Insignia Journal of International Relations
Edisi Khusus, Januari 2021, 66-80
P-ISSN: 2089-1962; E-ISSN: 2597-9868

Analisis Konten dalam Strategi Keamanan Siber Kuwait Berdasarkan Teori *Three Perspective Theory of Cyber Sovereignty*

Afrizal Fajri
Paramadina Graduates School of Diplomacy, Universitas Paramadina
Email: afrizalfajri@gmail.com

Abstrak

Perkembangan ruang siber saat ini begitu cepat dan dinamis berpengaruh pada banyak aspek kehidupan sosial masyarakat. Seperti layaknya dua hal yang kontradiktif, pastinya perkembangan ini membawa aspek yang tidak hanya positif namun juga negatif. Pada aspek positif, perkembangan teknologi ini membawa banyak kesempatan dan peluang baru terhadap sejarah peradaban manusia. Namun dengan keberadaan medium baru ini pula memunculkan jenis – jenis aktivitas kejahatan dengan metode baru dan diperlukan kemampuan yang lebih untuk menjaga infrastruktur teknologi informasi. Penelitian ini berusaha untun menganalisis strategi ruang siber Kuwait dalam dokumen strategi sibernya menggunakan metode analisis konten untuk mengetahui bagaimana fokus dan pendekatan yang diambil oleh Pemerintah Kuwait dalam mengatur ruang siber. Kerangka teori yang digunakan dalam penelitian ini menggunakan pendekatan *Three Perspective Theory of Cyber Sovereignty* yang menjelaskan pembagian lapisan dalam konteks kedalautan di ruang siber. Metode penelitian yang digunakan adalah metode campuran (*mix method*) untuk mengetahui aspek atau pendekatan apa yang lebih dominan dalam upaya Pemerintah Kuwait mengelola ruang siber di negaranya. Hasil dari penelitian ini mengindikasikan Kuwait cenderung mengambil kebijakan pada lapisan ekslusif (*core layer*). Aspek utama yang ditemukan dalam analisis ini adalah dalam hal bagaimana strategi mitigasi ancaman yang dapat hadir melalui ruang siber. Ini menunjukkan kebijakan yang ada pada level ekslusif dimana asumsi utamanya adalah kehadiran negara sangat diperlukan untuk membuat aturan dan pengelolaan dalam ruang siber.

Kata kunci*:* kedaulatan, Kuwait, siber

Abstract

Development of cyberspace is currently so fast and penetrates all aspects of social life. like two contradictory things, this development has implications that are not only positive but also negative. on the positive aspect, technology brings new opportunities for the advancement of human civilization. but with this new space it also brings more varied crimes and also the need for protection of information technology infrastructure. This research seeks to analyze Kuwait's cybersecurity strategy in its cybersecurity document using content analysis methods in understanding the focus and approach taken by the Kuwait's government. The theoretical framework used in this research uses Three Perspective Theory of Cyber Sovereignty which explains the division of layers in the context of sovereignty in cyberspace. The method used is a mixed method to determine which aspects and approaches are more dominant in the Kuwaiti government policy to manage cyber space in the country. Results of this study indicate that Kuwait tends to take policies that are in the exclusive layer. The main aspect is in terms of preventing threats that can exist through cyberspace. This shows that Kuwait's cyberspace policy tends to be exclusive, in the sense that the state must be present and regulate most of the cyberspace area.

Keywords: *cybersecurity, Kuwait, sovereignty*

PENDAHULUAN

Perkembangan dalam teknologi informasi merubah pola kegiatan masyarakat di berbagai aspek. Termasuk dalam ranah Hubungan Internasional, teknologi informasi telah menciptakan ruang baru dalam berinteraksi yaitu ruang siber. Mengenai siber ini, hubungan internasional memiliki diskursus dan perhatian tersendiri terhadapnya.

Beberapa aspek dalam hubungan internasional bersinggungan langsung dengan ruang yang dihadirkan oleh teknologi internet ini. Salah satu isu yang cukup menjadi perhatian adalah isu kedaulatan. Sifat dari teknologi internet yang cenderung bebas dan tidak terbatas wilayah menjadi tantangan tersendiri bagi kedaulatan negara. Peluang dan tantangan hadir bersamaan dengan perkembangan teknologi ini.

Strategi, kebijakan, dan langkah–langkah taktis perlu dikembangkan untuk mencegah isu–isu yang hadir dalam ruang siber seperti serangan siber (*cyber attack*) yang dapat melumpuhkan sistem teknologi informasi dan mengganggu aktivitas – aktivitas ekonomi masyarakat. Negara perlu melakukan upaya yang besar dalam sektor kemanan siber, mengevaluasi setiap perubahan kondisi sebagai dampak perkembangan teknologi, mengidentifikasi risiko dan ancaman, membuat target capaian sesuai dengan kebutuhan dan prediksi di masa yang akan datang, dan mengembangkan strategi dan kebijakan, serta mengimplementasikannya secara efektif (Mustafa, 2020).

Dalam merespon isu tersebut, Kuwait memiliki strategi terkait keamanan siber. Strategi tersebut tertuang dalam dokumen yang berjudul "*National Cyber Security Strategy for the State of Kuwait 2017-2020*". Penelitian ini bertujuan untuk menganalisa strategi Kuwait dalam merespon kehadiran ruang siber. Kerangka kerja yang digunakan dalam menganalisa mengadopsi dari teori "*Three Perspective Theory of Cyber Sovereignty*" yang ditulis oleh Hao Yeli. Kerangka teori ini mencoba menjelaskan bagaimana aspek dalam suatu negara dapat dibagi kedalam lapisan (*layer*) sesuai dengan sifatnya.

Analisis dilakukan dengan cara intepretasi terhadap isi dokumen yang kemudian di kuantifikasi dengan bantuan aplikasi MAXQDA. Hasil kuantifikasi tersebut kemudian diolah menjadi jaringan relasi antar aspek yang ditemukan menggunakan aplikasi GEPHI.

Kerangka Teori

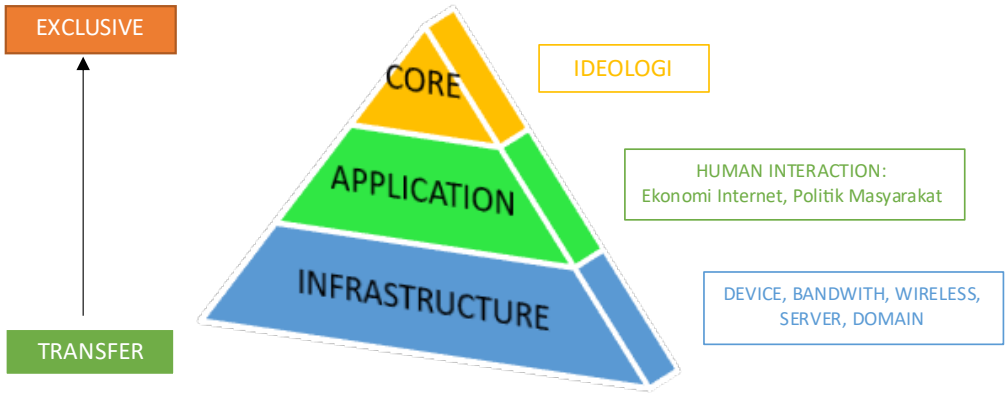
Keamanan ruang siber muncul menjadi tantangan global dalam diskursus tentang isu kedaulatan negara. Perdebatan muncul dalam agenda–agenda internasional mengenai bagaimana aturan diberlakukan dalam ruang siber, dan tantangan yang bersifat revolusioner terhadap tata kelola global di ruang siber. Kedaulatan siber menjadi fokus kontroversi yang cukup menyita perhatian (Yeli, 2017). Menurut Yeli (2017), ada tiga isu utama yang membuat ruang ini menjadi kontroversial.

Pertama adanya kontradiksi antara kedaulatan siber dan spirit yang dibawa oleh internet. Kedaulatan secara klasik telah dipahami sebagai kewenangan yang otonom terhadap suatu wilayah. Apabila ini diterapkan dalam ruang siber, maka akan terjadi fragmentasi dalam internet yang mengusung semangat tanpa batasan wilayah. Kedua, adanya kontradiksi antara kedaulatan siber dan HAM. Ini berkaitan dengan kebebasan berpendapat yang dibawa oleh internet akan berbenturan dengan intervensi negara atas nama kedaulatan siber yang cenderung akan melakukan restriksi terhadap kebebasan arus informasi. Ketiga, kontradiksi antara kedaulatan siber dengan keterlibatan berbagai pihak dalam pemerintahan. Hal ini berkaitan dengan tantangan bagi pola pemerintahan dimana internet memberi ruang yang sangat terbuka bagi berbagai pihak untuk ikut terlibat dalam tata kelola pemerintahan.

Walaupun kedaulatan secara tradisional dipahami sebagai hal yang esklusif, kedaulatan siber paling tidak harus mampu mengakomodir adanya transfer kontrol otoritas dalam era globalisasi ini (Yeli, 2017). Maka dari itu, Yeli memandang perlunya kerangka kerja yang dapat dijadikan acuan untuk membagi aspek–aspek mana yang menjadi domain bagi

negara dan sifatnya mutlak tidak dapat di intervensi (ekslusif) dan aspek mana yang didalamnya dapat melibatkan banyak pihak dan sifatnya bukan merupakan ancaman langsung terhadap haluan negara (transfer). Kerangka kerja ini yang kemudian diberi nama "*Three Perspective Theory of Cyber Sovereignty*".

Dalam menaganalisis strategi ruang siber Kuwait yang tertuang dalam dokumen strategi keamanan siber Kuwait berjudul "*National Cyber Security Strategy for the State Of Kuwait 2017-2020*" digunakan kerangka teori "*Three Perspective Theory of Cyber Sovereignty*" yang dikemukakan oleh Hao Yeli. Teori ini menjelaskan tentang piramida pembagian 3 *layer* / lapisan dalam struktur kedaulatan siber suatu negara. Pada puncak piramida disebut *Core*, kemudian diikuti *Application* di tengah, dan *Infrastructure* pada lapisan paling dasar piramida. Semakin di puncak piramida, aspek yang dibahas bersifat semakin *exclusive*. Sedangkan apabila di level dasar piramida, aspek tersebut bersifat terbuka atau *transfer.*



Sumber: Yeli, 2017.

Gambar 1
Lapisan Kedaulatan Siber

Dari kerangka teori pada gambar 1, dapat dijelaskan pembagian aspek dalam kedaulatan siber. Kerangka ini berbentuk segita yang memiliki 3 (tiga) lapisan dimana setiap lapisan merefleksikan tingkat urgensi dan seberapa jauh aktor–aktor di dalamnya dapat terlibat.

Pada lapisan paling atas dijelaskan bahwa aspek yang dikategorikan sebagai lapisan *core* atau *layer* tertinggi apabila berbicara tentang ideologi, hukum, keamanan, dan tata kelola pemerintahan. Dimana pada aspek ini merupakan sesuatu yang tidak dapat ditoleransi perlu keterlibatan negara sebagai pondasi untuk menjaga kepentingan nasional bangsa. Hal ini berangkat dari tiap negara yang memiliki kondisi sosial masyarakat yang dapat berbeda satu sama lain, sehingga pada lapisan ini hanya pemerintahan terkait yang dapat berperan lebih dan akses dari pihak eksternal tentunya akan sangat dibatasi.

Selanjutnya pada lapisan kedua, yaitu *Application,* berbicara tentang aspek kegiatan masyarakat dengan memanfaatkan ruang siber. Pada lapisan ini terlibat didalamnya berbagai *paltform* dan operator internet yang dalam dunia nyata telah terintegrasi dengan berbagai aspek kehidupan sehari–hari seperti perdagangan, aktivitas ekonomi, interaksi sosial, dan lain–lain. Level ini perlu dibuka aksesnya secara lebih luas dibanding pada lapisan pertama supaya terjadi kerja sama dan interaksi baik menyesuaikan dalam skala lokal, regional, maupun internasional. Salah satu aktivitas yang dapat masuk dalam level ini adalah apa yang disebut dengan *Cyberactivism,* yaitu konsep gerakan

sosial dimana menggunakan sumber daya internet atau ruang siber. Keberhasilan gerakan ini ditentukan berdasar seberapa banyak sumber daya yang didapatkan untuk memperbesar dukungan.

Dan lapisan terakhir *Infrastructure* berbicara tentang aspek yang lebih teknikal dan tata kelola teknologi informasi secara fisik. Lapisan ini berbicara tentang kemampuan infrastruktur yang perlu terus ditingkatkan untuk mencapai standar internasional guna mendukung interkonektivitas global. Level ini menganjurkan negara untuk mentransfer wewenangnya supaya tercapai interkonektivitas tersebut. Keterlibatan berbagai *stakeholder* dapat dibuka dan diizinkan untuk mengelola aspek–aspek yang berada pada level ini. Negara yang memiliki teknologi maju memiliki tanggungjawab untuk mengambil inisiatif dalam proyek perluasan standar konektivitas global ini kepada negara–negara yang memiliki teknologi lebih terbelakang. Hal ini dirasa penting karena semakin tingginya pengguna internet dan kemajuan teknologi, kebutuhan akan keamanan sistem juga semakin besar sebagai akibat terintegrasinya berbagai layanan. Negara maju perlu melakukan transfer teknologi dan inovasi yang telah dicapai untuk menyelesasikan adanya kesenjangan teknologi.

Terlihat dari sifat kedaulatannya, pada level Ekslusif maka negara akan membatasi keterlibatan pihak eksternal untuk terlibat. Sedangkan di lever transfer, aspek tersebut bersifat lebih terbuka sehingga sangat memungkinkan adanya *sharing* dari berbagai pihak baik informasi secara teknikal ataupun modernisasi infrasturktur alat–alat teknologi.

Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian *mixed method*. Menurut Creswell (2014), metode penelitian campuran (*Mixed Method*) merupakan pendekatan penelitian dengan mengkombinaskan antara penelitian kualitatif dengan penelitian kuantitatif. Penelitian *mixed method* akan berguna bila metode kuantitatif atau kualitatif tidak cukup akurat digunakan sendiri-sendiri dalam permasalahan penelitian, atau dengan menggunakan *mixed methood* akan dapat memperoleh pemahaman yang paling baik.

Sumber data yang digunakan dalam penelitian ini adalah sumber data sekunder yang diperoleh melalui *desk research* berupa dokumen yang berkaitan dengan penelitian yang sedang dilakukan. Sumber sekunder adalah sumber yang memberikan data kepada pengumpul data secara tidak langsung seperti melalui orang lain atau lewat dokumen (Sugiyono, 2013). Dalam melakukan analisis terhadap strategi keamanan *cyberspace* yang dilakukan oleh Kuwait, pertama kali yang dilakukan yaitu dengan mencari dokumen resmi dari Kuwait terkait strategi *cyber-security.* Dokumen ini kemudian akan dianalisis secara kontesktual dan kemudian dibuat kategori atau klasterisasi dengan bantuan aplikasi MAXQDA. Kategori atau klaster disusun atas hasil intepretasi terhadap aspek–aspek yang ditemukan dan dibahas dalam dokumen tersebut.

Setiap aspek yang ditemukan akan dicatat atau diklasifikasi ke dalam kerangka kerja (*Framework*) yang telah kita bangun di dalam aplikasi MAXQDA berdasarkan pendekatan teori yang digunakan pada pembahasan sebelumnya. Proses yang disebut kuantifikasi data ini dilakukan dengan membaca setiap paragraf/ kalimat/ frasa dalam dokumen strategi *cyber-security* Kuwait sampai selesai. Kuantifikasi data dalam aplikasi MAXQDA dibangun dengan suatu struktur yang disebut *code*. *Code* adalah setiap aspek/ kategori hasil intepretasi dari data tekstual. *Framework* yang di dapat dari telaah teori juga di translasi menjadi *code–code* di dalam aplikasi MAXQDA.

Strategi Keamanan Siber Kuwait

Strategi keamanan siber Kuwait tertuang dalam dokumen berjudul "*National Cyber Security Strategy for the State Of Kuwait 2017-2020*". Bagian ini akan membahas lebih lanjut tentang intepretasi strategi keamanan siber Kuwait serta aspek-aspek yang diatur oleh otoritas setempat. Berdasar telaah teori dan penelurusan dokumen, struktur *code* yang dibangun dalam analisis ini memiliki 3 (tiga) unsur utama yaitu: *Nation*, *Sovereignty*, dan *Aspects.*

Code {*Nation*} memiliki *sub-code* {*Core, Application,* dan *Infrastructure*}. *Code* ini menjelaskan tentang pembagian *layer* atau lapisan terhadap setiap aspek kehidupan dalam negara. Sesuai dengan kerangka teori, tiga lapisan ini menjelaskan bagaimana seharusnya negara mengelola ruang siber dan aspek – aspek mana saja yang harus dijaga secara ekslusif dan mana yang dapat di transfer dengan berbagai *stakeholder.*

Code {*Sovereignty*} berisi *sub-code* {*Exclusive* dan *Transfer*}. Keduanya merupakan sifat dari kedaulatan (*Sovereign*) yang melekat pada negara. Sifat ekslusif mengindikasikan bahwa hanya kewenangan tertentu yang dapat mengelolanya dan cenderung akan membatasi akses atau keterlibatan dari pihak eksternal. Sedangkan sebaliknya, pada sifat transfer menganjurkan bahwa aspek tersebut dapat dan perlu dikelola melibatkan banyak pihak guna mencapai suatu tujuan tertentu yang lebih baik.

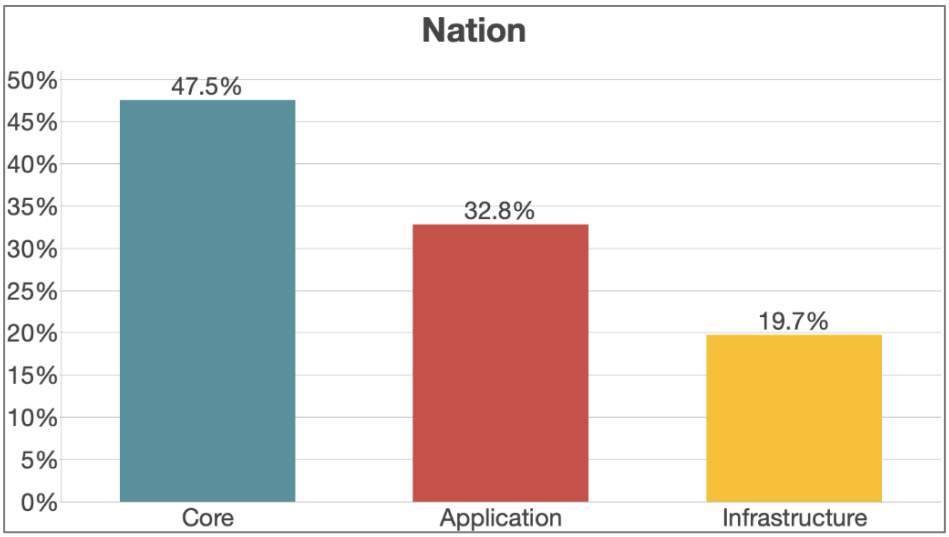
Code {*Aspects*} terdiri dari *sub-codes*: {*Economic Growth, Development of Civilization, Cyberspace Threats, The Need of Knowledge, Criminal Activities, Terorism, Cooperation and Collaboration, Threats Mitigation Strategies, State Governance, Private Sectors, Fundamental Rights, Transfer, Exclusive, Core, Application, Infrastructure*}. *Sub-codes* tersebut adalah hasil intepretasi dari penelurusan dokumen *cyber-security* Kuwait.

Aspek–aspek tersebut merupakan representasi dari keseluruhan sektor yang disinggung dalam kaitannya dengan strategi keamanan siber Kuwait. Lebih lanjut dijelaskan berikut.

Nation

Hasil dari analisis dalam *code Nation* ditemukan bahwa *layer Core* menempati presentase yang paling besar (47,5%) kemudian diposisi kedua *layer Application* (32,8%) dan terakhir adalah *layer Infrastructure* (19,7%).

Data gambar 2 di bawah menunjukkan bahwa dokumen strategi keamanan siber Kuwait sebagian besar membahas aspek–aspek yang ada pada *layer Core*. Sesuai telaah teori, segala hal yang berkaitan dengan ideologi negara ada pada *layer* ini. Maka, dapat kita pahami bahwa Kuwait sangat mementingkan segala hal yang menyangkut upaya menjaga ideologi negara. Implikasinya, strategi yang dilakukan oleh Kuwait dominan untuk mencegah penyalahgunaan ruang siber yang dapat mengancam keamanan dan ideologi.



Sumber: Diolah oleh Penulis, 2020.

Gambar 2
Code Nation

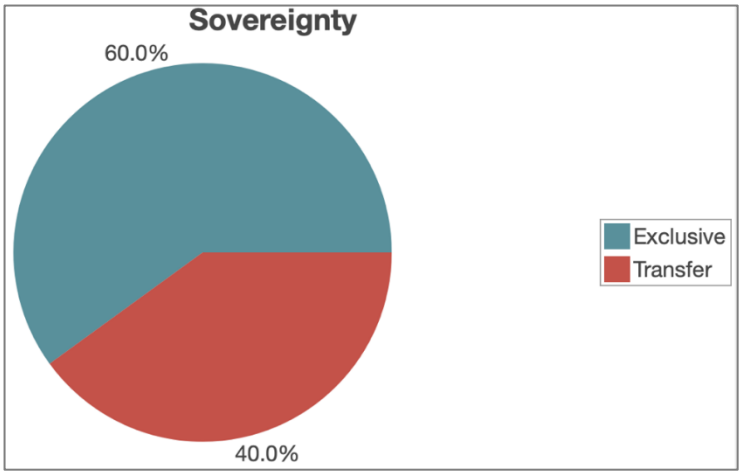
Pada *layer Application* angka yang didapat juga lumayan besar. Hal ini mengindikasikan bahwa Kuwait juga memperhatikan kegiatan masyarakatnya dalam medium siber. Negara hadir dengan melakukan *monitoring* pemanfaatan media digital dalam aktivitas masyarakat seperti perdagangan elektronik, sektor keuangan, dan aktivitas sosial.

Sedangkan pada *layer infrastructure*, walaupun mendapat angka hampir menyentuh 20 persen tidak menjadikan aspek ini menjadi prioritas utama dalam strategi Kuwait. Modernisasi peralatan Teknologi Informasi tidak terlalu menjadi isu yang banyak dibahas dalam dokumen strategi tersebut.

Sovereignty

Apabila pada *code Nation* kita membagi 3 *layer* aspek tata kelola negara di dalam ruang siber, pada *code Sovereignty* kita akan mengulas sifat aspek–aspek tersebut menjadi 2 yaitu terbuka (*Transfer*) atau cenderung lebih tertutup (*Exclusive*). Hasil pada penelusuran dokumen strategi siber Kuwait adalah sebagai berikut:

Sumber: Diolah oleh Penulis, 2020.



Gambar 3
Code Sovereignty

Diagram *sovereignty* (gambar 3) diatas menunjukan bahwa aspek yang diatur dalam strategi siber Kuwait bersifat cenderung tertutup (*Exclusive)* dengan persentase cukup mutlak diangka 60% dibanding yang lebih bersifat terbuka (*Transfer*) sebesar 40%. Data ini cukup sinkron dengan diagram hasil Analisa *Nation* dimana *code Core* memiliki presentase yang paling besar walapun tidak terlalu mutlak masih dibawah 50%. Secara teoritis, *Core* ada pada posisi puncak dalam segitiga *layer* "*Three Perspective Theory of Cyber Sovereignty*" dan semakin dipuncak maka sifat kedaulatannya akan semakin *Exclusive.* Dalam diagram *Nation*, dapat disimpulkan bahwa aspek *Application* cenderung berada posisi *exclusive* karena cukup menyumbang presentase yang signifikan pada diagram *Sovereignty* sehingga kedaulatan dengan sifat ekslusif cukup unggul mutlak pada diagram ini dengan angka 60%.

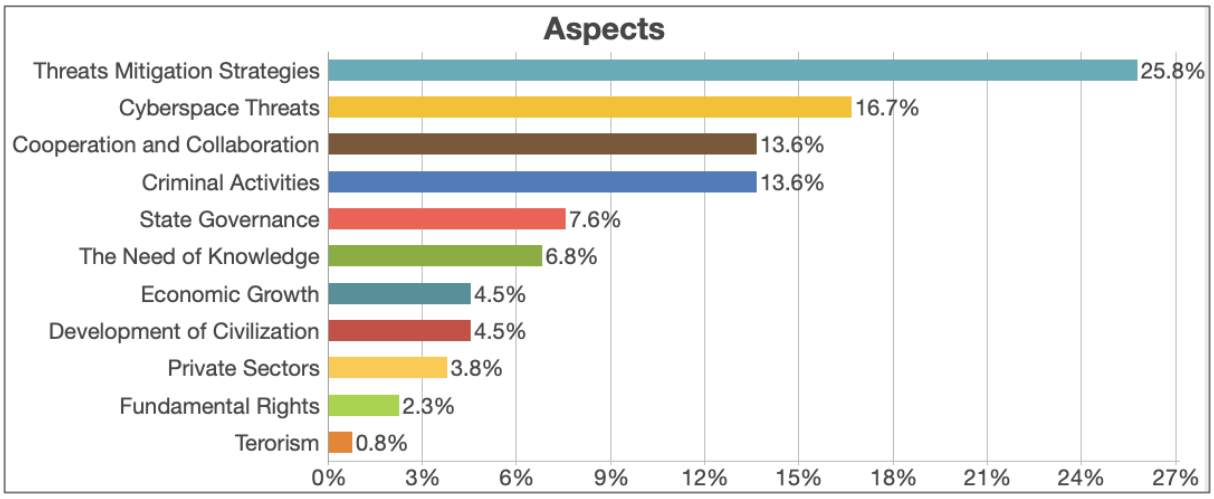
Hal lain yang dapat kita pahami dari data tersebut adalah bahwa dengan komposisi statistik seperti ini menunjukan Kuwait akan cenderung membatasi akses pihak eksternal untuk terlibat dalam aspek siber-nya. Selain itu, Kuwait juga tidak akan terlalu aktif dalam aktivitas *sharing knowledge* dan *infrastructure* teknologi informasi karena strategi yang dirancangnya memang lebih bersifat tertutup/ eksklusif. Menurut Radon, kedaulatan merupakan kekuasaan absolut atas suatu wilayah tertentu. Kekuasaan absolut atas wilayah tersebut menjadi dasar bagi pembentukan negara (Radon, 2004). Maka dari itu wajar jika Kuwait melakukan pendekatan yang bersifat ekslusif terhadap wilayahnya.

Dalam kerangka hubungan antar negara, kedaulatan juga merujuk pada pengertian kemerdekaan (*independence*) dan *vice versa*. Suatu negara merdeka adalah negara yang berdaulat. Negara yang berdaulat adalah negara merdeka dan tidak berada di bawah kekuasaan negara lain (Bartelson, 2006).

Aspects

Setelah menelusuri pembagian *layer* dan sifat kedaulatannya, bagian ini akan menjelaskan sektor atau aspek apa saja yang berkaitan dengan strategi siber Kuwait. Metode yang dilakukan dalam kalsterisasi aspek ini adalah dengan melakukan intepretasi terhadap frasa/ kalimat/ paragraf di seluruh isi dokumen strategi siber Kuwait.

Klasterisasi aspek ini dirasa penting untuk memahami secara komprehensif keterlibatan berbagai sektor berkaitan dengan strategi yang disusun oleh Kuwait, bukan hanya memahami sifat serta pembagian *layer* kedaulatannya saja. Aspek yang ditemukan adalah sebagai berikut:



Sumber: Diolah oleh Penulis, 2020.

Gambar 4
Aspek dalam Dokumen Strategi Siber Kuwait

Gambar 4 di atas menunjukkan keterlibatan aspek–aspek yang baik secara tekstual maupun kontekstual disebutkan dalam dokumen strategi siber Kuwait. Sebagaimana yang dapat kita lihat, bahwa aspek yang berkaitan dengan upaya mitigasi ancaman *cyberspace* menduduki posisi paling atas dengan 25,8% disusul dengan ancaman–ancaman dalam *cyberspace* (*Cyberspace Threats*) sebesar 16,7% dan kemudian aspek Kerja sama serta Perbuatan Kriminal memiliki angka yang sama 13,6%. Lima besar aspek ditutup oleh Tata Kelola Pemerintahan sebesar 7,6%.

Komposisi aspek ini telah merepresentasikan isi dari dokumen strategi siber Kuwait dimana di dalamnya memang sebagian besarnya adalah membahas upaya mitigasi hal–hal yang bersifat negatif dan dianggap mengancam stabilitas negara. Hal tersebut terlihat jelas dari lima besar aspek dengan presentase tertinggi yang menyebutkan secara spesifik aksi kriminal pada posisi 4 dan ancaman–ancaman siber secara umum di posisi 2 adalah hal negatif yang perlu diantisipasi.

Keberadaan aspek *State Governance* di posisi 5 juga memperkuat analisa awal kita dimana menyebut sifat kedaulatan dalam strategi ini yang cenderung ekslusif. Kuwait menaruh perhatian utama pada lembaga–lembaga pemerintahannya sebagai aktor untuk melakukan tindakan mitigasi serta intervensi bila dirasa ada hal yang mengancam stabilitas negara.

Aspek kerja sama di posisi 3 menggambarkan perlunya ada kolaborasi antarlembaga baik di pemerintahan maupun dengan pihak swasta. Namun, pembahasan pihak swasta sendiri hanya ada di peringkat 9 dengan persentase 3,8% yang mengindikasikan bahwa memang kehadiran negara dalam hal ini adalah sebagai aktor utama.

Relasi Data

Relasi data digunakan untuk melihat nilai keterhubungan dalam jejaring relasi aspek yang telah kita temukan sebelumnya. Dalam aplikasi MAXQDA, sebelumnya kita telah melakukan klasterisasi aspek berdasar intepretasi terhadap suatu data tekstual. Klasterisasi tersebut kemudian dapat kita konversi menjadi matriks yang menunjukan nilai keterhubungan antar aspek sebagai berikut:

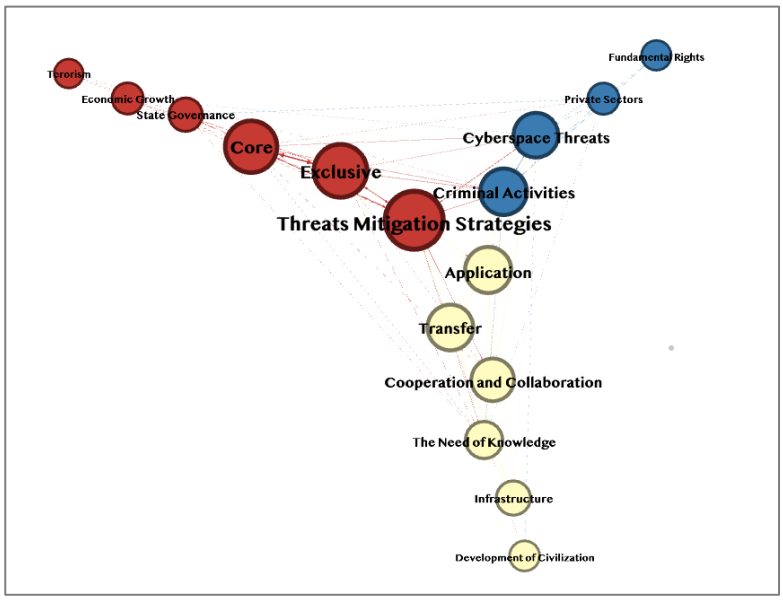
Code System	Asp...	Eco...	Dev...	Cyb...	The ...	Cri...	Tero...	Coo...	Thre...	Stat...	Priv...	Fun...	Sov...	Tran...	Excl...	Nati...	Core	Appl...	Infra...
Aspects																			
Economic Growth			1	1					2						1		2	2	
Development of Civilization		1		1					1					1				2	
Cyberspace Threats		1	1		2	8		4	8		2	1		3	3		4	3	2
The Need of Knowledge				2		3		2	4	1	1			2	2		1	3	2
Criminal Activities				8	3		1	3	6		2	3		4	6		5	5	
Terorism						1									1		1		
Cooperation and Collaboration				4	2	3			6					10	1		1	9	1
Threats Mitigation Strategies		2	1	8	4	6		6		3				5	15		13	8	3
State Governance					1				3		2				4		4		
Private Sectors				2	1	2				2		1					1		
Fundamental Rights				1		3					1								
Sovereignty																			
Transfer			1	3	2	4		10	5									11	8
Exclusive		1		3	2	6	1	1	15	4							27	2	
Nation																			
Core		2		4	1	5	1	1	13	4	1				27				
Application		2	2	3	3	5		9	8					11	2				
Infrastructure				2	2			1	3					8					

Sumber: Diolah oleh Penulis, 2020.

Gambar 5
Relasi Data

Angka–angka pada matriks gambar 5 menunjukan seberapa kuat hubungan antaraspek yang terjadi. Semakin besar angkanya maka semakin kuat hubungan antaraspek tersebut. Guna mempermudah analisa hubungan antar aspek tersebut, selanjutnya akan dibuat *network analysis* dari matriks tersebut. Prosedur yang dilakukan adalah dengan mengkonversi data matriks ini menjadi jaringan relasi dengan bantuan aplikasi GEPHI.

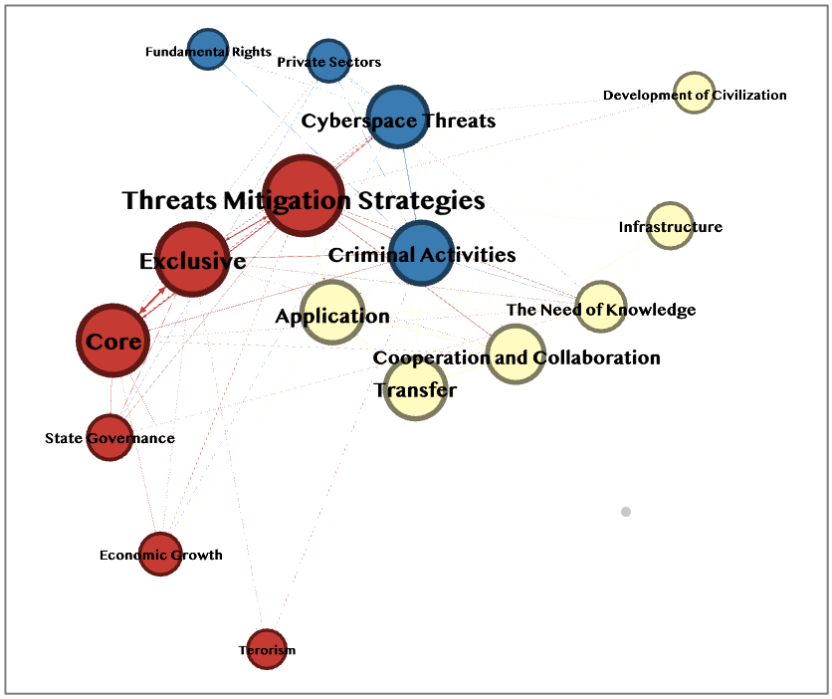
Untuk melakukannya, data matriks dari MAXQDA tersebut terlebih dahulu di-*export* menjadi file *excel*. Setelah itu data kemudian di-*import* ke dalam aplikasi GEPHI sehingga terbentuk jaringan relasi data sebagai berikut:



Sumber: Diolah oleh Penulis, 2020.

Gambar 6
Relasi jaringan antaraspek

Dapat terlihat aplikasi GEPHI membentuk relasi jaringan Gambar 6 dengan 3 klaster utama yaiut klaster warna Merah, Biru, dan Putih. Supaya memudahkan dalam proses analisis, modifikasi terhadap tampilan/ *layout* bisa dilakukan sebagai berikut:



Sumber: Diolah oleh Penulis, 2020.

Gambar 7
Modifikasi tampilan relasi jaringan antaraspek

Ketiga klaster di atas dapat dirinci sebagai berikut :

a. Klaster Merah berisi *Nodes*: *Threats Mitigation Strategies, Exclusive, Core, State Governance, Economic Growth, Terorism.*
b. Klaster Biru berisi *Nodes: Criminal Activities, Cyberspace Threats, Private Sectors, Fundamental Rights.*
c. Klaster Putih berisi *Nodes: Application, Transfer, Cooperation and Collaboration, The Need of Knowledge, Infrastructure.*

Dari jaringan relasi tersebut kita dapat melihat klasterisasi isu yang ada. Pertama, klaster merah menggambarkan aspek– aspek yang bersifat ekslusif. Paling kuat adalah isu tentang upaya mitigasi ancaman *cyberspace*. Kemudian berturut – turut adalah *State Governance, Economic Growth, dan Terorrism.* Pada klaster ini kehadiran serta intervensi negara sangat tinggi karena masuk dalam kategori aspek–aspek yang menentukan stabilitas negara.

Klaster biru menjelaskan aspek–aspek yang terlibat dalam kategori aktivitas yang merupakan ancaman dari *cyberspace*. Terbentuknya klaster ini mengindikasikan bahwa Kuwait melihat siber sebagai medium yang sangat berbahaya. Berbagai aktivitas kriminal dapat dilakukan dan perlu menjadi perhatian serius. Maka kemudian klaster ini sangat sangat berhubungan dengan klaster sebelmunya (merah) dan menempatkan mitigasi ancaman siber menjadi aspek yang paling kuat.

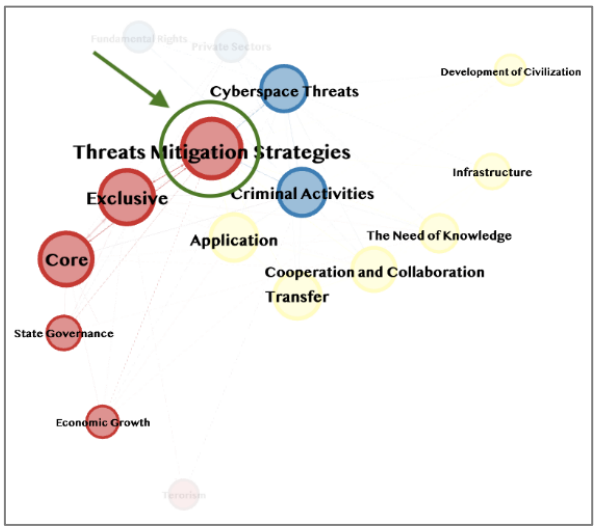
Klaster putih adalah klaster yang cenderung terbuka. Artinya keterlibatan pihak ekternal diluar negara sangat diijinkan dalam klaster ini. Intervensi negara tidak terlalu besar dan *sharing knowledge* maupun transfer teknologi sangat lazim dalam klaster ini. Beberapa aspek yang terlibat dalam klaster ini adalah

Cooperation and Colaboration, *The Need of Knowledge, Infrastructure,* dan *Development of Civilization.*

Analisis lebih lanjut akan dijelaskan pada pembahasan relasi jaringan tiap aspek pada poin–poin berikut.

Threats Mitigation Strategies

Aspek ini merupakan aspek yang mendominasi dalam dokumen strategi Kuwait. Dari sini kita dapat mengetahui bahwa siber menurut Kuwait adalah ruang yang sangat riskan dan berbahaya. Maka dari itu, aspek ini hampir memiliki relasi dengan seluruh aspek yang lain, yaitu dari klaster Merah: *Exclusive, Core, State Governance, Economic Growth, Terorism.* Dari klaster Biru: *Criminal Activities* dan *Cyberspace Threats.* Sedangkan dari klaster Putih: *Application, Transfer, Cooperation and Collaboration, The Need of Knowledge, Infrastructure.*

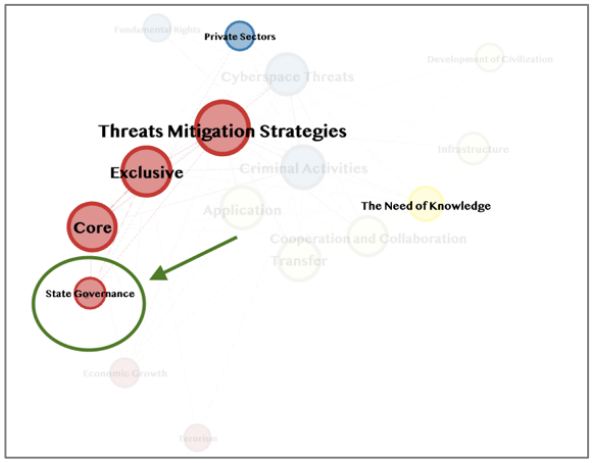


Sumber: Diolah oleh Penulis, 2020.

Gambar 8
Threat Mitigation Strategies

State Governance

Aspek ini menjelaskan lembaga–lembaga atau badan milik negara. Dari jaringan relasi terlihat aspek ini berada pada klaster ekslusif yang memang porsi kehadiran negara begitu besar disini. Maka dari aspek tidak terlalu memiliki banyak relasi dengan aspek yang lain, yaitu dari klaster Merah: *Threats Mitigation Strategies, Exclusive, Core, State Governance.* Dari klaster Biru hanya *Private Sectors* dan juga dari klaster Putih hanya *The Need of Knowledge.*

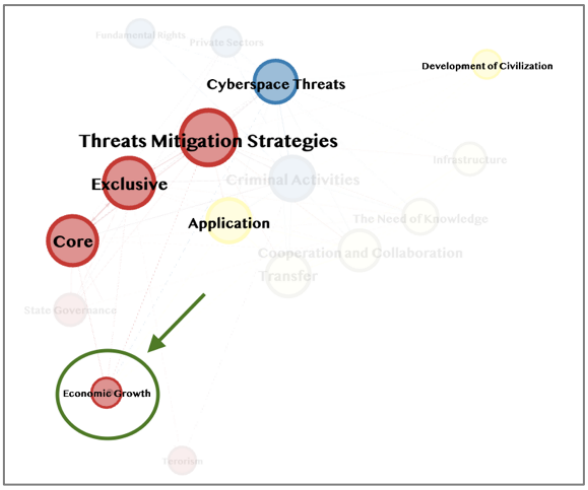


Sumber: Diolah oleh Penulis, 2020.

Gambar 9
State Governance

Economic Growth

Aspek ini menjelaskan upaya atau hal–hal yang terkait dengan pertumbuhan ekonomi. Apabila bicara ekonomi, peran negara memang begitu dibutuhkan untuk menjamin terjaganya situasi pasar yang kondusif. Bila kita perhatikan aspek ini hanya memiliki relasi dari klaster Merah: *Threats Mitigation Strategies, Exclusive,* dan *Core.* Dari klaster Biru hanya *Cyberspace Threats* dan juga dari klaster Putih ada *Applicatiom* dan *Development of Civilization.* Keterkaitan dengan klaster putih menunjukan bahwa aspek ini juga perlu melibatkan sektor–sektor lain. Sementara hubungannya denga *cyber threats* menandkan bahwa aspek ini dapat terganggu stabilitasnya dari berabagi Tindakan yang tidak konstruktif melalui media siber.



Sumber: Diolah oleh Penulis, 2020.

Gambar 10
Economic Growth

Terrorism

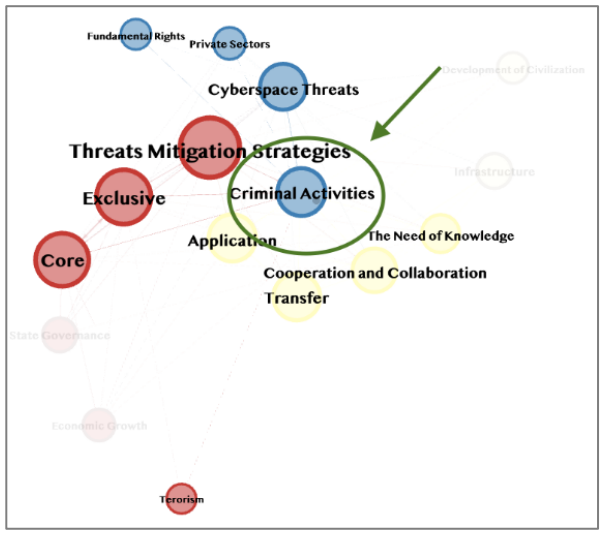
Terorisme tidak menjadi perhatian yang cukup serius. Tercatat hanya satu kali aspek ini dibahas dalam dokumen. *Node* juga digambarkan kecil yang menunjukan bahwa tidak terlalu signifikan. Aspek ini hanya sedikit memiliki relasi dari klaster Merah: *Exclusive* dan *Core* dan dari klaster Biru hanya *Criminal Activities*.

Sumber: Diolah oleh Penulis, 2020.

Gambar 11
Terrorism

Criminal Activities

Aktivitas kriminal menjadi aspek yang mengambil porsi cukup besar. Kuwait memang menaruh perhatian serius terhadap hal ini dengan seringkali menyebut bermacam–macam aksi kriminalitas pada dokumen strategis-nya. Maka aspek ini cukup banyak memiliki relasi dengan aspek yang lain, yaitu dari klaster Merah: *Threat Mitigation Strategies, Exclusive, Core, Terrrorism.* Dari klaster Biru: *Cyberspace Threats, Private Sectors, dan Fundamental Rights.* Sedangkan dari klaster Putih: *Application, Transfer, Cooperation and Collaboration,* dan *The Need of Knowledge.*



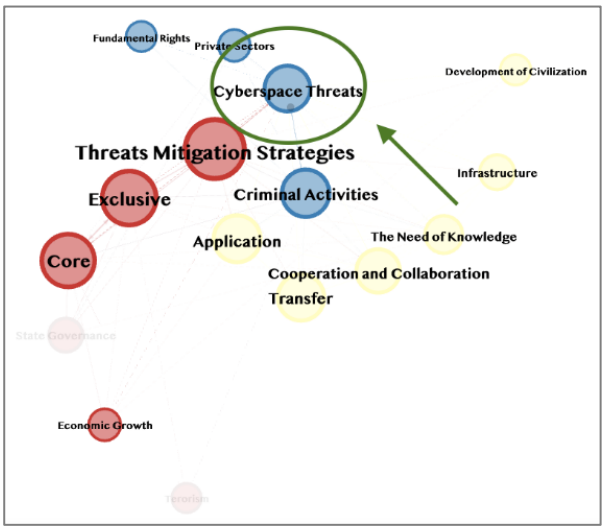
Sumber: Diolah oleh Penulis, 2020.

Gambar 12
Criminal Activities

Cyberspace Threats

Sama seperti kriminialitas, ancaman siber menjadi aspek yang porsinya sama besar. Keduanya merupakan perhatian utam Kuwait dalam dokumen strategi sibernya. Aspek ini hampir memiliki relasi dengan seluruh aspek yang lain, yaitu dari klaster Merah: *Threat Mitigation Strategies, Exclusive, Core, Economic Growth.* Dari klaster Biru: *Criminal Activities*, *Private Sectors,* dan *Fundamental Rights.* Sedangkan dari klaster Putih: *Application, Transfer, Cooperation and Collaboration, The Need of*

Knowledge, Infrastructure, Development of Civilization.

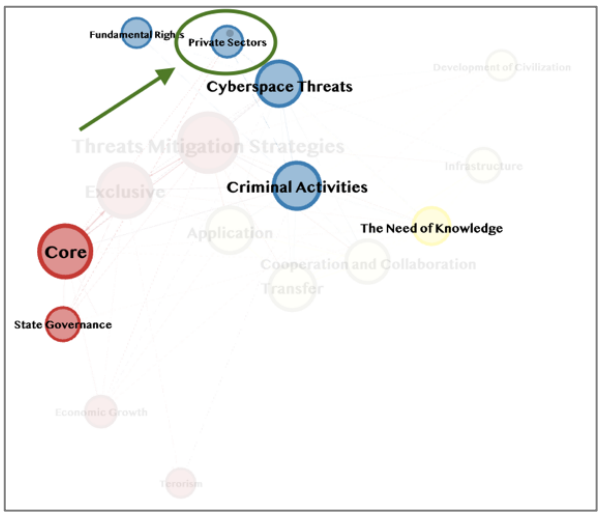


Sumber: Diolah oleh Penulis, 2020.

Gambar 13
Cyberspace Threats

Private Sectors

Keterlibatan sektor swasta tidak terlalu menjadi perhatian. Terlihat dari *node* yang hanya terbentuk kecil dalam jaringan relasi tersebut. Aspek ini hanya memiliki relasi dengan klaster Merah: *Core, State Governance.* Sedangkan dari klaster Biru: *Criminal Activities*, *Cyberspace Threats,* dan *Fundamental Rights.* Dari klaster Putih hanya *The Need of Knowledge.*

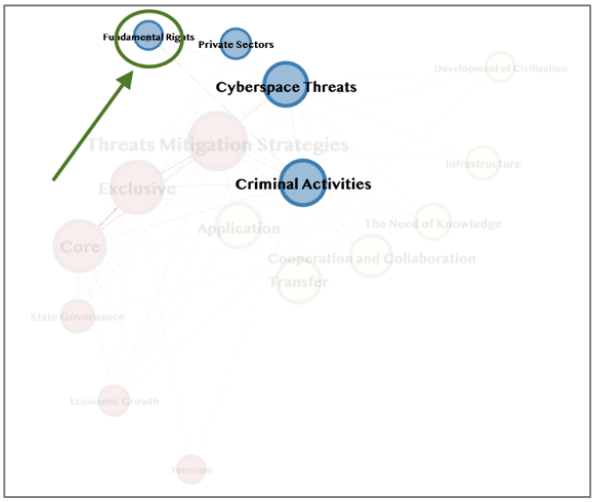


Sumber: Diolah oleh Penulis, 2020.

Gambar 14
Private Sectors

Fundamental Rights

Sama seperti *Private Sectors,* aspek ini tidak terlalu signifikan dan tidak terlalu banyak dibahas. Aspek ini hanya memiliki relasi dari klaster Biru yaitu: *Criminal Activities*, *Cyberspace Threats,* dan *Private Sectors.*

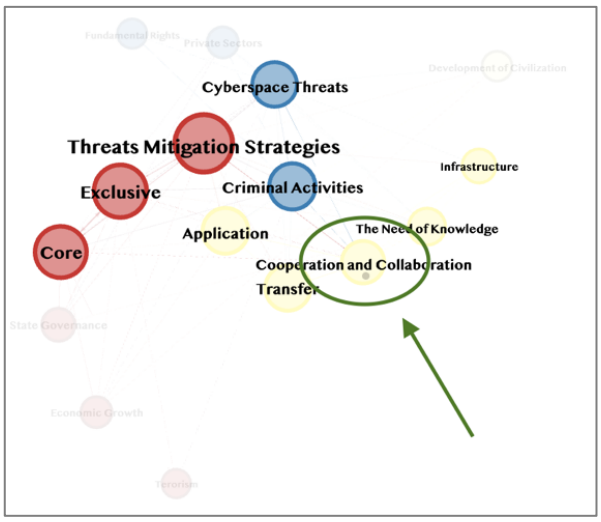


Sumber: Diolah oleh Penulis, 2020.

Gambar 15
Fundamental Rights

Cooperation and Collaboration

Aspek ini tentu berada pada klaster putih yang bersifat terbuka/ transfer. Pada dokumen strategi siber Kuwait kerja sama yang dilakukan menitikberatkan pada kolaborasi antar lembaga pemerintah dan swasta dalam menangani ancaman–ancaman siber. Keterlibatan pihak eksternal tentu cukup tinggi pada aspek ini. Karena luasnya sektor yang dicakupi, maka aspek ini memiliki banyak relasi dengan aspek lain, yaitu dari klaster Merah: *Threat Mitigation Strategies, Exclusive, Core.* Dari klaster Biru: *Criminal Activities, Cyberspace Threats.* Sedangkan dari klaster Putih: *Application, Transfer, The Need of Knowledge,* dan *Transfer.*

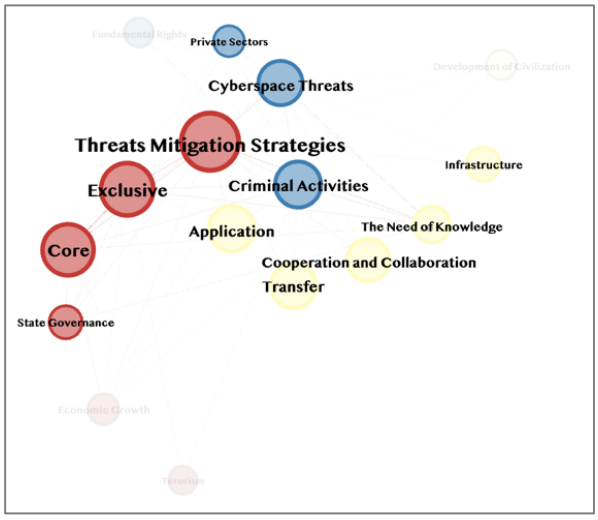


Sumber: Diolah oleh Penulis, 2020.

Gambar 16
Cooperation and Collaboration

The Need of Knowledge

Sharing Knowledge tentu hal yang lazim dilakukan untuk meningkatkan kemampuan SDM di bidang siber. Guna mensiasati berbagai ancaman siber, dibutuhkan SDM yang kompeten untuk merancang dan mengoperasikan infrastruktur keamanan siber. Kuwait menyadari betul bahwa kurangnya keterampilan di bidang ini akan berisiko terhadap keamanan sibernya. Maka aspek ini berada pada klaster terbuka karena diperlukan interaksi dan transfer ilmu pengetahuan. Karena banyak sektor yang terlibat membuat Aspek ini juga banyak relasi dengan aspek lain, yaitu dari klaster Merah: *Threat Mitigation Strategies, Exclusive, Core, State Governance.* Dari klaster Biru: *Criminal Activities, Cyberspace Threats, Private Sectors.* Sedangkan dari klaster Putih: *Application, Transfer, Cooperation and Collaboration, The Need of Knowledge,* dan *Infrastructure.*

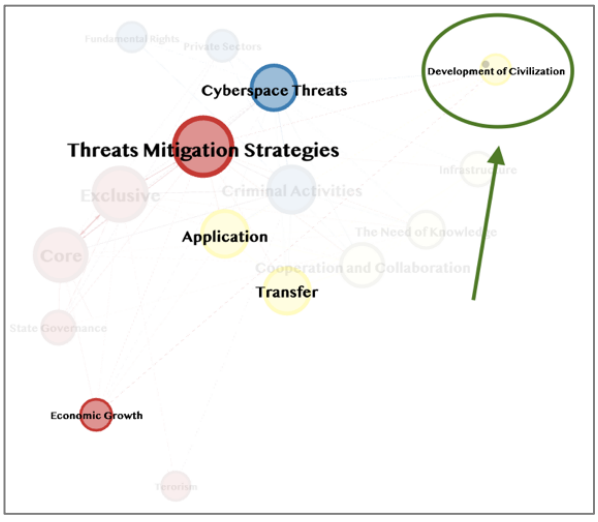


Sumber: Diolah oleh Penulis, 2020.

Gambar 17
Need of Knowledge

Development of Civilization

Aspek ini tidak terlalu banyak dibahas dalam dokumen strategi siber Kuwait. Hal ini mempertegas bahwa prioritas Kuwait terhadap strategi sibernya adalah untuk melakukan mitigasi terhadap ancaman yang dapat terjadi. Aspek ini memiliki relasi dari klaster Merah: *Threats Mitigation Strategies* dan *Economic Growth.* Dari klaster Biru hanya *Cyberspace Threats.* Sedangkan dari klaster Putih ada *Application* dan *Transfer.*



Sumber: Diolah oleh Penulis, 2020.

Gambar 18
Development of Civilization

KESIMPULAN

Penelitian ini menunjukan bahwa pendekatan yang dilakukan oleh Kuwait dalam merespon isu siber lebih bersifat eksklusif atau cenderung tertutup. Dokumen strategi yang dirilis oleh Kuwait cenderung melihat bahwa ruang siber bersifat berbahaya dan perlu untuk dilakukan strategi untuk memitigasi ancaman yang dapat hadir. Apa yang dilakukan Kuwait ini dapat dipahami sesuai dengan paradigma realis dalam hubungan internasional, yang menempatkan negara sebagai aktor utama dan harus hadir guna mempertahankan kedaulatan dan stabilitas negara.

DAFTAR PUSTAKA

Bartelson, Jens. (2006). The Concept of Sovereignty Revisited. *European Journal of International Law*, *17*(2), 463-474.

Creswell, J. W. (2013). *Research Design: Pendekatan Kualitatif, Kuantitatif dan Mixed*. Terjemahan Fawaid, A. Yogyakarta: Pustaka Pelajar.

Hong, Yu & Goodnight, G. (2019). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication*, 13, 1-19. DOI: 10.1080/17544750.2019.1687536.

Senol, Mustafa & Karacuha, Ertugrul. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*, 2020, 1-19. DOI: https://doi.org/10.1155/2020/5267564.

Radon, Jenik. (2004). Sovereignty: A Political Emotion, Not A Concept. *Stanford Journal of International Law*, *40*(195), 195-210.

Shen, Yi. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, 1, 81-93. DOI: 10.1007/s41111-016-0002-6.

Sugiyono, Sugiyono. (2013). *Memahami Penelitian Kualitatif*. Bandung: Alfabeta.

Yeli, Hao. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM*, *7*(2), 109–115.