Jurnal Kajian Ilmiah
e-ISSN: 2597-792X, ISSN: 1410-9794
Vol. 21 No. 2 (Mei 2021), Halaman: 171 – 184
Terakreditasi Peringkat 5 (SINTA 5) sesuai SK RISTEKDIKTI Nomor. 3/E/KPT/2019

Three Perspective Theory of Cyber Sovereignty dalam Strategi Keamanan Siber Singapura

Muawwan [1,*]

[1] Fakultas Falsafah dan Peradaban; Universitas Paramadina; Jl. Gatot Subroto No. 97, Telp. (021) 79181190; e-mail: muawwan@students.paramadina.ac.id

* Korespondensi: e-mail: muawwan@students.paramadina.ac.id

Submitted: **05/04/2021**; Revised: **12/05/2021**; Accepted: **11/05/2021**; Published: **27/05/2021**

Abstract

The escalation of cyber threats in Singapore has prompted the country to intensify its cyberspace security protection. Singapore then implemented numerous strategies by collaborating across agencies and actors to obtain a protective cyberspace security system. This research aimed at figuring out Singapore Cyber Security Strategy (SCSS) *documents comprehensively throughout textual analysis based on qualitative approach of an emerging-dominant elements in documents such as actor, instrument, politic, economy, research, and collaboration which were cooperated within actors. The author also fulfilled this analysis using qualitative approach to measure the data relation and the big picture of SCSS documents. Finally, the author found that Singapore's strategy in applications and infrasctructure aspects, the government intervened them intensively. Singapore, one of the highest technological expertise countries in Southeast Asia, was fuflnerable getting the threats or attacks. So, this country was regulating an excellent cyber system and infrastructure to proctect their cyber management system secure. Meanwhile, Singapore's policy in core aspects was a transfer due to the fact that Singapore was multi-ethnical and multi-culturalism country. Thus, Singapore's strategy for ideological aspects was not regulated significantly in SCSS documents.*

Keywords*: Cyber Security Strategy, Data Relation, Sovereignty*

Abstrak

Eskalasi ancaman terhadap ruang siber yang terjadi di Singapura telah mendorong negara tersebut untuk meningkatkan proteksi keamanan ruang sibernya. Singapura kemudian menerapkan berbagai strategi dengan cara menjalin kerjasama lintas instansi dan aktor untuk memperoleh sistem keamanan ruang siber yang lebih protektif. Tulisan ini bermaksud untuk memahami dokumen *Singapore Cyber Security Strategy* (SCSS) secara komprehensif dengan melakukan analisis kontekstual berdasarkan pendekatan kualitatif terhadap sejumlah unsur yang dominan muncul di dalam dokumen seperti aktor, instrument, politik, ekonomi, penelitian, dan kolaborasi yang dibangun di antara para aktor. Penulis juga melengkapi analisis ini dengan pendekatan kuantitatif untuk mengukur relasi data dan kecenderungan yang tergambar dari dokumen SCSS tersebut. Hasilnya, penulis menemukan bahwa pada level strategi di sektor application dan infrastruktur, pemerintah Singapura memiliki intervensi penuh dalam mengatur seluruh aktivitas di kedua aspek tersebut. Sebagai salah satu negara yang cukup signifikan di dalam pengelolaan teknologinya di kawasan Asia Tenggara, maka Singapura secara eksklusif berupaya membangun sistem dan infrastruktur siber yang mumpuni untuk melindungi tata kelola ruang siber mereka dari berbagai ancaman. Berbeda pada aspek core yang bersifat lebih terbuka (transfer) lantaran banyak dipengaruhi oleh multietnis dan multikulturalisme. Sehingga proteksi terhadap hal-hal yang bersifat ideologis tidak banyak diatur di dalam dokumen SCSS.

Kata kunci: Kedaulatan, Relasi Data, Strategi Keamanan Siber

1. Pendahuluan

Teknologi yang semakin canggih telah mengubah pola interaksi manusia dan negara. Indikator paling mudah tentu bisa dilihat dari peralihan model interaksi konvensional menuju digital yang menghendaki keterlibatan infrastruktur siber. Konsekuensinya, daya tahan ruang siber menjadi elemen penting untuk diperhatikan di dalam aktivitas kehidupan yang serba digital. Sebab bila tidak, hal ini dapat melahirkan gangguan tidak saja pada aspek perangkat siber suatu negara, tetapi juga berpotensi mengancam kedaulatannya. Pada titik inilah, strategi untuk meningkatkan keamanan ruang siber menemukan relevansinya.

Di level Asia Tenggara, Singapura termasuk negara yang cukup concern dalam keamanan siber. Predikat itu bisa dilihat dari catatan strategi siber Singapura yang terangkum di dalam dokumen *Singapore's Cyber Security Strategy* (SCSS). Melalui dokumen tersebut, Singapura menyiapkan aturan sekaligus sejumlah pendekatan demi terciptanya keamanan dan kelancaran lalu lintas lintas di ruang siber. Singapura merupakan salah satu negara di Asia Tenggara yang dikategorikan sebagai negara dengan posisi pertama pada keamanan siber dibandingkan dengan negara lainnya yang ada di dunia berdasarkan Global Security Index yang dirilis oleh International Telecommunications Union di tahun 2017. Sehingga, kondisi tersebut memungkinkan Singapura menjadi negara yang terdepan juga di kawasan sekitarnya dalam hal keamanan siber (International Telecommunication Union, 2017).

Keberadaan ruang siber dengan segala karakteristiknya memunculkan perhatian pada keamanan di ruang siber (Hughes et al., 2017). SCSS menyatakan bahwa Singapura memiliki keinginan dalam pembangunan kapasitas pada keamanan siber yang melibatkan berbagai pihak untuk menjadi mitranya. Pembangunan kapasitas dengan melibatkan negara lain menjadi kepentingan yang perlu dicapai terutama karena tidak terlepas dari ancaman siber yang tidak mengenal batas negara.

2. Metode Penelitian

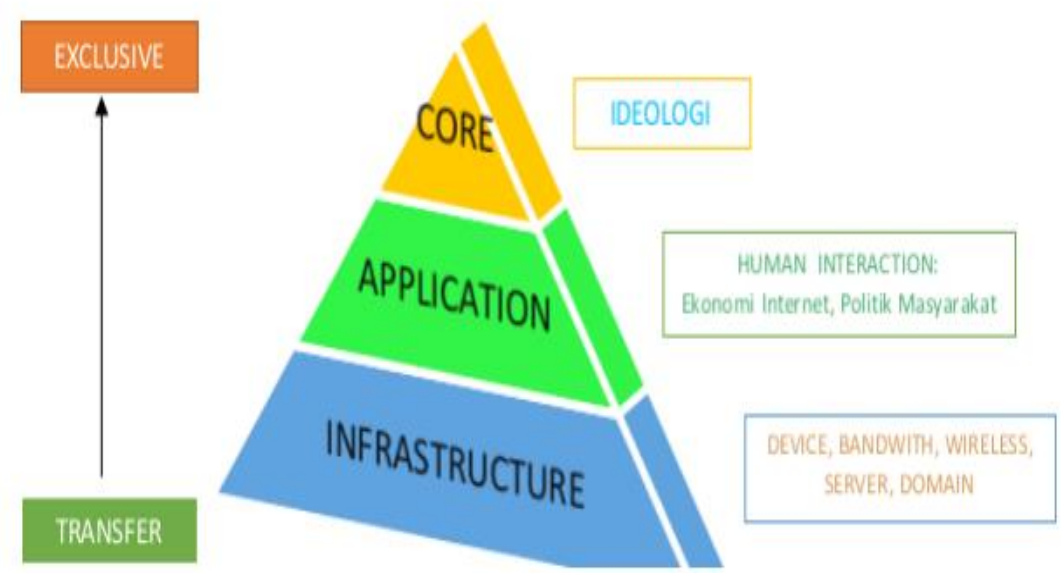
Melalui pendekatan *mix method*, penulis bertujuan untuk memperoleh gambaran besar tentang strategi kemanan siber Singapura dilihat dari sudut pandang teori kedaulatan. penulis mulai menganalisis secara kontekstual dokumen SCSS dengan menggunakan perangkat MAXQDA. Langkah pertama yang dilakukan adalah mempreteli frasa *cybersecurity strategy* melalui fitur MaxDictio kemudian *Interactive World Tree* yang menggambarkan cabang-cabang dari pohon besar bernama *cybersecurity strategy*. Cabang-cabang tersebut yang kemudian menjadi landasan penulis untuk menentukan aspek-aspek yang akan masuk dalam stuktur coding.

Setelah mendapatkan hasil kuantifikasi data kualitatif dari MAXQDA 2020, dilanjutkan dengan penggunaan aplikasi Gephi 0.9.2. Gephi merupakan perangkat lunak *open-source* yang berguna untuk melakukan visualisasi dan eksplorasi segala jenis grafik dan network. Penggunaan aplikasi tersebut digunakan untuk melihat atau menganalisis relasi data antara satu aspek dengan aspek lainnya dengan menggunakan *network analysis*. Analisa lanjutan

dilakukan dengan merelasikan data-data yang timbul diantara satu aspek dengan aspek lainnya dengan cara membuat *coding* dalam dokumen SCSS. *Coding* ini terbagi dalam tiga code (masing-masing code memiliki sub-code) yang terdiri dari *Code (Nation)* yang mempunyai *sub-code (Infrastructure), (Application)*, dan (*Core*). Kemudian *Code (Sovereignty)* mempunyai *sub-code (Transfer*) dan (*Exclusive*). Selanjutnya *Code (Aspect*) yang mempunyai *sub-code (Attack and Cases), (State actor), (Non-state actor), (Mitigation and Vision), (Research and Development), (Economic development), (Political action), (Public administration), (Collaboration)* dan (*Law*).

3. Hasil dan Pembahasan

Three Perspective Theory of Cyber Sovereignty atau Teori Kedaulatan Siber yang dipublikasikan oleh Hao Yeli (Disputes & Cyber, 2017) menekankan bahwa terdapat tiga klaster besar yaitu *infrastructure, application*, dan *core* yang selanjutnya mengarah pada dua sifat kedaulatan: *transfer* (terbuka) dan *exclusive* (tertutup).



Sumber: (Yeli, 2017)

Gambar 1. Pendekatan *Cyber Sovereignty*

Gambar 1 menjelaskan mengenai kerangka teori kedaulatan terkait keamanan siber sebuah negara meliputi prinsip dan kebijakan dalam mengimplementasikan strateginya. Dari aspek prinsip, keamanan siber negara berkaitan erat dengan *Core*. Posisinya di paling atas memperlihatkan bahwa core merupakan aspek paling prinsipil dan sentimentil karena menyangkut nilai, ideology, dan falsafah hidup yang perlu dilindungi dari berbagai bentuk ancaman. Sementara aspek *application* menjelaskan tentang interaksi warga negara maupun negara dan bagaimana strategi keamanan siber itu dieksekusi. Aspek penunjang lainnya yaitu *infrastructure* yang berkaitan dengan sejumlah perangkat atau instrument yang kemudian membentuk infrastruktur dasar ruang siber.

Kemudian juga dapat dipahami bahwa kedaulatan yang bersifat ideologis cenderung lebih eksklusif ketimbang kedaulatan yang bersifat interaktif seperti urusan pengembangan ekonomi, agenda politik nasional maupun internasional, dan pertukaran ilmu pengetahuan yang cenderung lebih terbuka (transfer). Bekal pemahaman inilah yang menjadi kerangka acuan penulis dalam menganalisis secara kualitatif dokumen strategi siber milik Negeri berlogo Singa ini.

3.1. Strategi Keamanan Siber Singapura

Keamanan siber Singapura menjadi salah satu focus perhatian utama yang ditingkatkan oleh pemerintahan Singapura. Perdana Menteri Singapura Lee Hsein Loong mengatakan bahwa Singapur menjadi target ancaman ruang siber dan intensitas serangan ruang siber terhadap Singapura sangat tinggi dibandingkan negara lainnya (Anshori & Ramadhan, 2019). Terdapat berbagai penyerangan ruang siber diberbagai level seperti jaringan internet pemerintah, penyerangan yang dikenal dengan *Advanced Persistent Threat* terhadap jaringan universitas dengan metode pengambilan data personil yang jaringannya berasal dari jaringan kementerian pertahanan Singapura.

Pada tahun 2005, Singapura melakukan berbagai upaya untuk meningkatkan keamanan ruang siber Singapura dengan dibentuknya cyber security masterplan dengan periode waktu 3 tahun (Authority, 2005). Pembentukan *master plan strategic* terhadap keamanan ruang siber bertujuan untuk melindungi Singapura dari berbagai ancaman siber baik eksternal maupun internal. Strategi tersebut memiliki metode untuk mendeteksi, mencegah dan menghadapi ancaman terhadap ruang siber yang memberikan dampak ke sektor masyarakat, sektor swasta dan sektor publik. Tahun 2013, singapura membuat rencana strategis lainnya untuk melindungi keamanan ruang siber singapura yaitu *national cyber security masterplan*, *cyber security research* and *development program* serta *national cyber security center*.

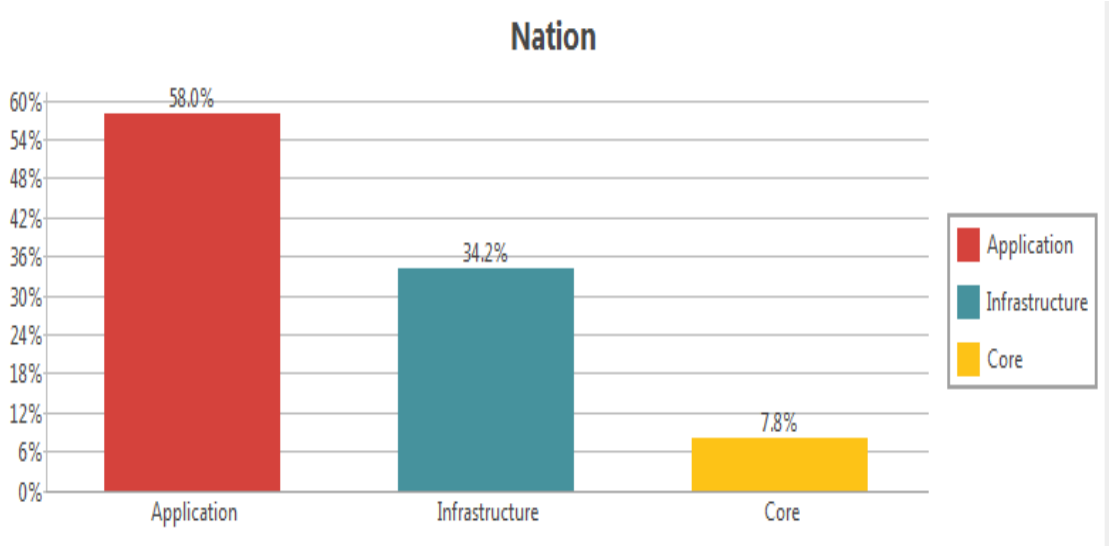
Pada tahun 2016 Singapura menerbitkan Singapore's Cybersecurity Strategy sebagai landasan kerangka kerja perlindungan ruang siber Singapura. Singapura melabeli negaranya sebagai "smart nation" yang mana istilah tersebut merujuk kepada peran Singapura sebagai agen baik teknologi untuk domestic Singapura maupun agen di Kawasan Asia Tenggara (Nations, 2012) (Martin, 2008).

Menteri Komunikasi dan Informasi Singapura, Yacoob Ibrahim, menyatakan di pembukaan ASEAN Ministerial Conference on Cybersecurity 2016 bahwa negara anggota ASEAN memerlukan kesadaran situasi yang lebih baik terkait dengan lingkungan ruang siber secara keseluruhan. Menurutnya, hal ini merupakan kunci untuk dapat memperbaiki higienitas ruang siber terutama dengan lebih baik mengarahkan upaya pencegahan ketika sudah mengetahui adanya kerentanan dan aktivitas ruang siber yang mencurigakan. Kemudian dengan kesadaran situasional pada keamanan siber maka suatu negara dapat mengambil langkah pencegahan yang tepat dalam mengahadapi ancaman dan kerentanan siber potensial pada masa yang akan datang (Anshori & Ramadhan, 2019).

Oleh karena itu, dibutuhkan strategi nasional yang komprehensif untuk menangani resiko dan ancaman yang muncul saat ini. Pada bagian ini, penulis mencoba mengurai lebih lanjut strategi keamanan siber Singapura serta aspek-aspek yang diatur oleh otoritas setempat. Sistematika yang dibangun penulis adalah dengan mengurai dokumen SCSS menjadi unit gramatikal (satuan kalimat) yang selanjutnya disebut dengan *corpus*.

3.1.1. Nation

Data yang penulis dapat dari hasil pengolahan menggunakan perangkat MAXQDA, ditemukan bahwa aspek Application sebesar 58,0% unggul dengan selisih cukup jauh dari aspek Infrastructure yang memperoleh 34,2% disusul aspek Core yang hanya 7,8%. Data kuantitatif ini menandakan bahwa strategi keamanan siber Singapura difokuskan pada implementasi dari strategi tersebut.



Sumber: Hasil Penelitian (2020)

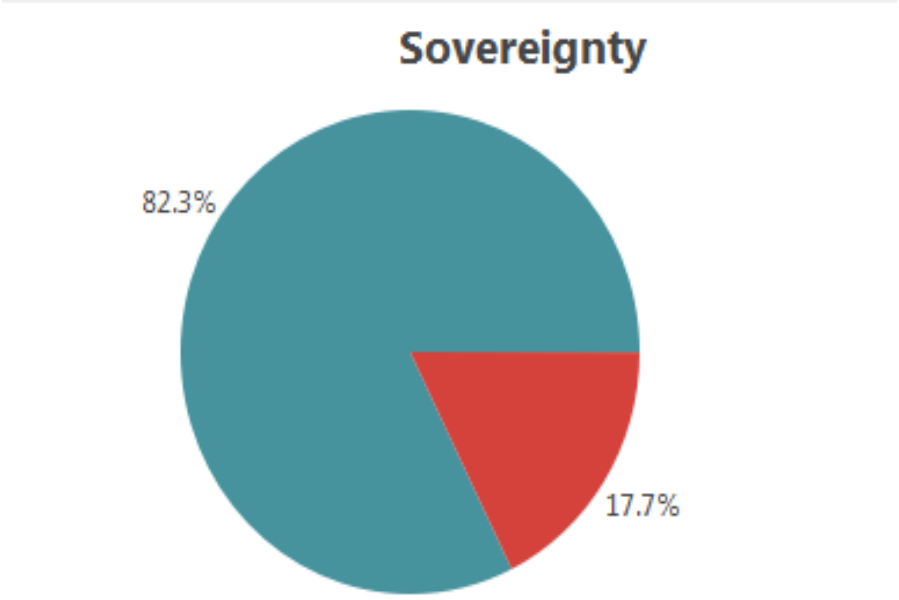
Gambar 2. Hasil Pengolahan Data Strategi Keamanan Siber Singapura dengan *Code Nation*

Dari Gambar 2 menunjukan bahwa Singpura menilai kedaulatan yang berkaitan dengan interaksi manusia (*Application*) sebagai bagian paling penting di antara kedaulatan-kedaulatan yang lain. Terbukti bahwa angka yang diperoleh lebih besar yaitu sejumlah 58,0% selanjutnya *Infrastructure* dengan jumlah 342% dan yang terendah adalah *Core* yang meraih angka 7,8%. Konsekuensi dari besarnya perhatian negara terhadap kedaulatan yang bersifat interaktif membuat aktivitas masyarakat di ruang siber menjadi lebih diatur karena besarnya intervensi negara. Secara kontekstual, hal ini tidak bisa dilepaskan dari kenyataan bahwa Singapura merupakan negara kecil namun punya peran dan posisi strategis dalam konstelasi Internasional.

Pada yang saat sama, fakta tersebut turut menjadi pertimbangan Singapura untuk lebih mengatur kedaulatan interaktifnya (*Application*). Maka dapat dipahami jika kemudian pada kedaulatan infrastruktur, Singapura mengaturnya dengan mendukung sektor *Application* sekaligus memperkuat keamanan dan pertahanan sibernya. Justru yang di luar dugaan penulis adalah pada aspek (Core) yang tidak diatur Singapura.

3.1.2. Sovereignty

Setelah mendapat gambaran mengenai beberapa aspek kedaulatan: infrastructure, application, dan core dari dokumen SCSS, di bawah ini penulis kemudian menampilkan sifat dari ketiga jenis kedaualatan tersebut.



Sumber: Hasil Penelitian (2020)

Gambar 3. Hasil Pengolahan Data Strategi Keamanan Siber Singapura

Komposisi perbandingan pada Gambar 3 sejalan dengan strategi keamanan Singpura yang fokus mengatur aspek kedaulatan *application*. Karena, kedaulatan *Application* memerlukan keterbukaan (transfer) agar strategi tersebut dapat berjalan efektif dan efisien. Buktinya, kedaulatan yang bersifat *transfer* memperoleh 82,3%. Angka yang jauh lebih besar dari kedaulatan bersifat tertutup yang hanya mendapat angka 17,7%.

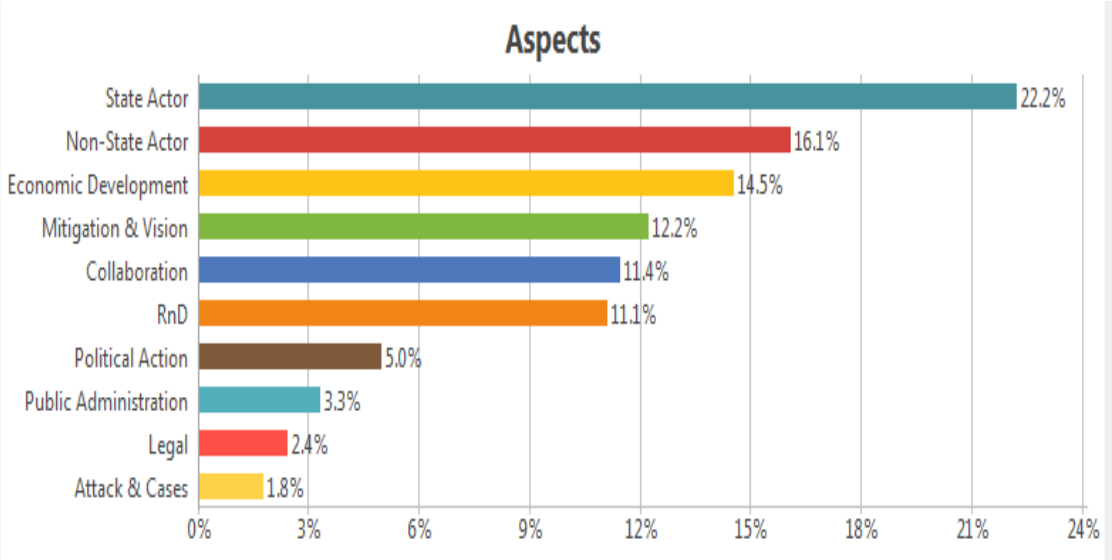
Dari sini penulis melihat Singapura tergolong negara yang *aware* untuk terus meningkatkan keamanan dan pertahanan sibernya. Karena bila diperhatikan, setelah *application*, kedaulatan yang juga penting untuk terus ditingkatkan Singapura adalah kedaulatan Infrastructure. Untuk itu, dua aspek tersebut menjadi prioritas dibanding core yang lebih bersinggungan dengan hal-hal ideologis. Itulah mengapa Singapura berorientasi pada perkembangan baik secara ekonomi, politik, maupun ilmu pengetahuan.

3.1.3. Aspect

Setelah penulis mengetahui strategi keamanan siber Singapura yang terangkum dalam SCSS menitikberatkan pada kedaulatan *application* disusul *infrastructure* yang sifatnya lebih terbuka dibanding *ideology* yang lebih eksklusif, maka penting untuk diketahui, selain ketiga kedaulatan tersebut, aspek mana saja yang juga menjadi *focus* Singapura.

Penulis membagi aspek ke dalam 8 struktur code yakni *State and actor, Economic Development, Political Action, Attack and Cases, Application, Infrastructure, Core,* dan *Transfer*. Seluruh aspek yang penulis sebutkan merupakan poin-poin besar dari dokumen SCSS yang

secara kontekstual dimasukkan ke dalam *Code* (*Aspects*) guna mengukur besaran fokus Singapura terhadap sejumlah aspek tersebut.



Sumber: Hasil Penelitian (2020)

Gambar 4. Hasil Pengolahan Data Strategi Keamanan Siber Singapura dengan *Code Aspects*

Melihat realitas data yang menunjukkan tingginya intensitas negara pada kedaulatan *Application*, sejurus kemudian peran negara terhadap aspek tersebut juga akan lebih aktif dalam mengatur aktivitas dan interaksi masyarakat dalam mengakses ruang siber. Terbukti dari data tampilan di atas, *state actor* merupakan aspek yang mendapat poin paling besar yakni 22,2%. Sebagai konsekuensi logis dari aktifnya peran negara, maka akan tinggi pula tingkat tingkat kerjasama yang dijalin antara negara dan aktor selain negara yang dalam hal ini meraih poin 16,1% setingkat di bawah *state actor*.

Hasilnya, dari bangunan kerjasama yang disusun secara aktif oleh Singapura itu, tidak lain dan tidak bukan menyimpan kepentingan ekonomis yang ingin dicapai sebesar 14,5%. Selain itu, Singapura juga aktif meningkatkan sektor keamanan dan pertahanan sibernya. Kenyataan tersebut penulis temukan dari upaya-upaya preventif, antisipatif, dan prospektif (*Mitigation and Vision*) Singapura dari dokumen SCSS yang gencar menjalin kerjasama dengan berbagai aktor dalam rangka menciptakan sistem keamanan ruang siber yang berdaya tahan (resilient). Pada aspek ini, diperolehlah angka 12,2%. Tidaklah berlebihan bila kemudian setingkat di bawah aspek mitigation dan vision ditempati aspek collaboration dengan poin sebesar 11,4%. karena keduanya merupakan satu kesatuan dari aspek konseptual dan realisasinya.

Sebagai negara yang memfokuskan strategi keamanan sibernya pada kedaulatan (*Application*), maka sudah menjadi keniscayaan bagi Singapura untuk turut aktif melakukan penelitian dan pengembangan baik dari sisi teknologi, kompetensi, dan relasi yang strategis guna menghasilkan infrastruktur siber yang supportif dan aplikatif. Sehingga didapatlah angka 11,1 untuk merepresentasikan tingkat prioritas Singapura pad aspek ini. bagian yang tentu tak

boleh dilupakan, hal ini sejalan dengan visi Singapura yang ingin membangun ekosistem ruang siber yang resilient.

Untuk mewujudkan itu, Singapura pun mengecilkan upaya-upaya politis dan mengurangi hal-ihwal yang berhubungan dengan administrasi untuk memperlancar upaya strategis sebagaimana yang penulis temukan dari konten dokumen SCSS. Di samping itu, pendekatan tersebut juga dapat mencegah Singapura dari challenges yang berpotensi menghambat realisasi terhadap capaian pada kedautan (*Application*) dan peningkatan infrastruktur ruang siber. Dibuktikan aspek-aspek seperti *political action, public administration, legal*, dan *attack and cases* tidak menjadi prioritas Singapura yang masing-masing meraih angka 5,0% untuk political action, 3,3% untuk public administration, legal 2,4%, dan attack and cases 1,8%.

3.2. Relasi Data

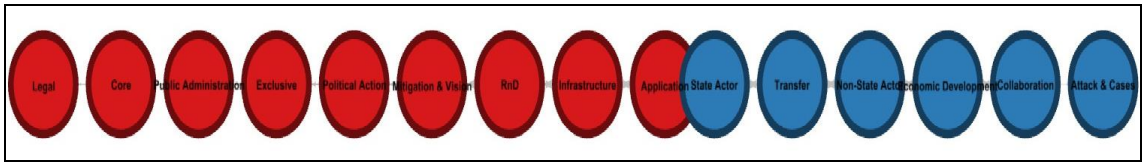
Sebelum mengurai lebih lanjut, data kualitatif yang sudah penulis peroleh dari hasil pengolahan menggunakan MAXQDA, kemudian ditransformasi ke dalam bentuk matrix. Matrix inilah yang selanjutnya penulis konversi menggunakan aplikasi Gephi.

Code System	Infrastructure	Application	Core	Sovereignty	Transfer	Exclusive	Aspects	Attack & Cases	Mitigation & Vision	Public Administration	Legal	RnD	Collaboration
Nation													
Infrastructure		62	8		42	13		6	41	14		25	18
Application	62		11		85	17		1	62	16	14	55	54
Core	8	11			2	13		1	10		1	9	2
Sovereignty													
Transfer	42	85	2			2		4	31	11	12	48	89
Exclusive	13	17	13		2			2	16	3		11	3
Aspects													
Attack & Cases	6	1	1		4	2					2		1
Mitigation & Vision	41	62	10		31	16				11	3	27	15
Public Administration	14	16			11	3			11		5	10	11
Legal		14	1		12			2	3	5		4	9
RnD	25	55	9		48	11			27	10	4		18
Collaboration	18	54	2		89	3		1	15	11	9	18	
Economic Development	31	62	8		77	6		5	33	5	6	41	45
Political Action	12	26	6		24	6		1	9	6	8	7	16
State Actor	59	109	13		113	24		5	52	19	6	54	80
Non-State Actor	39	76	3		110	8		5	33	9	4	45	72

Sumber: Hasil Penelitian (2020)

Gambar 5. Hasil Pengolahan Data dengan Aplikasi MAXQDA

Gambar 5 menjelaskan bagaimana keterkaitan antar aspek dapat dihitung dan diolah menggunakan software Maxqda. Data tersebut menjelaskan semakin tinggi angka yang didapatkan, maka semakin tinggi data tersebut menjadi aspek utama dari dokumen nasional keamanan siber Singapura. Setelah ditransformasi, hasil akhir yang diperoleh dari pengolahan menggunakan Gephi adalah sebagai berikut:



Sumber: Hasil Penelitian (2020)

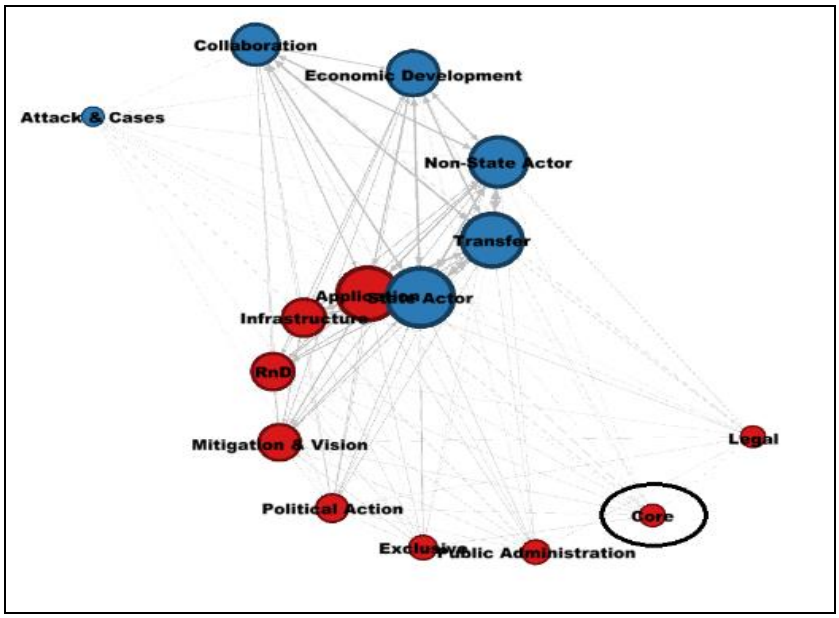
Gambar 6. Hasil Pengolahan Data dengan Aplikasi Gephi

Gambar 6 memperlihatkan bagaimana relasi data yang diolah berdasarkan Gephi tersebut telah menghasilkan dua klaster besar antara merah dan biru. Di mana, klaster biru terdiri dari nodes yang berurutan dari besar ke kecil yaitu: *State actor, Transfer, Non-state actor, Economic Development, Political Action, dan Attack and Cases*. Sedangkan di klaster merah yang berurutan dari besar ke kecil diisi node *Application, Infrastrcuture Core.*

Dari tampilan data di atas, penulis dapat memahami bahwa relasi data pada klaster biru merupakan aspek-aspek yang memiliki banyak keterkaitan dibanding klaster merah. Meski pada klaster biru, peran negara tampak begitu dominan bukan berarti kehadirannya membuat sifat kedaulatannya eksklusif. Sebaliknya, negara justru menjadi aktor yang telah mengatur kedaulatannya lebih terbuka.

3.2.1. Core

Gambar 7 menunjukan bagaimana analisis penulis terhadap dokumen SCSS, tidak banyak data yang penulis temukan bersinggungan dengan kedaulatan yang berhubungan dengan *Core*. Sehingga pada Gambar 7 di atas dapat dilihat betapa *Core* bukan termasuk bagian dari prioritas Singapura. Namun demikian, aspek *Core* tetap menjadi acuan Singapura di dalam membangun strategi keamanan dan pertahanan ruang sibernya.



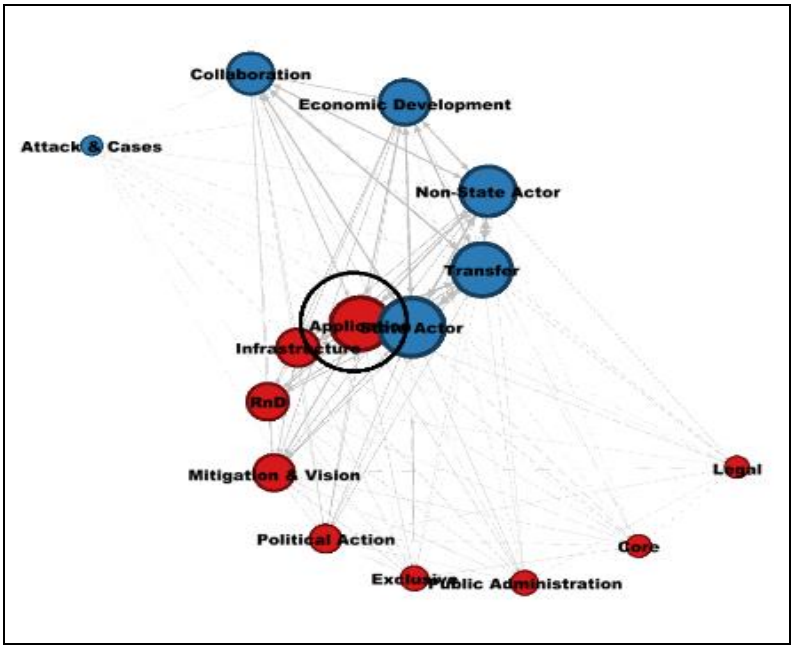
Sumber: Hasil Penelitian (2020)

Gambar 7. Hasil Pengolahan Data menggunakan Aplikasi Gephi dengan Cluster Core

3.2.2. Application

Gambar 8 memaparkan gagasan atau strategi keamanan siber Singapura ini bisa diidentifikasi dari aspek *application* ini. Besarnya perhatian Singapura pada aspek tersebut menandai besarnya peran negara dalam mengatur aktivitas warga negaranya di ruang siber. Singapura memandang langkah itu diperlukan untuk menyediakan ruang siber yang lebih protektif dengan melibatkan seluruh aspek untuk memastikan bahwa interaksi atau aktivitas

ruang sibernya terlindungi dengan baik. Namun pada titik yang lain, intervensi negara berdampak pada terbatasnya interaksi masyarakat Singapura dalam mengakses ruang siber.

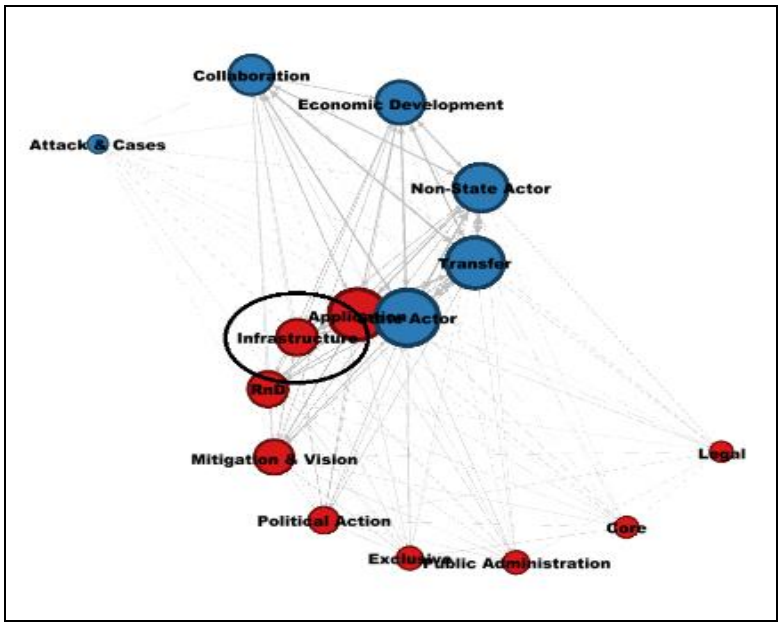


Sumber: Hasil Penelitian (2020)

Gambar 8. Hasil Pengolahan Data menggunakan Aplikasi Gephi dengan Cluster Application

3.2.3. Infrastructure

Gambar 9 ini merupakan afirmasi bahwa Singapura termasuk negara yang fokus dalam mengatur interaksi masyarakatnya di dalam ruang siber.



Sumber: Hasil Penelitian (2020)

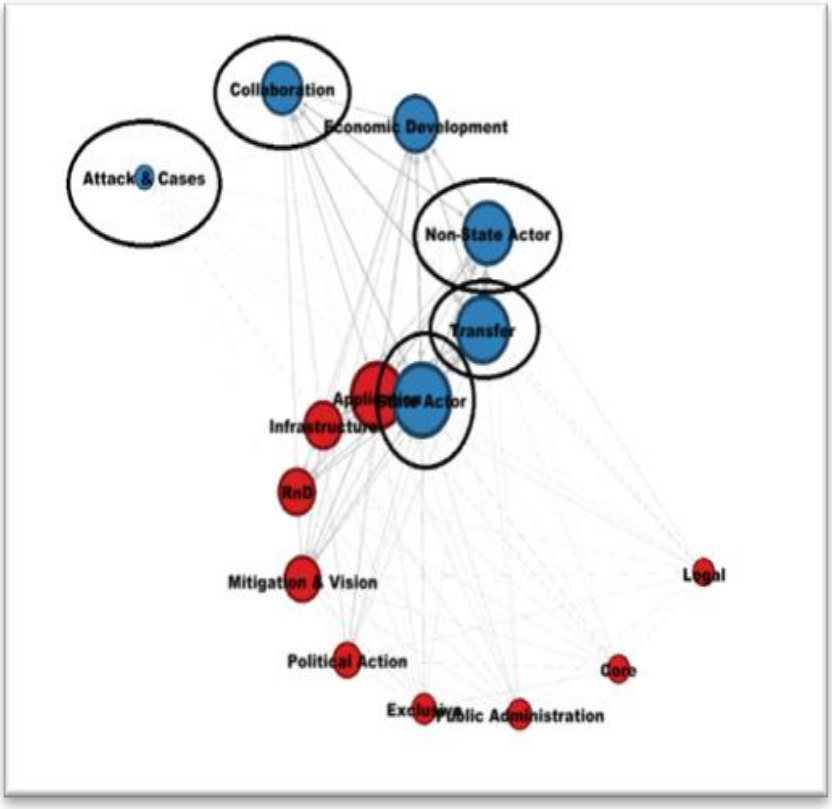
Gambar 9. Hasil Pengolahan Data menggunakan Aplikasi Gephi dengan *Cluster Infrastructure*

Untuk mewujudkan visi tersebut, Singapura tentu perlu meningkatkan infrastruktur sibernya. Maka dapat dilihat infrastruktur tergolong aspek yang cukup besar di antara aspek-

aspek lain seperti *state actor* dan *application*. Atau dengan kata lain, semakin besar porsi negara dalam mengatur interaksi masyarakatnya, semakin kompleks pula infrastruktur yang dibutuhkan. Dan semakin terbuka pula sifat kedaulatannya karena Singapura harus menjalin kerjasama dengan para aktor baik negara maupun *private sectors* (Cyberspace et al., 2017). Kemudian disusul dengan keterhubungan yang intens antara Infrastructure dan aspek RnD serta Mitigation. Dengan begitu, maka akan berdampak pada pertumbuhan ekonomi Singapura (Australian Cyber Security Growth Network, 2019).

3.2.4. State and Non-State Actor, Attack and Cases, Collaboration and Transfer

Pada bagian ini, secara keseluruhan pelaksanaan strategi keamanan siber Singapura dikendalikan oleh dua aktor*: state actor* dan *non-state actor*. Kedua aktor ini memiliki peran yang sama karena berada pada klaster yang sama. Penetrasi negara sebagai actor yang secara kuantitatif unggul pun tidak akan lebih dominan karena mendapat pembanding yang seimbang dari aktor-aktor di luar negara. Hal ini sangat dipengaruhi oleh sifat keterbukaan (*transfer*) Singapura yang juga besar pada aspek ini.



Sumber: Hasil Penelitian (2020)

Gambar 10. Hasil Pengolahan Data Aplikasi Gephi dengan *Cluster Non-State Actor*

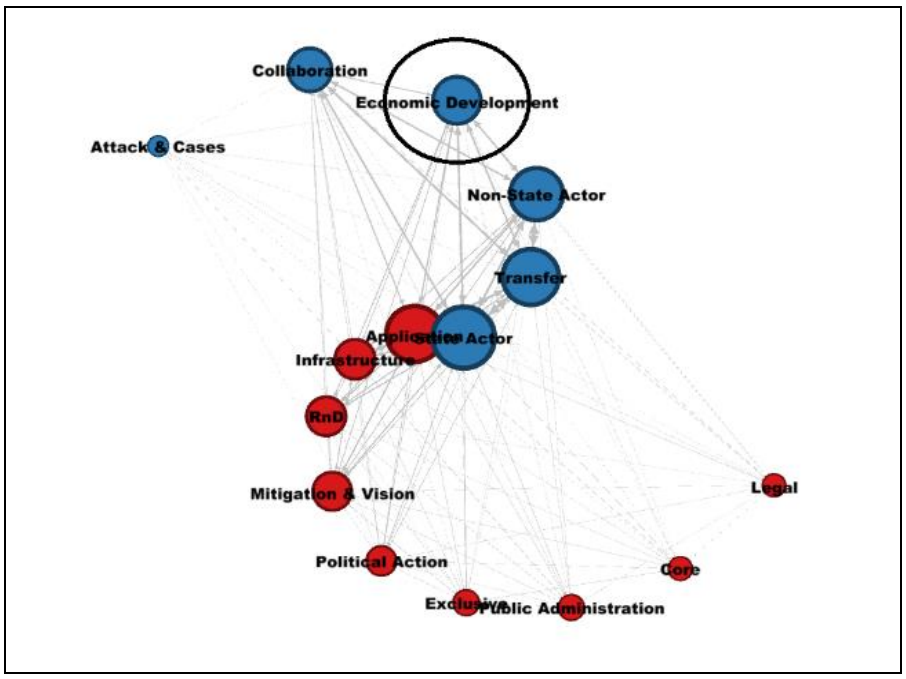
Singapura merupakan negara dengan tingkat kedaulatan yang bersifat terbuka (transfer) terutama dalam hal peningkatan kerjasama demi pengembangan teknologi untuk mitigasi dan melindungi ruang siber. Ini menjadi bagian yang tak kalah penting dari strategi Singapura di dalam dokumen SCSS. Oleh sebab itu, node ini terhubung bersama node-node lain yang menandakan bahwa strategi ruang siber Singapura mengatur semua node-nya

tersebut dengan sifat dan prinsip yang lebih terbuka. Interaksi ini hanya akan dapat berjalan bilamana Singapura aktif melakukan kolaborasi yang terbuka dengan berbagai pihak.

Dilihat dari keterhubungannya, aspek kolaborasi juga terkoneksi dengan aspek-aspek lainnya yang mengindikasikan bahwa kolaborasi ini dibutuhkan sebagai driver untuk menggerakkan aspek-aspek lainnya. Fakta bahwa Singapura menganggap penting aspek *Collaboration* ini bisa dikonfimasi dari posisi node yang berada pada klaster biru atau klaster prioritas Singapura. Selain itu, *Attack and Cases* merupakan kunci utama dari pengembangan dan pencegahan adalah meningkatkan kolaborasi (Savira & Suharsono, 2013).

3.2.5. Economic Development

Gambar 11 menjelaskan bahwa aspek perkembangan ekonomi (economic development) termasuk aspek yang mendapat posisi penting dalam dokumen strategi keamanan siber Singapura terlihat dari raihan angka 14,5%. Porsi tersebut juga menempatkan aspek perkembangan ekonomi di urutan ketiga setelah aspek state actor dan non state actor. Besarnya perhatian Singapura terhadap aspek ekonomi menandakan bahwa negara ini cukup berkepentingan untuk mengembangkan sektor perekonomiannya.



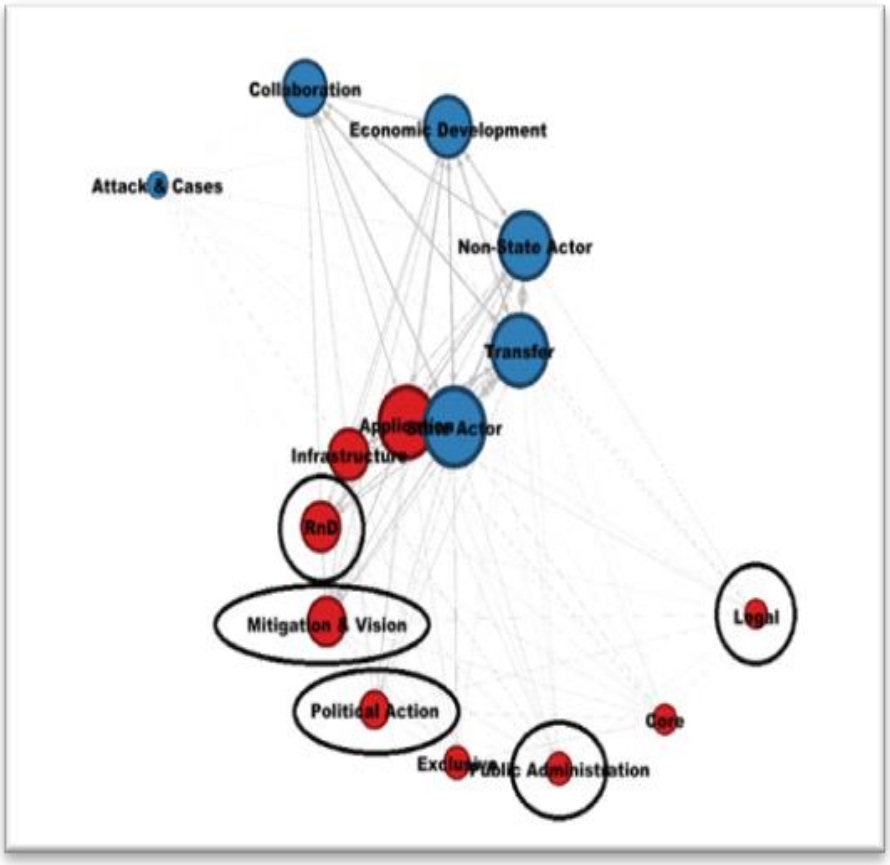
Sumber: Hasil Penelitian (2020)

Gambar 11. Hasil Pengolahan Data Aplikasi Gephi dengan *Cluster Economic Development*

3.2.6. Political Action, RnD, Mitigation & Vision, Public Administration and Legal

Berdasarkan hasil pengolahan aplikasi Gephi pada Gambar 12, Political Action berada pada barisan klaster yang sama dengan aspek economic development. Pasalnya, implementasi aspek ini pada saat yang sama selalu berjalan beriringan dengan perkembangan ekonomi. Keduanya bersifat reciprocal karena saling memengaruhi satu sama lain. Bukan hanya itu, besarnya implikasi political action juga menentukan aspek mana saja yang ingin diatur dan tidak. Dalam hal ini, aspek legal dan *public administration* bukanlah aspek yang ingin diatur

sebagai wujud dari kebijakan pemerintah Singapura melakukan debirokratisasi. Debirokratisasi menjadi lanskap (*vision*) yang diharapkan dapat mempercepat munculnya inovasi teknologi melalui RnD dan *Mitigation* untuk menciptakan sistem keamanan dan pertahanan *cyberspace* yang *resilient*.



Sumber: Hasil Penelitian (2020)

Gambar 12. Hasil Pengolahan Data Aplikasi Gephi dengan *Cluster Political Action*

4. Kesimpulan

Strategi keamanan Singapura secara kontekstual lebih mengarah pada pengaturan negara terhadap aspek aktor negara, *application, infrastructure*, aktor selain negara, perkembangan ekonomi (*economic development*), kolaborasi, *research and development* (RnD) dan mitigasi. Ide besar dari strategi tersebut adalah menekankan pada dominasi peran negara yang dominan dalam menciptakan ruang siber yang aman merupakan keniscayaan. Meski demikian, secara kedaulatan Singapura bersifat terbuka. Apalagi relasi yang dibangun tersebut juga mengarah pada pengembangan ekonomi, politik, dan infrastruktur tata kelola siber. Sedangkan aspek-aspek lainnya *seperti core, legal, public administration* tidak banyak diatur oleh otoritas Singapura karena di samping bukan termasuk aspek-aspek prioritas, juga karena berlawanan dengan prinsip Singapura yang lebih menganut paham liberalism. Hambatan-

hambatan yang bersifat administratif dan birokratis sebisa mungkin dikurangi demi terciptanya tata kelola siber yang lebih maju.

Daftar Pustaka

Anshori, M. F., & Ramadhan, R. A. (2019). Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week. *Padjadjaran Journal of International Relations*, *1*(1), 39. https://doi.org/10.24198/padjir.v1i1.21591

Australian Cyber Security Growth Network. (2019). *Cyber Security Opportunities in the ASEAN Region*. 15–17.

Authority, I. M. D. (2005). *Three-year Infocomm Security Masterplan Unveiled*. Infocomm Media Development Authority. https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2005/20050712110643

Cyberspace, N. R., Summit, W., Cybersecurity, N., Aims, S., Smart, M., Safe, N., Lee, P. M., Chieh, L. W., Auyong, H., Thean, T., & Policy, P. (2017). *"NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit | CCDCOE," 2016. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html. 2 Kwang, Kevin. "National Cybersecurity Strategy Aims to Make Smart Nation Safe:* . https://doi.org/10.1111/1468-2346.12504.2

Disputes, T., & Cyber, O. (2017). *A Three-Perspective Theory*. *2*(2), 109–115.

Hughes, B. B., Bohl, D., Irfan, M., Margolese-Malin, E., & Solórzano, J. R. (2017). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Technological Forecasting and Social Change*, *115*, 117–130. https://doi.org/10.1016/j.techfore.2016.09.027

International Telecommunication Union. (2017). Global Cybersecurity Index (GCI) 2017. In *ITU-D Global*.

Martin, W. (2008). Singapore's Cybersecurity Strategy. *Southern Crossroads: Perspectives on Religion and Culture*, 63–88. https://doi.org/10.4324/9780203462010-8

Nations, U. (2012). ** The views expressed in this paper are those of the authors and do not necessarily represent those of the United Nations*. *September*, 1–9.

Savira, F., & Suharsono, Y. (2013). Singapore Cyber Landscape 2019. In *Journal of Chemical Information and Modeling* (Vol. 01, Issue 01).

Yeli, H. (2017). *A Three-Perspective Theory*. *2*, 109–115.