan siber ASEAN.

Permasalahan ketiga adalah ASEAN tidak berusaha membangun kesadaran akan ancaman siber pada masyarakatnya. Padahal, yang menjadi pengguna terbesar siber di ASEAN merupakan masyarakat sipil bukan militer atau pemerintah. Namun, upaya untuk menanggulangi siber yang dilakukan oleh ASEAN sejauh ini lebih berpusat pada pemerintahan dan militer. Hal ini terlihat dari dokumen-dokumen yang dibuat oleh ASEAN memiliki target pemerintahan negara –negara yang bergabung dengan ASEAN, begitupun juga dengan penguatan siber lebih banyak dipusatkan pada kekuatan militer seperti kerjasama antara India dengan Vietnam dalam pembangunan laboratorium forensik digital di Vietnam, peningkatan kemampuan pertahanan siber oleh Singapura dan Brunei Darussalam pada militernya.

Keempat, peningkatan kemampuan penanggulangan siber ASEAN berpusat pada militer. Peningkatan kemampuan pertahanan dan penyerangan siber pada militer merupakan salah satu upaya yang dibutuhkan dalam pencapaian keamanan siber. Namun, serangan siber lebih banyak tertuju pada sektor publik, bukan sektor militer.[11] Dengan kata lain, sektor publik lebih rentan dan lebih memerlukan peningkatan kekuatan sebanding dengan peningkatan keamanan siber pada militer. Usaha ini belum dilakukan cukup besar oleh kawasan ASEAN, sehingga dapat dilihat sebagian besar serangan siber pada ASEAN tertuju pada sektor publik, seperti website pemerintahan, penyebaran virus pada ponsel dan

[9]Joshua Kurlantzick, “ASEAN’s Future and Asian Integration,” Council on Foreign Relations, International Institutions and Global Governance Program, Working Paper, November 2012 dan Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *asia policy*(18), 131-159. P.142
[10]Joshua Kurlantzick, “ASEAN’s Future and Asian Integration,” Council on Foreign Relations, International Institutions and Global Governance Program, Working Paper, November 2012
[11]European Parliament Committee on Foreign Affirs, “Draf Report on Cyber Security and Cyber Defence,” June 2012, 4.

pc masyarakat, tindakan espionage dan pencurian dana perbankan yang bersumber dari tabungan individu serta serangkaian bentuk serangan publik lainnya. Selain itu, pada

serangan siber tidak bisa dipastikan bahwa serangan berasal dari militer atau publik, namun target penyerangan dapat dipastikan akan lebih banyak kepada sektor publik. Hal ini memberikan gambaran bahwa militer tidak dapat serta merta melakukan serangan balasan dan melakukan prosedur militer dalam membalas serangan di dunia maya.

Permasalahan terakhir yang dialami oleh ASEAN dalam siber adalah ketidaksamaan kemampuan negara-negara di ASEAN, sebagian negara di ASEAN merupakan negara dengan teknologi maju dan sudah berkembang merata diseluruh wilayah negaranya, sedangkan sebagian wilayah ASEAN lainnya masih memiliki teknologi sederhana dan dalam upaya pengembangan teknologi serta pengembangan sektor ICT untuk insfrastruktur pentingnya serta belum mengalami pemerataan keseluruh wilayah negerinya. Ketimpangan situasi ini membuat tidak semua negara di ASEAN memiliki kesadaran akan ancaman siber yang sama, karena ancaman yang dirasakan oleh satu negara belum tentu ancaman bagi yang lain karena negara tersebut belum memiliki teknologi sejenis atau masih dalam upaya pengembangan. Hal ini juga memuat sulitnya bagi ASEAN untuk mengembangan kerangka kerja yang jelas dan dapat dilaksanakan oleh seluruh negara.

Walaupun demikian, siber tetaplah merupakan isu yang sangat penting bagi ASEAN.Terlihat bahwa ancaman serta permasalahan siber juga melanda ASEAN, sehingga kedepannya ASEAN perlu melakukan sebuah langkah kongkrit untuk meningkatkan keamanan sibernya. Salah satu upaya yang dapat dilakukan adalah kerjasama dengan mitra wicara ASEAN yang memiliki kapasitas dan kapabilitas mengenai siber yang lebih baik. Penulis berargumen bahwa Australia yang merupakan mitra wicara ASEAN merupakan negara tujuan kerjasama yang tepat dengan uraian yang akan diberikan pada bagian selanjutnya.

C. ANALISIS : KERJA SAMA SIBER DENGAN AUSTRALIA

Australia merupakan negara dengan kondisi keamanan siber yang sudah sangat baik. Hal ini bisa dilihat dari strategi kemanan siber yang dimiliki oleh Australia yang dirilis pada April 2016. Strategi kemanan siber Australia dibentuk atas dasar peningkatan keterhubungan melalui dunia maya oleh warga Australia yang terkoneksi dengan semua orang dipenjuru dunia. Sebagai bukti dari peningkatan tersebut adalah 90 persen warga Australia adalah pengguna internet yang aktif, sebagian besar warga Australia menghabiskan satu hari

perminggu untuk mengakses internet, serta 84% bisnis baik skala medium maupun kecil di Australia telah terkoneki dengan internet.[12] Strategi keamanan siber Australia memiliki lima tema aksi hingga tahun 2020.[13] Kelima tema aksi tersebut meliputi kemitraan siber nasional, pertahanan siber yang kuat, tanggung jawab global dan pengaruhnya, pengembangan dan inovasi, serta penggunaan siber yang cerdas.[14]

Setiap tema aksi yang direncanakan dalam strategi keamanan siber Australia, memiliki keunggulan masing-masing. Untuk menciptakan kemitraan siber nasional, Australia melakukan beberapa kinerja meliputi pelaporan mengenai perkembangan strategi yang telah diimplementasikan, melakukan pertemuan rutin dengan para pimpinan yang memiliki kepentingan dalam keamanan siber, membentuk sebuah lembaga yang bertanggung jawab untuk memantau kemananan siber Australia serta sebagai pusat dalam pengembangan kemanan siber Australia. Lembaga ini dikenal dengan Cyber Sercurity Center (CSC), serta mendanai aktivitas penelitian terkait kemanan siber yang akan memberi pengaruh pada pengembangan ekonomi Australia.[15]

Selain meningkatkan kemitraan siber nasional, Australia dalam wacana kemanan siber juga melakukan peningkatan pertahanan dalam bidang siber. Dalam konteks ini, pemerintah Australia membuat sebuah pendekatan berlapis guna mengetahui dan menghadapi ancaman siber yang datang.[16] Pendekatan berlapis ini memiliki 3 komponen yang saling berkaitan. Lapis pertama adalah *Australian Cyber Security Center* yang melakukan pembagian informasi rahasia tentang keadaan gawat sekaitan dengan kondisi kemanan siber kepada para mitra terutama mitra bisnis utama.[17] Lapis kedua adalah *Joint Cyber Threat Center*. Lapisan ini terdiri dari pemerintah Australia, pebisnis dan peneliti. Lapis ini lebih menekankan pada penyebaran informasi sensitif mengenai ancaman yang ada di bidang siber. Sedangkan lapis ketiga adalah *Online Cyber Threat Sharing Portal*,

[12] Australia's Cyber Security Strategy https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf diakses pada tanggal 26 juni 2017, p. 14
[13] Alistair Haskett.2016."Australian Govermenet Releases Its Cyber Security Strategy". Australia:Herbert Smith Freehills.p.1.
[14] Alistair Haskett , p.1
[15] Australia's Cyber Security Strategy https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf diakses pada tanggal 26 juni 2017, p. 58
[16] Australia's Cyber Security Strategy , Page 32
[17] Cyber Security, Threats, Challenges, Opportunities. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf diakses pada tanggal 26 juni 2017, p.32

merupakan sebuah portal online di internet yang berisi organisasi yang membagi informasi mengenai ancaman dan hasil analisis mengenai ancaman-ancaman siber yang ada.[18] Strategi Australia ini juga memperlihatkan bahwa Australia telah berusaha menanamkan kesadaran keamanan siber pada publiknya untuk menanggulagi ancaman siber.

Tanggung jawab global terhadap kemanan siber juga menjadi prioritas Australia sebaga bentuktanggung jawab dalam menekan angka kejahatan siber di seluruh dunia. Pada poin ini, kemungkinan kerjasama berpeluang besar untuk dilakukan. Dua aspek yang ditekankan pada bagian ini adalah melakukan kemitraan internasional guna mencegah aktivitas kejahatan siber dengan fokus pada wilayah indo-pasifik. Sedangkan di poin lain, Australia juga mengajak untuk membangun kapasitas siber di wilayah indo-pasifik melalui kemitraan baik publik maupun swasta.[19] Australia juga menerbitkan strategi keterlibatan dalam masalah siber Internasional serta menggalakkan internet terbuka, gratis dan aman yang memungkinkan semua negara menghasilkan pertumbuhan dan peluang online.[20] Dalam hal ini, sangat memungkinkan bagi ASEAN untuk merintis kerjasama siber dengan Australia, karena selain negara ini terbuka untuk melakukan kerjasama, secara spesifik pada KTT peringatan 40 tahun ASEAN-- Australia tahun 2014 di Myanmar, Australia menyampaikan keinginannya untuk menjadi mitra terpercaya ASEAN tidak hanya di bidang ekonomi tetapi juga bidang politik dan keamanan.[21]

Pada bagian pengembangan dan inovasi, Australia membangun pusat pertumbuhan kemanan siber dengan sektor swasta guna mengkooridinasikan jaringan inovasi kemanan siber nasional yang menjadi pionir dalam penelitian dan inovasi keamanan siber yang mutakhir, Mempromosikan dan produk dan layanan keamanan siber Australia untuk pengembangan dan ekspor dengan fokus khusus di wilayah indo-pasifik.[22]

Selain itu, pemerintah Australia membentuk Academic Center of Cyber Security Excellence di berbagai universitas yang bertujuan untuk meningkatkan angkatan kerja yang paham mengenai keamanan siber. Selain itu, bekerja sama dengan sektor swasta dan internasional sangat dibutuhkan guna menigkatkan kesadaran mengenai kemanan siber untuk seluruh

[18]Cyber Security, Threats, Challenges, Opportunities, p. 32
[19]Cyber Security, Threats, Challenges, Opportunities, p.39
[20]Cyber Security, Threats, Challenges, Opportunities, p.39
[21]Masyarakat ASEAN, “Kerjasama ASEAN-Australia semakin Meningkat”, *Masyarakat ASEAN Edisi 6, 2014*, p 11
[22]Cyber Security, Threats, Challenges, Opportunities, p. 45

masyarakat. Kedua poin yang dipaparkan diatas adalah aksi yang dilakukan oleh pemerintah Australia guna membentuk pengguna siber yang cerdas.[23]

Dari pemaparan diatas mengenai kelebihan yang dimiliki oleh Australia di bidang keamanan siber, bisa disimpulkan bahwa sebenarnya Australia mampu menjadi *role model* pengembangan kemanan siber dunia. Hal ini bisa dilihat dari beberapa aspek yakni Australia begitu inovatif dalam memberikan solusi mengenai masalah siber global melalui penerbitan strategi keterlibatan dalam masalah siber Internasional serta menggalakkan internet terbuka, gratis dan aman yang memungkinkan semua negara menghasilkan pertumbuhan dan peluang online. Pengembangan kemanan siber merupakan lahan bisnis baru bagi negara jika mampu dikembangkan dengan baik.[24] Dari data yang dilansir melalui model yang dibentuk di Amerika Serikat, resiko kemanan siber dalam dunia bisnis akan meningkat 38% tiap tahunnya. Dengan resiko yang tinggi inilah, investasi negara dalam pengembangan alat dan pelatihan mengenai kemanan siber harus ditingkatkan. Pengeluaran guna perlindungan kemanan siber untuk kawasan Asia Pasifik, dilansir sekitar 22 milyar USD pada tahun 2020, hal ini kemudian memberikan kesempatan Australia guna pengembangan industri mengenai kemanan siber.[25] Keamanan siber yang terbentuk nantinya bukan hanya untuk melindungi negara dan dunia bisnis saja, akan tetapi keamanan semua individu guna melindungi diri mereka sendiri secara online.

Sebenarnya pembangunan keamanan siber Australia bukanlah yang terbaik didunia. Saat ini Australia berada di posisi ke 9 untuk *packet rate attacks*.[26] Sedangkan untuk vendor kemanan siber, Australia berada pada urutan ke 8 dengan jumlah 15 vendor, jauh tertinggal jika dibandingkan dengan negara yang berada diposisi pertama yakni Amerika Serikat yang memiliki 827 vendor.[27] Akan tetapi, walaupun bukan yang terbaik, Australia tetaplah merupakan negara tujuan kerjasama potensial bagi ASEAN mengingat beberapa hal : pertama, ASEAN merupakan negara tetangga terdekat bagi Australia, sehingga keamanan kawasan ini akan menjadi hirauan yang tinggi bagi negara benua ini. Kedua, walaupun bukan yang terbaik didunia, tetapi pengembangan siber Australia dapat menutupi kekurangan siber ASEAN yang lebih berfokus kepada siber di bidang militer.

[23] Australia's Cyber Security Strategy,p. 51
[24] Cyber Security Sector Competitiveness Plan https://www.avcal.com.au/sb_cache/associationnews/id/244/f/Cyber%20Security%20SCP%20-%20FINAL.pdf diakses pada 26 juni 2017
[25] Australia's Cyber Security Strategy , p. 17
[26] Cyber Security, Threats, Challenges, Opportunities,p. 12
[27] Cyber Security, Threats, Challenges, Opportunities , p. 44

Uraian diatas telah menjelaskan mengenai kelemahan ASEAN yang dimiliki oleh ASEAN dalam bidang pengembangan siber yaitu 1) Belum memiliki rangking dan prioritas kerentanan sektor infrastruktur negara, 2) Dokumen ASEAN mengenai siber masih ambigu, 3) ASEAN tidak berusaha untuk membangun kesadaran masyarakatnya akan ancaman siber, 4). Peningkatan kemampuan penanggulangan siber berfokus pada bidang militer dan 5). Tidak meratanya kemampuan siber negara-negara anggota ASEAN. Penulis melihat bahwa ASEAN bisa mendapatkan keuntungan melalui kerjasama dengan Australia, setidaknya ada tiga poin kelemahan yang dapat diperbaiki dengan bekerjasama. Kelemahan pada poin satu dan dua dapat dengan memanfaatkan keberadaanAustralia Academic Center of Cyber Security Excellence yang memiliki program untuk mempersiapkan generasi muda akan bahaya siber. Pembelajaran pada pusat studi ini akan dapat membantu ASEAN untuk menetapkan skala prioritas sekaitan dengan sektor infrastrukturnya, sehingga langkah pencegahan selanjutnya akan lebih mudah untuk dirumuskan. Dengan memiliki rangking dan prioritas yang telah terpetakan dengan baik, diharapkan ASEAN akan dapat merumuskan dokumen strategi yang lebih praktikal, sehingga mudah untuk diaplikasikan pada saat serangan siber melanda.

Untuk poin kelemahan ASEAN yang keempat dapat dieliminir melalui contoh *priority concern* yang diperlihatkan oleh Australia. Kerjasama siber dengan Australia memberikan peluang bagi ASEAN untuk alih teknologi informasi mengenai cara kerja berbagai Center yang dibuat oleh Australia seperti *Australian Cyber Security Center, Joint Cyber Threat Center, Online Cyber Threat Sharing Portal*. Pada dasarnya ketiga center tersebut bertujuan untuk memperkuat pertahanan siber pada sektor publik khususnya perlindungan terhadap dunia usaha. Studi banding keberbagai center ini akan membantu untuk memperkaya kemampuan ASEAN untuk menyiapkan langkah kongkrit dalam mencegah bahaya serangan siber, khususnya pada sektor publik. Sementara itu, kelemahan pada poin 3 dan 5 bukan tidak mungkin teratasi melaui alih informasi dari negara mitra kerjasama. Akan tetapi sebenarnya permasalahan ini relatif lebih ringan dan dapat diatasi secara internal oleh ASEAN.

Penulis berasumsi bahwa kerjasama dengan mitra wicara Australia akan memberikan keuntungan seperti yang telah dijelaskan diatas, sehingga diharapkan ASEAN akan dapat membangun sistem keamanan siber yang kuat dan lebih baik dimasa yang akan datang.

D. KESIMPULAN DAN REKOMENDASI

ASEAN merupakan sebuah kawasan yang memiliki interaksi dan pengguna internet yang tinggi. ICT merupakan salah satu sektor penting bagi pembangunan dan perkembangan

ASEAN kedepan. Namun, ada beberapa hal mengenai keamanan siber yang perlu diperhatikan oleh ASEAN untuk mendapatkan keuntungan dari dunia maya dibandingkan dengan ancaman siber. Oleh karena itu, berikut beberapa rekomendasi yang diberikan oleh penulis untuk keamanan siber ASEAN kedepannya.

1. ASEAN perlu meningkatkan kemampuan dan kemapanan teknologi ICT dalam rangka pembangunan dan perkembangan kawasan
2. ASEAN perlu memetakan sektor-sektor penting dan rentan akan ancaman siber pada infrasturkturnya.
3. ASEAN perlu meningkatkan keamanan siber tidak hanya pada level militer namun juga pada pemberian kesadaran akan ancaman siber pada masyarakatnya untuk membuat kawasan ASEAN yang lebih aman akan ancaman siber
4. ASEAN perlu membuat dokumen yang lebih komprehensif dan lebih praktis dalam upaya penanggulangan ancaman siber
5. Salah satu upaya yang dalam dilakukan oleh ASEAN untuk meningkatkan keamanan siber adalah dengan melakukan kerjasama dengan mitra wicara ASEAN, salah satunya Australia sebagai negara yang memiliki kapasitas dan kapabilitas siber yang lebih baik

DAFTAR PUSTAKA

Alistair Haskett.2016."Australian Govermenet Releases Its Cyber Security Strategy". Australia:Herbert Smith Freehills

Australia's Cyber Security Strategy https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf diakses pada tanggal 26 juni 2017

Cyber Security Sector Competitiveness Plan https://www.avcal.com.au/sb_cache/associationnews/id/244/f/Cyber%20Security%20SCP%20-%20FINAL.pdf diakses pada 26 juni 2017

Cyber Security, Threats, Challenges, Opportunities. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf diakses pada tanggal 26 juni 2017

European Commission, "Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a
High Level of Network and Information Security across the Union," Commission Stafforking
Document, February 7, 2013

European Parliament Committee on Foreign Affirs, "Draf Report on Cyber Security and Cyber Defence," June 2012, 4.

Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *asia policy*(18), 131-159

Joshua Kurlantzick, "ASEAN's Future and Asian Integration," Council on Foreign Relations, International Institutions and Global Governance Program, Working Paper, November 2012

Lewis, JAmes "Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia," prepared for the Lowy Institute MacArthur Asia Security Project, March 7, 2013

Masyarakat ASEAN, "Kerjasama ASEAN-Australia semkain Meningkat", *Masyarakat ASEAN Edisi 6, 2014*

Perlroth, Scott and Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally", *The New York Times*, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html, 29 Juni 2017

The Straits Times Asia,Cyber attack: Ransomware cases reported in Asia, http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia, 29 Juni 2017