Jurnal Kajian Ilmiah
e-ISSN: 2597-792X, ISSN: 1410-9794
Vol. 21 No. 2 (Mei 2021), Halaman: 195 – 208
Terakreditasi Peringkat 5 (SINTA 5) sesuai SK RISTEKDIKTI Nomor. 3/E/KPT/2019

Strategi Lebanon Dalam Meningkatkan Keamanan Ruang Siber

Alfonsus Maria de Liguori Sakunab [1], Anggraeni Silvia [1,*]

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

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

Submitted: **06/04/2021**; Revised: **16/04/2021**; Accepted: **11/05/2021**; Published: **27/05/2021**

Abstract

Cybersecurity has attracted attention in the study of international relations. This issue is important because most of life is connected to cyberspace. This research analyzes Lebanon's cybersecurity strategy in its official cybersecurity documents. The theoretical framework used in this study is the Three Perspective Theory of Cyber Sovereignty. The theory is explaining the division of layers in the context of sovereignty in cyberspace. The method used in this research is quantitative research obtained through the MAXQDA and GEPHI. The applications that are used in this research are to provide evidence of data in the Lebanese national strategy document. The results of this study indicate that the Lebanese security strategy documents tend to be exclusive. The Lebanese government is more dominant in discussing matters that are administrative, theoretical, principal, and planning.

Keywords: *Cyber Security, Sovereignty, Strategy, Lebanon*

Abstrak

cKeamanan siber merupakan salah satu isu yang menarik perhatian dalam studi hubungan internasional. Isu ini menjadi penting tatkala hampir sebagian besar unsur kehidupan terhubung ke ruang siber. Penelitian ini berupaya menganalisis strategi keamanan siber Lebanon dalam dokumen resmi kemananan sibernya. Kerangka teori yang digunakan dalam dalam penelitian ini menggunakan *Three Perspective Theory of Cyber Sovereignity* yang menjelaskan pembagian lapisan dalam konteks kedaulatan di ruang siber. Metode yang digunakan ialah metode penelitian kuantitatif yang diperoleh melalui aplikasi MAXQDA dan GEPHI untuk memberikan bukti data dalam menganalisis dokumen strategi keamanan nasional Lebanon. Hasil penelitian ini menunjukkan bahwa dokumen strategi keamanan siber Lebanon cenderung bersifat eksklusif. Pemerintah Lebanon lebih dominan membahas hal-hal yang bersifat administratif, teoretis, prinsipil dan perencanaan.

Kata kunci: Keamanan Siber, Kedaulatan, Strategi, Lebanon

1. Pendahuluan

Teknologi, informasi dan komunikasi menjadi elemen penting pada abad 21 yang mana dimanfaatkan dalam berbagai lini kehidupan, keamanan siber menjadi hal prioritas bagi seluruh negara. Setiap negara dengan kekuatan dan kapasitasnya membuat strategi dalam mengatur keamanan sibernya. Upaya ini sebagai cara untuk mempertahankan kepentingan negara dan kedaulatan. Selain itu, keamanan siber dalam sebuah negara sebagai tindakan preventif dalam menghadapi serangan yang mengganggu keamanan nasional. Pada zaman digital, manusia

memiliki ketergantungan terhadap perangkat digital, yang praktis dan masif adalah berupa menyampaian layanan pengirim berbasis teks, audio dan video yang terintegrasi dalam sebuah aplikasi. Ketergantungan ini membuka celah baru mengenai keamanan siber baik secara individu maupun secara organisasi maupun entitas di sebuah negara (Maharsi, 2000).

Menyikapi fenomena perkembangan di dunia saat ini, maka negara perlu merancang dan mengatur strategi yang tepat dalam aspek ketahanan dan keamanan nasional dalam ruang siber. Berkaitan dengan itu, pemerintah Lebanon pun telah memiliki strategi keamanan siber yang mengatur dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. Strategi keamanan siber nasional Lebanon disusun berdasarkan semangat kehidupan berbangsa dan bernegara. Strategi ini tentu sebagai acuan bersama bagi semua warga, organisasi dan pemerintah untuk menjaga *national interest*.

Tujuan dari penulisan ini adalah menganalisis dokumen strategi keamanan Siber Lebanon secara kualitatif. Analisis ini bertolak dari pemahaman tentang konsep kedaulatan yang dapat ditemukan dalam strategi keamanan siber Lebanon. Setelah memahami teori kedaulatan dan aspek-aspeknya, penulis kemudian mencoba untuk menganalisis dokumen ini secara kuantitatif tentang peran institusi, kebijakan pemerintah, interaksi sosial dan peningkatan internet. Semua aspek yang dibahas dalam dokumen ini berguna untuk melindungi negara dari serangan dan terlebih sebagai strategi kemanan nasional Lebanon.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini ialah dengan menggunakan aplikasi analisis MAXQDA dan Gephi. Melalui aplikasi MAXQDA, penulis membuat *coding* terhadap isi dokumen strategi keamanan siber Lebanon berdasarkan kerangka teori kedaulatan negara dan aspek. Terdapat tiga garis besar yang dicoding dalam dokumen ini yakni *Nation, Sovereignity* dan *Aspects*.

Data kualitatif diperoleh dengan menggunakan aplikasi MAXQDA. Pengelolaan analisis melalui aplikasi dapat membantu untuk memberikan bukti data guna memperkuat penulis dalam menganalisis dokumen strategi keamanan siber Lebanon.

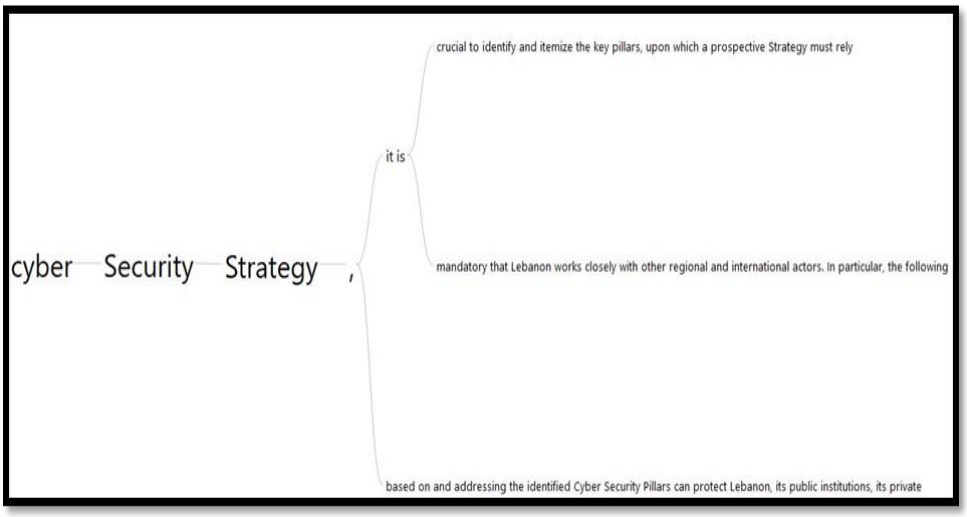
3. Hasil dan Pembahasan

Penulis menganalisis strategi keamanan siber Lebanon dengan membaca dan memahami teori kedaulatan dalam *Three Perspective Theory of Cyber Sovereignity* yang menjelaskan pembagian lapisan dalam konteks kedaulatan di ruang siber. Teori ini dipahami dalam pembagian kategori, yakni: *core, application, infrastructure* – yang kemudian mengarah pada dua sifat kedaulatan yakni kedaulatan *exclusive* (tertutup) dan kedaulatan yang bersifat *transfer* (terbuka).

Teori kedaulatan terbagi dalam tiga lapisan/unsur. Secara singkat dapat dikatakan bahwa lapisan *Core* membahas mengenai sikap, pemikiran atau ideologi sebuah negara. *Core* biasanya cenderung bersifat *exclusive.* Lapisan ini menekankan bahwa peran tertinggi terletak

pada otoritas internal dan kemerdekaan negara yang tidak dapat diganggu gugat oleh negara lain. Selanjutnya, aspek *Application* lebih memfokuskan pada upaya kerjasama dalam berbagai bidang kehidupan demi pengembangan keamanan nasional. Maka itu, *Application* membutuhkan interaksi dan komunikasi dengan berbagai pihak di dalam negara (*Exclucive*) maupun membangun kerjasama dengan pihak luar (*Transfer*). Negara mengejar pembangunan nasional secara teknis yang dapat terlihat dan terukur. Pembangunan itu harus sampai kepada pelaksanaan secara teknis dengan pengadaan perlengkapan jaringan, internet, pelatihan SDM dalam bidang IT, dan sebagainya. Inilah yang termasuk dalam aspek *Infrastructure,* dimana sudah tersedianya perlengkapan untuk meningkatkan keamanan siber Nasional (Yeli, 2017). Teori dasar inilah yang menjadi bahan acuan penulis untuk menganalisis dokumen strategi keamanan nasional Lebanon.

Untuk melihat secara garis besar tentang fokus pembahasan dokumen strategi keamanan siber ini, maka pada tahap penelitian awal penulis menggunakan item *interactive word tree* yang ada pada aplikasi MAXQDA.



Sumber: Hasil Penelitian (2020)

Gambar 2. *Cyber Security* dalam *National Cyber Security Strategy*

Dari gambar 2 dapat dilihat bahwa keamanan siber Lebanon berorientasi pada beberapa hal berikut: a). *Cyber security Strategy: it is crucial to identfy and itemize the key pillars, upon which a prospective strategy must rely on.* b). *Cyber security Strategy: it is mandatory that Lebanon works closely with other regional and international actors.* c). *Cyber security Strategy: based on and addressing the identified cyber security pillars can protect Lebanon, its public institutions, its private sector and its citizens from the above threat, thanks to a codified, systematic, nation wide, all-encompasing action plan.*

Metode *interactive world tree* menunjukan fokus dari dokumen resmi keamanan ruang siber Libanon yaitu pentingnya Lebanon melakukan kerjasama dengan berbagai sektor dalam lingkup keamanan ruang siber (Araz, 2019). Kerja sama dilakukan untuk meningkatkan keamanan ruang siber dari berbagai sisi seperti pertahanan, pencegahan, perlindungan dari

berbagai ancaman baik internal maupun eksternal. Selain itu, mendukung pengembangan dan meningkatkan kapasitas serta peran badan keamanan ruang siber Lebanon.

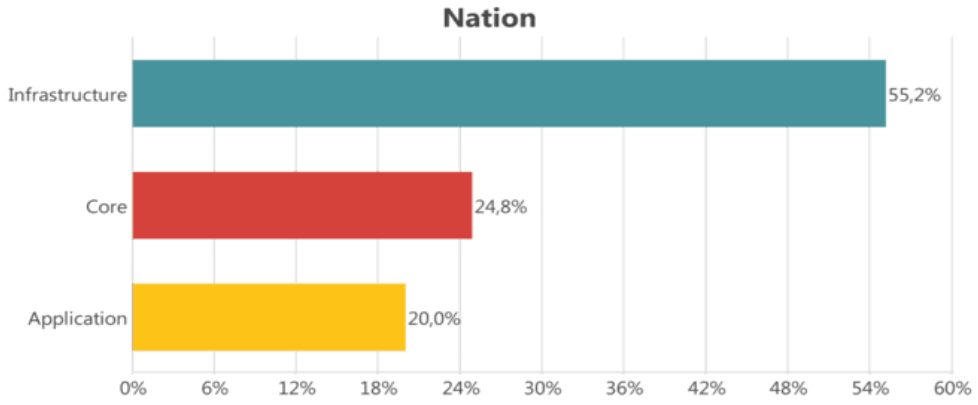
Pemerintah terus mengevaluasi serangan pertahanan dan keamanan di Lebanon dengan membuka jalan bagi kerja sama dengan berbagai aktor regional dan internasional. Dalam sebuah penelitian ditemukan bahwa terdapat 1645 kerentanan yang terjadi di sekitar wilayah perbatasan Lebanon yang mempengaruhi pembangunan infrastruktur, kerusakan ekonomi dan kehidupan warga sipil. Penyebab utama yang diidentifikasi ialah kurangnya praktik keamanan inti yakni *patch management*. Maka perlu ada evaluasi yang perlu melibatkan berbagai pihak dari sektor publik dan swasta untuk melakukan analisis dan mitigasi resiko dengan lebih baik (Fadlallah et al., 2020).

3.1. Strategi Keamanan Siber Lebanon

Strategi keamanan siber Lebanon memiliki beberapa unsur, institusi dan kebijakan-kebijakan yang saling mempengaruhi satu sama lain. Maka itu, berangkat dari pemahaman tentang teori kedaulatan, penulis menemukan bahwa dokumen strategi keamanan Lebanon memiliki poin-poin penting dalam meningkatkan pertahanan dan keamanan nasionalnya. Dalam dokumen ini, terdapat tiga poin penting yang kemudian penulis coding dalam 3 poin besar yakni: *Nation, Sovereignity dan Aspects*. Pertama, *code* {*Nation*} memiliki *sub-code* {*Core, Application,* dan *Infrastructure*}. *Code* ini menjelaskan tentang aspek kedaulatan yang diatur oleh dokumen ini. Kedua, *code* {*Sovereignity*} berisi *sub-code* {*Exclusive* dan *Transfer*}. Keduanya membahas tentang sifat dari kedaulatan. Ketiga, *code* {*Aspects*} merupakan bagian penting dari analisis kualitatif terhadap dokumen Strategi keamanan siber Lebanon. Terdiri dari *sub-codes*: {*Economy development, Teroris threats, Cyber crime, Public adminitrations, Citizen, Legal, Institution, Cyber security strategy, Social interactions, Cyber space, Social-culture}.*

3.1.1 Nation

Penulis kemudian menganalisis data menggunakan MAXQDA seperti gambar 3.



Sumber: Hasil Penelitian (2020)

Gambar 3. Analisa Strategi Keamanan Siber Lebanon

Gambar 3 merupakan hasil analisis terhadap dokumen Strategi Keamanan Siber Lebanon. Berdasarkan analisis tersebut, penulis berpandangan bahwa *infrastructure* (55,2%) banyak dibahas dan diatur dalam dokumen ini. Pemerintah berperan penting dalam

mengembangkan dan meningkatkan kerjasama untuk mendukung keamanan siber nasional. Pengembangan dan penyediaan segala hal menyangkut keamanan siber Lebanon juga memperhatikan prinsip-prinsip yang berkaitan dengan kehidupan ekonomi dan politik. Berkaitan dengan *Core (24,8%),* prinsip-prinsip kedaulatan nasional masih cukup dijaga oleh negara.

Berkaitan dengan strategi keamanan siber Lebanon, Uni Eropa memainkan peran penting dalam mewujudkannya. Lebanon sebagai salah satu negara penerima manfaat program pengembangan digital regional UE. Program ini merupakan proyek bersama antara UE dan Dewan Eropa yang bertujuan untuk mendorong undang-undang dan kebijakan untuk memperluas kapasitas kelembagaan pemerintah MENA (*Middle East and North Africa*) untuk mengelola ancaman digital. Lebanon memperoleh akses ke lokakarya kejahatan dunia maya dan para ahli di bidangnya. Untuk langkah ke depannya, pemerintah Lebanon harus mengalokasikan jumlah yang cukup untuk menjamin implementasi skala penuh dari cetak biru keamanan siber (Araz, 2019).

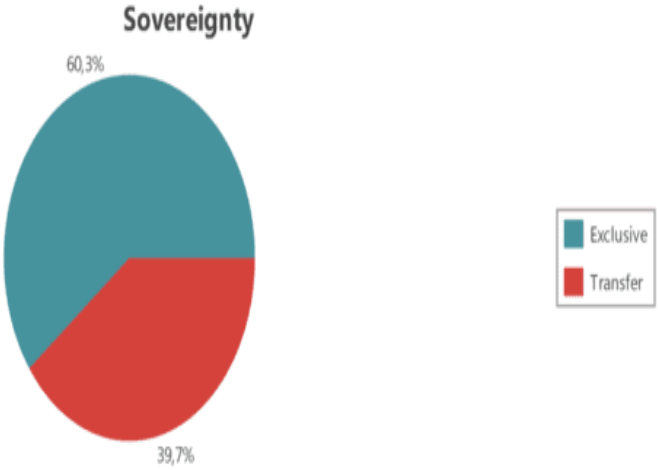
Lebanon Bersama dengan Uni Eropa membangun kerjasama guna meningkatkan keamanan dan pertahanan untuk menghadapi serangan dan ancaman ruang siber (EEAS, 2018). Memperkuat kerjasama dengan Uni Eropa dilakukan karena Pemerintah Lebanon menyadari pentingnya kerangka hukum dan kebijakan yang efesien untuk dikembangkan hingga kebutuhan untuk meningkatkan kapasitas nasional dalam menanggulangi segala bentuk kejahatan ruang siber seperti *cyber terrorism*. Keikutsertaan Lebanon dalam pengembangan kerjasama internasional ruang siber tersebut juga memiliki tujuan dasar yaitu agar terciptanya pedoman, kerangka kerja yang sinergis, berdasarkan pertukaran dan koordinasi yang mendalam antara Lebanon dan aktor lain (Mansour, 2017). Kerjasama internasional ruang siber selaras dengan kepentingan nasional Lebanon yang ingin mengembangkan teknologi di ranah siber, memperkuat solidaritas berbagai negara serta untuk memerangi ancaman siber.

Selanjutnya, *Application* memiliki presentase sebesar 20,0 %, tampaknya aturan-aturan dalam dokumen ini mengenai hal-hal teknis pemakaian dan pengelolaan teknis belum terlalu banyak dibahas. Ini menjadi catatan bahwa kebijakan-kebijakan yang sudah tertuang dalam dokumen belum diimplementasikan dalam banyak program, pelatihan dan pengembangan jaringan kemanan secara nyata.

Hemat penulis, aspek *infrastructure* yang dibahas dalam dokumen belum diatur secara teknis. Tentang bagaimana pengelolaan teknisnya, program bagi peningkatan SDM dalam bidang IT, peningkatan jaringan fisik, dan sebagainya. Perolehan angka yang besar dari *infrastructure* (55,2%) tidak menjamin peningkatan kemanan siber nasional Lebanon.

3.1.2 Sovereignity

Selanjutnya, penulis menganalisa lapisan kedaulatan untuk mengetahui perbandingan antara sifat kedaulatan tertutup dan terbuka seperti pada gambar diagram 4.



Sumber: Hasil Penelitian (2020)

Gambar 4. Sifat Strategi Keamanan Siber Lebanon

Gambar 4 menunjukkan bahwa kedaulatan *Exclusive* mendapat porsi sebesar 60,3 %, sedangkan *Transfer* sebesar 39,7 %. Perolehan ini dapat dikatakan bahwa Lebanon menitiberatkan kepentingan nasionalnya secara maksimal. Segala kebijakan dan prinsip yang dibahas mengutamakan kepentingan keamanan warga negaranya. Perolehan *Exclusive* yang besar ini ini juga menunjukkan bahwa Lebanon masih cukup tertutup dengan kebijakan keamanan siber.

Lebanon merupakan salah satu negara yang fokus terhadap keamanan ruang siber, hingga pada tahun 2018 Lebanon menjadi mendapat peringkat 17 di kawasan Arab dan pada tingkat global mendapatkan peringkat 124 (CSR, 2019). Peringkat tersebut merupakan hasil dari survey terhadap komitmen anggota negara terhadap keamanan ruang siber dalam peningkatan perhatian dan kewaspadaan. Peringkat tersebut diberikan oleh *International Tellecomunication Union* (International Telecommunication Union (ITU), 2019).

Peringkat tersebut tidak hanya menunjukkan angka, melainkan adanya eksekusi dari komitmen yang dilakukan oleh pemerintah Lebanon untuk meningkatkan keamanan, pertahanan dan kesadaran akan pentingnya ruang siber. Inisiatif di bidang digital menjadikan Lebanon memiliki strategi yang komprehensif dalam melindungi Negara dari berbagai ancaman siber yang sulit diprediksi. Dokumen resmi keamanan ruang siber atau disebut dengan "Lebanon National Cyber Security Strategy" (Lebanon, 2019) menjadi landasan bagaimana strategi Lebanon dalam membangun kebijakan serta kerangka hukum yang diterapkan di Lebanon. Selain itu, dokumen tersebut menjadi pedoman dalam mengukur efesiensi, keefektifan dan keaktifan berbagai aktor dalam perlindungan ruang siber Lebanon.

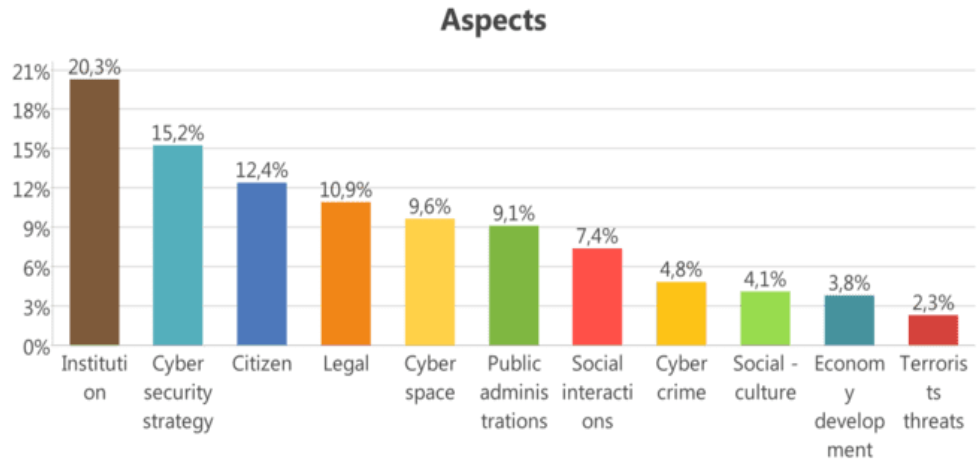
Namun, tak dipungkiri juga bahwa Lebanon membuka diri dan melakukan kerja sama dengan negara-negara berkembang lainnya yang menghasilkan aspek *Transfer* sebesar 39,7% untuk meningkatkan *Infrastrucutre* dalam negara. Hal ini terlihat jelas dengan angka yang cukup besar dalam peningkatan dan pengembangan *Infrastrucutre.* Dapat dikatakan bahwa pertahanan kedaulatan yang *exclusive* dikuatkan dengan fokus negara pada pengembangan

infrastructure secara intern. Jadi, negara dengan prinsip dan kebijakannya ingin mendukung kemajuan teknologi, informasi dan komunikasi demi penguatan keamanan siber Nasional.

3.1.3 Aspects

Lapisan terakhir yang dianalisa adalah *aspects*. Yang menjadi ciri khas strategi kemanan siber Lebanon ialah penekanan pada pengembangan *infrastructure* melalui kebijakan yang ditetapkan. Negara berpegang pada prinsip dan aturan untuk mendukung kepentingan keamanan nasional. Oleh karena sifat *exclusive* mendominasi kedaulatan, maka yang menjadi prioritas ialah warga negara dan kepentingan nasional.

Dalam menjalankan kedaulatannya, ada beberapa unsur pendukung yang ditemukan di dalamnya. Penulis melakukan analisis dan membuat *coding* dengan nama *Aspects,* yang terdiri dari *sub-code*, yakni: {*Economy development, Teroris threats, Cyber crime, Public adminitrations, Citizen, Legal, Institution, Cyber security strategy, Social interactions, Cyber space, Social-culture}.* Berikut ini disajikan seberapa besar aspek tersebut mempengaruhi kedaulatan dan keamanan siber negara:



Sumber: Hasil Penelitian (2020)

Gambar 5. Aspek dalam Strategi Keamanan Siber Lebanon

Pada gambar 5, perolehan data menunjukkan bahwa ada banyak aspek pendukung bagi Lebanon dalam meningkatkan pertahanan dan keamanan siber. *Institution* merupakan aspek yang paling dominan disinggung dalam dokumen ini yakni sebesar 20,3 %. Peran pemerintah, warga negara, dan organisasi-organisasi cukup penting dalam menjaga kedaulatan negara. Perolehan ini bersinggungan dengan pengembangan *Infrastructure* dalam kedaulatan. Maka itu, upaya ini kemudian diikuti oleh *Cyber security strategy* sebesar 15,2%. Strategi ini memberikan solusi untuk menjamin keamanan siber ke sektor publik, swasta dan warga negara, serta untuk membangun upaya kolektif nasional.

Strategi keamanan nasional menempatkan *citizen* menjadi fokus negara untuk melindungi dari *terrorists threats*. Lebanon mengatur kebijakan dan prinsip-prinsip secara *Legal.* Negara mendukung kerangka kerja akreditasi, sertifikasi dan standarisasi teknis terkait sistem keamanan siber. Aturan-aturan dominan berisikan tentang pemanfaatan dan pengelolaan

internet (*cyber space*) secara memadai. Namun, perlu diangkat bahwa *terrorists threats* mendapat porsi yang kecil dibandingkan dari aspek lainnya. Untuk menekan ancaman ini, terdapat *social interactions* yang turut membantu meningkatkan keamanan siber nasional.

Terrorists threats yang dihadapi oleh Lebanon datang dari luar dan dalam negara. Seiring meningkatnya ancaman siber yang menyerang Lebanon, pemerintah menyusun strategi membangun dan memelihara dunia maya yang aman untuk melindungi kepentingan nasional serta mengedepankan hak-hak dasar warga negara. Aspek ini memiliki hubungan paling dominan dengan kejahatan siber dan *citizen*. Ancaman terorisme dapat menyerang keamanan negara melalui tekonologi dan informasi dengan menyebarkan rasa takut untuk memperoleh keuntungan politik. Di zaman digital saat ini, kelompok teroris dapat mencuri data tanpa harus memiliki perlatan teknologi yang canggih (Samuel et al., 2014).

3.2 Relasi Data

Setelah itu, penulis kemudian melanjutkan analisis dengan menggunakan MAXQDA untuk memperoleh relasi data antara satu dengan yang lainnya.

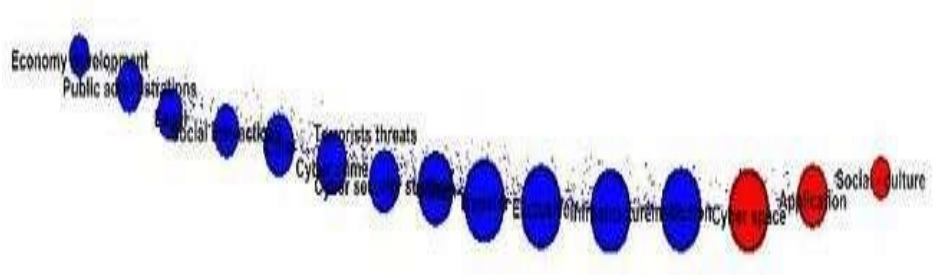
Code System	Asp...	Eco...	Terr...	Cyb...	Pub...	Citiz...	Legal	Insti...	Cyb...	Soci...	Cyb...	Soci...	Sov...	Excl...	Tra...	Nati...	Core	App...	Infr...
Aspect																			
Economy development				2	1	3		1	3		1			5	4		2	1	8
Terrorists threats				2	1			1			1			3	3				3
Cyber crime		2	2			3	3	2	2		2	1		4	3		3	4	9
Public administrations		1	1			6	5	4		1	1			15	5		2	3	22
Citizen		3		3	6		4	16	7	3	3	2		19	7		11	6	23
Legal				3	5	4		10	6	2	2			5	9		4	5	23
Institution		1	1	2	4	16	10		15	10	3	2		24	16		15	11	43
Cyber security strategy		3		2		7	6	15		1	3	1		18	8		9	8	25
Social interactions					1	3	2	10	1		4	1		7	11		2	3	17
Cyber space		1	1	2	1	3	2	3	3	4		4		17	8		7	15	18
Social - culture				1		2		2	1	1	4			6	1		5	2	2
Sovereignty																			
Exclusive		5	3	4	15	19	5	24	18	7	17	6			2		11	5	21
Transfer		4	3	3	5	7	9	16	8	11	8	1		2			3	3	10
Nation		11	3	16	27	40	32	69	42	22	40	9		37	16		7	11	18
SUM	0	31	14	40	66	113	78	173	106	62	89	27	0	162	93	0	81	77	242

Sumber: Hasil Penelitian (2020)

Gambar 6. Hasil Analisis MAXQDA

Dari gambar 6 dapat dilihat terdapat relasi data antara satu dengan yang lainnya. Data tersebut menjelaskan semakin tinggi angka yang didapatkan, maka semakin tinggi data tersebut menjadi aspek utama dari dokumen nasional keamanan siber Lebanon. Misalnya, angka 43 pada kolom terakhir (*infrastructure*) memiliki relasi dengan (*insitution*).

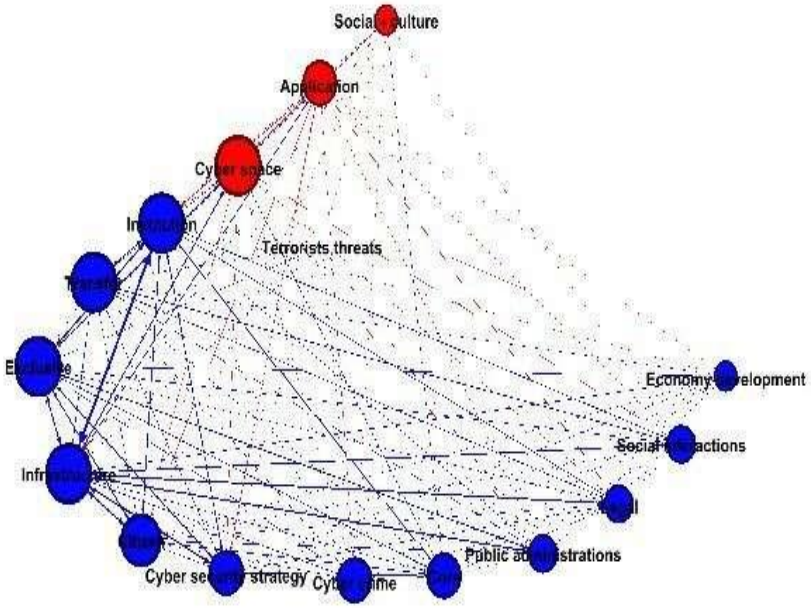
Selanjutnya, penulis melakukan pengolahan data menggunakan GEPHI adalah sebagai berikut:



Sumber: Hasil Penelitian (2020)

Gambar 7. Grafik Aspek Strategi Keamanan Siber Lebanon

Gambar 7 menunjukkan bahwa ada relasi data yang berkaitan antara satu aspek dengan aspek lainnya, yang dibagi dalam dua cluster warna: Biru dan Merah. Dominasi cluster warna biru tersebut menggambarkan bagaimana cluster biru lebih tertutup. Sifat tertutup tersebut dilandaskan atas dasar kebijakan pemerintah Lebanon dalam mengaplikasikan keamanan siber Lebanon. Berbeda dengan cluster berwarna merah yang memiliki sifat lebih terbuka dimana Lebanon memahami pentingnya kerjasama internasional yang signifikan dengan lembaga dan aktor lain karena ancaman ruang siber tidak mengenal batas negara.



Sumber: Hasil Penelitian (2020)

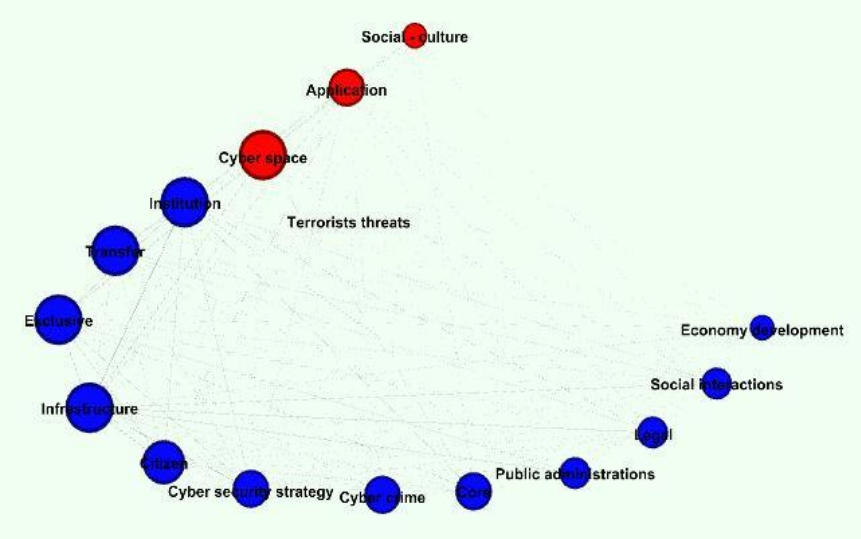
Gambar 8. Cluster Aspek Strategi Keamanan Siber Lebanon

Gambar 8 merupakan metode untuk memudahkan dalam menelaah relasi data, penulis melakukan penyesuaian terhadap tampilan data dengan menyematkan fitur tambahan pada pengaturan layout GEPHI. Temuan yang dapat diperoleh dari kedua cluster tersebut adalah sebagai berikut: a). Cluster merah terdiri dari nodes: *Cyber space, Application, Social-culture.* b). Cluster biru terdiri dari nodes: *Transfer, Exclusive, Institution, Infrastructure, Economy development, Terrorist threats, Cyber crime, Citizen, Cyber security, Public adminitrations, Legal, Core, Social interactions*.

Dari gambar 8 dapat dikatakan bahwa ada relasi data antara aspek yang satu dengan aspek lainnya. Selanjutnya, penulis ingin menunjukkan pembahasan relasi data yang terdapat dalam tiap aspek. Berikut spek yang memiliki relasi dengan semua aspek yang ada di dalam dokumen strategi keamanan siber Lebanon. Aspek-aspek tersebut adalah *Institution, Cyber space, Transfer, Exclusive dan Infrastructure*.

Gambar 9 menunjukan bahwa aspek *Institution* merupakan aspek yang mendominasi dalam dokumen strategi keamanan siber Lebanon dan memiliki relasi dengan seluruh aspek lain, baik dari klaster merah maupun klaster biru. Seorang pakar institusional berpandangan bahwa institusi berperan penting dalam menjaga keamanan siber nasional. Institusi dapat

menyediakan informasi, mengurangi biaya transaksi dan menjadi titik penting koordinasi. Menurutnya, keterlibatan institusi untuk menciptakan stabilitas dan kemanan dunia pasca Perang Dingin (Baylis & Smith, 2005).



Sumber: Hasil Penelitian (2020)

Gambar 9. Cluster Aspek Strategi Keamanan Siber Lebanon

Berikutnya ialah aspek *Cyber space* yang juga memiliki relasi dengan semua aspek dalam dokumen. Aspek *Institution* membahas tentang keterlibatan pemerintah, warga negara dan organisasi dalam menguatkan pengembangan keamanan negara dan pemanfataan teknologi secara maksimal (Lebanon, 2017). Keterlibatan semua pihak menjadi hal yang krusial karena dengan dilibatkannya semua aktor baik pemerintah, masyarakat, lembaga dan aktor lainnya, maka akan menumbuhkan kesadaran terhadap pentingnya mengetahui langkah yang strategis dalam melindungi informasi baik yang bersifat pribadi atau umum.

Pemerintah Lebanon memiliki tanggung jawab untuk memberikan keamanan siber dan melakukan tindakan preventif dalam mencegah ancaman dari luar. Oleh karena itu, *Institution* melakukan usaha dengan membangun relasi *social-interactions* dan membuat kebijakan secara *Legal* demi kepentingan keamanan nasional. Selain itu, aspek *Cyber space* mendapat perhatian dalam dokumen ini. Pembahasan mengenai regulasi ruang siber ternyata mempertimbangkan juga aspek pendukung lainnya, seperti: *social-culture, institution, citizen, legal, public adminitrations, economy developments, terrroris threats.*

3.2.1 Social Culture dan Application

Relasi yang ditunjukkan oleh aspek *Social Culture* hampir menyentuh semua aspek lainnya. Aspek ini tidak memiliki relasi dengan aspek dari klaster biru, yakni: *economy developments, public adminitrations, legal dan terroris threats*. Yang dimaksudkan dengan aspek *social culture* dalam dokumen ini ialah bagaimana perilaku *citizen* dalam menanggapi prinsip dan kebijakan publik dari pemerintah Lebanon. Respon yang baik dari warga dan semua

elemen diperlukan untuk membangun kebiasaan hidup dalam pemanfaatan media teknologi dan informasi bagi pertahanan dan keamanan nasional.

Aspek *Application* menunjukkan aspek yang penting dan aspek tersebut memiliki relasi cukup banyak dengan aspek lainnya, terkecuali dengan aspek *terroris threats* dan *core*. Aspek *Application* berbicara mengenai hal-hal teknis dalam peningkatan jaringan internet guna mendukung keamanan siber nasional Lebanon. Aspek ini cukup penting sehingga memperoleh angka sebesar 20,0 % dalam *Nation*.

3.2.2 Cyber Security Strategy

Aspek *Cyber Security Strategy* memiliki relasi yang cukup luas dengan aspek-aspek lainnya pada dokumen keamanan siber Lebanon. Relasi yang luas ini menunjukkan bahwa dokumen ini sungguh memfokuskan pembahasan mengenai strategi dan regulasi tentang keamanan siber.

Namun, *cyber security strategy* tidak memiliki relasi yang kelihatan dengan aspek *public administrations*. Penulis berpendapat bahwa strategi yang tertuang dalam dokumen tersebut belum sepenuhnya membahas aksi nyata dari pemerintah bidang keamanan siber nasional. Aksi nyata tersebut tidak hanya berupa dokumen yang dipublikasikan, namun pemerintah Lebanon mengambil berbagai upaya dalam peningkatan kapasitas seperti badan intelejen, *think tank* dan aktor lain dalam perlindungan ruang siber Lebanon. Peningkatan kapasitas akan menjadi dasar bagi Lebanon dalam menghadapi ancaman ruang siber yang tidak bisa diprediksi seperti perang siber, *cyber terror* dan kasus ancaman lain.

3.2.3 Cyber Crime

Nilai aspek *Cyber Crime* berdasarkan analisis dalam dokumen ini adalah sebesar 4,8%. Aspek ini hampir memiliki relasi data dengan aspek-aspek lainnya, terkecuali aspek *public adminitrations* dan *social-interactions*. *Cybercrime* menjadi salah satu ancaman terbesar bagi Lebanon untuk segera ditanggulangi (J. Hejase, 2015). *Cybercrime* hadir karena adanya kelemahan sistem yang dimiliki sehingga kelemahan tersebut menjadi ancaman tersebut yang dapat menyerang *software* diberbagai sektor seperti bisnis, pemerintahan dan sektor lain. Ancaman tersebut dapat menyebabkan dampak yang besar dibandingkan ancaman tradisional.

Secara kontekstual, Lebanon menyadari bahwa ada upaya yang datang dari luar untuk mengacaukan keamanan sibernya. Sebab, Lebanon memiliki kelemahan dengan tidak adanya undang-undang tentang perlindungan lembaga pemerintah, perusahaan swasta dan hak individu dalam dunia maya. Kelemahan ini dapat menimbulkan kejahatan siber dalam negara. Penulis coba melihat relasi data dalam *code system (Ms. exel)* mengenai relasi *cyber crime* dan *institution* yang hanya mendapat angka sebesar 2. Relasi yang kecil ini menunjukkan bahwa upaya keamanan dalam mencegah kejahatan siber dari lembaga, pemerintah dan individu belum maksimal. Masing-masing pihak hanya mengamankan data dan sistem mereka dan belum ada strategi keamanan yang kolaboratif.

3.2.4 Public Adminitrations dan Legal

Aspek *public adminitrations* memiliki relasi data dengan hampir semua aspek lainnya. Hanya saja aspek *cyber security strategy, cyber space* dan *terroris threats* yang tidak memiliki relasi dengan aspek *public adminitrations.* Secara kontekstual, aspek *public adminitrations* dalam dokumen ini telah dibahas secara baik. Aspek ini menjadi hal yang penting dalam menjalankan fungsi administrasi keamanan dan penerapan sistem informasi yang aman. Yang menjadi catatan berdasarkan perolehan relasi data di atas ialah bagaimana strategi yang telah dibahas di dalam dokumen dapat diteruskan menjadi kebijakan administrasi yang konkret dalam kehidupan bernegara.

Sedangkan aspek *legal* hampir memiliki relasi data dengan semua aspek di dalam dokumen ini. Hanya saja *legal* tidak bersinggungan dengan aspek *economy development* dan *terroris threats*. Seperti yang penulis baca dalam dokumen keamanan siber Lebanon bahwa pemerintah belum membuat regulasi dalam peraturan yang tertulis/undang-undang. Maka itu tak heran kalau beberapa lembaga, perusahaan swasta atau individu bebas mengatur keamanan siber mereka sendiri.

3.2.5 Social Interactions, Economy Development dan Citizen

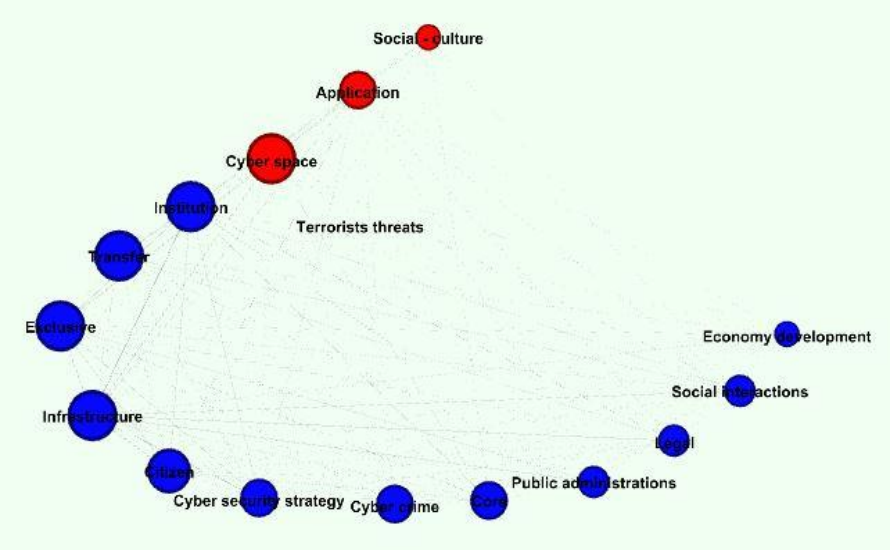
Aspek *social interactions* memiliki relasi dengan hampir semua aspek, terkecuali aspek *cyber space, economy development* dan *terroris threats.* Penulis berpendapat bahwa kerja sama dan interaksi secara intern di dalam negara belum dibangun secara maksimal. Pemerintah belum mengumpulkan kekuatan dari pihak lembaga swasta atau individu dalam memperkuat peningkatan jaringan teknologi dan komunikasi. *Social Interactions* perlu dikembangkan lagi untuk membangun kerjasama dalam pertahanan dan keamanan nasional.

Selanjutnya, aspek *economy development* memiliki relasi dengan hampir semua aspek, terkecuali aspek *social interactions, legal,* dan *terroris threats*. Pengembangan ekonomi yang disinggung dalam dokumen ini memberikan gambaran bahwa aspek ekonomi tidak cukup mempengaruhi keamanan siber nasional. Ekonomi menjadi isu yang dibahas tersendiri dalam kebijakan pemerintah Lebanon, sehingga tidak mendapat perhatian lebih dalam dokumen.

Aspek *citizen* memiliki relasi dengan hampir semua aspek, terkecuali aspek *terroris threats*. Aspek *Citizen* memperoleh hasil sebesar 12,4 %. Perolehan angka ini menunjukkan bahwa warga mendapat fokus dan perhatian yang cukup dalam setiap pertimbangan kebijakan keamanan siber Lebanon. Negara hadir untuk melaksanakan pengembangan dan pembangunan nasional serta memanfaatkan teknologi demi kemajuan warganya. Dokumen ini cukup luas membahas mengenai keamanan dan kesejahteraan warga negaranya.

Dari keseluruhan data menunjukkan Lebanon cukup ketat untuk memprioritaskan kepentingan nasional, *infrastructure* sistem teknologi dan informasi, serta peningkatan kualitas warga negaranya. Lebanon cukup tertutup dengan strategi keamanan sibernya. Kerjasama intern yang melibatkan antara pemerintah, lembaga swasta dan individu menjadi hal krusial untuk diaplikasikan. Ketiga aktor tersebut memiliki peran strategis dalam mengembangkan dan meningkatkan sistem / strategi keamanan siber nasional Lebanon.

Dokumen ini baru sampai pada pembahasan teoretis semata. Belum ada implementasi yang real, terpola dan terukur dari pemerintah Lebanon dalam bidang keamanan siber. Oleh karena itu, Lebanon mesti terbuka dan komunikatif untuk membangun jaringan dan kerja sama dengan negara dan organisasi internasional dalam meningkatkan strategi keamanan siber nasionalnya. Selain itu, titik fokus dokumen ini ialah kembali kepada penguatan institusi (negara, warga negara dan organisasi). Dokumen ini mendesak adanya tindakan wajib, kritis, operasional, yakni Pembentukan resmi Badan Informasi Keamanan Siber Nasional.



Sumber: Hasil Penelitian (2020)

Gambar 10. Cluster Aspek Strategi Kemanan Siber Lebanon

4. Kesimpulan

Berdasarkan hasil analisis kuantitatif penulis terhadap dokumen *National Cyber Security Strategy* Lebanon dapat disimpulkan dokumen ini menempatkan aspek *Institution* (warga negara, lembaga dan organisasi) di pusat tanggung jawabnya dalam meningkatkan pertahanan dan keamanan siber nasional Lebanon. Melalui kesadaran aspek itulah ingin dibangun upaya kolektif secara nasional dan mencapai kerja sama yang lebih kuat di tingkat regional dan internasional. Kesimpulan ini berangkat dari pembahasan yang dominan mengenai *Institution (20,3 %),* disusul dengan *cyber security strategy (15,2 %), citizen (12,4 %), Legal (10,9 %), cyber space (9,6%),* dan disusul aspek pendukung lainnya dalam peningkatan keamanan siber nasionalnya. Penulis berpandangan bahwa aspek kedaulatan yang menjadi fokus Lebanon adalah pengembangan *infrastructure (55,2 %)* yang bersifat *exclusive (60,3 %).* Lebanon memprioritaskan peran *institution* dalam mengelola dan melaksanakan strategi keamanan siber nasional. Dokumen ini lebih dominan membahas hal-hal yang bersifat intern, administratif, teoretis, prinsipil dan perencanaan.

Daftar Pustaka

Araz, S. (2019). *Lebanon's cybersecurity strategy emerges*.

Baylis, & Smith. (2005). *The Globalization of World Politics: 3e*. Oxford University Press.

CSR. (2019). *5th Annual Global Cyber Security Forum – Lebanon*. Cyber Security Review.

EEAS. (2018). *Addressing Cybersecurity Challenges in Lebanon*. European External Actio Service.

Fadlallah, Y., Sbeiti, M., Hammoud, M., Nehme, M., & Fadlallah, A. (2020). On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*. https://doi.org/10.1109/ISDFS49300.2020.9116446

International Telecommunication Union (ITU). (2019). Global Cybersecurity Index 2018. In *Measuring the Digital Transformation*.

J. Hejase, H. (2015). Cyber Warfare Awareness in Lebanon: Exploratory Research. *International Journal of Cyber-Security and Digital Forensics*, *4*(4), 482–497. https://doi.org/10.17781/p001892

Lebanon. (2019). *Lebanon National Cyber Security Strategy*.

Lebanon, R. of. (2017). *Cybersecurity in Lebanon*. Republic of Lebanon. Telecommunications Regulatory Authority.

Maharsi, S. (2000). Pengaruh Perkembangan Teknologi Informasi Terhadap Bidang Akuntansi Manajemen. *Jurnal Akuntansi Dan Keuangan*, *2*(2), 127–137. https://doi.org/10.9744/jak.2.2.pp.127-137

Mansour, R. (2017). *The International Strategy For Cyber Security*. Lebarmy.Gov.Lb.

Samuel, K. O., Rozaini, W., Osman, S., Al-Khasawneh, Y., & Duhaim, S. (2014). Cyber Terrorism Attack Of The Contemporary Information Technology Age: Issues, Consequences And Panacea. *International Journal of Computer Science and Mobile Computing*, *3*(5), 1082–1090.

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Institute for National Strategic Security, National Defense University*, *7*(2), 108–115.