Vol. 1, No. 4 November 2020 E-ISSN:2723 – 6595
http://jiss.publikasiindonesia.id/ P-ISSN:2723 – 6692

STRATEGI KEAMANAN SIBER KOREA SELATAN

Dinanda Diadeska Diara
Universitas Paramadina
Jakarta, Indonesia
Email: deskaliem@gmail.com

Artikel info

Artikel history:
Diterima: 27 Oktober 2020
Diterima dalam bentuk revisi: 07 November 2020
Diterima dalam bentuk revisi: 19 November 2020

Keywords:
Cybersecurity, South Korea, Cybersecurity Strategy

Abstract: *This study aims to understand and analyze South Korea's cybersecurity strategy in order to know the level of security and the role of each aspect of the cybersecurity strategy inSouth Korea. Besides, it also aims to make it a reference for a country to build or strengthen its country's cyber security strategy so as to prevent misuse of information. as well as data of each citizen as well as important country data in the cyber world. The method used in this study is a quantitative method by analyzing theapplication of the concept of sovereignty theory along with its aspects and quantitative methods by providing the results of data analysis on strategic patterns and the realization of South Korean cybersecurity data using the MAXQDA 2020 application, and GEPHI 0.9.2. The results of the author's quantitative analysis of the document South Korea's Cybersecurity Strategy can be concluded that the context of the South Korean cybersecurity strategy has a tendency towards state regulation of the national aspects of cybersecurity, cybersecurity awareness, cyberspace threats, international rules, laws and regulation, cyber crisis nation-wide, cyber. crime, as well as cyber infrastructure and it is open*

Abstrak: Penelitian ini bertujuan untuk memahami dan menganalisa strategi keamanan siber Korea Selatan agar dapat diketahui tingkat keamanan dan peran tiap aspek strategi keamanan siber pada Korea Selatan selain itu juga bertujuan agar dapat dijadikan referensi oleh suatu negara untuk membangun maupun memperkuat strategi keamanan siber negaranya sehingga mencegah penyalahgunaan informasi maupun data tiap warga negara maupun data penting negara yang ada di dunia siber. Metode yang digunakan pada penelitian ini adalah metodekuantitatif dengan menganalisa penerapan konsep teori kedaulatan beserta aspek-aspeknya dan metode kuantitatif dengan
memberikan hasil analisa data pola strategi dan realasi data

keamanan siber Korea Selatan menggunakan aplikasi MAXQDA 2020, dan GEPHI 0.9.2. Hasil analisis kuantitatif penulis terhadap dokumen *South Korea's Cybersecurity Strategy* dapat disimpulkan bahwa konteks strategi keamanan siber korea sealtan memiliki kecenderungan arah pada pengaturan negara terhadap aspek *national cybersecurity, cybersecurity awarness, cyberspace threats, international rules, laws and regulation, cyber crisis nation-wide, cyber crime, serta cyber infrastructure* dan bersifat terbuka.

Kata kunci: Keamanan Ruang Siber, Korea Selatan, Strategi Keamanan Siber

Koresponden author: Dinanda Diadeska Diara
Email: deskaliem@gmail.com

artikel dengan akses terbuka dibawah lisensi
CC BY SA
2020

Pendahuluan

Dewasa ini, kemajuan teknologi memaksa suatu negara untuk bertransformasi pada bidang diplomasi dan keamanan nasional untuk menjaga kedaulatan serta stabilitas negaranya. Hal ini ditandai dengan pendekatan aktifitas hubungan internasional suatu negara dalam diplomasi digitalnya (Bjola & Pamment, 2018). Internet sebagai sebuah "*the networks of the networks*" ke seluruh dunia, menjadikannya suatu ruang baru yang dinamakan *Cyberspace* (Eoghan, 2001).

Adapun *cyberspace* adalah suatu ruang komunikasi global dimana tak ada negara yang berhak mengatur informasi yang dilakukan antara dua orang atau lebih. Tentunya dengan adanya *cyberspace* memberikan dampak positif dan negatif. Salah satu dampak negatif yang timbul dari *cyberspace* adalah terjadinya *cyber crime* (Howard, 1995).

Maraknya *cyber crime* memerlukan perhatian serius dalam mengembangkan *cybersecurity* bagi sebuah negara. Definisi *security* dalam operasi informasi adalah semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun *cyber attack*. *Cybersecurity* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Mekanisme ini ditujukan untuk melindungi informasi baik dari *physical attack* maupun *cyber attack*. *Cybersecurity* merupakan upaya untuk melindungi informasi dari *cyber attack* (Plano, 2000).

Eksistensi dunia *cyber* sekarang menjadi urusan dunia internasional dan bukan hanya menjadi urusan domestik suatu negara lagi. Hal ini karena dampak dan pengaruh yang ditimbulkan dapat menimpa siapa saja, tidak terikat waktu dan tempat. Sebagai contoh, penyebaran virus "I love u " pada tahun 2000 yang menyerang ke 45 juta sistem jaringan di dunia dan memberikan dampak kerugian kurang lebih sekitar 10 miliar USD (Sørensen & Jackson, 2005) Menurut *Korea Information Technology Research Institute* (KITRI), gagasan

Best of the Best dirancang untuk melatih para ahli komputer untuk melawan serangan *cyber* dari dalam maupun luar negeri. Korea Selatan adalah salah satu negara yang paling terhubung dengan internet di dunia. Artinya, Korea menjadi rentan terhadap *cyber*, terutama oleh negara tetangganya yaitu Korea Utara. Penelitian kali ini mengkaji tentang strategi keamanan siber korea selatan dengan metode kuantitatif menggunakan aplikasi GEPHI DAN MAXQDA, penulisingin meneliti sejauh mana strategi keamanan siber yang diterapkan oleh korea selatan untuk menjaga kedaulatan dan stabilitas negaranya (Dimas., n.d.).

Metode Penelitian

Dalam suatu penelitian, diperlukan konsep atau rancangan yang berisi rumusan dan gagasan perihal objek yang akan diteliti. Penelitian ini meniliti tentang strategi keamanan siber Korea Selatan dimana metode penelitian yang digunakan adalah metode kuantitatif. Metode kuantitatif yang digunakan dalam penelitian ini adalah dengan menganalisa penerapan konsep teori kedaulatan beserta aspek-aspeknya yang diolah menggunakan bantuan *software* MAXQDA 2020 dan GEPHI 0.9.2. Analisa lanjutan dilakukan dengan merelasikan data-data yang timbul diantara satu aspek dengan aspek lainnya serta menerapkan metode *network analysis* menggunakan bantuan *software* GEPHI dan MAXQDA. Proses analisanya adalah memperoleh matriks dari relasi data lalu matriks akan dikonversi dalam bentuk sajian data analisis jaringan GEPHI. Adapun penggunaan *software* tersebut memberikan hasil analisa data pola strategi dan relasi data keamanan siber Korea Selatan.

Hasil dan Pembahasan

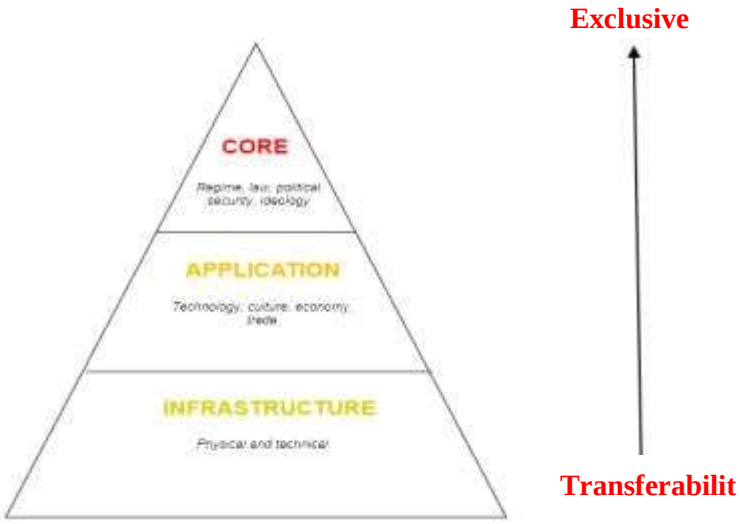
1. Strategi Kemanan Siber Korea Selatan

Untuk menjawab *research question* pertama mengenai prioritas Korea Selatan dalam mengatur keamanan siber, menggunakan penerapan konsep kedaulatan, kemudian diolah dalam bentuk aplikasi *software* MAXQDA. Mekanismenya adalah melakukan *coding* dalam dokumen *national cyber security strategy. Coding* ini terbagi dalam tiga *code* (masing- masing *code* memiliki *sub-code*) dengan penjabaran sebagai berikut:

- *Code* (*Nation*) dengan *sub-code*: *core, infrastructure*, dan *application*;
- *Code* (*Sovereignty*) dengan *sub-code*: *exlusive* dan *transfer;*
- *Code* (*Aspects*) dengan *sub-code*: *National cybersecurity, cybersecurity awareness, cyberspace threats, international rules, laws and regulations, cyber crisis nation-wide, cyber crime dan critical infrastructure.*

2. Kerangka Teori

Untuk menganalisa strategi keamanan siber Kanada yang ada dalam dokumen *national cybersecurity strategy* maka akan menggunakan pendekatan konsep kedaulatan dunia maya. Pendekatan konsep ini terdiri dari tiga bagian yaitu *core; application; dan infrastructure.* Hubungan antara bagian itu memiliki sifat yakni kedaulatan *exclusive* (tertutup) dan kedaulatan yang bersifat *transfer* (terbuka) (Yeli, n.d.)

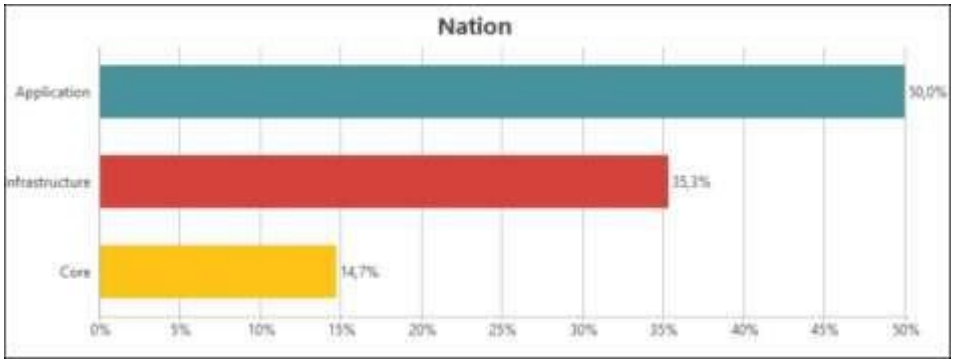


Gambar 1 Prinsip Teori Kedaulatan

Bagian pertama dalam pendekatan konsep kedaulatan dalam gambar x adalah *core*, bagian ini berfokus pada prinsip negara mengenai keamanan siber. Selanjutnya adalah *application*, yang berfokus pada interaksi antar aktor (individu, kelompok individu, negara, kelompok negara, sistem internasional) (Soltani, F., Naji, S., & Amiri, 2015). Bagian ketiga adalah *infrastructure*, yang menjadi alat atau teknologi dalam menjalankan keamanan siber. Dalam pengaplikasian kontekstualnya tingkat *core* bersifat *exclusive* karena bagian dari penerapan kedaulatan negara dalam keamanan siber. Lalu untuk tingkat *application dan infrastructure* mempunyai sifat *transfer* karena cenderung terbuka dan dinamis dalam interaksinya (Yeli, n.d.).

3. Code (Nation)

Untuk dapat mendapatkan hasil analisa kedaulatan pada suatu negara yang mana pada penelitian ini adalah Korea Selatan, maka penulis melakukan analisa pada data olahan menggunakan MAXQDA. Data yang diambil bersumber dari *National Security Office* Korea Selatan (National Security Office of South Korea, 2019) yang didapatkan dari MAXDA adalah kedaulatan yang diatur oleh Korea Selatan dalam dokumen *South Korea's Cybersecurity Strategy* (KSCSS) didominasi oleh aspek *Application* (50,0%) disusul secara berturut-turut oleh *Infrastructure* (35,3%) dan *Core* (14,7%).



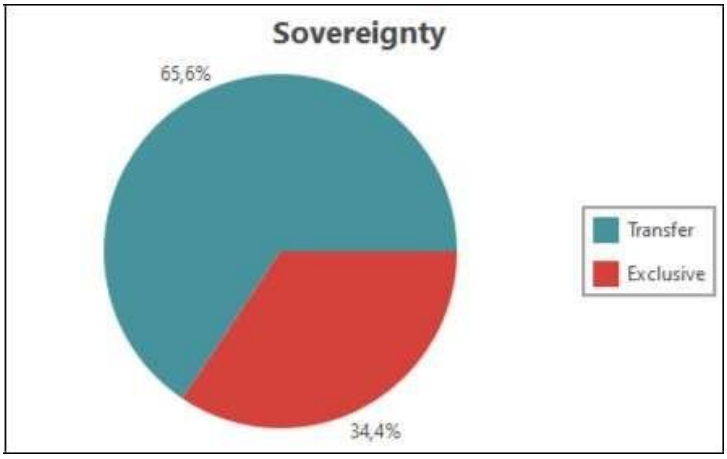
Gambar 2 Persentase aspek kedaulatan Korea Selatan

Gambar 2 merupkan data persentase aspek kedaulatan Korea Selatan. Dari data tersebut dapat dilihat bahwa persentase *application* mendominasi dibandingkan aspek lainnya yang mana dapat diasumsikan bahwa pemerintah Korea Selatan serius dalam mengatur interaksi yang terjadi dalam ruang siber namun hal ini tentunya menimbulkan perdebatan karena negara dapat melanggar privasi individu alih-alih melindungi keamanan negara.

Namun, Korea Selatan dalam aspek *infrastructure* memiliki persentase 35% yang mana berarti Korea Selatan memberikan kelonggaran terhadap pengembangan alat, jaringan ataupun infrastruktur penunjang kegiatan siber.

4. Code (Sovereignty)

Seperti yang diketahui pada konsep teori kedaulatan bahwa jenis dari ketiga bagian aspek kedaulatan berhubungan dengan sifat dari kedaulatan itu sendiri yaitu *exclusive* atau *transferability.* Berdasarkan besaran persentase tiap aspek kedaulatan Korea Selata yang tercantum pada dokumen KSCSS, berikut adalah perbandingan kedaulatan yang bersifat *exclusive* dan *transferability.*



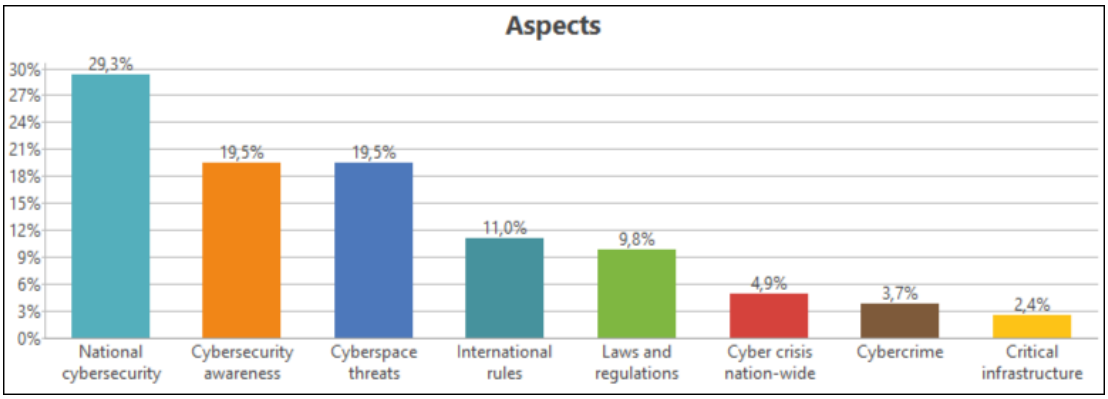
Gambar 3 Persentase sifat aspek kedaulatan

Data di atas menyajikan fakta yang menarik. Bila pada poin sebelumnya diketahui bahwa kehadiran negara didominasi pada aspek *Application*, namun pada persentase sifat aspek kedaulatan menampilkan hasil bahwa aspek kedaultan yang bersifat terbuka (transfer) lebih besar dibandingkan aspek kedaulatan dengan sifat terututup (exclusive). Bila diperhatikan dengan seksama, akumulasi nilai dari aspek kedaulatan *Application* dan *Infrastructure* yang diatur dalam KSCSS menunjukkan angka yang lebih besar dibandingkan dengan aspek Ideologi. Kesimpulannya adalah Korea Selatan cukup dominan dalam konteks keamanan siber yang mana aspek ideologi yang bersifat *exclusive* dan aspek ideologi yang bersifat *transferability* diatur oleh otoritas yang bertanggung jawab.

Jika dilihat pada konsep segitiga kedaulatan aspek *application* dan *infrastructure* bersifat *transferability* dan peralihan antara *transferability* dengan *exclusive* maka sudah sewajarnya jika persentase sifat dari aspek kedaulatan Korea Selatan lebih mendominasi sifat terbuka. Maka, Korea Selatan melakukan penetrasi terhadap aspek-aspek kedaulatan yang sifatnya terbuka.

5. Code (Aspects)

Untuk dapat melakukan penetrasi, maka perlu dilakukan analisa terhadap unsur-unsur negara yang merupakan perhatian otoritas setempat dalam mengatur keamanan siber di wilayahnya. Hasil analisa tersebut adalah didapatkan poin-poin aspek kedaulatan Korea Selatan sebagai berikut yang terbagi ke dalam kelompok *National cybersecurity, Cybersecurity awareness, Cyberspace threats, International rules, Laws and regulations, Cyber crisis nation-wide, Cyber crime dan Critical infrastructure*. Poin-poin aspek ini didapatkan dari KSCSS yang penulis interpretasikan ke dalam code {*Aspects*} sehingga dapat diketahui pengaturan, kehadiran maupun interaksi negara Korea Selatan dengan berbagai aspek.



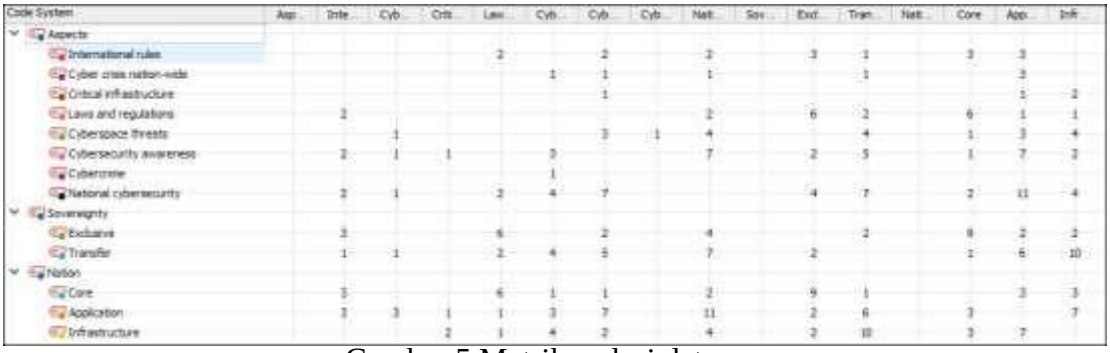
Gambar 4 Poin Aspek Kedaulatan Korea Selatan

Berdasarkan Gambar 4 diketahui bahwa national *cybersecurity* mendominasi Korea Selatan yang mana memberi ruang yang cukup besar bagi aktor non-negara untuk ikut serta dalam kerjasama penanganan isu keamanan siber. Persentase selain national *cybersecurity* adalah *Critical infrastructure* yang mana persentasenya sangat kecil di dalam KSCSS. Keamanan siber Korea Selatan lebih fokus kepada aspek *Cybersecurity awareness* dan *Cyberspace threats* dan juga berkolaborasi antar lembaga non pemerintah maupun pemerintah dengan kelompok masyarakat. Aspek international rules memiliki persentase lebih besar dibandingkan *laws and regulations* meskipun aspek *cyber crisis nation-wide* menjadi salah satu alasan dibalik hadirnnya negara dalam berbagai aspek kedaulatan yang bersifat terbuka. Namun, faktanya adalah hanya 4,9% perhatian yang diberikan otoritas Korea Selatan terhadap aspek *cyber crisis nation-wide*. Selain itu aspek *cybersecurity awareness* memiliki persentase yang cukup besar dalam dokumen KSCSS, hal ini dapat dipahami karena jumlah kehadiran aspek national cybersecurity yang dominan dalam tiap aspek keamanan siber Korea Selatan. Jika ingin mendapatkan gambaran utuh tentang bagaimana cara Korea Sekatan menjalankan strategi kemanan siber maka perlu dilakukan realasi data-data dengan aspel-aspek peraturan yang terdapat didalam KSCSS. Penjabaran dalam *code* (*aspects*) ini dimulai dari *sub-code National cybersecurity* dengan yang paling mendominasi sebesar (29,3%); *cybersecurity awareness* (19,5 %); *cyberspace threats* (19,5%); *international rules* (11%); *laws and regulations* (9,8%); *Cyber crisis nation-wide*

(4,9%); *cyber crime* (3,7%); dan yang paling sedikit *critical infrastructure* (2,4%). Melihat penjabaran *sub-code* tersebut, *National cyber security* terpilih menjadi *code* (*aspect*) dengan presentase tertinggi. Lalu Bagaimanakah cara Korea Selatan dalam melaksanakan strategi keamanan siber?

6. Relasi Data

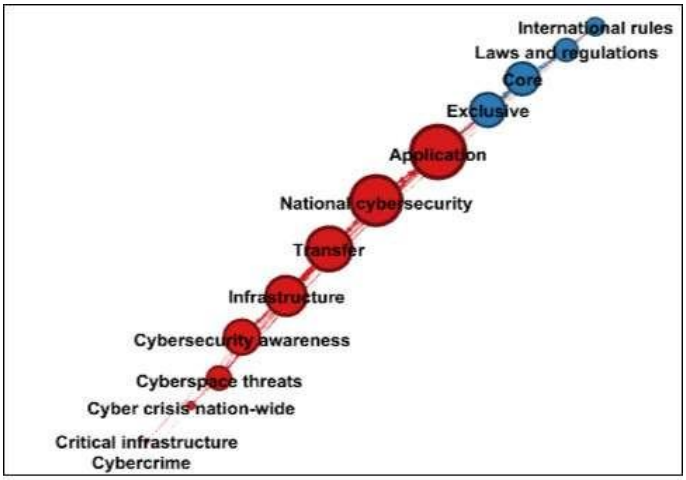
Seperti yang telah diberitahukan sebelumnya bahwa untuk mendapatkan gambaran yang utuh mengenai strategi keamanan siber suatu negara maka perlu dilakukan analisa lanjutan. Analisa lanjutan dilakukan dengan merelasikan data-data yang timbul diantara satu aspek dengan aspek lainnya dengan menerapkan metode *network analysis* menggunakan GEPHI dan MAXQDA. Proses analisanya adalah memperoleh matriks dari relasi data lalu matriks akan dikonversi dalam bentuk sajian data analisis jaringan GEPHI.



Code System	App...	Inte...	Cyb...	Crit...	Law...	Cyb...	Cyb...	Cyb...	Nati...	Sov...	Excl...	Tran...	Nati...	Core	App...	Infr...
Aspects																
International rules					2		2		2		3	1		3	3	
Cyber crisis nation-wide						1	1		1			1			3	
Critical infrastructure							1								1	2
Laws and regulations		2							2		6	2		6	1	1
Cyberspace threats			1				3	1	4			4		1	3	4
Cybersecurity awareness		2	1	1		3			7		2	5		1	7	3
Cybercrime						1										
National cybersecurity		2	1		2	4	7				4	7		2	11	4
Sovereignty																
Exclusive		3			6		2		4			2		8	2	2
Transfer		1	1		2	4	5		7		2			1	6	10
Nation																
Core		3			6	1	1		2		9	1			3	3
Application		3	3	1	1	3	7		11		2	6		3		7
Infrastructure				2	1	4	2		4		2	10		3	7	

Gambar 5 Matriks relasi data

Gambar diatas merupakan matriks yang akan dikonversikan pada GEPHI. Hasil yang diperoleh dari relasi data menggunakan GEPHI adalah sebagai berikut:

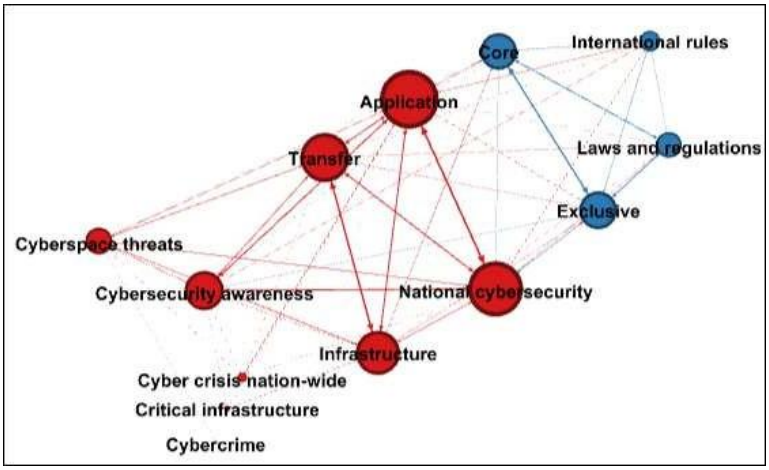


Gambar 6 Hasil relasi data utama GEPHI

Gambar di atas menunjukkan bagaimana relasi data antara satu aspek dengan aspek lainnya menghasilkan dua cluster data besar: Merah dan Biru. Setelah diketahui bentuk pengolahan dari MAXQDA ke Gephi, berikutnya adalah menambahkan fitur yang untuk membaca relasi secara lebih mendalam dari bentuk *layout radial axis.* Langkahnya adalah Pilih *layout radial axis > node placement > group nodes by: modularity class > order node in spar/axis: weighted degree > draw spar/axis as spiral: click for check list.* Gambar akan

ditunjukan untuk mengetahui hasil dari *setting* yang sudah dilakukan pada langkah-langkah modifikasi data dari *layout radial axis* pada gambar 7.

Berikut ini adalah bentuk *layout* (*spiral*) *radial axis* Gephi:



Gambar 7 Detail relasi data GEPHI

Agar mempermudah penjelasan hasil relasi data di GEPHI maka 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 [C1] terdiri dari *nodes* (berurutan dari besar ke kecil)*: Application, National cybersecurity, Transfer, Infrastructure, Cyberspace*

b. threats, Cybersecurity awareness, Cyber crisis nation-wide, Critical infrastructure, Cyber crime.

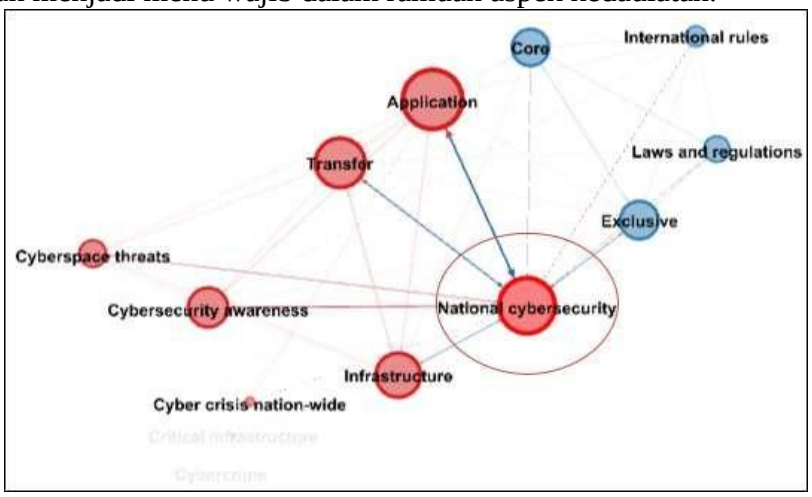
c. Cluster Hijau [C2] terdiri dari: *Exclusive, Core/Ideologi, Laws and regulations, International rules.*

Sehingga dapat dipahami bahwa relasi data yang terdapat pada [C1] merupakan aspek-aspek yang memiliki kaitan dengan pengaturan atau tata kelola keamanan siber yang bersifat lebih terbuka dibandingkan dengan relasi data [C2] yang cenderung lebih ekslusif milik otoritas negara. Hal itu dapat dikonfirmasi bila melihat masing-masing *node* yang terkelompok pada [C1] dan [C2]. Untuk penjelasan yang lebih terperinci penulis menyajikannya pada poin-poin di bawah ini.

7. National cybersecurity

Dari hasil pengolahan MAXQDA pada Gambar 4 diketahui bahwa aspek *national cybersecurity* pada Korea Selatan adalah sebesar 29,3% dan dilihat dari relasi data yang terjadi bahwa aspek ini tidak memiliki relasi dengan seluruh aspek yang ada di dalam KSCSS. Namun, aspek *nationak cybersecurity* pada [C1] hanya *transfer, application,* dan *infrastructure* sedangkan pada [C2] berada pada *exclusive* dan *core/ideologi* sehingga dapat disimpulkan bahwa aspek *national cybersecurity* dokumen KSCSS memiliki kaitan dengan seluruh aspek kedaulatan baik dari tataran ideologi maupun interaksi dan infrastruktur sistem informasi. Dengan kata lain, aspek *national cybersecurity* terhadap keamanan siber

Korea Selatan menjadi menu wajib dalam ramuan aspek kedaulatan.

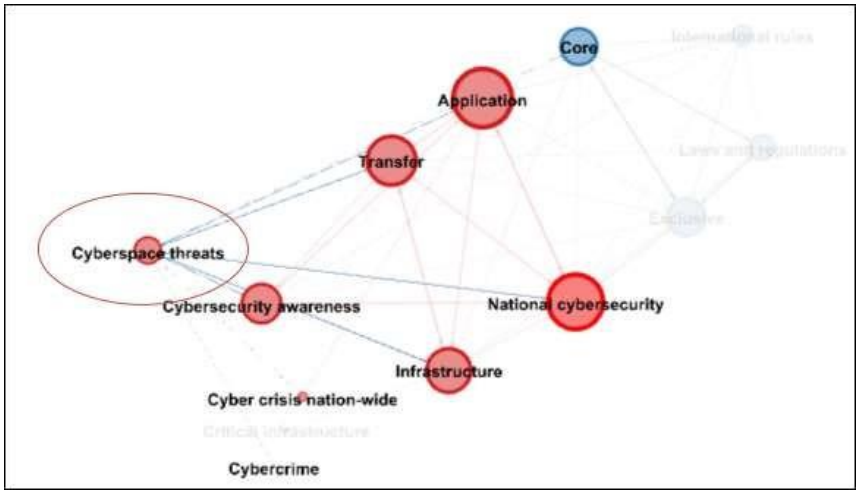


Gambar 8 Relasi *national cybersecurity* Korea Selatan terhadap aspek lain

8. Cyberspace threats

Dari pengolahan MAXQDA pada Gambar 4 diketahui bahwa persentase aspek *cyberspace threats* memiliki 19,5%. Namun, Aspek ini memiliki relasi yang cukup luas dengan aspek-aspek lainnya pada dokumen KSCSS. Hal ini tentu wajar bila melihat *cybespacer threats* atau ancaman siber sebagai konsep utama dalam penyusunan strategi keamanan siber Korea Selatan.

Akan tetapi, dengan tidak adanya temuan pada aspek *Cyber crime* yang secaraeksplisit menyebutkan jenis serangan tertentu, penulis menemukan bahwa konteks ancaman siber yang dituangkan dalam KSCSS bersifat general. Bisa diperhatikan pada relasi data berikut dimana aspek *cyberspace threats* memiliki relasi dengan aspek *national cybersecurity.* Artinya, ada patokan khusus untuk mendefinisikan ancaman siber yang dimaksud pada dokumen KSCSS.

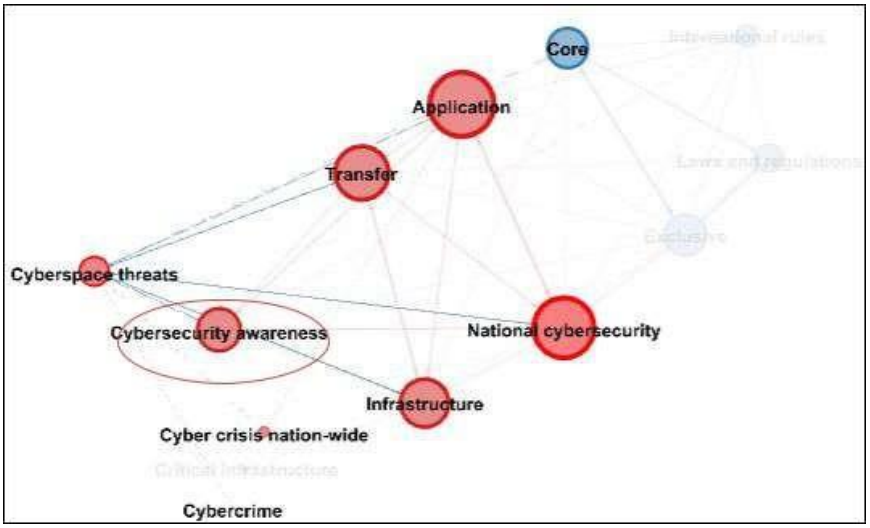


Gambar 9 Relasi aspek *cyberspace threats* Korea Selatan terhadap aspek lainnya

9. Cybersecurity awareness

Persentase yang dimiliki aspek *cybersecurity awareness* memiliki nilai yang sama dengan aspek *cybersecurity threats*. Dalam dokumen KSCSS, aspek ini dinyatakan sebagai salah satu aspek penting dan selain itu aspek ini memiliki relasi hampir dengan seluruh aspek lainnya kecuali data *laws and regulations*.

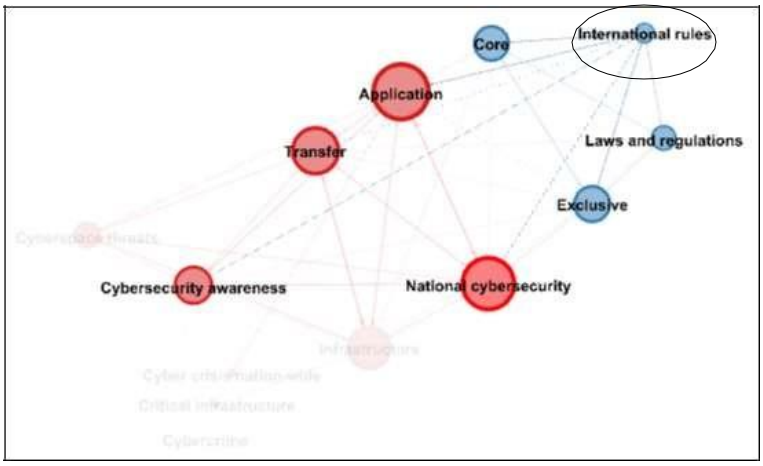
Secara kontekstual, dapat dimaknai sebagai upaya Korea Selatan guna melindungi kepentingan nasionalnya melalui kehadiran unsur pertahanan dan keamanan negara dalam isu keamanan siber. Negara berupaya untuk melakukan proteksi terhadap seluruh aspek kedaulatan (*core, application, infrastructure; exclusive/*transfer) serta aspek turunan lainnya. Konteks ini dapat diperluas lagi bila melihat kaitannya dengan *national cybersecurity.* Otoritas Korea Selatan memberikan porsi khusus bagi militer (aktor negara) untuk turut andil dalam pengamanan ruang siber negara tersebut. Di sisi lain, kehadiran militer tetap diatur secara administratif melalui perlembagaan siber negara.



Gambar 10 Relasi aspek *cybersecurity awareness* Korea Selatan terhadap aspek lainnya

10. International rules

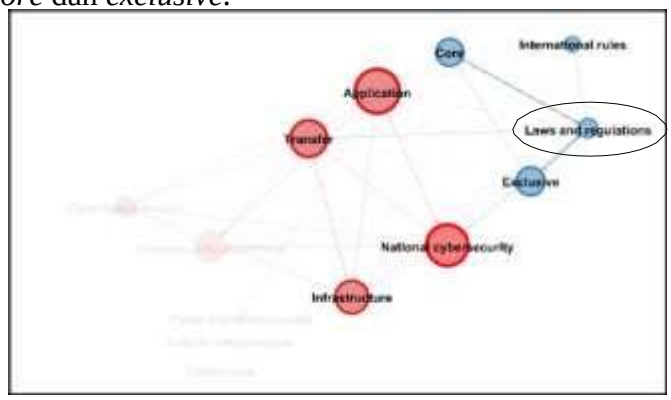
Berdasarkan hasil olahan data MAXQDA diperoleh persentase aspek *international rules* sebesar 11%. Aspek *internation rules* sanbat berhubungan dengan ketentuan, aturan maupun regulasi negara dalam mengatur keamanan siber maupun kedaulatan negara. Hubungan penting antara *international rules* dengan *core* Korea Selatan dapat dilihat pada Gambar 11. Sehingga dapat disimpulkan bahwa prinsip, regulasi, ideologi negara juga harus sejalan dengan aturan maupun regulasi yang berlaku secara global atau internasional.



Gambar 11 relasi aspek *international rules* Korea Selatan dengan aspek lainnya

11. Laws and regulations

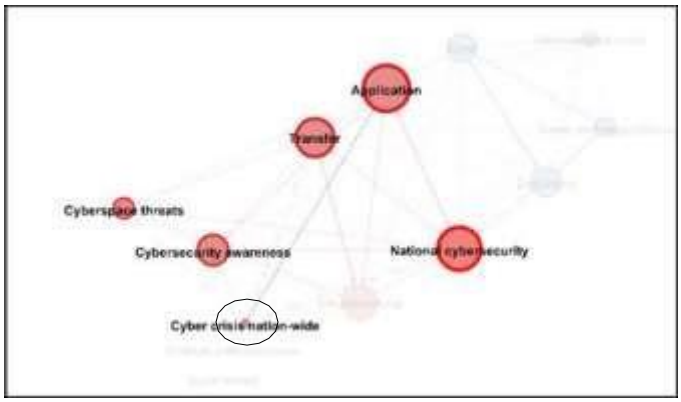
Berdasarkan hasil olahan data MAXQDA, persentase aspek *laws and regulation* adalah 9,8% dan sama seperti *international rules* bahwa *laws and regulation* tentunya bersifat tertutup dan sangat erat kaitannya dengan prinsip negara karena mengatur kebijakan suatu negara yang dapat dilihat relasinya pada Gambar 12 bahwa *laws and regulations* hanya berelasi dengan *core* dan *exclusive*.



Gambar 12 relasi *laws and regulations* Korea Selatan dengan aspek lainnya

12. Cyber crisis nation-wide

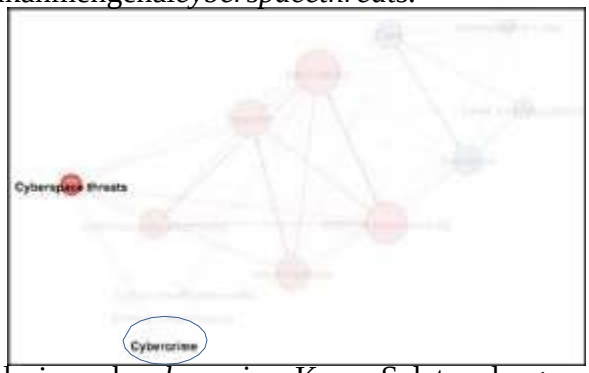
Berdasarkan hasil olahan data MAXQDA pada Gambar 4 dapat diketahui bahwa persentase aspek ini adalah 4,9% dan berdasarkan relasi data yang dilakukan diketahui bahwa *cyber crisis nation-wide* berhubungan dengan *application* yang mana termasukdalam aspek kedaulatan yang bersifat terbuka namun tidak berhubungan dengan aspek kedaulatan terbuka lainnya dan dikarenakan persentase yang cukup rendah maka aspek ini tidak akan terlalu mempengaruhi keamanan siber Korea Selatan.



Gambar 13 Relasi aspek *cyber crisis nation-wide* Korea Selatan terhadap aspek lainnya

13. Cyber crime

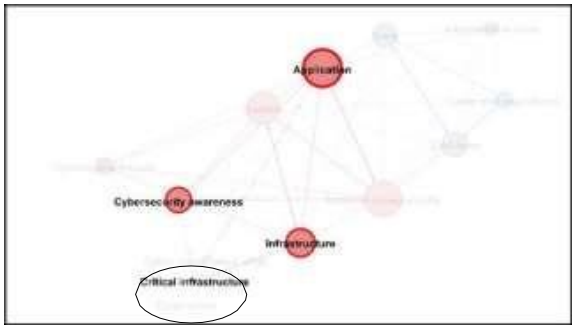
Persentase aspek *cyber crime* yang didapatkan dari hasil olahan data MAXQDA yang dapat dilihat pada Gambar 4 adalah sebesar 3,7% dan berdasarkan relasi daata diketahui bahwa *cyber crime* hanya berhubungan dengan *cyberspace threats* namun walaupun cukup rendahnya persenase *cyber crime* tidak menutup kemungkinan jika keamanan siber Korea Selatan terganggu maka akan meningkatkan kejadikan kejahatan siber. Maka penting untuk tetap mengatur kebijakanmengenai*cyberspacethreats.*



Gambar 14 relasi aspek *cyber crime* Korea Selatan dengan aspek lainnya

14. Critical infrastructure

Berdasarkan hasil olahan data MAXQDA diketahui bahwa aspek ini memiliki persentase terendah yaitu 2,4% dan relasi aspek ini terhadap aspek lainnya adalah aspek ini termasuk dalam bagian *application* dan *infrastructure* namun juga berhubungan dengan *cybersecurity awareness*. Maka walaupun persentasenya terendah karena berelasi dengan kedua aspek utama terbesar yang bersifat *transferability* maka aspek ini juga harus tetap dipertahankan dan ditingkatkan.



Gambar 15 Relasi aspek *critical infrastructure* Korea Selatan dengan aspek lainnya.

Kesimpulan

Berdasarkan analisis kuantitatif penulis terhadap dokumen *South Korea's Cybersecurity Strategy* dapat disimpulkan bahwa konteks strategi keamanan siber korea sealtan memiliki kecenderungan arah pada pengaturan negara terhadap aspek *national cybersecurity, cybersecurity awarness, cyberspace threats, international rules, laws and regulation, cyber crisis nation-wide, cyber crime, serta cyber infrastructure* dan bersifat terbuka. Fokus negara untuk mengamankan menjadi paramater penting bagaimana negara menjalankan fungsinya terhadap kebebasan dalam ruang siber di Korea Selatan.

Langkah pendekatan Korea Selatan terhadap keamanan siber memiliki celah yang cukup fundamental terhadap privasi individu-individu saat mengakses ruang siber. Adapun hal lain yang cukup menarik adalah korea selatan melakukan terobosan progresif terhadap aspek pengembangan teknologi serta infrastruktur sistem informasi meskipun pada aspek kedaulatan, Korea Selatan cenderung konservatif. Kebebasan teknologi serta didukung regulasi yang tepat memberikan keamanan bagi kelompok siber untuk membuat ekosistem siber yang efektif.

Dokumen KSCSS menunjukan bahwa strategi Korea Selatan dalam konteks keamaan siber menyangkut hal-hal yang bersifat teknis, administratif, kolaboratif, dan praktis. Pun demikian, Korea Selatan menggunakan pendekatan terbuka terhadap perkembangan tekonologi sehingga berbagai pihak baik pemerintah maupun diluar pemerintah bisa bersinergi membentuk suatu aliansi yang konstruktif untuk mencapai kepentingan nasional Korea Selatan.

Pengalaman analisa yang mendalam dan *advance* ini didapatkan dari *software* MAXQDA yang mampu mengkategorikan seberapa besar prioritas yang ada bagi strategi keamanan siber Korea Selatan. Analisis jaringan yang dimiliki Gephi juga menyusun konektivitas yang adadalam unsur-unsur keamanan siber Korea Selatan. Kombinasi analisa ini kemudian menjadikan data yang terpetakan dengan baik. Gambaran mengenai apa yang diperlukan bagi Kanada terhadap strategi keamanan sibernya serta faktor-faktor apa saja masuk dalam katergori keamanan siber telah teridentifikasi, Prioritas dan faktor tersebut terdiri dari *nation* (*core, infrastructure, application*); *sovereignty* (*exclusive* dan *transfer*) dan *aspects* (*national cybersecurity, cyberspace threats, cybersecurity awareness, international rules, laws and regulations, cyber crisis nation-wide, cyber crime,* dan *critical infrastructure*).

Bibliografi

Bjola, C., & Pamment, J. (2018). *Countering online propaganda and extremism: The dark side of digital diplomacy*. Routledge.

Dimas. (n.d.). (n.d.). *Microsoft bangun pusat cyber di Korea*. https://kriptologi.com/2016/03/09/microsoftbangun-pusat-cybersecurity-di-korea

Eoghan, C. (2001). *Digital Evidence and Computer Crime*. A Harcourt Science and Technology Company.

Howard, & J. D. (1995). *An Analysis of Security Insidents of the Internet*.

National Security Office of South Korea. (2019). *International Telecommunication Union*.

Plano, & J. C. (2000). *Kamus Hubungan Internasional*. Abardin.

Soltani, F., Naji, S., & Amiri, R. E. (2015). Levels of Analysis in International Relations and Regional Security Complex Theory. *Journal of Public Administration and Governance*.

Sørensen, G., & Jackson, R. (2005). *Pengantar Studi Hubungan Internasional*.

Yeli, H. (n.d.). *A Three-Perspective Theory of Cyber Sovereignty*. *2*, 109–115.