Jurnal Kajian Ilmiah
e-ISSN: 2597-792X, ISSN: 1410-9794
Vol. 21 No. 1 (Januari 2021), Halaman: 69 – 84
Terakreditasi Peringkat 5 (SINTA 5) sesuai SK RISTEKDIKTI Nomor. 3/E/KPT/2019

Strategi Keamanan Siber Malaysia

Putri Bilqis Oktaviani [1], Anggraeni Silvia [1],*

[1] Fakultas Falsafah dan Peradaban; Universitas Paramadina; Jl Gatot Subroto, (021) 79181190; e-mail: putri.oktaviani@students.paramadina.ac.id, anggraeni.silvia@students.paramadina.ac.id

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

Submitted: **28/12/2020**; Revised: **04/01/2021**; Accepted: **07/01/2021**; Published: **15/01/2021**

Abstract

This research discusses the analysis of security strategy policies made by the Malaysian government in the protection and development of Malaysian cyberspace. This research will explain in detail the strategy of developing challenges as well as the aspects that support the Malaysian cyber space to be saved by the Malaysian cyber space. This research will further discuss the Malaysian security strategy through the official document of the Malaysian security strategy which will later be analyzed through the MAXQDA and GEPHI applications in order to classify the various categories that support it. This research will use the security concept published by Hao Yeli in Three - Perspective Theory of Cyber Sovereignty to classify ideas and data. This research finds that the security of the Malaysian system needs to be developed from both capacity and capability so that the government needs to work together with various related parties

***Keywords**: Cyber Security, Cybersecurity Challenges, Soveignty*

Abstrak

Penelitian ini membahas tentang analisis kebijakan strategi keamanan siber yang dibuat oleh pemerintah Malaysia dalam perlindungan dan pengembangan keamanan ruang siber Malaysia. Penelitian ini akan menjelaskan secara details strategi, tantangan serta aspek – aspek yang mendukung pengembangan ruang siber Malaysia guna mengamankan ruang siber Malaysia. Penelitian ini akan membahas lebih jauh strategi keamanan Malaysia melalui dokumen resmi strategi keamanan siber Malaysia yang nantinya akan di bedah melalui aplikasi MAXQDA dan GEPHI guna mengklasifikasikan berbagai kategori yang mendukung. Penelitian ini akan menggunakan konsep keamanan yang dipublikasikan oleh Hao Yeli dalam *A Three – Perspective Theory of Cyber Sovereignty* guna mengkasifikasikan gagasan dan data dengan menggunakan metode penelitian kuantitatif. Penelitian ini menemukan bahwa keamanan siber Malaysia perlu dikembangkan baik dari kapasitas maupun kapabilitas sehingga pemerintah Malasyaia perlu bekerjasama dengan berbagai pihak yang terkait.

Kata kunci: *Cyber Security*, Tantangan Keamanan *Cyber*, Kedaulatan

1. Pendahuluan

Globalisasi memberikan dampak yang signifikan terhadap berbagai aspek kehidupan seperti perkembangan teknologi, informasi, komunikasi, hilangnya batas negara, mudahnya individu untuk melakukan migrasi ke negara lain. Di lain pihak globalisasi juga memberikan dampak gelap terhadap berbagai negara yang belum siap menghadapi dampak globalisasi seperti hadirnya isu keamanan non tradisional, dampak *Multi National Cooperation* (MNC) serta hadirnya ruang siber dimana negara saat ini berlomba-lomba membangun teknologi untuk mendukung perkembangan ruang siber.

Keamanan siber menjadi salah satu perhatian bagi negara untuk mengamankan ruang siber karena di masa kini. Ruang siber dilindungi oleh system internet yang terkoneksi, termasuk hardware, software dan data dari kejahatan siber(Disputes & Cyber, n.d.). Keamanan ruang siber di abad 21 menjadi hal yang signifikan disebabkan adanya sifat ketergantungan dari entitas baik individu, kelompok, organisasi dan entitas lain terhadap teknologi berbasis computer dan internet. Perhatian terhadap keamanan ruang siber menjadi focus utama bagi pengguna untuk terhindar dari kegiatan kejahatan siber. Kejahatan siber mengalami peningkatan disebabkan karena aksi kejahatan siber di dunia maya lebih murah, memiliki resiko lebih rendah dibandingkan dengan serangan fisik dan lebih murah. Alat yang digunakan oleh para pelaku tindak kejahatan siber yaitu computer dan akses internet (Jang-Jaccard & Nepal, 2014).

Ruang siber memiliki berbagai tantangan dan dampak yang signifikan terhadap perkembangan negara salah satunya Malaysia. Malaysia menjadi salah satu negara yang mengembangkan strategi keamanan siber berbasis kerangka kerja untuk diimplementasikan. Strategi keamanan tersebut di bentuk pada tahun 2018 dimana Malaysia memahami bahwa isu yang hadir di lingkungan internasional semakin berkembang, tantangan dan dampak ruang siber semakin nyata dilihat dari dari berbagai contoh kasus penyerangan ruang siber di Makaysia, dampak terhadap kehidupan social, ekonomi dan berbagai aspek lainnya.

Penelitian ini akan fokus terhadap Analisa strategi kebijakan keamanan siber Malaysia yang dipublikasikan pada tahun 2018. Penelitian ini akan menggunakan konsep kedaulatan yang terdiri dari berbagai elemen seperti aspek ruang siber, kebijakan negara, infrastruktur dan berbagai elemen lainnya untuk menganalisa lebih mendalam terhadap konteks yang hadir di dalam kebijakan keamanan ruang siber. Pemahaman terkait ruang siber Malaysia dalam tulisan ini akan memberikan Analisa mendalam terkait urgensi yang mendorong Malaysia untuk membangun kerangka strategi keamanan siber, efek terhadap kehidupan di Malaysia di tinjau dari berbagai aspek seperti ekonomi, social, kebijakan, infrastruktur dan aspek lainnya.

2. Metode Penelitian

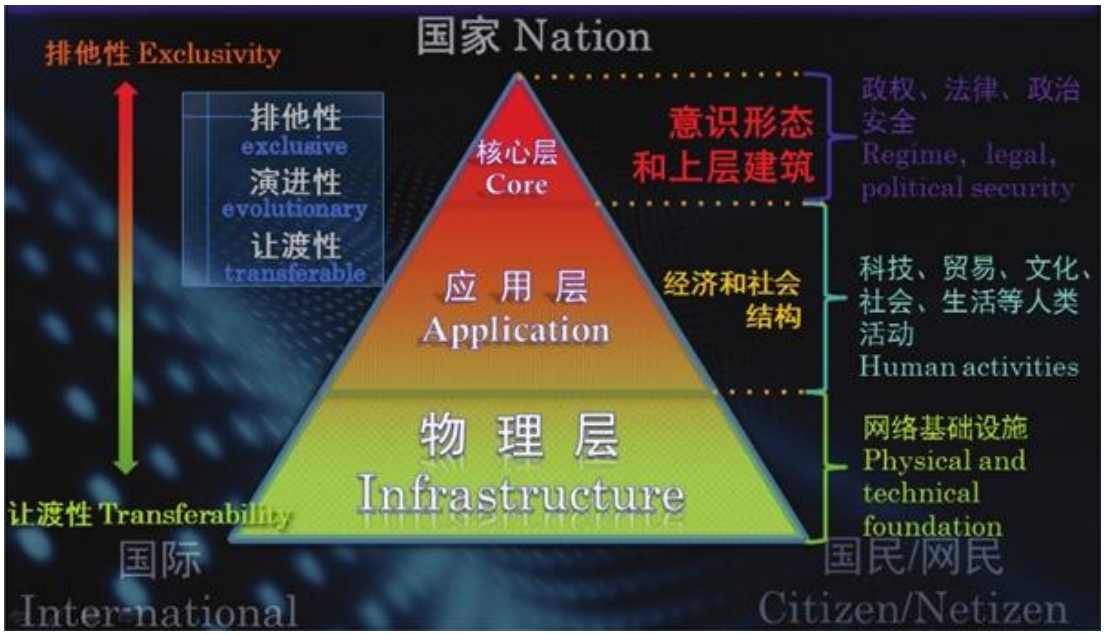
Peneliti dalam menganalisa penelitian ini akan membagi dalam beberapa tahap. Tahap pertama yaitu peneliti melakukan analisa secara kontekstual terhadap dokumen strategi keamanan siber Malaysia menggunakan MAXQDA. MAXQDA merupakan sebuah aplikasi yang digunakan untuk membantu menganalisa dengan cara melakukan *coding* berdasarkan pendekan kedaulatan yang digunakan.

Penulis menggunakan MAXQDA dengan membentuk tiga kategori yaitu *Nation, Sovereignty*, dan *Aspects.* Kategori aspek akan dikembangkan berdasarkan Analisa strategi keamanan siber Malaysia 2018 yang nantinya akan memberikan berbagai sub aspek untuk menganalisa lebih jauh strategi keamanan siber tersebut seperti *policy enforcement, economic effect, challenging, development of technology* dan berbagai aspek lainnya.

Analisa MAXQDA dalam pembedahan keamanan siber Malaysia digunakan untuk menjawab rumusan masalah terkait bagaimana pembentukan strategi keamanan siber Malaysia serta bagaimana pengaplikasian kerangka kerja keamanan siber Malaysia.

3. Hasil dan Pembahasan

Analisa kebijakan keamanan siber Malaysia dalam penelitian ini akan menggunakan pendekatan keamanan yang dipublikasikan oleh Hao Yeli dalam A Three – Perspective Theory of Cyber Sovereignty. Hao Yeli memberikan sudut pandang sebuah kedaulatan yang dapat ditinjau dari tiga elemen yaitu *core, application*, *structure.* Ketiga elemen tersebut mengacu kepada induk data yaitu bangsa. Di sisi lain, Hao Yeli juga memaparkan bagaimana elemen tersebut memiliki sifat yang dapat mempertajam Analisa keamanan siber yaitu *exclusivity* dan *transferability.* Hao Yeli memberikan sebuah ilustrasi menggunakan diagram untuk menganalisa kebijakan keamanan siber tersebut menggunakan pendekatan kedaulatan (Disputes & Cyber, n.d.).



Sumber: Yeli (2017)

Gambar 1. Teori Cyber Sovereignty

Gambar 1 merupakan pemaparan yang diberikan oleh Hao Yeli yang menjelaskan bagaimana konsep dari keamanan siber ditinjau dari beberapa elemen. Dalam tulisan Hao Yeli, Hao Yeli menjelaskan kedaulatan terbagi menjadi tiga elemen.

1. *Core*

   Konteks *core* merujuk kepada hal yang merujuk terhadap sudut pandang negara, seperti prinsip, kebijakan, hukum, rezim, keamanan nasional, dan berbagai aspek lainnya.

2. *Application*

Aplikacation menjelaskan bagaimana interaksi yang terjalin antara individu, negara, regional dan berbagai lainnya yang dilihat dari interaksi yang terjadi antar aktor

3. *Infrastructure*

   Kategori terakhir adalah infrastruktur, kategori tersebut merujuk terhadap teknik dasar, ketersediaan teknologi, pembuatan kebijakan, pembentukan kerangka kerja, pengembangan kerja sama dan berbagai aspek lainnya.

Ketiga elemen tersebut memberikan pengembangan terhadap bagaimana arah dan sifat kebijakan keamanan siber Malaysia yang lebih mengarah kepada sifat yang ekslusif (tertutup dan private) karena pada hakikatnya, kebijakan yang dibuat oleh negara akan lebih bersifat ekslusif, karena negara yang lebih memahami kepentingan nasionalnya sendiri. Maka dari pandangan tersebut dapat diambil sebuah pertanyaan mendasar terkait aspek seperti apa yang mendorong berdirinya dan berkembangnya sebuah strategi keamanan siber di Malaysia serta bagaimana pengaplikasian kerangka kerja keamanan siber Malaysia.

Penelitian keamanan siber ini akan dituangkan secara kualitatif namun peneliti juga akan memaparkan data secara kuantitatif demi memperkuat argument dan validasi data sehingga untuk penelitian strategi keamanan siber Malaysia akan menjadi lebih jelas, terkorelasi satu sama lain dan comprehensive.

Pada tahap pertama, penulis akan menganalisa secara mendalam focus utama strategi keamanan siber Malaysia 2018 menggunakan aplikasi MAXQDA yang kemudian akan penulis gambarkan menggunakan *interactive word tree*.

Sumber: Hasil Penelitian (2020)

Gambar 2. *Cyber Security* didalam *National Strategi of Malaysia's Cyber Security*

Data pada gambar 2 merupakan penarikan data yang diambil dari MAXQDA untuk menjelaskan bagaimana focus keamanan siber Malaysia. Dapat dilihat dari data diatas bahwa keamanan siber memiliki berbagai elemen yaitu

1. *Cyber security strategy: the need to develop information security awareness*
2. *Cyber security strategy: development that provides the framework for key performance indicator and outcome based on evaluation*
3. *Cyber security strategy team: list figures and tables 8 list of 9 acronyms*
4. *Cyber security strategy team: the academy of Science Malaysia*

5. *Cyber security strategy adopts a risk based cyber security ecosystem*

Data diatas memberikan gambaran bagaimana Malaysia menghadapi berbagai ancaman keamanan siber dengan cara mengembangkan kapasitas secara progressive. Fokus utama strategi keamanan siber Malaysia di dominasi oleh hadirnya berbagai kasus penyerangan keamanan siber.

Penyerangan terhadap keamanan siber mengalami eskalasi di Malaysia, sehingga Malaysia membuat kerangka kerja strategi keamanan siber untuk meningkatkan perhatian pengguna ruang siber demi keamanan data, jaringan, teknologi dan aspek lainnya. Selain kerangka kerja strategi keamanan siber Malaysia, Malaysia juga sudah membangun penegak hukum yang terfokus pada tindak kejahatan criminal siber sejak 2015 mengingat tingginya tingkat penyerangan ruang siber baik dari dalam maupun dari luar negeri (Tamyez, 2019)

3.1 Strategi Keamanan Siber Malaysia

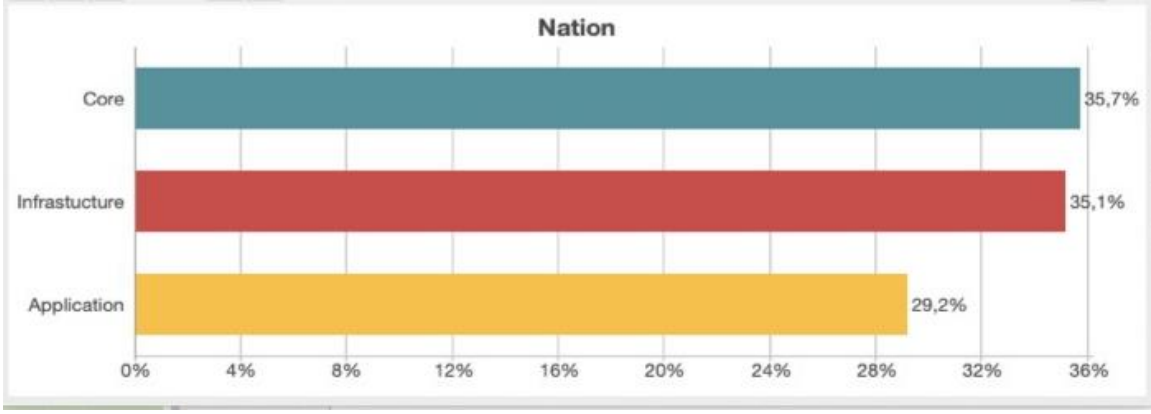
Pada sub bab ini, peneliti akan menguraikan lebih merinci terkait strategi keamanan siber yang di bentuk oleh Malaysia. Analisa strategi keamanan siber hadir guna memperkuat pondasi keamanan siber Malaysia mengingat meningkatnya ancaman pada dunia siber yang tidak hanya dilihat dari angka namun kompleksitasnya seperti jaringan, alat kejahatan siber yang lebih efesien, canggih dan efektif (Abomhara & Køien, 2015). Penulis akan memberikan penjelasan lebih mendalam didorong dengan hadirnya klasifikasi *coding* berbagai aspek yaitu *nation, sovereignty* dan aspek pendukung yang berasal dari hasil olah data MAXQDA dan Gephi.

Code Nation yang terdiri dari 3 elemen yaitu *core, application,* dan *infrastructure. Code* ini merujuk kepada dokumen strategi keamanan siber Malaysia. Data tersebut dianalisa dan di masukkan kedalam kategori yang sesuai dengan tiga elemen tersebut. *Code sovereignty* merujuk kepada sifat dari kedaulatan yang dibuat berdasarkan dokumen strategi keamanan siber. Sifat tersebut dibagi menjadi dua yaitu *exclusivity* – tertutup, dan transferability – terbuka. *Code aspect*, kode aspek ini diambil dari pengolahan data lebih menjauh dalam dokumen strategi keamanan siber di Malaysia. Terdapat lima aspek dan dua sub aspek, yaitu *Policy enforcement, challenging, modern threat* dengan dua sub aspek yaitu *economic effect dan cyber security cases, development of technology, dan social life.*

Pengambilan aspek tersebut dianalisa berdasarkan pemahaman secara kontekstual di dalam dokumen keamanan siber Malaysia. Aspek tersebut saling berkaitan satu sama lain dengan aspek code lain karena aspek tersebut menjadi fondasi bagaimana dokumen keamanan siber ini nantinya dapat terealisasikan dengan baik dan bisa menghadapi berbagai tantangan yang tidak bisa diprediksi kedepannya.

3.1.1 *Nation*

Pengolahan data *nation* menggunakan MAXQDA memiliki jumlah persentase yang cukup tinggi pada bagian *Core dengan 35.7%,* lalu diikuti *application* dengan 35.1% dan *infrastructure* dengan presentasi jumlah yaitu 29.2%.



Sumber Hasil Penelitian (2020)

Gambar 3. Analisa Strategi Keamanan Siber Malaysia

Gambar 3 merupakan analisa data strategi keamanan nasional siber Malaysia yang diolah menggunakan software MAXQDA untuk mengklasifikasikan kedalam elemen pokok. Data tersebut menjelaskan bahwa negara, dengan unsur didalamnya seperti regime, hukum, kebijakan, sanki, kerangka kerja, dan unsur lainnya didominasi oleh negara karena pada dasarnya negara memiliki jangkauan yang lebih luas untuk menganalisa strategi keamanan siber dengan berpacu kepada kepentingan nasional, tantangan di dalam internal dan di lingkungan internasional, mengatur kerangka kerja baik dalam dalam level domestic maupun internasional.

Malaysia memiliki beberapa kasus penyerangan ruang siber seperti yang terjadi pada *computer crime* act 1987, *telemedicine act 19981*, *Electronic Commerce* 2006 dan berbagai kasus serangan keamanan ruang siber sehingga pada 01 September 2016 didirikan Lembaga penegak hukum untuk menangani semua kasus yang berkaitan dengan ruang siber di Malaysia. Lembaga penegak hukum tersebut menjadi contoh bagaimana *core* memiliki pengaruh yang besar tehadap strategi keamanan global.

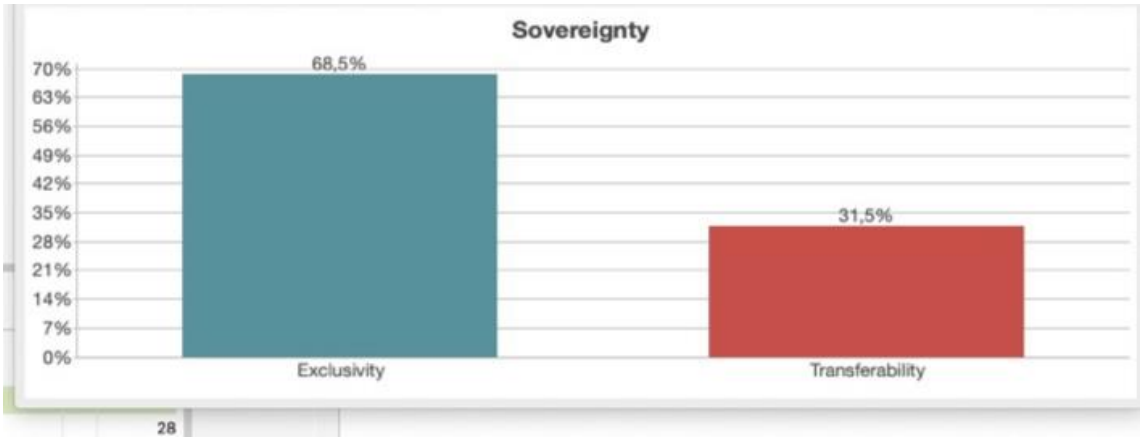
Beralih kedalam sub *nation* kedua adalah infrastructure (Raja Azrina Raja Othman, 2018). Pada dasarnya, infrastruktur menjadi fondasi dasar bagi Malaysia untuk mengembangkan keamanan siber. Infrastruktur menjadi landasar bagaimana Malaysia mengambil Langkah dalam menghadapi tantangan dan ancaman terhadap keamanan ruang siber yang juga dihadapi oleh negara lain. Dokumen strategi keamanan siber Malaysia dijadikan patokan karena sudah terkandung Analisa terkait bagaimana teknologi apa yang harus dikembangkan, kebijakan keamanan siber seperti apa yang harus di dirikan. Kebijakan keamanan siber Malaysia mulai dibentuk pada tahun 2005, hal tersebut di dorong oleh berbagai macam kasus penyerangan keamanan siber di Malaysia.

Application menjadi sub *nation* terakhir. Presentasenya berada pada jumlah 29,2%. Data tersebut menjelaskan bagaimana applikasi merupakan relasi antar actor baik individu, kelompok, negara, kelompok negara, dan level internasional. Aplikasi tersebut juga berhubungan dengan code lainnya karena menjadi hal dasar untuk mengembangkan keamanan siber dengan menjalin relasi antar entitas. Aplikasi menjadi garda terdepan untuk

melindungi keamanan manusia karena berhubungan erat dengan aktivitas yang dilakukan oleh manusia. Dengan di lindingunginya ruang siber seperti dunia maya, teknologi, dan lainnya hal tersebut juga akan menunjang keamanan manusia itu tersendiri karena akan melindungi keamanan data, tidak ada kebocoran data individu, kelompok, dan actor lain di ruang siber. Keamanan individu menjadi tugas utama bagi negara (*core*) untuk melindungi rakyat.

3.1.2 *Sovereignty*

Kategori kedua adalah *sovereignty, sovereignty* merujuk kepada sifat terhadap data yang akan dianalisa, apakah akan bersifat *exclusivity* (terbuka) atau *transferability* (tertutup). Data dibawah ini mempresentasikan bagaimana Analisa dokumen strategi keamanan siber Malaysia bersifat exklusif dengan persentase 68,5% berbanding dengan transferability yang memiliki presentase 31,5%



Sumber Hasil Penelitian (2020)

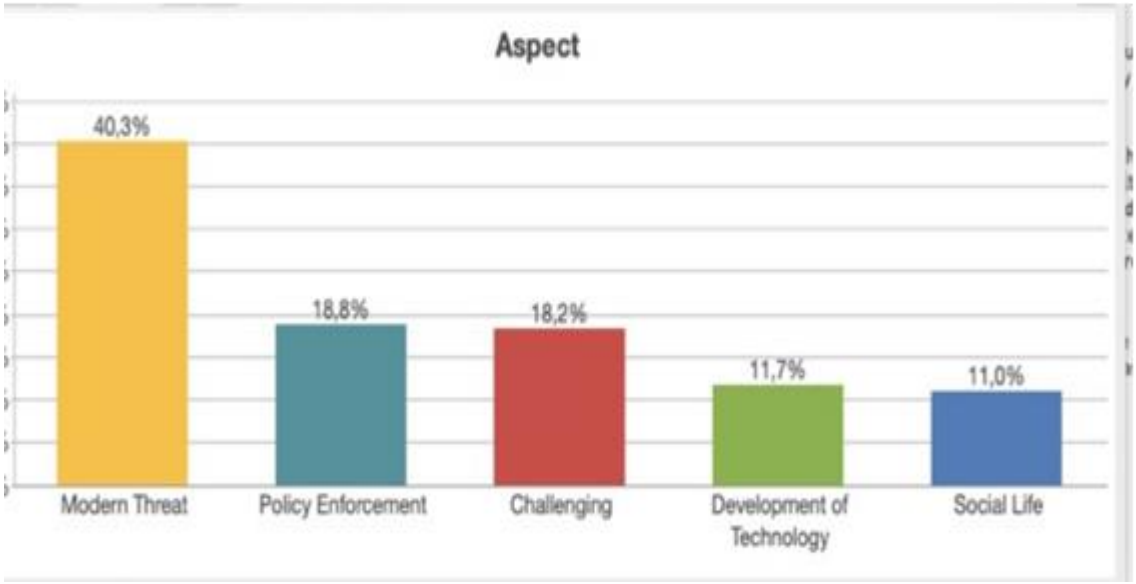
Gambar 4. Sifat Strategi Keamanan Siber Malaysia

Gambar 4 merupakan hasil olahan data melalui software MAXQDA guna memahami sifat dari strategi nasional keamanan siber Malaysia. Data diatas memberikan gambaran bagaimana Malaysia memiliki sifat yang didominasi dengan sifat eksklusif. Hal tersebut menjelaskan bahwa negara memiliki kekuasaan tertinggi dalam mengatur kebijakan dan strategi keamanan siber, mengantisipasi dan meminimalisir serangan keamanan di ruang siber. Negara juga menjadi kunci utama dalam menggerakan perkembangan perkembangan teknologi, mengatur perkembangan bisnis dampak dari keamanan siber.

Walau Malaysia memiliki persentasi 31,6 dengan sifat transferability namun tidak menutup kemungkinan bahwa Malaysia memiliki inisiatif untuk mengembangkan teknologi siber dengan melakukan Kerjasama dengan negara lain. Dokumen strategi keamanan siber Malaysia memaparkan bagaimana keamanan siber juga menjadi isu keamanan global, sehingga membutuhkan kerangka Kerjasama yang kuat, standar kebijakan dan teknologi yang tepat dan memadai, dan 75ersama-sama menghadapi ancaman yang dihadapi terkait keamanan ciber karena isu keamanan siber bersifat terbuka di ruang bebas. Isu penyerangan keamanan siber akan berdampak kepada negara lain sehingga hal tersebut menimbulkan kesepahaman untuk melakukan Kerjasama secara aktif, transparan dan berkelanjutan.

3.1.3 Aspek

Kategori terahir yang dianalisa adalah aspek. Data aspek pada penelitian ini akan diolah dan dianalisa dari dokumen strategi keamanan siber Malaysia pada tahun 2018. Analisa dokumen tersebut menjadi dasar dalam pemahaman bagaimana strategi keamanan siber Malaysia terbentuk dan diimplementasikan. Seperti yang sudah di jelaskan pada sub bab sebelumnya bahwa aspek didalam penelitian ini memiliki 5 sub aspek dengan 2 sub aspek pendukung yaitu *policy enforcement, economic effect, challenging, development of technology* dan *modern threat* dengan dua sub aspek pendukung yaitu *economic effect* dan Cyber Security Cases. Berikut penyajian data aspek ditunjukkan pada Gambar 5.



Sumber Hasil Penelitian (2020)

Gambar 5. Grafik Klasifikasi Strategi Keamanan Malaysia

Hasil klasifikasi data keamanan nasional siber Malaysia menggunakan Software MAXQDA. Dapat dilihat dari table diatas terkait pembahasan dalam dokumen keamanan siber Malaysia. Dokumen keamanan siber Malaysia memiliki angka yang tinggi dalam *Modern Threat dengan presentase* 40,3%. Malaysia memahami bahwa saat ini, Malaysia berada dalam situasi keamanan non tradisional yang terfokus kepada keamanan siber.

Dalam *modern threat,* terdapat sub aspek yaitu *economic effect* dan *cyber security cases*. Kedua kategori tersebut menjadi salah satu latar belakang dokumen strategi keamanan siber dilihat dari tingginya kasus criminal ruang siber di Malaysia. Selain itu, *modern threat* juga didorong oleh dampak ekonomi seperti bagaimana presentase pendapatan dalam pengembangan bisnis teknologi keamanan strategi atau dampak negative seperti pengeluaran terhadap pengembangan infrastruktur untuk mendorong kemajuan teknologi keamanan siber. Dalam konteks kejahatan siber, terdapat berbagai contoh seperti intrusi jaringan, penyebaran virus didalam system computer, pencurian identitas hingga indikasi Tindakan terorisme yang berdampak ke lingkungan internasional (Reddy & Reddy, 2014).

3.2. Korelasi Data

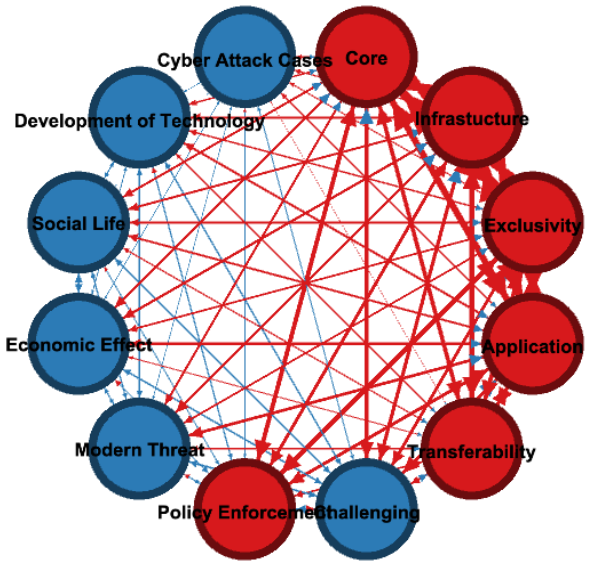
Data dibawah merupakan pengolahan data yang peneliti analisis menggunakan MAXQDA.

Code System	Asp...	Poli...	Chal...	Mod...	Eco...	Cyb...	Dev...	Soci...	Sov...	Excl...	Tran...	Nati...	Core	Appl...	Infra...
Aspect															
Policy Enforcement			12	6	8	4	7	5		27	10		27	20	20
Challenging		12		10	9	5	8	9		19	11		22	23	22
Modern Threat		6	10		6	3	8	7		11	8		13	18	17
Economic Effect		8	9	6		3	4	11		11	5		15	14	15
Cyber Attack Cases		4	5	3	3		2	1		6	1		6	7	7
Development of Technology		7	8	8	4	2		6		9	6		9	13	12
Social Life		5	9	7	11	1	6			11	7		13	12	13
Sovereignty															
Exclusivity		27	19	11	11	6	9	11			26		61	37	48
Transferability		10	11	8	5	1	6	7		26			25	23	29
Nation															
Core		27	22	13	15	6	9	13		61	25			41	50
Application		20	23	18	14	7	13	12		37	23		41		48
Infrastucture		20	22	17	15	7	12	13		48	29		50	48	

Sumber Hasil Penelitian (2020)

Gambar 6. Hasil Analisis MAXQDA

Gambar 6 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 Malaysia.



Sumber Hasil Penelitian (2020)

Gambar 7. Grafik Aspek Strategi Keamanan Malaysia

Gambar 7 menunjukan aspek satu dan aspek lainnya saling berkaitan satu sama lain, hal tersebut menunjukan bahwa hadirnya peran negara pada saat ini dalam enghadapi perkembangan teknologi, ancaman keamanan siber, penegakan hukum terkait tindak criminal siber sangat dibutuhkan. Globalisasi tidak menghilangkan otoritas, serta legitimasi pemerintah Malaysia. Berikut penjelasan lebih dalam terkait keterkaitan aspek. Gambar 8 merupakan hasil

pengolahan data keamanan nasional siber Malaysia yang telah diolah dari MAXQDA lalu dibentuk grafik melalui software Gephi.

Sumber Hasil Penelitian (2020)

Gambar 8. Grafik Strategi Keamanan Malaysia

Gambar 8 merupakan hasil analisa data menggunakan Gephi, dengan menggunakan fitur yang mempermudah untuk menelaah relasi data satu dengan data yang lainnya. Fitur tersebut dinamakan dengan *layout* Gephi. Hasil yang didapatkan dari olahan data tersebut adalah

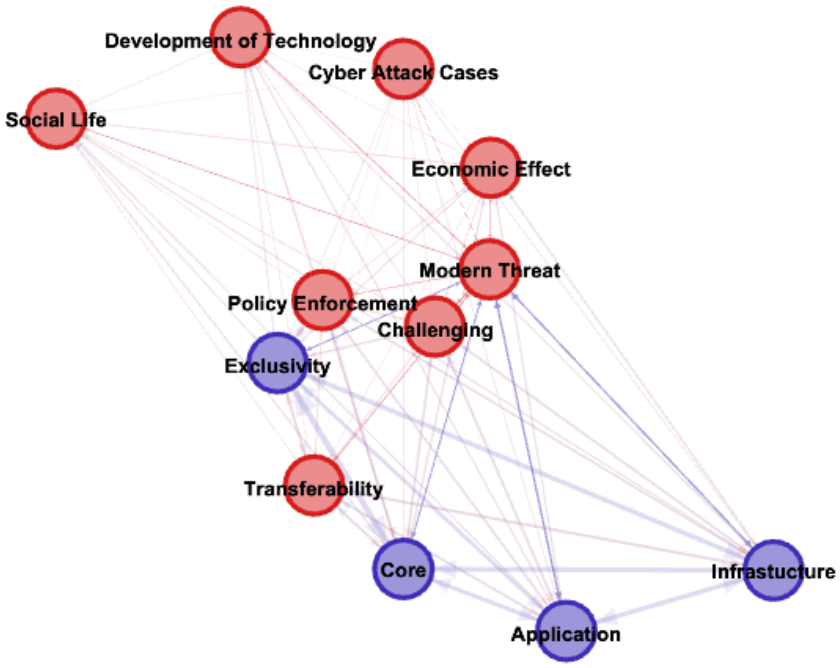
1. Cluster Merah terdiri dari berbagai *nodes* (berurutan dari besar ke kecil)*: Application, Infrastructure, Policy Enforcement, Exclusivity, Transferability,* dan *Core*.
2. Cluster Biru terdiri dari: *Cyber Attack Case, Modern Threat, Economic Effect, Social Life, Development of Technology, Challenging*

Cluster yang berwarna merah lebih mengarah kepada sifat yang terbuka, yang artinya strategi keamanan siber dilakukan Kerjasama demi mencapai kedamaian dan mengatasi ancaman strategi keamanan siber. Namun, berbeda dengan cluster biru, cluster biru menunjukan bagaimana sifatnya yang lebih tertutup, dimana cluster biru bersifat tertutup yang mengarah kepada kebijakan dan otoritas negara Malaysia dalam menindaklanjuti strategi keamanan siber Malaysia. Berikut akan peneliti jelaskan lebih jauh ditinjau dari sub aspek yang ada:

3.2.1. Modern Threat

Gambar 9 menunjukkan hasil olahan dari Gephi untuk meninjau aspek pertama yaitu *Cyber Threat. Cyber Threat* terhubung kedalam berbagai aspek lainnya. Pada hakikatnya, aspek ancaman modern tersebut terdiri dari dua sub aspek didalamnya yaitu *Economic.* Dalam sub aspect yaitu *economic effect*, inovasi, investasi menjadi elemen penting dalam mendapatkan dampak positif ekonomi dengan mendayagunakan kemampuan dalam mengolah berbagai media keamanan siber. Peluang tersebut menjadi tantangan untuk Malaysia dalam melakukan kompetisi secara terbuka dengan lingkungan Internasional.

Kompetisi tersebut dalam pengembangan teknologi informasi komunikasi dalam ruang siber sehingga Malaysia mendapatkan benefit seperti hak cipta, investasi dan berbagai hal lainnya. Namun, dalam dokumen tersebut dokumen keamanan siber Malaysia juga memaparkan bahwa hadirnya tantangan dalam ekonomi menjadi perhatian utama. Hal tersebut karena jika Malaysia tidak mendayagunakan kemampuan, sumber daya yang ada, maka Malaysia akan mengalami keruigian dalam bidang keamanan siber seperti mahalnya peralatan untuk keamanan ruang siber.



Sumber Hasil Penelitian (2020)

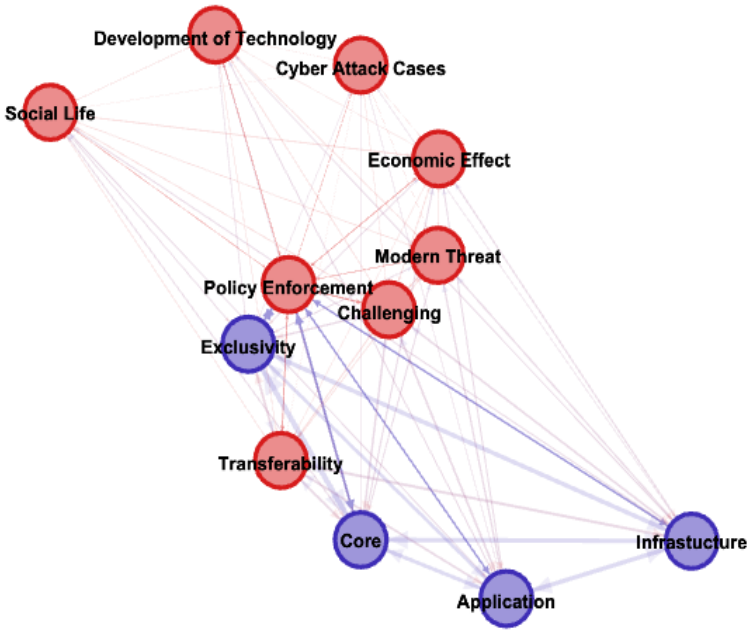
Gambar 9. Grafik Pengaguh Aspek *Modern Threat*

Berbeda dengan kasus penyerangan keamanan siber, dimana seperti dijelaskan dalam bab sebelumnya bahwa hadirnya peningkatan kasus penyerangan keamanan siber di Malaysia sehingga Malaysia membangun strategi keamanan sibernya demi menciptakan terjaganya keamanan siber di Malaysia demi membangun menghadapi berbagai macam ancaman keamanan siber (Perumal et al., 2018).

3.2.2. *Policy Enforcement*

Gambar 10 merujuk kepada *Policy enforcement* yang memiliki persentase 18,8%. Aspek ini menunjukan bahwa negara memainkan peran penting dalam strategi keamanan siber Malaysia. Kebijakan, kerangka kerja sama terhadap keamanan ruang siber tidak akan terealisasikan dan tidak dapat diaplikasikan jika tidak ada kebijakan yang jelas, penegak hukum yang tepat serta ruang lingkup seperti sanki terhadap para pemain ruang siber jika terdapat hal yang dilakukan diluar peraturan (Abdullah et al., 2018).

Peran negara mengalami penguatan dalam melakukan control, pengawasan, pengaplikasian kebijakan, mendeteksi ancaman dan memaksimalkan ruang siber untuk memenuhi kepentingan nasional. *The Royal Malaysian Police* (RMP) menjadi badan penegak utama dalam menangani keamanan ruang siber Malaysia yang terdiri dari berbagai kasus seperti kejahatan dalam perangkat komputer, internet dan kasus siber yang dapat mempengaruhi global (Kandan & Idris, 2010).



Sumber Hasil Penelitian (2020)

Gambar 10. Grafik Pengaguh Apek *Policy Enforcment*

Kebijakan keamanan siber tidak dapat dipisahkan dengan tantangan, peka terhadap perkembangan teknologi, memahami status quo yang terjadi di masyarakat. Sehingga *policy enforcement* menjadi salah satu aspek yang penting dalam mengoperasionalkan keamanan siber Malaysia.

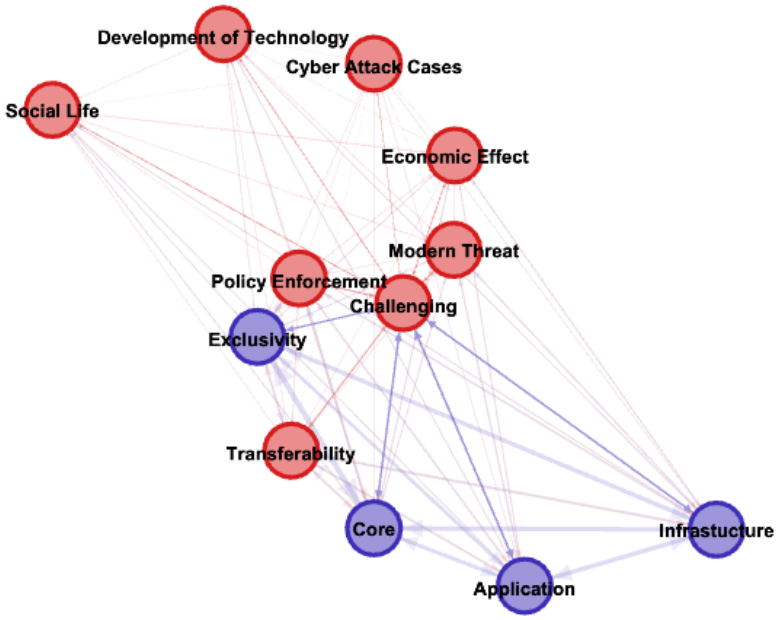
Kebijakan yang di terapkan oleh Malaysia dalam perlindungan keamanan data ruang siber diaplikasikan dengan ketat oleh pemerintah Malaysia dan aktor dari penegak hukum lainnya mengingat aksi kejahatan ruang siber Malaysia mengalami peningkatan.

3.2.3. Challenging

Gambar 11 merupakan hasil olahan dokumen strategi keamanan siber Malaysia yang menunjukan hadirnya tantangan dengan persentase 18,2%. Tantangan yang dihadapi oleh Malaysia terdapat di berbagai aspek seperti teknologi keamanan siber, konektivitas ICS, skills pengoperasian teknologi siber, hadirnya penyalahgunaan ruang siber seperti penyebaran hoax, anggaran dana, hadirnya kebocoran data pengguna dalam penggunaan ruang siber seperti di dunia maya, terjadinya berbagai Tindakan criminal terkait keamanan siber.

Tantangan tersebut menjadi tugas besar bagi Malaysia untuk menghadapi isu keamanan siber dengan meningkatkan potensi keamanan siber dengan melakukan kerja sama dengan berbagai pihak dari berbagai kalangan seperti individu, organisasi, negara, dan entitas lainnya demi menjaga keamanan data pengguna agar tidak disalah gunakan (Tamyez, 2019).

Tantangan tersebut pada hakikatnya menjadi tantangan bagi Malaysia dan lingkungan internasional sehingga dibutuhkan Kerjasama yang transparan, terbuka, berkelanjutan baik dalam teknologi, regulasi maupun *sharing knowledge* terhadap skill peningkatan pengoperasionalan ruang siber.

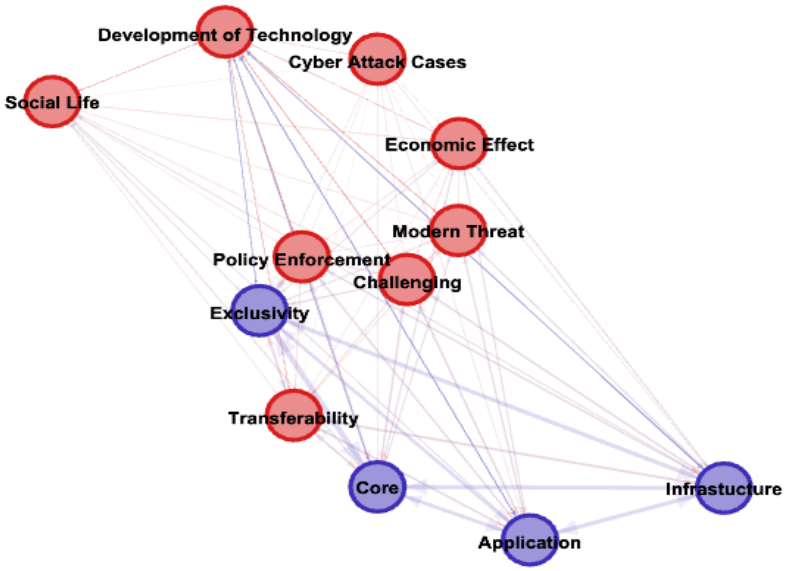


Sumber Hasil Penelitian (2020)

Gambar 11. Grafik Pengaruh Apek *Challenging*

3.2.4. Development of Technology

Gambar 12 menjelaskan bahwa, angka yang dimiliki dalam aspek pengembangan teknologi yaitu 11.7% dimana memberikan gambaran bahwa pengembangan teknologi menjadi kategori yang krusial dalam keamanan siber karena pengembangan teknologi terhubung ke berbagai sub aspek lain. Pengembangan teknologi dipengaruhi oleh berbagai faktor seperti kasus peyerangan data siber di berbagai infrastruktur yang tersedia, pengaruh ruang siber alam kehidupan social, dan bernegara (Supayah & Ibrahim, 2016).



Sumber Hasil Penelitian (2020)

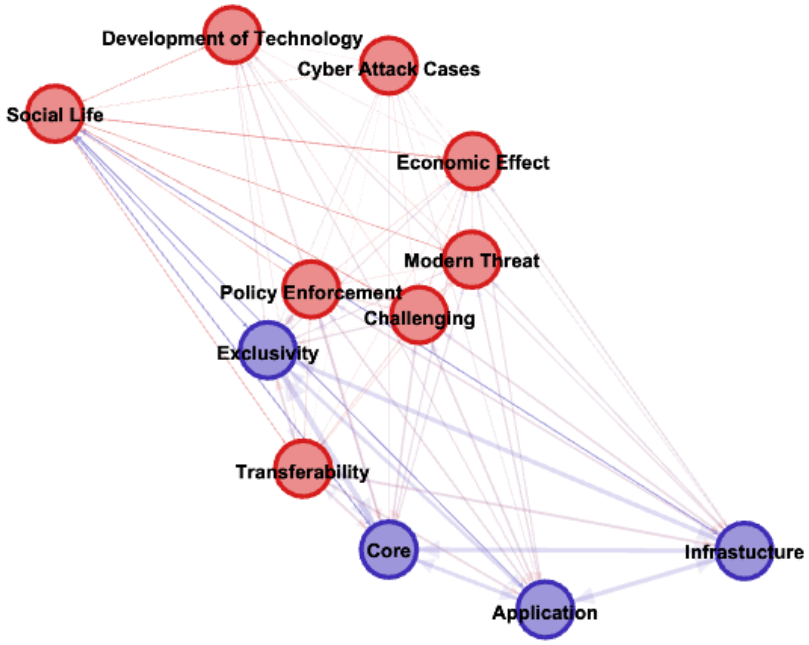
Gambar 12. Grafik Pengaguh Apek *Development Of Technology*

Perkembangan teknologi menjadi kunci utama dalam keamanan siber di Malaysia. Teknologi siber Malaysia merupakan proses evolusi dengan tujuan untuk mengamankan data siber yang dimiliki entitas yang ada di berbagai kalangan, baik keamanan individu, kelompok, negara, atau entitas lainnya (Supayah & Ibrahim, 2016). Sehingga pengembangan teknologi menjadi fondasi dasar bagi negara untuk mengamankan keamanan siber di ruang yang bebas dan terbuka baik dengan inovasi yang dibuat oleh berbagai actor didalam negeri maupun melakukan kerangka Kerjasama dengan negara lain.

Menjaga keamanan data ruang siber menjadi tantangan bagi berbagai aktor mengingat meningkatnya kejahatan dunia siber. Pemerintah dan organisasi yang focus terhadap keamanan data siber menjadi garda dalam pengamanan data ruang siber. Pemerintah dan aktor lain melakukan kerjasama pengamanan data ruang siber guna melindungi data dan menghindari aksi kejahatan di dunia siber.

3.2.5. Social Life

Gambar 13 menunjukkan bahwa *social life* memiliki persentase sebesar 11%. Social Life dalam dokumen strategi keamanan siber melingkupi keamanan masyarakat dari berbagai aspek yang berhubungan dengan keamanan siber seperti perlindungan data pengguna, terlindunya social media yang masyarakat miliki, hadirnya penegak hukum untuk korban yang menjadi korban penyalahgunaan data ruang siber.



Sumber Hasil Penelitian (2020)

Gambar 13. Grafik Pengaguh Apek *Social Life*

Masyarakat saat ini pada umumnya sangat bergantung kepada teknologi ruang siber, sehingga negara memiliki peran yang sangat penting untuk menjaga dan melakukan evaluasi terhadap berbagai kasus keamanan siber. Ketergantungan teknologi oleh masyarakat

menjadikan negara harus meningkatknya kapasitas dan kapabilitas dalam memelihara keamanan siber.

Keterbukaan akses data pengguna memiliki resiko yang tinggi, karena ruang siber memiliki sifat yang bebas dan terbuka sehingga negara perlu berkerja sama dengan pihak lain untuk memaksimalkan potensi perlindungan keamanan siber. Perlindungan keamanan siber meliputi infrastruktur ruang siber dengan mencegah, mendeteksi hingga menghadapi kendala dan insiden yang hadir di dunia maya (Tushar P Parikh, 2017).

Perlindungan data ruang siber pada era kontemporer menjadi hal krusial bagi berbagai entitas. Mengingat berkembangnya teknologi yang semakin pesat dan hadirnya sifat ketergantungan terhadap teknologi menjadikan tantangan terhadap peningkatan keamanan ruang siber. Perkembangan teknologi yang semakin canggih sejalan dengan meningkatnya kejahatan yang memiliki sifat flexible. Keamanan data entitas baik individu, organisasi, kelompok dan entitas lainnya menjadi tugas bagi para pengguna untuk lebih menjaga data dari ruang siber agar menghindari dan tidak mengalami kejahatan siber seperti penguntitan, pencurian data, penyebaran virus melalui jaringan computer.

4. Kesimpulan

Strategi keamanan siber Malaysia menjadi garda terdepan dalam melindungi data, jejaring, teknologi dan aspek lainnya baik dari pengguna maupun dari mitra. Perkembangan teknologi keamanan siber menjadi kunci utama bagi Malaysia guna membangun jaringan, data yang aman sehingga Kerjasama dengan berbagai mitra tidak terancam oleh isu keamanan non tradisional seperti serangan keamanan siber, hacking, jaringan yang terganggu dan lain sebagainya. Strategi keamanan siber membutuhkan pondasi dasar yaitu regulasi yang tepat, kapasitas dan kapabilitas yang mengikat serta kerangka Kerjasama dengan berbagai pihak dengan aman dan terjaga agar tantangan keamanan strategi bisa diatasi oleh Malaysia dan berbagai pihak. Berbagai aspek telah diteliti sehingga dapat memberikan sebuah gambaran bagaimana tantangan terhadap keamanan siber di dalam negeri maupun lingkungan internasional. Standar regulasi dengan berbagai mitra yang akan bekerja sama dengan Malaysia juga akan memberikan dampak yang tinggi terhadap berbagai aspek seperti peningkatan ekonomi, perlindungan kepada para pengguna dunia maya, website, dan jejaring lainnya.

Daftar Pustaka

Abdullah, F., Salwa Mohamad, N., Yunos, Z., Malaysia, C., & Kembangan, S. (2018). Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. *Journal of Cyber Security*, *1*, 22–31.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

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

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kandan, M. J., & Idris, N. A. (2010). *Guidelines on Computer Security*. 1–32.

Perumal, S., Pitchay, S. A., Samy, G. N., Shanmugam, B., Magalingam, P., & Albakri, S. H. (2018). Transformative cyber security model for Malaysian government agencies. *International Journal of Engineering and Technology(UAE)*, *7*(4), 87–92. https://doi.org/10.14419/ijet.v7i4.15.21377

Raja Azrina Raja Othman. (2018). *CYBER SECURITY Towards A Safe and Secure Cyber Environment*.

Reddy, G. N., & Reddy, G. J. U. (2014). *A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies*. http://arxiv.org/abs/1402.1842

Supayah, G., & Ibrahim, J. (2016). An Overview of Cyber Security in Malaysia. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *6*(4), 12–20. https://doi.org/10.12816/0036698

Tamyez, P. F. (2019). *The Challenges and Solutions of Cybersecurity Among Malaysian Companies*. *April*, 103–125. https://doi.org/10.4018/978-1-5225-9078-1.ch005

Tushar P Parikh, A. R. P. (2017). Cyber security : Study on Attack , Threat , Vulnerability. *International Journal of Research in Modern Engineering and Emerging Technology*, *5*(6), 1–7.