Journal of Social and Economics Research

Volume 6, Issue 1, June 2024

P-ISSN: 2715-6117 E-ISSN: 2715-6966

Open Access at: https://idm.or.id/JSER/index.php/JSER

ANALYSIS OF THE IMPLEMENTATION OF THE "ASEAN CYBER SECURITY FRAMEWORK" IN SINGAPORE IN 2020

ANALISIS PENGIMPLEMENTASIAN "ASEAN CYBER SECURITY FRAMEWORK" DI SINGAPURA TAHUN 2020

Angel Aurelia[1], Andini Egista Maheswari S.[2]

[1,2] Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Udayana

E-mail: aurelia.2212521044@student.unud.ac.id[1], andini1305@gmail.com[2]

ARTICLE INFO

Correspondent

Angel Aurelia
aurelia.2212521044@student.unud.ac.id

Key words:

Security, Non-Traditional, ASEAN, Cybersecurity.

Website:
https://idm.or.id/JSER/index.php/JSER

Page: 2168 - 2179

ABSTRACT

This research examines the development of the implementation of the ASEAN Cyber Security Framework from 2017-2020 in Singapore in the year 2020. By applying Contemporary Security Theory and Government Policy Theory, the author analyzes that cybercrime is included in security issues and the implementation of the ASEAN Cyber Security Framework in 2020. The author uses a descriptive qualitative method through the analysis of secondary data from journals, news articles, and official reports from Singapore. This research reveals that Singapore has strengthened its position in enhancing cooperation and coordination in the field of cybersecurity through various initiatives, such as Singapore's Safer Cyberspace Masterplan 2020, and by collaborating with cybersecurity firms. The findings of this study also show that Singapore has achieved the highest ranking in the Global Cybersecurity Index and has enhanced its national capabilities in facing cyber threats. Therefore, Singapore has become a model for the implementation of the ASEAN Cyber Security Framework and has made a significant contribution to the development of a more effective cybersecurity framework in the ASEAN region.

INFO ARTIKEL

Koresponden
Angel Aurelia
aurelia.2212521044@student.unud.ac.id

Kata kunci*:*
Keamanan, Non-Tradisional, ASEAN, Keamanan Siber.

Website:
https://idm.or.id/JSER/index.php/JSER

Hal: 2168 - 2179

ABSTRAK

Penelitian ini mengkaji perkembangan implementasi ASEAN *Cyber Security Framework* 2017-2020 di Singapura pada tahun 2020. Dengan menerapkan *teori Contemporary Securities* dan teori Kebijakan Pemerintah, penulis menganalisa bahwa kejahatan siber termasuk dalam permasalahan keamanan dan pengimplementasian ASEAN *Cyber Security Framework* di tahun 2020. Penulis menggunakan metode kualitatif deskriptif melalui analisis data sekunder dari jurnal, berita, dan laporan resmi Singapura. Penelitian ini mengungkap bahwa Singapura telah memperkuat posisinya dalam meningkatkan kerjasama dan koordinasi di bidang keamanan siber melalui berbagai inisiatif seperti *Singapore's Safer Cyberspace Masterplan* 2020 dan berkolaborasi dengan firma siber sekuritas. Temuan penelitian ini juga menunjukkan bahwa Singapura berhasil mencapai peringkat tertinggi dalam *Global Cybersecurity Index* dan meningkatkan kemampuan nasionalnya dalam menghadapi ancaman siber. Oleh karena itu, Singapura telah menjadi teladan dalam penerapan ASEAN *Cyber Security Framework* dan berkontribusi signifikan terhadap pengembangan kerangka keamanan siber yang lebih efektif di kawasan ASEAN.

PENDAHULUAN

Pada tahun 1960an, proses deindustrialisasi dimulai di banyak negara Barat. Sebaliknya, globalisasi menyebabkan munculnya pusat-pusat industri baru seperti Jepang, Taiwan, dan kemudian Tiongkok, yang berbasis pada ekspor barang konsumsi ke negara-negara maju. Setelah tahun 1945, kemunculan teknologi nuklir, biologi molekuler, fisika partikel, serta ilmu- ilmu lainnya menjadi latar belakang lahirnya berbagai teknologi saat ini, termasuk internet. Tak lupa bidang sejarah ilmu pengetahuan juga mencapai titik balik yang besar mulai tahun tersebut. Perkembangan dan penguasaan teknologi tidak hanya berdampak pada konsep sosial masyarakat, namun juga sifat ancaman yang lebih modern dan kompleks yang ada di ranah maya terhadap pertahanan dan keamanan negara. Ancaman dunia maya global kini lebih berbahaya, terorganisir, dan canggih dibandingkan sebelumnya. Sebab, semakin meningkatnya ketergantungan negara terhadap teknologi informasi dan komunikasi berbanding lurus dengan potensi risiko dan ancaman yang dihadapi. Saat ini, negara-negara maju memandang dunia maya sebagai kawasan strategis yang perlu dikelola dengan baik karena ancaman dunia maya dapat mempengaruhi situasi perekonomian, sistem pertahanan, dan keamanan nasional suatu negara.

Ancaman global perang siber ini memerlukan perhatian yang lebih besar dari negara- negara di seluruh dunia karena mengatasi ancaman dunia maya tidak akan efektif tanpa kerja sama internasional yang kuat. Memang benar bahwa negara-negara ASEAN sendiri sudah mulai menyadari potensi bahaya dari ancaman dunia maya, dan isu ini telah menjadi agenda utama dalam beberapa Forum Regional ASEAN (ARF), bahkan pada tahun 2015 ARF sudah mencakup sebuah rencana. Forum Regional Keamanan Teknologi Informasi dan Komunikasi dan Pemanfaatan Teknologi Informasi dan Komunikasi Daerah. Topik-topik yang dibahas dalam agenda ARF biasanya terbatas pada penanggulangan kejahatan siber dan terorisme siber, tanpa menyebutkan kerja sama untuk memerangi ancaman perang siber. Keamanan data pribadi telah menjadi perhatian utama bagi negara-negara anggota ASEAN, karena terdapat indikasi bahwa ASEAN telah menjadi target utama aktivitas kejahatan dunia maya. Urgensi peran ASEAN dalam keamanan data pribadi juga terkait dengan potensi ASEAN dalam ekonomi digital pada tahun 2025 yang akan melebihi APBN sebesar $1 triliun, seiring dengan perkembangan layanan digital seperti keuangan dan jasa keuangan yang diperkirakan akan mencapai peningkatan dalam sektor komersial terus berlanjut (A.T. Kearney, 2018).

Faktanya, ASEAN mempunyai potensi untuk menambah modal terhadap PDB hingga satu dekade dalam ekonomi digital. Namun, jika hanya sedikit negara anggota yang dapat mencapai tujuan ini, maka mereka tidak akan dapat menanggung risiko yang diakibatkannya. Memang, sebagai organisasi regional, ASEAN dapat berperan sebagai penyalur dalam upaya meningkatkan pengetahuan dan keterampilan negara-negara yang tertinggal. Untuk mendukung ambisi ekonomi dan digital ASEAN, strategi 2021-2025 bertujuan untuk membangun tatanan ruang siber multilateral berbasis aturan yang terbuka, aman, stabil, dapat diakses, dapat dioperasikan, dan damai. Hal ini akan dibangun melalui penerapan norma-norma perilaku negara yang bertanggung jawab secara sukarela dan tidak mengikat, langkah-langkah membangun kepercayaan, dan peningkatan kapasitas kolaboratif melalui peningkatan kerja sama di dalam ASEAN dan dengan mitra dialog ASEAN. Tahun 2016 merupakan tahun yang penting bagi topik keamanan siber. Tahun ini, Singapura memimpin kawasan ini dalam menjadi tuan rumah Konferensi Tingkat Menteri Keamanan Siber (*Cybersecurity Ministerial Conference*/AMCC), yang merupakan platform informal pertama yang didedikasikan untuk diskusi keamanan siber. Hingga saat ini, isu keamanan siber telah dibahas di berbagai platform regional untuk kerja sama keamanan ekonomi. Kelompok Kerja Ahli Keamanan Siber (CS EWG) ASEAN *Defense Ministers Meeting Plus* (ADMM-Plus) juga dibentuk pada tahun 2016, diikuti dengan pembentukan Pertemuan Interim Keamanan Forum Regional ASEAN (ARF). Pada tahun 2017, kami berupaya menggunakan ICTs (ISM *on* ICTs *Security*) untuk memisahkan masalah keamanan siber dari ARF. Pertemuan antarsesi ini berfokus pada pemberantasan terorisme dan kejahatan transnasional. Pada bulan Oktober 2019, AMCC ke-4 mendukung pembentukan Komite Koordinasi Keamanan Siber ASEAN (Cyber-CC). Komite ini menyatukan perwakilan dari badan-badan keamanan siber sebagai badan formal untuk mengoordinasikan upaya keamanan siber dan mendorong koherensi kebijakan regional. Penciptaan berbagai platform yang berfokus pada keamanan siber merupakan suatu perkembangan yang disambut baik, tidak hanya mencakup aspek teknis, tetapi juga mencakup aspek diplomatik, politik, dan militer yang merupakan bagian integral dari isu-isu multi-

keamanan siber dan disiplin ilmu. Hal ini membuka jalan bagi koordinasi yang lebih mendalam dalam upaya keamanan siber ASEAN. Ini disebut CIIP (Perlindungan Infrastruktur Informasi Kritis).

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kualitatif di mana kajian literatur menjadi pokok penting dalam penelitian ini. Penelitian kualitatif dipilih karena pendekatan ini memungkinkan untuk menggali pemahaman yang mendalam tentang fenomena yang diteliti. Penelitian kualitatif berfokus pada makna, pandangan, dan pengalaman subjek, serta konteks di mana fenomena tersebut terjadi (Creswell, 2014). Pendekatan ini sangat sesuai untuk mengkaji isu-isu kompleks yang tidak bisa diukur dengan metode kuantitatif, serta memungkinkan peneliti untuk menggali data secara lebih rinci dan kontekstual.

Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah deskriptif kualitatif. Pendekatan deskriptif bertujuan untuk memberikan gambaran secara sistematis mengenai fenomena atau masalah yang diteliti, tanpa berusaha untuk menguji hipotesis atau membuat prediksi (Miles & Huberman, 1994). Dalam penelitian ini, pendekatan deskriptif digunakan untuk menggambarkan data yang diperoleh dari sumber sekunder, seperti berita, jurnal ilmiah, dan dokumenter, serta untuk memahami konteks dan makna dari data tersebut. Pendekatan ini memungkinkan peneliti untuk menyajikan data secara mendetail dan menyeluruh, sehingga dapat memberikan pemahaman yang lebih komprehensif tentang fenomena yang diteliti.

Data dan Jenis Data

Data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder adalah data yang telah dikumpulkan oleh pihak lain dan bukan oleh peneliti sendiri (Creswell, 2014). Penggunaan data sekunder dalam penelitian ini meliputi berbagai sumber yang relevan, yaitu:

1. Berita: Artikel-artikel berita yang relevan dengan topik penelitian diambil dari berbagai media massa. Berita sebagai sumber data dapat memberikan informasi terkini dan pandangan dari berbagai perspektif mengenai topik yang diteliti.
2. Jurnal: Artikel-artikel ilmiah yang dipublikasikan dalam jurnal-jurnal akademik terkait dengan topik penelitian. Jurnal ilmiah menyediakan data yang berbasis penelitian dan kajian ilmiah yang terpercaya.
3. Laporan: Laporan yang berasal dari organisasi pemerintahan Singapura mengenai kondisi keamanan siber di Singapura.

HASIL DAN PEMBAHASAN

Pada tahun 2020, lanskap keamanan siber global dipenuhi dengan aktivitas siber berbahaya seperti *phishing* dan *ransomware* yang sebagian besar disebabkan karena *lockdown*. Namun, pada akhir tahun 2020, dunia lebih terkejut lagi dengan berita pelanggaran rantai pasokan yang membuat ribuan bisnis dan perusahaan di seluruh dunia rentan terhadap serangan. Sorotan ancaman siber membahas dua masalah keamanan siber penting pada tahun 2020 yakni dampak siber dari pandemi COVID-19 dan serangan rantai pasokan SolarWinds (*Cyber Security Agency of Singapore*, 2020). Sepanjang tahun 2020, pelaku ancaman memanfaatkan serangkaian peristiwa penting terkait COVID-19 untuk melakukan aktivitas

mengancam di jaringan mereka. Di Singapura, pengamatan terhadap ancaman siber terkait COVID-19, seperti *phishing* dan *ransomware*, secara umum sejalan dengan tren global dan bertepatan dengan peningkatan kebijakan anti-korupsi untuk menerapkan kebijakan bekerja dari rumah, seiring dengan penerapan teknologi baru yang diterapkan oleh individu dan dunia usaha keberlangsungan bisnis. Dengan meningkatnya ketergantungan pada infrastruktur digital dan besarnya minat masyarakat terhadap pengembangan dan distribusi vaksin, pelaku ancaman kemungkinan akan terus menyesuaikan taktiknya untuk mengimbangi pandemi yang semakin berkembang.

Dari Desember 2019 hingga Maret 2020, kasus pertama seseorang yang terinfeksi virus ini dilaporkan di Singapura dan WHO menyatakan COVID-19 sebagai pandemi. Sejak saat itu, kinerja di semua bidang kehidupan mengalami penurunan, khususnya sektor medis yang terus terkena dampak dari munculnya pasien virus corona. Dari bulan Maret hingga Mei 2020, lebih dari sepertiga umat manusia dikurung dalam kurungan kecil yang disebut *lockdown*, dan Singapura mulai menerapkan *Singapore's Circuit Breaker*. Pada masa *lockdown*, Singapura juga menghadapi beberapa serangan siber seperti peningkatan kebocoran data dan kredensial. Spionase dunia maya yang melakukan penelitian juga semakin intensif. Pada bulan Juni dan Juli 2020, jumlah orang yang terinfeksi di seluruh dunia mencapai 10 juta orang. Pada tahap ini, sektor teknologi mulai terkena dampak karena karyawan dan pengguna online terus-menerus menjadi sasaran rekayasa sosial. Lalu, terjadi serangan spionase dunia maya dan *ransomware* menargetkan pusat-pusat penelitian vaksin, regulator, dan saluran distribusi vaksin. Hal ini membuat pihak berwenang memperingatkan adanya peningkatan kejahatan dunia maya terkait vaksin (*Cyber Security Agency of Singapore*, 2020).

Akselerasi digital juga telah memungkinkan penjahat dunia maya untuk mengambil keuntungan dari berbagai bidang seperti penipuan *Business E-mail Compromise* (BEC) dan pelanggaran keamanan melalui perangkat *Internet-of-Things* (loT) yang semakin banyak mengambil keuntungan dari korban mereka. Sementara itu, meski ketakutan dan kecemasan seputar virus corona masih ada, dunia maya dapat menjadi sarang konflik dan provokasi. Digitalisasi telah mempercepat dan memperkuat penyebaran berita palsu dan misinformasi yang disengaja, sehingga memperkuat ketegangan dan prasangka yang ada. Dunia maya dapat menjadi titik awal serangan dan ancaman kriminal yang kompleks terhadap dunia fisik. Lebih buruk lagi, upaya global untuk mengembangkan vaksin yang efektif melawan penyakit virus corona baru (COVID-19) memungkinkan penyerang dunia maya untuk meliput setiap detail informasi vaksin, termasuk penelitian, produksi, regulasi, dan distribusi. Secara global, pada tahun 2020 terjadi lonjakan kampanye *phishing* yang menggunakan referensi terkait pandemi dan meniru otoritas kesehatan terkait. Aktivitas jahat ini paling umum terjadi antara bulan Maret dan Mei 2020. Sekitar 1.500 URL berbahaya diamati dan jumlah ini lebih dari dua kali lipat dibandingkan kuartal sebelumnya. Peningkatan ini kemungkinan besar disebabkan oleh upaya peretas untuk menipu bisnis dan layanan yang banyak diminati selama pemadaman listrik di Singapura, seperti ritel online dan portal pembayaran. Tren ini mereda pada bulan Juli 2020, ketika penjahat dunia maya mengubah taktik mereka untuk memanfaatkan kepentingan publik dalam peristiwa dan perkembangan penting. Aktivitas siber tersebut lebih berbahaya karena menargetkan entitas publik atas nama "*colleague*".

Pada awal tahun 2020, seorang pegawai Dewan Hukum menerima email yang meminta transfer mendesak lebih dari $1 juta dari akun email rekannya ke rekening bank yang tidak dikenal. Permintaan mencurigakan ini mengejutkan petugas polisi yang melaporkan email tersebut karena dia merasa tidak mengirimkan uangnya. Investigasi mengungkapkan bahwa penjahat dunia maya telah mengakses akun "*colleague*" melalui email *phishing* dan mengirimkan total enam email ke karyawan lain dalam upaya mengelabui mereka agar mentransfer uang ke rekening bank mereka. Tindakan lebih lanjut kejadian ini telah dilaporkan ke SPF. Setelah akun email yang disusupi ditemukan, kredensialnya disetel ulang dan akses peretas ditolak. Sebagai tindakan pencegahan, semua staf Dewan Hukum telah disarankan untuk mengubah rincian *login* akun email mereka dan pemberitahuan telah dikeluarkan untuk memperingatkan staf tentang penipuan *phishing*.

Mengingat tantangan-tantangan ini, Singapura berupaya memperkuat ketahanan sektor infrastruktur informasi penting mereka. CSA memberikan pengawasan intensif dan terpusat terhadap kemampuan keamanan siber nasional untuk melindungi Singapura dalam dua bidang:

1) Memperkuat ketahanan sektor CIL Singapura;
2) Menjaga kewaspadaan dan kesiapsiagaan untuk merespons insiden dunia maya secara efektif.

Pada tahun 2019, CSA dan Koalisi Ketahanan Global Asia-Pasifik meluncurkan Pusat Pembagian dan Analisis Informasi Teknologi Operasional (OT-ISAC). OT-ISAC adalah platform yang membantu organisasi di sektor CII berbagi intelijen ancaman siber. Hal ini memungkinkan dunia usaha untuk merespons ancaman siber dengan lebih cepat dan pulih dari insiden siber dengan lebih mudah. Namun, ancaman terhadap jaringan teknologi operasional tetap tinggi pada tahun 2020 karena pelaku ancaman berupaya mengganggu layanan penting dan proses industri. OT-ISAC menyaksikan perkembangan yang mengkhawatirkan dalam lingkungan ancaman siber teknologi operasional dengan semakin canggihnya penyerang. Pada tahun 2020 terdapat beberapa insiden besar yang menyebabkan sistem teknologi operasional menjadi sasaran serangan siber. Hal ini biasanya disebabkan oleh tiga alasan:

1) Peningkatan konvergensi teknologi operasional dan informatika
2) Penyerang ransomware yang menargetkan aset teknologi operasional, dan
3) Peningkatan penemuan kerentanan teknologi operasional yang kritis.

Sama seperti para penyerang yang bekerja sama untuk melakukan serangan siber, dunia usaha juga dapat membentuk kolaborasi dan kemitraan lintas sektor untuk mendeteksi serangan serupa dan mendapatkan informasi tentang ancaman siber untuk dapat melindungi jaringan mereka secara lebih efektif. Organisasi juga harus mengadopsi praktik terbaik industri untuk melindungi diri dari meningkatnya ancaman *ransomware* dan serangan yang ditargetkan. Praktik-praktik ini mencakup penerapan segmentasi antara jaringan TI dan OT, penerapan solusi antivirus, dan memastikan bahwa risiko yang terkait dengan kerentanan sistem dan perangkat lunak dapat dimitigasi. Jika memungkinkan, data sensitif yang penting juga harus dienkripsi, dicadangkan secara teratur, dan disimpan secara offline. Yang terakhir, upaya yang dilakukan perusahaan untuk meningkatkan kesadaran akan keamanan siber di kalangan pekerjanya, seperti memberikan peringatan tentang ancaman terbaru dan melatih karyawan untuk mengenali tanda-tanda phishing dan aktivitas siber berbahaya lainnya, perlu diperkuat.

MINDEF/SAF dan pusat penelitian keamanan siber iTrust bersama-sama menjadi tuan rumah *Critical Infrastructure Security Showdown* (CISS) ke-4 di Singapore University of Technology (SUTD) dari tanggal 27 Juli hingga 7 Agustus 2020. Latihan ini pertama kali dilakukan secara online mengingat adanya pembatasan COVID-19 dan diikuti oleh 146 peserta dari seluruh dunia, dari akademisi, sektor publik dan swasta. MINDEF/SAF telah mengembangkan keahlian mendalam dalam pertahanan siber OT dan menyadari pentingnya memahami kerentanan baru seiring dengan berkembangnya vektor serangan potensial. Seiring dengan terus berkembangnya CISS, MINDEF/SAF berkolaborasi dengan mitra di industri dan akademisi untuk mengatur dan berpartisipasi dalam kegiatan sembari berkontribusi pada ekosistem keamanan siber regional dan melindungi keamanan nasional dari ancaman siber sekaligus memberikan pertahanan siber.

Pada tahun 2020, jumlah perusakan situs web lokal menurun meskipun terjadi peristiwa penting seperti *Singapore's General Election* (GE 2020) dan *US Presidential Election.* Faktanya, dari Juli hingga Oktober 2020, terdapat lebih dari 320 juta total interaksi Facebook (reaksi, komentar, dan share) terkait dengan dua kandidat pada pemilu presiden AS 2020 (Biden dan Trump), sementara rata-rata bisnis di AS hanya menerima 1.100 tampilan halaman per bulan. Peristiwa politik besar pada tahun 2020, seperti GE 2020 dan pemilihan presiden AS yang disebutkan di atas sering kali memicu aktivitas peretasan tetapi tidak ada tren perusakan situs web ".sg". Infrastruktur TI yang aman dan andal sangat penting untuk keberhasilan pelaksanaan GE 2020. Adanya pembatasan sosial, solusi dan proses tambahan perlu dikembangkan untuk memfasilitasi proses pemilu. Salah satu contohnya adalah penggunaan aplikasi seluler VoteQ untuk mengatasi kepadatan yang berlebihan di tempat pemungutan suara. Secara umum, CSA belum melihat adanya peningkatan signifikan dalam aktivitas siber berbahaya, seperti *phishing* atau perusakan situs web, sebelum atau setelah periode GE tahun 2020. Namun, untuk memastikan kelancaran GE 2020, CSA bekerja sama dengan Kementerian Komunikasi dan Informasi (MCI), GovTech, Kementerian Dalam Negeri (MHA), dan Departemen Pemilihan Umum (ELD) untuk mengembangkan pencegahan dan respons masalah potensi ancaman dunia maya.

Diluncurkan pada tahun 2016, Strategi Keamanan Siber Singapura menetapkan visi, tujuan, dan prioritas negara tersebut untuk ruang siber yang tangguh dan tepercaya. Tujuannya adalah untuk mendorong partisipasi seluruh pejabat pemerintah, penyedia layanan penting, industri keamanan siber, individu dan mitra internasional melalui empat pilar utama:

PILAR 1: Membangun Ketangguhan Infrastruktur.
Terdapat beberapa inisiatif yang dilakukan Singapura di tahun 2020 seperti bekerja sama dengan GovTech, Kementerian Kesehatan, dan lembaga lainnya untuk memastikan keamanan siber layanan elektronik Pemerintah seperti *Singpass and Corppass,* layanan elektronik yang menggunakan *Cloud Komersial*, dan teknologi COVID-19 seperti *Trace Together*. Selain itu, Singapura juga mengawasi keamanan siber Jenderal Singapura Pemilu 2020 dan memberitahu partai politik serta kandidat mengenai potensi ancaman dunia maya yang dapat mengganggu pemilu juga termasuk salah satu agendanya. Hal ini sejalan dengan fokus utama ASEAN *Cybersecurity Framework* 2017-2020 yaitu *Incident Response*, *Cyber Policy*, *Governance*,

and *Legislation*, dan kooperasi dengan berbagai pihak agar dapat melindungi ruang sibernya.

PILAR 2: Menciptakan Ruang Siber yang Lebih Aman
Terdapat beberapa inisiatif yang dilakukan Singapura di tahun 2020 seperti meluncurkan *Singapore's Safer Cyberspace Masterplan* untuk menciptakan ruang siber yang lebih aman dan terjamin, meluncurkan *Cybersecurity Labelling Scheme* yang pertama untuk meningkatkan keamanan loT pada perangkat pintar. Hal ini sejalan dengan fokus utama ASEAN *Cybersecurity Framework* 2017-2020 yaitu *Incident Response* dan *Confidence Building*.

PILAR 3: Mengembangkan Ekosistem Keamanan Siber yang Aktif
Terdapat beberapa inisiatif yang dilakukan Singapura di tahun 2020 mengambil alih program *National Cybersecurity Research & Development* (NCR) untuk mengkoordinasikan proses penelitian dan pengembangan serta inovasi keamanan siber Singapura, meluncurkan inisiatif SG *Cyber Talent* yang bertujuan untuk menjangkau 20.000 individu selama tiga tahun, dan meluncurkan SG *Cyber Educators* pada *Singapore Cybersecurity Education Symposium* yang pertama. Hal ini sejalan dengan fokus utama ASEAN *Cybersecurity Framework* 2017-2020 yaitu *Incident Response Capacity Building* dan *Awareness Building*.

PILAR 4: Memperkuat Kemitraan Internasional
Terdapat beberapa inisiatif yang dilakukan Singapura di tahun 2020 seperti menyelenggarakan SICW kelima tahun 2020 dalam keadaan hibrid yang dihadiri lebih dari 6.000 peserta dari 60 negara, berkolaborasi dengan PBB untuk mengembangkan daftar periksa penerapan norma-norma keamanan siber. Hal ini sejalan dengan fokus utama ASEAN *Cybersecurity Framework* 2017-2020 yaitu *Confidence Building, International Collaboration, Cyber Policy,* dan *Measures and Norms.*

Implementasi Teori

1. **Implementasi Konsep Keamanan Non-Tradisional**
   Konsep keamanan non-tradisional menyatakan bahwa negara saat ini tidak berfokus pada keamanan militer saja namun terdapat ancaman-ancaman lain yang bersifat non-militer dan dapat mengancam kedaulatan sebuah negara seperti keamanan siber. Setelah dunia internasional melihat serangan cyber internasional pada tahun 2000-an, masalah keamanan cyber telah mendapat perhatian lebih dari komunitas keamanan. Di beberapa negara tertentu, masalah keamanan cyber telah diangkat ke tingkat politik tinggi dan menjadi sorotan utama dalam agenda keamanan nasional (Putra & Punzalan, 2013). Singapura juga telah melihat keamanan siber sebagai sebuah ancaman untuk negaranya. Hal ini dapat dilihat dari beberapa inisiatif Singapura yang terus meningkatkan kapasitas teknologinya agar keamanan data masyarakat dapat diamankan. Semasa Covid-19, Singapura lebih memfokuskan inisiatifnya pada kerjasama dan pembuatan kebijakan efektif untuk mengatasi ancaman siber yang masif pada Covid-19. Inisiatif seperti ini menekankan bahwa Singapura percaya pada konsep keamanan non-tradisional. Kebijakan keamanan siber telah dirumuskan dengan maksud untuk mempertahankan integritas sistem informasi dan jaringan komunikasi negara, sementara badan-badan keamanan siber nasional dalam berbagai bentuknya telah dibentuk untuk melembagakan kebijakan-kebijakan ini (Putra & Punzalan, 2013). Sebagian besar doktrin keamanan siber ini diartikulasikan dalam bahasa norma-norma keamanan tradisional yang

menekankan pada keamanan dan kedaulatan negara. Penulis sadar bahwa Singapura telah menganggap ancaman siber sebagai keamanan non-tradisional sebelum Covid-19 dan lebih memfokuskan diri pada kebijakan dan inisiatif seperti *Singapore's Safer Cyberspace Masterplan* karena ancaman yang lebih banyak pada masa Covid-19.

2. **Implementasi Teori Kebijakan**
   Kebijakan adalah tindakan yang dan keputusan pemerintah dengan maksud tertentu guna mengatasi suatu permasalahan. Kebijakan yang terlahir selalu mempunyai tujuan untuk diterapkan pada kelompok atau negara dimana kebijakan tersebut dikembangkan. Situmorang (2016) menjelaskan bahwa implementasi kebijakan merupakan salah satu tahapan kebijakan publik, dan juga merupakan variabel terpenting yang sangat mempengaruhi keberhasilan kebijakan yang berkaitan dengan penyelesaian permasalahan publik. Sejak munculnya COVID-19 yang meningkatkan kejahatan siber, beberapa negara menginisiasikan beberapa kebijakan untuk melindungi kedaulatan negaranya dalam dunia siber. Dalam hal ini Singapura, sebagai salah satu negara anggota ASEAN, juga berupaya memperbaiki kebijakannya sebelum COVID-19 dengan kondisi negaranya semasa COVID. Banyaknya permasalahan di bidang keamanan siber yang merugikan negara, membuat Singapura mencoba mengimplementasikan kebijakan tersebut ke lingkup domestiknya. Melalui empat pilar utama dari strategi keamanan siber Singapura yang lahir di tahun 2016, membuat negara ini lambat laun dapat memperbaiki kondisi negaranya pasca COVID-19 dengan berbagai upaya yang dilakukannya. Terbukti bahwa teori kebijakan dan implementasiannya relevan dengan kondisi Singapura semasa COVID-19, terutama perihal penanganan ancaman keamanan siber.

Menggunakan Model Analisis Kebijakan Segitiga (*Policy Analysis Triangle Model*) oleh Walt dan Gilson, kita dapat menganalisis implementasi Singapura terhadap "ASEAN *Cyber Security Framework*" pada tahun 2020 dengan memperhatikan empat aspek utama: konteks, konten, proses, dan aktor.

a. **Konteks**
   Lanskap keamanan siber global pada tahun 2020 sangat dipengaruhi oleh pandemi COVID-19, yang menyebabkan peningkatan serangan siber seperti phishing dan ransomware. Di Singapura, situasi ini diperparah oleh lockdown yang mengharuskan banyak aktivitas beralih ke online, meningkatkan ketergantungan pada infrastruktur digital. Pandemi juga mempercepat adopsi teknologi baru yang, meskipun membantu dalam menjaga kontinuitas bisnis, juga membuka celah baru bagi pelaku ancaman untuk mengeksploitasi. Tantangan ini menciptakan kebutuhan mendesak bagi Singapura untuk memperkuat ketahanan sibernya, terutama di sektor infrastruktur informasi kritis (CII).

b. **Konten**
   Isi dari pengimplementasian ASEAN *Cyber Security Framework* mencakup berbagai inisiatif seperti respons insiden, kebijakan dan legislasi siber, serta kerja sama internasional. Singapura telah merespons ini dengan meluncurkan beberapa inisiatif domestik seperti Strategi Keamanan Siber yang mencakup empat pilar utama: membangun ketangguhan infrastruktur, menciptakan ruang siber yang lebih aman, mengembangkan ekosistem keamanan siber yang aktif,

dan memperkuat kemitraan internasional. Inisiatif-inisiatif ini selaras dengan fokus ASEAN dalam meningkatkan kapasitas respons insiden dan membangun kepercayaan di antara negara anggota.

c. **Proses**
Proses implementasi kebijakan di Singapura melibatkan langkah-langkah strategis untuk mengintegrasikan kerangka kerja ASEAN ke dalam kebijakan nasional. Misalnya, peluncuran *Masterplan Cyberspace* yang lebih aman dan Skema Pelabelan Keamanan Siber menunjukkan upaya proaktif Singapura dalam merespons ancaman siber yang meningkat selama pandemi. Selain itu, kegiatan seperti *Critical Infrastructure Security Showdown* dan keterlibatan aktif dalam kolaborasi internasional melalui SICW (*Singapore International Cyber Week*) menunjukkan pendekatan berkelanjutan Singapura dalam memperkuat kesiapan siber.

d. **Aktor**
Aktor yang terlibat dalam implementasi kebijakan ini mencakup berbagai pihak, mulai dari pemerintah seperti *Cyber Security Agency of Singapore* (CSA), sektor swasta, lembaga akademis, hingga organisasi internasional. CSA memainkan peran kunci dalam mengkoordinasikan upaya nasional dan memfasilitasi kerjasama lintas sektor. Kemitraan dengan perusahaan teknologi, serta inisiatif seperti OT-ISAC (*Operational Technology Information Sharing and Analysis Center*), memungkinkan berbagi intelijen ancaman yang lebih efektif, menunjukkan pentingnya kolaborasi dalam menghadapi ancaman siber yang kompleks.

Dengan mengaitkan teori Model Analisis Kebijakan Segitiga ini, kita dapat melihat bagaimana Singapura tidak hanya merespons secara reaktif terhadap tantangan siber yang muncul akibat pandemi, tetapi juga secara proaktif memperkuat ketahanan nasionalnya melalui berbagai kebijakan dan inisiatif yang sejalan dengan kerangka kerja ASEAN. Analisis ini menunjukkan bahwa keberhasilan implementasi kebijakan tidak hanya ditentukan oleh isi kebijakan itu sendiri, tetapi juga oleh konteks, proses, dan aktor yang terlibat dalam keseluruhan ekosistem kebijakan.

SIMPULAN

Ancaman dunia maya global kini menjadi lebih berbahaya, lebih terorganisir, dan lebih canggih dibandingkan sebelumnya. Hal ini disebabkan oleh semakin meningkatnya ketergantungan negara terhadap teknologi informasi dan komunikasi berbanding lurus dengan potensi risiko dan ancaman yang dihadapi. Ancaman global siber memerlukan peningkatan perhatian dari negara-negara di seluruh dunia karena tanpa kerja sama internasional yang kuat, upaya melawan ancaman siber tidak akan efektif. Memang benar bahwa negara-negara ASEAN sendiri mulai menyadari potensi bahaya dari ancaman siber, dan isu tersebut telah menjadi topik utama diskusi di beberapa Forum Regional ASEAN (ARF) yang pada tahun 2015 sudah mencakup rencana-rencananya. Hal ini akan dicapai melalui penerapan norma- norma perilaku negara yang bertanggung jawab secara sukarela dan tidak mengikat, langkah- langkah membangun kepercayaan, dan peningkatan kapasitas kerja sama melalui peningkatan kerja sama di dalam ASEAN dan dengan mitra dialog ASEAN. Tahun 2016 merupakan tahun besar bagi keamanan siber. Tahun ini, Singapura memimpin kawasan ini dalam menjadi tuan rumah

Konferensi Tingkat Menteri Keamanan Siber (*Cybersecurity Ministerial Conference*/AMCC), yang merupakan platform informal pertama yang membahas keamanan siber.

Dari penjelasan yang sudah dipaparkan, penulis tertarik untuk membahas lebih lanjut mengenai upaya Singapura mengimplementasikan *ASEAN Cyber Security Framework* yang kami batasi di tahun 2020. Penelitian ini diharapkan mampu memberikan manfaat baik di segi akademis maupun praktis serta bertujuan untuk mengetahui keberhasilan pemerintah Singapura dalam pengimplementasian ACCT terutama bidang siber pada masa COVID-19. Penulis menggunakan 4 studi literatur untuk mendukung penulisan penelitian ini. Adapun teori yang digunakan antara lain, teori keamanan nasional dalam konteks isu global kontemporer pada perspektif hubungan internasional dan teori kebijakan yang diteruskan dengan keberadaan kebijakan yang diimplementasikan. Penelitian ini menggunakan jenis penelitian kualitatif dengan pendekatan deskriptif kualitatif dan data yang digunakan dalam penelitian ini adalah data sekunder. Metode pengumpulan data dalam penelitian ini adalah dokumentasi dan metode analisis data yang digunakan adalah analisis deskriptif.

Pandemi virus corona (COVID-19) telah mengubah situasi di banyak negara di dunia secara drastis. Singapura, salah satu negara anggota ASEAN, sudah merasakan dampak negatif. virus ini dengan meningkatnya kejahatan keamanan siber di negaranya. Para pelaku kejahatan memanfaatkan situasi pandemi ini untuk melakukan aktivitas kriminal dan mendapatkan keuntungan sebanyak-banyaknya. Sejak kasus pertama dilaporkan di Singapura pada akhir tahun 2019, ancaman dunia maya telah muncul, dimulai dengan peningkatan pelanggaran data dan kredensial. Hal serupa juga terjadi pada bulan-bulan berikutnya. Namun, mengingat situasi yang tidak sesuai, Singapura mengambil tindakan segera untuk memperkuat ketahanan sektor infrastruktur informasi yang penting. Melalui empat pilar utama Strategi Keamanan Siber Singapura, yang diluncurkan pada tahun 2016, berbagai inisiatif diambil untuk membantu negara ini secara bertahap meningkatkan status nasionalnya pasca COVID-19. Hal ini juga sesuai dengan implementasi teori yang diusung penulis yakni konsep keamanan non-tradisional dan teori kebijakan. Kedua implementasi teori tersebut berhasil membuktikan bahwa keduanya relevan untuk mengkaji topik yang dibahas.

DAFTAR PUSTAKA

Andhika, L. R. (2019). Pemodelan Kebijakan Publik: Tinjauan dan Analisis Untuk Risalah Kebijakan Pemerintah. Jurnal Riset Pembangunan, 2(1), 22-35.

Anthony, M. C. (2016). An Introduction to Non-Traditional Security Studies: A Transnational Approach. Nanyang Technological University.

Anthony, M. C., & Alistair, D. B. C. (2013). Non-Traditional Security in Asia: Issues, Challenges, and Framework for Action. Institute of Southeast Asian Studies.

Cyber Security Agency of Singapore. (2021). Singapore Cyber Landscape 2020 (Pp. 1–33). Cyber Security Agency of Singapore.

Muadi, S., Ismail, M. H., & Ahmad, S. (2016). Konsep dan Kajian Teori Perumusan Kebijakan Publik. JRP (Jurnal Review Politik), 6(2): 195-224.

Permatasari, I. A. (2020). Kebijakan Publik (Teori, Analisis, Implementasi dan Evaluasi Kebijakan). The journalish: Social and Government, 1(1): 33-37.

Rizki, A. M. (2018). Langkah Singapura Dalam Meningkatkan Kesadaran Negara Anggota Asean Untuk Meningkatan Keamanan Siber. SENASPOLHI (Seminar Nasional Ilmu Politik dan Hubungan Internasional), 1: 178-188.

Setiyawan, A. (2020) Penguatan Kerjasama Cyber Defense Asean Guna Menghadapi Ancaman Cyberwar. Jurnal Pertahanan Universitas Gadjah Mada, 322-332.

Tampubolon, T., & Ramadhan, R. (2020). Asean Personal Data Protection (Pdp): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara. Padjadjaran Journal of International Relations, 1(3): 270.

Tay, K. L. (2023). Asean Cyber-Security Cooperation: Towards a Regional Emergency-Response Framework. The International Institute for Strategic Studies. https://www.iiss.org/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/