IMPLEMENTASI ASEAN CYBER CAPACITY PROGRAM (ACCP) DALAM MENANGGULANGI KEJAHATAN SIBER DI INDONESIA 2016-2020

Oleh: Ridwan Sofyan
Pembimbing: Irwan Iskandar , S.IP., MA
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya, Jl. H.R. Soebrantas Km 12,5 Simp. Baru, Pekanbaru 28293
Telp/Fax. 0761-63277

ABSTRACT

This research analyzes how the ASEAN Cyber Capacity Program (ACCP) was implemented in tackling cyber crime in Indonesia in 2016-2020. ACCP is a collaboration in increasing the regional cyber capacity of Southeast Asian countries. This regime was initiated by Singapore in October 2016 and in followed by all ASEAN countries by sending several representatives from these countries. In recent years, Indonesia and other ASEAN countries have often received cyber attacks from irresponsible parties. Therefore, this research aims to see how ACCP is implemented in tackling cyber crime.

This research uses qualitative research methods with primary data obtained through interviews, as well as secondary data originating from various existing reading sources such as books, journals, newspapers and others. This research uses a liberalism perspective, nation-state level of analysis and international regime theory.

The results of this research show that Indonesia implements ACCP in several ways, namely, by participating in discussion facilities and sharing information on cyber security issues through the Singapore International Cyber Week (SICW) and the ASEAN Ministerial Conference on Cyber Security (AMCC) to explore deeper issues regarding cyber security in Southeast Asia, then providing training and improving the quality of the national Computer Emergency Response Team (CERT) through the ASEAN-Singapore Cybersecurity Center of Excellence. After five years, ACCP cooperation is still developing and becoming a facility for ASEAN countries to exchange information, and improving cyber security.

***Keywords** : ASEAN Cyber Capacity Program, Cyber Crime, Cyber Security*

PENDAHULUAN

Studi keamanan telah mengalami pergeseran, semenjak awal tahun 1990-an. Definisi "keamanan" di pertanyakan. dan di interpretasikan menjadi beberapa pengertian baru. Dalam pengertian tradisional, "keamanan" hanya mencakup keamanan yang berkaitan dengan negara dan ancaman militer negara lain, namun pengertian yang lebih modern mengenai studi keamanan berfokus kepada aktor non negara dan ancaman non militer[1]

Studi keamanan yang modern tersebut disebut juga *non traditional security* (NTS) isu-isu dalam NTS dilihat sebagai segala bentuk ancaman yang tidak hanya mengancam kedaulatan negara dan teritorialnya, tetapi juga mengancam keamanan Masyarakat, baik kelompok atau individu, salah satunya ialah *cyber crime* yang juga telah menjadi sebuah isu penting dalam kemanan suatu negara, karena dampak *cyber crime* dapat menyerang infrastruktur penting milik negara-negara seperti bank,layanan informasi, bahkan informasi militer suatu negara.[2]

Pada 2016 Kominfo mendapatkan laporan yang ememberitahukan bahwa Situs resmi Bank Indonesia mengalami serangan peretas (hacker). serangan peretas dilakukan dengan model DDOS (Distributed Denial of Service) yang membuat server bank menjadi kacau, bank Indonesia merupakan salah satu infrastruktur penting bagi Indonesia, Hammam selaku Deputi Kepala Bidang Teknologi Informasi Energi dan Material Badan Pengkajian dan Penerapan Teknologi (TIEM BPPT) mengatakan "Infrastuktur kritis itu harus memiliki tingkat keamanan yang tinggi, mampu menahan bahaya, dan bisa segera pulih jika mengalami serangan yang sifatnya merusak". Bahkan, Hammam menilai, penerapan teknologi keamanan siber sudah sangat mendesak.[3]

Melihat Adanya urgensitas untuk melindungi infrastruktur penting negara maka Kerjasama international di bidang keamanan siber harus segera dibentuk dan dilaksanakan karena *cyber crime* merupakan kejahatan non tradisional yang dapat mengancam eksistensi suatu negara. Upaya negara-negara anggota ASEAN untuk mengadopsi kerangka kerjasama yang komprehensif guna mencapai kerjasama keamanan siber. Hingga kini, kerangka keamanan siber ASEAN yang komprehensif belum dapat dikembangkan meskipun telah dilaksanakan berbagai pertemuan resmi oleh ASEAN. Indonesia sendiri, telah meratifikasi Undang-Undang Nomor 5 Tahun 2009 tentang Pengesahan *United Nations Convention Against Transnational Organized Crime*.[4]

The Association of Southeast Asian Nations (ASEAN) adalah sebuah organisasi regional di kawasan Asia Tenggara yang saat ini beranggotakan 10 negara yaitu Indonesia, Malaysia, Singapura, Filipina, Thailand, Brunei Darussalam, Kamboja, Myanmar, Laos, dan Vietnam[5]

---

[1] Agus Trihartono,2020, *keamanan dan sekuritasi dalam hubungan internasional*,melvana publishing: Batam

[2] Ibid

[3] KOMINFO. *Kenali 4 Jenis Kejahatan Siber* (2022, February 1).

[4] Peraturan Pemerintah Nomor 5 Tahun 2009 tentang Pengesahan United Nations Convention Againts Transnational Organized Crime

[5] SetnasASEAN (2021). *Daftar Negara-negara*

-

Organisasi ini berdiri pada tahun 1967 di Bangkok atas gagasan dari Indonesia, Malaysia, Singapura, Filipina, dan Thailand. Tujuan awal dari didirikannya ASEAN adalah sebagai wadah untuk berdialog dan bekerja sama antara negara-negara di kawasan yang tujuannya untuk meningkatkan kerja sama di bidang ekonomi, sosial, budaya, dan pendidikan, sekaligus untuk peningkatan perdamaian regional melalui prinsip keadilan dan peraturan hukum yang merujuk pada prinsip UN Charter. Seiring dengan semakin matangnya ASEAN sebagai sebuah organisasi regional, kerja sama yang dilakukan ASEAN juga berkembang[6]

Berkembangnya teknologi setiap tahunnya, menyebabkan aksi kejahatan *cyber crime* semakin meluas di berbagai negara ASEAN, hal ini menimbulkan kekhawatiran di berbegai pihak, sehingga pada 13 september 2003 pada saat *Telecommunications and IT Ministers Meeting* (TELMI) yang ke 3 di laksanakan di singapura menyatakan bahwa *cyber security* adalah sebuah hal yang benar-benar ada dan tidak dapat diabaikan begitu saja, kesimpulan dari pertemuan ini adalah setiap negara anggota ASEAN wajib membentuk *Computer Emergency Response Team* (CERT)[7], walaupun kebijakan ASEAN ini mewajibkan setiap negara anggota harus memiliki CERT pada tahun 2005, namun pada kenyataannya kebijakan ini baru terwujudkan di tahun 2012 ketika seluruh negara anggota sudah memiliki CERT mereka masing-masing.[8]

Untuk mempertahankan dunia maya dan berbagai infrastruktur teknologi informasi mereka dari *cyber crime*, negara anggota ASEAN membuat sebuah kebijakan yaitu *ASEAN Cyber Capacity Program* (ACCP) yang di inisiasi oleh Singapura pada tahun 2016, area fokus di bawah program ini mencakup kebijakan siber, undang-undang, pengembangan strategi, serta respons terhadap insiden *cyber crime*.[9]

KERANGKA TEORI

1. Perspektif Liberalisme

Perspektif yang digunakan dalam penelitian ini adalah perspektif liberalisme, liberalisme adalah salah satu dari beberapa perspektif yang berkembang dalam studi hubungan internasional. Perspektif liberalisme telah membawa dampak yang mendalam terhadap bentuk masyarakat industrial modern, Di era dimana globalisasi ekonomi semakin meningkat dan meluas, perspektif liberalis tetap menjadi salah satu perspektif dominan dalam percaturan politik global.

Kaum liberalis memfokuskan perhatiannya pada fungsi hukum dan peran institusi internasional, dengan tesis yang mengatakan hukum dan institusi internasional mendorong penyesuaian dankerjasama internasional (regulatory liberalism thesis). Institusi

ASEAN Beserta Sejarah Singkat, 25 februari 2021

[6] ASEAN (1967). *The Asean Declaration (Bangkok Declaration) Bangkok,* 8 August 1967

[7] ASEAN (2003). *Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime* (AMMTC), Singapura.

[8] ASEAN (2003). *Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime* (AMMTC), Singapura

[9] Prime Minister Office Singapore (2016) *Prime Minister Lee Hsien Loong delivered this speech at the inaugural Singapore International Cyber Week on 10 October 2016*.

internasional dapat berupa organisasi-organisasi internasional formal yang mewakili negara-negara, tetapi juga aturan-aturan resmi, kesepakatan-kesepakatan, dan konvensi-konvensi yang memfasilitasi interaksi antar negara.[10]

2. Teori Rezim Internasional

Teori efektivitas rezim dikemukakan oleh Arild Underdal berpendapat bahwa "sebuah rezim dapat dianggap efektif dapat dilihat dari sejauh mana ia berhasil menjalankan serangkaian fungsi tertentu atau memecahkan masalah yang memotivasi pembentukannya. Dalam menganalisis keefektifitasan suatu rezim, Underdal mengembangkan tiga variabel yang meliputi: 1) Variabel terikat (*dependent variable*), 2) Variabel bebas (*independent variable*), dan 3) Variabel intervensi (*intervening variable*).[11]

Pada variabel terikat, menurut Underdal, rezim dapat dikatakan efektif apabila suatu organisasi atau negara berhasil melakukan fungsi tertentu atau menyelesaikan permasalahan yang menjadi motif penyelenggaraannya. Underdal , melakukan pemilahan antara efektivitas rezim dengan variabel dependen yang terdiri dari keluaran (output), hasil (outcome), dan dampak (impact) yang ada dalam rezim. Output adalah kondisi yang dilihat dari sebelum dan sesudah rezim atau peraturan yang dikeluarkan oleh rezim baik secara tertulis maupun tidak tertulis seperti konvensi, treaty, deklarasi, atau norma-norma, Bagian ini dimaksudkan untuk memandu perilaku aktor utama, dalam hal ini negara. Kemudian, outcome adalah produk rezim yang menyebabkan perubahan perilaku anggotanya karena implementasi rezim. Kemudian, impact, yaitu dampak dan pengaruh yang muncul dari diimplementasikannya sebuah rezim dalam memenuhi kebutuhannya di bawah pengaruh rezim.[12]

Selanjutnya, dalam variabel bebas terbagi menjadi dua tipe variabel, yaitu tipe masalah (problem malignancy) atau disebut problem types dan kapasitas penyelesaian masalah (problem-solving capacity). Pada *problem malignancy* merupakan kerumitan dan kegawatan masalah yang terdiri dari tiga karakter, yaitu ketidaksepahaman (*incongruity)*, adanya kepentingan nasional (*asymmetry*), dan perbedaan yang terakumulasi (*cumulative cleavages*). Efektivitas suatu rezim dapat diuji berdasarkan dari kerumitan dan kegawatan suatu masalah yang sedang dihadapi. Jika masalah tersebut memiliki kerumitan atau kegawatan yang tinggi, maka tingkat keefektivitasan rezim akan semakin kecil dan berdampak kepada sulitnya melakukan kerja sama atau penyelesaian masalah.[13]

Underdal berpendapat bahwa kerumitan atau permasalahan dapat diatasi dengan *problem-solving capacity* apabila terdapat setting kelembagaan

[10] Lamy, S., Baylis, J., Smith, S., and Owens, P. (2012). *Introduction to Global Politics, second edition*. New York: Oxford University Press.

[11] Underdal Arlid (2001) "*Environmental Regime Effectiveness: Confronting Theory with Evidence"* The MIT Press Cambridge, Massachusetts London England

[12] Ibid

[13] Underdal, Arild. 2002 "*One Question, Two Answers". Cambridge: MIT Press.*Hlm 6

yang ada dalam rezim, kemudian ditangani oleh lembaga atau sistem dengan power yang terdistribusi dengan baik, serta didukung oleh keahlian atau skills dan energi yang memadai. Terakhir, terdapat juga variabel intervensi (*intervening variable*), sebuah variabel yang merupakan akibat dari variabel-variabel independen, tetapi juga bagian dari variabel yang berpengaruh terhadap variabel dependen. Variabel intervensi di sini menggunakan *level of collaboration*, atau tingkat kolaborasi antara anggota dari sebuah rezim. Untuk mengukur tingkat kolaborasi dapat menggunakan *six-point ordinal scale*.[14]

3. Level Analisis Negara

Level analisa penelitian ini adalah negara (state-level analysis). Dimana ketika melihat pada upaya ASEAN dalam memberikan kebijakan mengenai *cyber crime* dipengaruhi oleh negara-negara yang bergabung didalamnya. Menurut Rourke[15], pada level analisis ini, penjelasan tentang perilaku negara ditentukan oleh faktor-faktor internal dari negara tersebut, yang diperlukan ketika seorang peneliti menggunakan level analisis negara adalah pemahaman tentang bagaimana berbagai aktor (birokrat, kelompok kepentingan dan badan legislatif) di dalam negara berperan dalam pengambilan kebijakan luar negeri. Tingkat analisis negara akan menghasilkan penjelasan yang tidak terlalu makro seperti yang dihasilkan pada tingkat analisis sistem, namun tidak pula terlalu mikro seperti ketika menggunakan level analisis individu.

HASIL DAN PEMBAHASAN

1. Pembentukan Kerjasama Regional *ASEAN Cyber Capacity Program*

Pembentukan ACCP pada tahun 2016 menjadi salah satu terobosan baru negara-negara ASEAN dalam mengatasi *cybercrime*, yang mana sebelumya forum diskusi ASEAN mengenai masalah *cyber* cukup terbatas, Kerjasama ini di inisiasi oleh Singapura dengan mengeluarkan dana sebesar 10 juta dollar yang bertujuan untuk membiayai sumber-sumber daya, keahlian (*expertise*), dan pemberian pelatihan untuk memperkuat kemampuan negara-negara ASEAN di bidang *cyber*. Selain itu, ACCP juga memberi saran mengenai prosedur pembentukan badan siber nasional dan penyusunan peraturan di bidang siber.[16]

Serangan yang terjadi tidak hanya pada sektor pemerintahan akan tetapi juga terjadi di sektor keuangan dan yang di incar oleh serangan ini bukan hanya pemerintahan saja akan tetapi masyarakat juga menjadi target dengan adanya beberapa website palsu yang mengaku sebagai website resmi dari pemerintahan dan kepolisian singapura, oleh karena itu pada 2015 pemerintah singapura mendirikan *Computer Service Agency* (CSA), dalam menangani perkembangan kasus *Cyber Crime* CSA dinilai oleh pemerintah singapura telah melaksankan kinerja dengan cukup baik, CSA juga telah menyusun strategi keamanan siber nasional yang mana strategi ini memiliki 4 komponen utama

[14] Ibid

[15] Rourke, J. T., *International Politics on the World Stage*, 5th ed., (Connecticut: Dushking Publishing Group, 1995).

[16] *Asean Cyber Capacity Program* Cybil Portal di akses 20 februari 2024

yang nantinya akan diterapkan dalam *ASEAN cyber capacity program.*[17]

Pertama adalah dengan melakukan peningkatan keamanan siber pada fasilitas negara yang penting, yang kedua dengan bekerjasama dengan para pengusaha dan masyarakat dalam menjaga keamanan siber serta mensosialisasikan bahwa keamanan *cyber* bukan hanya masalah pemerintah akan tetapi juga merupakan masalah bagi mereka, seperti perusahaan yang membutuhkan keamanan dalam menyimpan data keuangan mereka, dan untuk masyarakat agar lebih berhati-hati dengan website yang mencurigakan karena bisa saja didalam website tersebut ada malware yang jika di klik nantinya bisa merusak perangkat si pengguna dan bahkan bisa berpindah ke perangkat lain, kemudian peningkatan sumber daya manusia yang memiliki pengetahuan *cyber security*, karena di bandingkan negara-negara besar lain, ASEAN masih ketinggalan dalam hal *cyber security*, peningkatan sumber daya manusia dapat dilakukan dengan pemberian pendidikan kepada para programmer untuk menjadi profesional dalam hal *cyber security* dengan cara meningkatkan serta memiliki fasilitas universitas yang memadai dimana para siswa bisa melakukan pertahanan melawan serangan siber, yang terakhir ialah mengadakan kerjasama dengan negara-negara lain untuk melawan *cyber crime* karena penyerang siber tidak menghormati yurisdiksi. Serangan dapat datang dari mana saja di dunia serta Alamat IP yang digunakan oleh penyerang mungkin bukan penyerang utama yang sebenarnya, oleh karena itu bekerja sama dengan pemerintah negara lain akan sangat membantu dalam berbagi informasi antar intelijen, bekerja sama untuk memblokir serangan, menutup jaringan, dan saling belajar praktik baik.[18]

2. Urgensitas Indonesia Bergabung dengan *ASEAN Cyber Capacity Program*

Masifnya kerugian yang diakibatkan oleh serangan siber dan kurangnya pengetahuan negara dan perusahaan membuat berbagai pihak merasa perlunya ada kerjasama yang dapat menjadikan iklim perdagangan di kawasan Asia Tenggara menjadi aman dari serangan peretas. Saat ini masing-masing negara yang ada di kawasan Asia Tenggara dan organisasi internasional khususnya organisasi pemerintah internasional seperti ASEAN bersama-sama mencari solusi dari permasalahan cybersecurity. untuk menanggulangi berbagai masalah tersebut, ASEAN mulai menginisiasi program yang bernama ASEAN Cyber Capacity Program (ACCP).[19]

Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman-ancaman dan serangan siber yang terjadi serta menjelaskan posisi ketahanan siber Indonesia saat ini, sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki

[17] katherine_chen. PMO | PM Lee Hsien Loong at the Singapore International Cyber Week Opening Ceremony. from website: https://www.pmo.gov.sg/Newsroom/pm-lee-hsien-loong-singapore-international-cyber-week

[18] CSA Singapore | Information for Security & IT Professionals. From Default website: https://www.csa.gov.sg/information-for/security-it-pofessionals diakses 20 februari 2024

[19] Ibid

kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber, dengan Indonesia berpartisipasi dalam ACCP membuka berbagai informasi baru dan kebijakan baru dalam Menyusun stratetegi keamanan siber yang bertujuan untuk memperkuat Indonesia dalam persiapan serta pemulihan pada saat serangan siber terjadi.

Bagi Indonesia kerjasama regional di bidang keamanan siber merupakan suatu hal yang baru, biasanya perundingan antar negara-negara ASEAN mengenai kejahatan siber dilakukan dalam forum AMMTC, yang mana forum ini juga membahas tentang kejahtatan-kejahatan transnasional lainnya sehingga pembahasan mengenai isu *cyber crime* tidak terlalu dalam, namun dengan adanya ACCP dapat memperluas ruang diskusi serta kerjasama negara-negara ASEAN dalam menanggulangi kejahatan siber.[20]

Indonesia sendiri melihat keamanan siber hampir sama seperti Singapura, terutama dalam sebuah kasus kejahatan siber yang melibatkan dua negara hendaknya setiap negara dapat menunjuk sebuah instansi pemerintah untuk dijadikan *point of contact* di bidang keamanan siber. Daftar *point of contact* merupakan hal yang sangat esensial untuk memudahkan komunikasi dan koordinasi antar negara, khususnya apabila terdapat insiden yang melibatkan 2 negara ASEAN atau lebih yang perlu segera mendapatkan penanganan. Kemudian Indonesia juga melihat bahwa mekanisme pertukaran pengetahuan antar negara-negara ASEAN sangat penting, sehingga harus segera dikembangkan dengan cara semua negara anggota mulai mengimplementasikan latihan bersama di bidang teknologi informasi dan komunikasi.[21]

3. Implementasi *ASEAN Cyber Capacity Program* oleh Indonesia tahun 2016-2020

Singapore International Cyber Week (SICW)

Semenjak Indonesia bergabung dengan ACCP pada 2016 indonesia langsung ikut serta dalam pertemuan pertama *Singapore international cyber week* (SICW), SICW merupakan sebuah forum diskusi untuk membahas mengenai masalah kejahatan siber serta peningkatan keamanan siber di negara-negara ASEAN, pada waktu itu Indonesia di wakilkan oleh menkopolhukam Wiranto, beliau berbicara pada forum tersebut bahwa Indonesia merupakan salah satu negara di Asia yang memiliki pengguna internet cukup tinggi dimana pengguna internet pada 2016 mencapai 132,7 juta penduduk menggunakan internet artinya, 65 persen penduduk di Indonesia mengakses internet dan hampir semuanya merupakan pengguna setia media sosial seperti *facebook* dan *twitter*, dengan melihat angka ini tentunya indonesia menjadi salah satu

[20] KOMINFO *Menkopolhulkam ajak seluruh negara kolaborasi jadi mitra dalam keamanan siber* https://polkam.go.id/menko-polhukam-ajak-seluruh-negara-kolaborasi-dan-jadi-mitra-dalam-keamanan-cyber/

[21] Factsheeton Asean Cyber Capacity Program https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-

target pasar *e-commerce* yang terbesar di Asia Tenggara.[22]

Selain pembentukan departemen khusus, dalam SICW Indonesia juga melihat beberapa negara mempunyai undang-undang khusus yang mengatur tentang privasi pengguna digital, sementara indonesia pada saat itu hanya memiliki UU ITE 2008 tentang transaksi elektornik, kemudian indonesia melihat pentingnya memiliki undang-undang khusus yang mana digunakan untuk mengatur privasi keamananan data pengguna, UU ITE 2008 dinilai kurang efektif untuk mengatur keaman privasi pengguna internet, oleh karena itu pada tahun 2016 dibentuk undang-undang baru untuk mengamankan privasi pengguna.[23]

ASEAN Ministerial Conference on Cyber Security (AMCC)

Untuk membangun sebuah kapasitas siber suatu negara ACCP juga melaksanakan *Asean ministrial Conference on cyber security* (AMCC) di dalam program SICW untuk membantu mewujudkan tujuan tersebut, di dalam AMMC negara-negara ASEAN berdiskusi dan merencanakan program kegiatan siber untuk memperkuat kerentanan regional dalam menghadapi insiden siber, program ini selalu dilakukan setiap tahunnya dan juga merupakan rangkaian acara SICW.

AMCC menindaklanjuti arahan yang diberikan oleh para Pemimpin ASEAN pada KTT ASEAN ke-32 pada bulan April 2018, khususnya untuk lebih mengoordinasikan upaya keamanan siber ASEAN di antara berbagai platform tiga pilar ASEAN. AMCC sepakat bahwa diperlukan mekanisme keamanan siber ASEAN yang formal untuk mempertimbangkan dan memutuskan isu-isu diplomasi siber, kebijakan, dan operasional yang saling terkait. Direkomendasikan agar mekanisme yang diusulkan harus fleksibel dan juga mempertimbangkan berbagai dimensi, termasuk pertimbangan ekonomi.[24]

AMCC dihadiri oleh para Menteri dan Pejabat Senior yang bertanggung jawab atas Keamanan Siber dan Teknologi Informasi dan Komunikasi (TIK) dari 10 Negara Anggota ASEAN, termasuk Sekretaris Jenderal ASEAN Dato Lim Jock Hoi. AMCC itu sendiri Implementasi ACCP memberikan pengaruh besar bagi perkembangan kemanan siber di indonesia, semenjak pertama kali bergabung pada 2016 indonesia telah mengalami perubahan terhadap penetapan hukum di bidang siber, kemudian indonesia juga telah membuat sebuah badan khusus (BSSN) untuk meningkatkan perkembangan teknologi siber serta mempertahankan Indonesia dari ancaman serangan siber.

terbagi dalam 2 sesi pertemuan, dimana sesi pertama dikhususkan bagi negara anggota ASEAN. Sedangkan sesi kedua diperuntukkan bagi negara

[22] Industry.co.id. *132,7 Juta Pengguna Internet Indonesia Didominasi Anak Muda*. from Industry.co.id website: https://www.industry.co.id/read/18784/1327-juta-pengguna-internet-indonesia-didominasi-anak-muda di akses 18 maret 2024

[23] Ahmad, H. *IR-PERPUSTAKAAN UNIVERSITAS AIRLANGGA*.https://repository.unair.ac.id/102829/4/4.%20BAB%20I%20PENDAHULUAN.pdf di akses 4 april

[24] Chelsa_Cher *PMO | SM Teo Chee Hean at the 4th Singapore Internationa*l cyber week website: https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-4th-Singapore-International-Cyber-Week

anggota ASEAN ditambah dengan negara-negara mitra dialog.[25]

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)

ACCP juga merencanakan untuk membentuk fasilitas pendidikan cyber yang berspusat di Singapura, *ASEAN Singapore Cybersecurity Centre of Excellence* (ASCCE) akan berfungsi sebagai melakukan pelatihan dan penelitian, melatih CERT nasional di ASEAN, dan meningkatkan pertukaran informasi antar CERT nasional, Proyek ini akan didanai oleh anggaran sebesar SGD30 juta selama lima tahun (2019-2023).[26]

Peluncuran *ASEAN Singapore Cybersecurity Centre of Excellence* (ASCCE) untuk membangun ruang siber yang lebih aman dan tangguh melalui program peningkatan kapasitas siber bagi pejabat senior kebijakan dan teknis ASEAN. ASCCE akan melibatkan para pakar dan pelatih siber terkemuka serta berkolaborasi dengan Negara-negara Anggota ASEAN, Mitra Dialog ASEAN, dan mitra internasional lainnya dalam merancang dan melaksanakan program peningkatan kapasitas keamanan siber. Fasilitas pelatihan ASCCE akan berlokasi di pusat kota singapura mulai April 2020, sedangkan Fasilitas *Cyber Range* di Politeknik Temasek akan beroperasi penuh mulai Oktober 2019.[27]

Berkat pelatihan insiden siber serta peningkatan kualitas CERT , Indonesia juga sudah memulai untuk membuat sebuah tim untuk mengatasi insiden siber yang terjadi di organisasi pemerintahan serta perangkat daerah yang disebut dengan GOV-CSIRT, walaupun pada saat ini masih terbatas pada pemerintahan provinsi akan tetapi kedepannya Indonesia memiliki rencana untuk mengembangkan program ini hingga ke tingkat kota.[28]

SIMPULAN

ASEAN Cyber Capacity Progam (ACCP) merupakan kerjasama regional yang terbentuk atas dasar kebutuhan bersama negara-negara anggota ASEAN dalam pertahanan keamanan siber di Asia Tenggra yang di inisiasi oleh Singapura, ACCP dibentuk dengan tujuan utama membangun kapasitas siber di Negara-negara anggota ASEAN, kemudian meningkatkan kemampuan regional untuk merespons ancaman siber yang terus berkembang dan membangun ruang siber ASEAN yang aman dan tangguh.

Rezim ACCP merupakan rezim yang efektif dinilai menggunakan konsep efektivitas rezim dari Arild Underdal. Dinilai dari *independent variabel* beserta indikator yang ada dalam variabel tersebut yakni *problem of coordination*, *symmetry* dan *cross-cutting clevages*, ACCP merupakan rezim yang mampu mempertemukan anggotanya untuk berkoordinasi serta mengambil tindakan untuk menghadapi permasalahan atau isu yang dihadapi, Pada variabel tersebut juga ACCP juga

[25] CSA *AMCC 2019*.from Default website: https://www.csa.gov.sg/NewsEvents/speeches/2019/Asean-Ministerial-Conference-on-Cybersecurity-2019

[26] CSA. (2019). ASEAN-Singapore Cybersecurity Centre of Excellence. Retrieved from website: https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence

[27] Ibid

[28] BSSN. *Gov-CSIRT Indonesia* | www.bssn.go.id.from https://www.bssn.go.id/gov-csirt/

dinilai efektif karena berhasil mempertemukan anggotanya dengan kepentingan yang sama dalam menghadapi isu atau permasalahan keamanan siber. Selain koordinasi dan juga kepentingan anggota rezim yang sama, dalam pengimplementasian ACCP, negara anggotanya juga dapat berdiskusi bersama dalam menghadapi permasalahan serta memberikan solusi bersama.

Selanjutnya rezim ACCP dinilai dari variabel *problem solving capacity* dengan indikator *institutional setting*, *distribution of power* dan *skill* serta *energy*, rezim ACCP merupakan rezim yang mampu menjadi fasilitator, dan juga pengawas dalam pertamuan – pertemuan yang dilakukan oleh anggotanya guna untuk memastikan negara anggotanya dalam pengimplementasian ACCP berjalan sesuai kenginginan rezim atau tidak. Dan dalam hal menangani permasalahan keamnan siber negara anggota rezim dinilai telah menjalankan aturan dan juga prinsip yang ada dalam ACCP dan dengan pengawasan ACCP sebagai rezim

Keberadaan ACCP juga meningkatkan pengalaman kerjasama Indonesia di bidang keamanan siber, sehingga jika nantinya indonesia akan melakukan kerjasama bilateral maupun regional dengan negara-negara di luar Asia Tenggara indonesia sudah memiliki informasi serta pengalaman di bidang kerjasama siber, dengan adanya pengalaman tersebut indonesia akan semakin disegani dalam kerjasama di bidang siber lainnya.

Peningkatakan kapasitas siber dan *cyber security* indonesia pasca implementasi ACCP 2016-2020 terus meningkat dan semakin kuat, hal ini dibuktikan dengan skor indeks keamanan siber indonesia yang terus meningkat setiap tahunnya dalam GCI, perkembangan pelatihan tim insiden siber oleh ASCCE terhadap tim respon insiden indonesia yang dilatih langsung melalui interpol, membuat BSSN semakin tanggap dalam menghadapi insiden siber.

Daftar Pustaka

Agus Trihartono,2020, *keamanan dan sekuritasi dalam hubungan internasional,*melvana publishing: Batam

Asean Cyber Capacity Program Cybil Portal di akses 20 februari 2024

ASEAN (1967). *The Asean Declaration (Bangkok Declaration) Bangkok*, 8 August 1967

ASEAN (2003). *Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime* (AMMTC), Singapura.

ASEAN (2003). *Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime* (AMMTC), Singapura

Ahmad, H. *IR-PERPUSTAKAAN UNIVERSITAS AIRLANGGA*.https://repository.unair.ac.id/102829/4/4.%20BAB%20I%20PENDAHULUAN.pdf di akses 4 april

BSSN. *Gov-CSIRT Indonesia* | www.bssn.go.id.from https://www.bssn.go.id/gov-csirt/

CSA Singapore | Information for Security & IT Professionals. From Default website: https://www.csa.gov.sg/information-

for/security-it-pofessionals diakses 20 februari 2024

CSA *AMCC 2019*.from Default website: https://www.csa.gov.sg/NewsEvents/speeches/2019/Asean-Ministerial-Conference-on-Cybersecurity- 2019

CSA. (2019). ASEAN-Singapore Cybersecurity Centre of Excellence. Retrieved from website: https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence

Chelsa_Cher *PMO | SM Teo Chee Hean at the 4th Singapore Internationa*l cyber website:https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-4th-Singapore-International-Cyber-Week

Industry.co.id. *132,7 Juta Pengguna Internet Indonesia Didominasi Anak Muda*. from Industry.co.id website: https://www.industry.co.id/read/18784/1327-juta-pengguna-internet-indonesia-didominasi-anak-muda di akses 18 maret 2024

katherine_chen. PMO | PM Lee Hsien Loong at the Singapore International Cyber Week Opening Ceremony. from website: https://www.pmo.gov.sg/Newsroom/pm-lee-hsien-loong-singapore-international-cyber-week

KOMINFO. *Kenali 4 Jenis Kejahatan Siber* (2022, February 1).

KOMINFO *Menkopolhulkam ajak seluruh negara kolaborasi jadi mitra dalam keamanan siber* https://polkam.go.id/menko-polhukam-ajak-seluruh-negara-kolaborasi-dan-jadi-mitra-dalam-keamanan-cyber/

Lamy, S., Baylis, J., Smith, S., and Owens, P. (2012). *Introduction to Global Politics, second edition*. New York: Oxford University Press.

Prime Minister Office Singapore (2016) *Prime Minister Lee Hsien Loong delivered this speech at the inaugural Singapore International Cyber Week on 10 October 2016*.

Peraturan Pemerintah Nomor 5 Tahun 2009 tentang Pengesahan United Nations Convention Againts Transnational Organized Crime

Rourke, J. T., *International Politics on the World Stage*, 5th ed., (Connecticut: Dushking Publishing Group, 1995).

SetnasASEAN (2021). *Daftar Negara-negara ASEAN Beserta Sejarah Singkat,* 25 februari 2021

Underdal Arlid (2001) "*Environmental Regime Effectiveness: Confronting Theory with Evidence"* The MIT Press Cambridge, Massachusetts London England

Underdal, Arild. 2002 "*One Question, Two Answers". Cambridge: MIT Press.*Hlm 6