Strategi Keamanan Siber Nasional Qatar
(Qatar's National Cyber Security Strategy)

Anggraeni Silvia & Adi Muhajirin
Universitas Paramadina &
Universitas Bhayangkara Jakarta Raya
E-mail:anggraeni.silvia@students.paramadina.ac.id
adi.muhajirin@dsn.ubharajaya.ac.id

Abstract

Along with the development of technology, cyber threats that occur in modern countries has been switched from traditional to non-traditional. That development of technology bears the advancement of science and bring a variety of the interstate. Currently, the country prioritizes in social, economic, law, security, defense and other aspect to Information and Communication Technology. Increasing the cyber threat of Qatar, the governance draws up National Cyber Security Strategy (NCSS) with the aim of building and maintaining a safe cyberspace for protecting national interest and preserves fundamental rights and Qatar's community value. Collectively this aim gives protection and preparing cyber threats with proactive approach. This paper aims to deeply understand Qatar National Cyber Security Strategic by conducting a qualitative analysis of the context of document through the concept of sovereignty approach, nation and contained aspects. The description of aspects that can be seen from the data security relationship, technology development, policies, capabilities, strategic approaches, cyber threats and challenges. Qatar pays special attention to cybersecurity and protection of its vital national information infrastructure as dependence on Information and Communication Technology (ICT) and the internet grows in the country.

Key Word: Cyber Security Strategy, Cyber Threats, Sovereignty

Abstrak

Seiring dengan perkembangan teknologi, ancaman keamanan yang terjadi negara-negara modern beralih dari tradisional ke non-tradisional. Perkembangan teknologi tersebut melahirkan kemajuan ilmu pengetahuan dan membawa berbagai implikasi hubungan antar negara. Saat ini negara memprioritaskan aspek social, ekonomi, hukum, keamanan, pertahanan dan lainnya ke dalam teknologi informasi dan komunikasi. Meningkatnya ancaman siber yang menyerang Qatar, pemerintah menyusun National Cyber Security

Strategy (NCSS) yang memiliki tujuan membangun dan memelihara dunia maya yang aman untuk melindungi kepentingan nasional serta melestarikan hak-hak dasar dan nilai masyarakat Qatar. Secara kolektif tujuan ini memberikan dasar untuk melindungi dan mempersiapkan ancaman dunia maya dengan pendekatan proaktif. Tulisan ini bertujuan untuk memahami secara mendalam QNCSS dengan melakukan analisis kualitatif terhadap konteks dari dokumen tersebut melalui pendekatan konsep kedaulatan, bangsa dan aspek-aspek yang ada di dalamnya. Penjabaran aspek yang dapat dilihat dari relasi data keamanan, pembangunan teknologi, kebijakan, kapabilitas, pendekatan strategik, ancaman siber dan tantangan. Qatar memberikan perhatian khusus pada keamanan siber dan perlindungan infrastruktur informasi vital nasional karena ketergantungan pada Teknologi Informasi dan Komunikasi (TIK) dan internet tumbuh di negara itu.

Kata kunci: Strategi Keamanan Siber, Ancaman Siber, Kedaulatan

Pendahuluan

Qatar merupakan negara dengan ekonomi yang berkembang pesat. Perkembangan ekonomi tersebut didukung dengan kemajuan informasi dan komunikasi yang memperluas jaringan dunia maya Qatar. Teknologi dan infrormasi dalam *cyberspace* Qatar telah menjadi bagian integral dari masyarakat, pemerintah dan industry bisnis. Ketahanan dan keamanan di dunia maya sangat penting bagi kesuksesan dan pertumbuhan Qatar yang berkelanjutan. Oleh karena itu, dibutuhkan strategi nasional yang komprehensif untuk menangani resiko dan ancaman yang muncul saat ini. Saat ini, teknologi memfasilitasi masyarakat namun juga meningkatkan resiko merusak norma sosial dan berbagai ancaman *cyberspace*. Ancaman tersebut datang dari *hacker* dan *hacktivist* bukan hanya dari dalam bahkan pihak asing.

Teknologi memungkinkan Qatar untuk mempertahankan pertumbuhan dan perkembangan ekonomi, memberikan standar hidup yang lebih tinggi untuk generasi mendatang, menciptakan lapangan kerja dan mendorong inovasi. Sejak tahun 2013, Qatar merupakan salah satu negara di Timur Tengah yang rentan akan ancaman siber, contohnya pada November 2013 hingga Maret 2014 kawasan Timur Tengah dan Afrika Utara menerima spam SMS sebesar 1.7 Miliyar teks per bulan. (Qatar National Cyber Security Strategy 2014) Keamanan siber merupakan salah satu capaian terpanjang manusia sepanjang Era Horizontal Abad 21. Dengan demikian, negara dan bangsa haruslah mempu melakukan akselerasi keamanan seiring dengan situasi negara. Dalam hal ini, negara mesti mandiri secara fisik dan psikologi. Kekuatan negara dibentuk oleh keamanan yang mapan dari variasi

ancaman.[1] Menghadapai era globalisasi yang telah membuka era borderless akibat perkembangan teknologi informasi maka jalan yang harus ditempuh oleh setiap negara yaitu dengan menerima perkembangan tersebut.[2]

Qatar memiliki penetrasi Internet yang besar dengan 97,4% rumah tangga menggunakan teknologi nirkabel, per 30 Juni 2016.[3] Menurut World Economic Forum (WEF) tentang Global Indeks Persaingan untuk tahun 2015-2016, Qatar menunjukan peringkat 14 dari 140 negara di dunia dan diperingkat pertama secara global dalam pengadaan produk teknologi pemerintah. (Forum 2015) Bahkan pada tahun 2015 Qatar menduduki peringkat ke-31 di dunia dari 167 negara di bidang teknologi dan infomasi yang diterbitkan oleh International Telecommunication Union (ITU) di bawah naungan PBB.[4] Laporan ini menyimpulkan bahwa Qatar adalah salah satu negara yang berkembang pesat dengan ekspansi yang stabil dalam konektivitas online. Cadangan gas alam yang melimpah, populasi yang relatif kecil serta partisipasi tinggi dalam bisnis dan politik internasional juga menjadikannya target yang sangat menarik untuk serangan dunia maya.

Untuk menanggapi ancaman cyber suatu negara membutuhkan pengelolaan keamanan cyber melalui regulasi kebijakan di bidang *cyber security* dan *cyber defense*. Kesadaran keamanan informasi dapat memainkan peran penting dalam menghadapi serangan *cyberspace* oleh *hacker*. Ancaman yang ditimbulkan oleh hacker dapat berupa perang jaringan. Ada tiga poin tambahan dalam membahas perang jaringan yaitu *Cyber warfare*[5], *Limited cyber warfare*[6] dan *Unrestricted cyber warfare*[7]. Untuk mengatasi tantangan dunia siber, Qatar meningkatkan upaya keamanan sibernya dengan membentuk Qatar's National Center for Information Security (Q-CERT) bersama Carnegie Melon University yang dibentuk pada Desember 2005 menggabungkan badan swasta dan pemerintah untuk memantau dan mengelola berbagai macam risiko dunia maya serta melindungi informasi penting negara infrastruktur. The Cyber Security Division, melalui Q-CERT dan Critical Information Infrastructure Protection (CIIP) memastikan bahwa ancaman online dapat dipantau dan diatasi. Divisi ini bertujuan untuk melindungi sensitive information dan memastikan keamanan di Internet bagi Qatar. (Communications n.d.)

---

1 Adi Rio Arianto, Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21, Jurnal PIR, (Medan, Hubungan Internasional Universitas Potensi Utama, 2020)

2 Chotimah, Hidayat Chusnul. "Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia." Jurnal Diplomasi, Volume 7 No. 4, 2015.

3 Qatar National Cyber Security Strategy, (Doha, Minister of Information and Communications Technology, 2014)

4 International Telecommunication Union, *Measuring the Information Society Report*, (Geneva, International Telecommunication Union, 2016)

5 *Cyber Warfare* merupakan tambahan untuk operasi militer (kunci utamanya adalah superior dalam informasi)

6 *Limited cyber warfare information* infrastructur atau struktur informasi adalah media, target dan juga senjata untuk menyerang

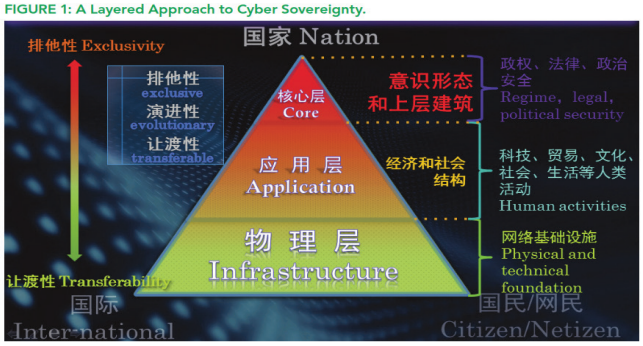
7 *Unrestricted cyber warfare* tidak ada perbedaan antara target sipil dan militer

Pendekatan *Cyber Sovereignty*

Pembahasan mengenai kerangka teori mengacu pada teori kedaulatan yang memiliki sifat *exclusivity* (tertutup) dan *transfer* (terbuka), serta dibagi ke dalam kategori *core*, *application* dan *infrastructure*. Sifat kedaulatan eksklusif pada dasarnya merupakan kedaulatan tradisional namun mempertimbangkan pengalihan kendali pada era globalisasi. Negara menentukan dan memutuskan elemen kedaulatan apa yang harus dipertahankan dan apa yang dapat ditransfer.[8] Keamanan siber telah muncul sebagai tantangan global dan menjadi ancaman keamanan tingkat satu bagi negara berdaulat. Perdebatan yang memanas di forum internasional mengenai aturan dunia maya, dan tantangan sistemik dan revolusioner terhadap tata kelola global di dunia maya.

Kedaulatan dunia maya pasti menjadi fokus kontroversi besar meskipun tingkat konsensus tertentu awalnya dicapai oleh Information Security Group of Governmental Experts (GGE) of the United Nations, namun perbedaan yang mendalam terus membelah komunitas internasional, khususnya yang berkaitan dengan tiga masalah yaitu; Pertama, kontradiksi antara kedaulatan dunia maya dan eksklusivitas klasik kedaulatan negara bertentangan dengan internet yang memiliki konsep interkonektivitas tak terbatas. Jika penekanan ditempatkan pada kedaulatan dunia maya dapat menyebabkan masing-masing negara untuk mendirikan negara yang terpisah dunia maya sendiri, sehingga mengakibatkan fragmentasi internet. Kedua, kontradiksi antara kedaulatan dunia maya dan hak asasi manusia. Ini mencerminkan ketegangan antara prinsip kebebasan berbicara internet, dan intervensi negara atas nama kedaulatan dunia maya, yang membatasi arus informasi yang bebas. Ketiga, kontradiksi antara kedaulatan dunia maya dan keterlibatan berbagai pemangku kepentingan dalam pemerintahan. Dikatakan bahwa kedaulatan dunia maya akan memicu kontroversi pola tata kelola internet; artinya, dipimpin oleh pemerintah yang berdaulat tata kelola akan menantang pola yang ada tata kelola multi-partai.

FIGURE 1: A Layered Approach to Cyber Sovereignty.



Gambar 1. Pendekatan Cyber Sovereignty

[8] Hao Yeli. "A Three-Perspective Theory of Cyber Sovereignty." PRISM Volume 7, No 2, 2017

Pada Gambar 1, Hao Yeli memberikan sudut pandang bahwa pendekatan *Cyber Sovereignty* yang dapat ditinjau dari tiga elemen yaitu *core, application, structure*. Ketiga elemen tersebut mengacu kepada induk data yaitu *Nation*. Di sisi lain, Hao Yeli juga memaparkan bagaimana elemen tersebut memiliki sifat yang dapat mempertajam Analisa keamanan siber yaitu *exclusivity* dan *transferability*. Hao Yeli memberikan sebuah ilustrasi menggunakan diagram untuk menganalisa kebijakan keamanan siber tersebut menggunakan pendekatan kedaulatan. Gambar 1 di atas menggambarkan bahwa level *infrastructure* memiliki kunci mempertimbangkan level analisis dunia maya yang mengarah pada interkonektivitas. Pada level ini negara harus bersedia secara kolektif mentransfer otoritas untuk kepentingan standarisasi dan interkonektivitas tersebut. Negara dengan kapasitas dunia maya yang berkembang dengan baik harus mengambil inisiatif untuk memperluas konektivitasnya ke negara-negara yang kurang mampu untuk menjembatani kesenjangan global. Pada level *application*, dapat dikaitkan dengan banyaknya cakupan platform internet dunia maya yang telah mengintegrasikan berbagai sector seperti teknologi, budaya, ekonomi, perdagangan dan aspek kehidupan sehari-hari atau aktivitas manusia. Di level ini, kedaulatan dunia maya harus disesuaikan dengan kondisi local, dengan tujuan untuk mencapai keseimbangan yang dinamis serta kebebasan dan ketertiban.

Level paling tinggi adalah *core* atau ideologi terdiri dari rezim, hukum dan keamanan politik. pada level ini negara memiliki kendali pengelolaan penuh atas dunia maya yang meliputi strategi, pengembangan teknologi dan penanggulangan ancaman. Pemahaman yang komperhensif mengenai ketiga tingkat tersebut semakin memperjelas perbedaan antara sifat multilateral yang didorong oleh kedaulatan negara dan multi partai. Kedaulatan eksklusif dan transfer memiliki perbedaan penerapan dalam berbagai area dalam dunia maya seperti yang berhubungan dengan ideologi, kebijakan, hukum, kelembagaan dan masalah keamanan.

Aktor di balik kontradiksi kedaulatan dunia maya adalah negara dan komunitas internasional. Di balik kontradiksi kedaulatan dunia maya dan hak asasi manusia adalah negara dan warga negara. Kontradiksi kedaulatan dunia maya dan tata kelola multi-pemangku kepentingan melibatkan negara, warga negara, dan komunitas internasional. Berdasarkan prinsip internasional modern yurisprudensi, kedaulatan dunia maya harus mencerminkan hak dan tanggung jawab nasional dan dasar untuk pembangunan tatanan dunia maya yang bermanfaat. Di era internet, hukum rimba seharusnya memberi jalan untuk solidaritas dan tanggung jawab bersama. Koneksi yang dibatasi harus memberi jalan pada keterbukaan. Intoleransi harus diganti dengan pemahaman dan nilai-nilai sepihak harus mengalah menghormati perbedaan sambil mengakui pentingnya keanekaragaman

Metode Penelitian

Melalui pendekatan kualitatif, penulis bertujuan untuk memperoleh gambaran

besar tentang strategi kemanan siber Qatar dilihat dari sudut pandang konsep kedaulatan. Pertanyaan kritisnya tentu saja jawaban atas alasan mendasar yang mengarah pada: [Q1] aspek kedaulatan (core, application, infrastructure; exclusive atau transfer) mana sajakah yang menjadi fokus Qatar dalam mengatur keamanan siber negara? [Q2] bagaimanakah cara Qatar melaksanakan strategi keamanan siber negara guna menghadapi berbagai ancaman siber (cyber threats)? Setelah itu, data kualitatif yang diperoleh akan disajikan secara kuantitatif guna memberikan penguatan bukti serta relasi data antara aspek yang diatur dengan tata kelola yang dilaksanakan oleh Qatar untuk mengimplementasikan strategi keamanan siber.

Dalam menganalisis *National Cyber Security Strategy*, penulis menggunakan aplikasi MAXQDA 2020 untuk membangun analisa kontekstual pada dokumen Qatar NCSS. Aplikasi tersebut bertujuan untuk mengkuantifikasi data kualitatif yang disusun oleh pemerintah Qatar. Setelah mengkuantifikasi data kualitatif tersebut bisa terlihat fokus pemerintah Qatar dalam menanggulangi ancaman siber. Melalui aplikasi MAXQA 2020, penulis dapat membedah isi dari data kualitatif menggunakan kerangka teori *cyber sovereignty* yaitu *core, application, infrastructure, exclusive* dan *transfer*. Masing-masing point penting di dalam data QNCSS dapat dikuantifikasikan ke dalam kerangka teori tersebut dan menambahkan code untuk aspek-aspek yang dibahas dalam data kualitatif.

Setelah mendapatkan hasil kuantifikasi data kualitatif dari MAXQDA 2020, dilanjutkan dengan penggunaan aplikasi Gephi 0.9.2. Gephi merupakan perangkat lunak *open-source* yang berguna untuk melakukan visualisasi dan eksplorasi segala jenis grafik dan network. Penggunaan aplikasi tersebut digunakan untuk melihat atau menganalisis relasi data antara satu aspek dengan aspek lainnya dengan menggunakan network analysis. Analisa lanjutan dilakukan dengan merelasikan data-data yang timbul diantara satu aspek dengan aspek lainnya dengan cara membuat *coding* dalam dokumen Qatar National Cyber Security Strategy. *Coding* ini terbagi dalam tiga code (masing-masing code memiliki sub-code) dengan penjabaran sebagai berikut:

a. *Code (Nation)* dengan *sub-code: core, infrastructure*, dan *application*;
b. *Code (Sovereignty*) dengan *sub-code*: *exclusive* dan *transfer*;
c. *Code (Aspects*) dengan *sub-code*: *Security/Defense, Technology Development, Policy/ Political Action, Capabilities, Strategic Approach, Cyber Threats Challenges*

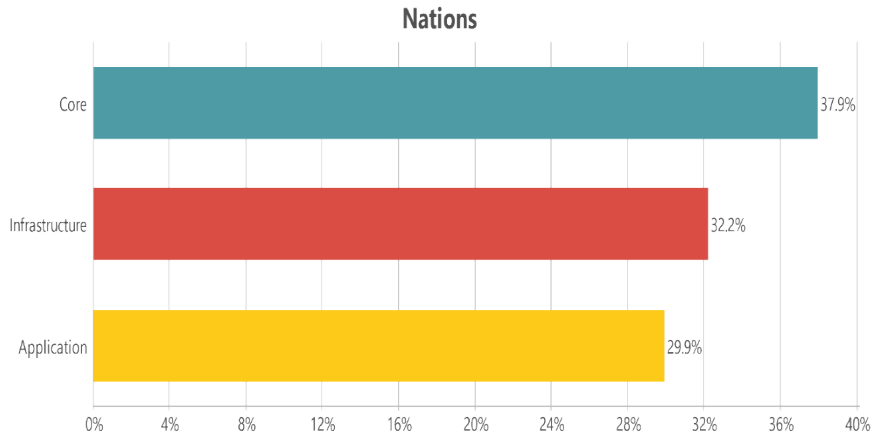
Qatar National Cyber Security Strategy

Perekonomian Qatar berkembang pesat didukung kemajuan informasi dan komunikasi yang memperluas jaringan dunia maya Qatar. Ketahanan dan keamanan siber sangat penting bagi kesuksesan dan pertumbuhan Qatar yang berkelanjutan. Oleh karena itu, dibutuhkan strategi nasional yang komprehensif untuk menangani resiko dan ancaman yang muncul. Pada bagian ini, penulis mencoba untuk mengurai

lebih lanjut tentang strategi keamanan siber Qatar serta aspek-aspek yang diatur oleh otoritas setempat. Sistematika yang dibangun penulis adalah dengan mengurai dokumen QNCSS menjadi unit gramatikal (satuan kalimat) yang selanjutnya disebut dengan *corpus*.

Nations

Temuan yang diperoleh dari hasil olahan data menggunakan MAXQDA didapati bahwa kedaulatan yang diatur oleh Qatar dalam dokumen QNCSS didominasi oleh aspek Core/Ideologi (37,9%), setelah itu aspek infrastruktur sebesar 32,2% dan dengan nilai yang terendah yaitu application sebesar 29,9%. Presentase tersebut menggambarkan seberapa besar aspek *nations* yang bersinggungan juga dengan aspek-aspek lainnya.



Gambar 2. Presentase Code (Nations) pada QNCSS

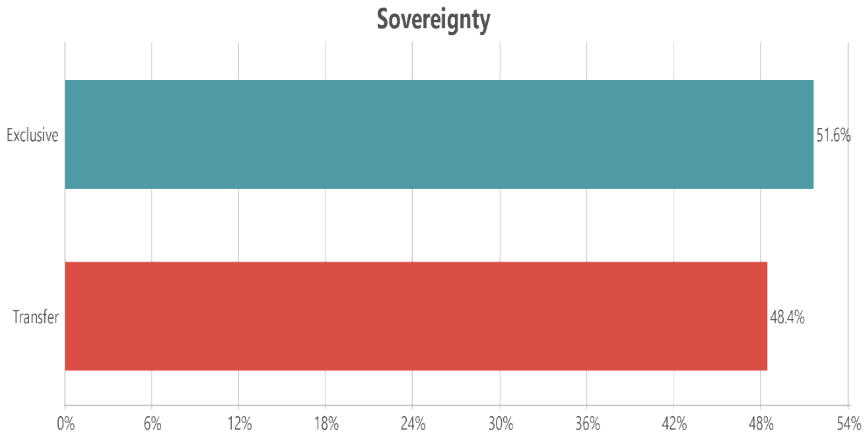
Dengan perolehan nilai tertinggi, *core* atau ideologi menggambarkan bahwa pemerintah Qatar memiliki peran yang sangat penting dalam strategi keamanan siber. Salah satu peran pemerintah Qatar adalah pada tahun 2014 mengeluarkan undang-undang guna memerangi kejahatan teknologi informasi. Undang-undang tersebut mencakup 54 pasal, dan mendefinisikan 11 istilah hukum yaitu *information technology, information network, information system, information processing, password data, website, Electronic crime, electronic card,service provider,* dan *customer data*. Qatar adalah contoh ideal untuk menggambarkan dampak suatu bangsa yang mungkin dihadapi karena kejahatan dunia maya.

Infrastruktur pada posisi kedua, menggambarkan bahwa satu hal yang penting bagi strategi keamanan siber adalah membangun teknologi. Dengan harapan semakin canggih teknologi yang dimiliki oleh Qatar maka semakin besar pula keamanan yang akan diperoleh. Presentasi terkecil adalah *application*, namun jika dilihat selisih antara *infrastructure* dan *application* hanya sebesar 2,3%. Dapat disimpulkan bahwa pemerintah Qatar juga sangat memperhatikan aktivitas individu dalam dunia maya.

Namun aktivitas manusia juga dapat menjadi ancaman seperti *hacktivist, cybercrime syndicates, Trojans* dan virus-virus lainnya, sehingga peran pemerintah dalam pengawasan terhadap aktivitas di *cyberspace* sangat diperlukan.

Kedaulatan/*Sovereignty*

Setelah mengetahui besaran aspek kedaulatan yang diatur oleh otoritas Qatar yang tercantum dalam dokumen QNCSS, perbandingan antara sifat kedaulatan tertutup dan terbuka yang diatur oleh Qatar dapat dilihat pada diagram berikut ini:



Gambar 3. Presentase Code (Sovereignty) pada QNCSS

Dalam QNCSS, sifat kedaulatan berada dalam level eksklusif dengan perolehan nilai 51,6%. Artinya, negara lebih dominan dalam mengelola strategi keamanan siber. Sehingga, kebijakan keamanan dan ketahanan yang ditawarkan oleh negara dapat menjamin seluruh pihak dari ancaman siber. Namun, selisih dari eksklusif dan transfer hanya sebesar 3,2% yang berarti Qatar tidak menutup diri untuk melakukan kerja sama dengan pihak ketiga untuk membangun infrastruktur yang akan meningkatkan keamanannya. Kedaulatan eksklusif dan transfer memiliki perbedaan penerapan berbagai area dalam dunia maya seperti yang berhubungan dengan ideologi, kebijakan, hukum, kelembagaan dan masalah keamanan.

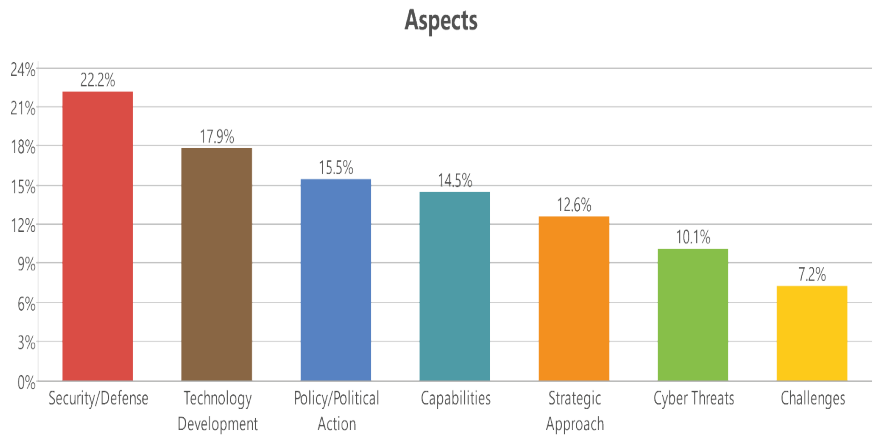
Dari data *nation* dan *sovereignty* di atas dapat diambil kesimpulan bahwa *core* atau ideologi berkaitan erat dengan kedaulatan eksklusif. Hal tersebut merupakan tujuan dari pemerintah Qatar untuk melindungi dan mempersiapkan ancaman dunia maya dengan pendekatan proaktif serta mendeteksi, menanggapi dan memulihkan. Publikasi *Global Cybersecurity Index* 2017 (GCI) menunjukkan bahwa Qatar menempati urutan ketiga dalam inisiatif untuk memerangi kejahatan dunia maya.[9] Qatar's *Cybercrime Investigation Center and Information Security Center* bekerja sama

[9] International Telecommunication Union, (Geneva, Global Cybersecurity Index (GCI), 2017)

secara kolektif untuk mengamankan data dan menghapus kejahatan online yang mengeksploitasi teknologi. *Qatar's Ministry of Transportation and Communication* yang dikenal sebagai ictQATAR melakukan peningkatan keamanan siber Qatar dan untuk mencapai tujuan teknologi Negara. Q-CERT mempertahankan Threat Monitoring System (TMS), yang merupakan *fully automated security-related data collection* dari *distributed sensor* seperti SPAMTRAPS dan HONEYPOTS untuk menganalisis dan melaporkan visibilitas yang lebih besar, jaringan, dan kesadaran situasi ancaman. (Q-CERT n.d.)

Aspects

Untuk dapat mengetahui lebih lanjut, maka perlu dilakukan analisa terhadap aspek-aspek yang berkaitan dengan fokus QNCSS tersebut. Hasilnya, aspek yang berkaitan ada 7 aspek yaitu: *Security/Defense, Technology Development, Policy/Political Action, Capabilities, Strategic Approach, Cyber Threats* dan *Challenges.*



Gambar 4. Presentase Aspek-Aspek pada QNCSS

Poin ini menunjukkan data yang terbagi ke dalam kelompok *security/defense, technology development, policy/political action, capabilities, strategic approach, cyber threats,* dan *challenges.* Seluruh aspek tersebut merupakan isi dari QNCSS yang secara kontekstual guna mengetahui seberapa besar keterkaitan antara aspek satu dengan aspek lainnya. Dalam grafik tersebut aspek yang paling tinggi adalah security/ defense, ini mencerminkan bahwa Qatar mendesain NCSSnya guna memenuhi kebutuhan keamanan atau ketahanan. Qatar merupakan negara di Timur Tengah yang rentan mengalami ancaman siber. Menanggapi hal tersebut, pemerintah Qatar gencar membangun teknologi dan mengeluarkan berbagai kebijakan siber. Kapabilitas pemerintah Qatar dalam NCSS merupakan pendekatan strategis dalam menaggulangi ancaman siber dan menghadapi tantangan globalisasi. (Qatar National

Cyber Security Strategy 2014)

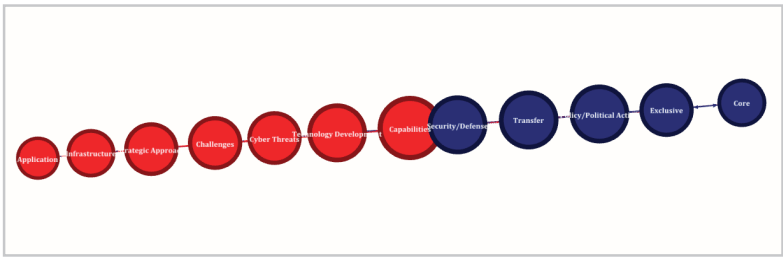
NCSS menjadi garda terdepan dalam melindungi data, jejaring, teknologi dan aspek lainnya baik dari pengguna maupun dari mitra. Perkembangan teknologi keamanan siber menjadi kunci utama bagi Qatar guna membangun jaringan, data yang aman sehingga Kerjasama dengan berbagai mitra tidak terancam oleh isu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

Korelasi Data

Code System	Asp...	Cap...	Secu...	Chal...	Cyb...	Polic...	Strat...	Tech...	Sov...	Excl...	Tran...	Nati...	Core	App...	Infra...
Aspects															
Capabilities			6	1	2	2	4	8		10	4		6	3	6
Security/Defense		6		4	8	9	4	9		12	9		13	5	6
Challenges		1	4		7	5	5	6		10	4		6	2	3
Cyber Threats		2	8	7		2	2	2		8	2		6	7	2
Policy/Political Action		2	9	5	2		8	4		12	7		11	5	3
Strategic Approach		4	4	5	2	8		6		3	5		4	2	3
Technology Development		8	9	6	2	4	6			3	7		2	6	7
Sovereignty															
Exclusive		10	12	10	8	12	3	3			1		27	1	1
Transfer		4	9	4	2	7	5	7		1			1	10	13
Nations															
Core		6	13	6	6	11	4	2		27	1				1
Application		3	5	2	7	5	2	6		1	10				
Infrastructure		6	6	3	2	3	3	7		1	13		1		

Gambar 5. Matrix Relasi Data pada MAXQDA 2020

Hasil akhir dari pengolahan relasi data menggunakan GEPHI adalah sebagai berikut:



Gambar 6. Hasil Relasi Data Utama pada GEPHI

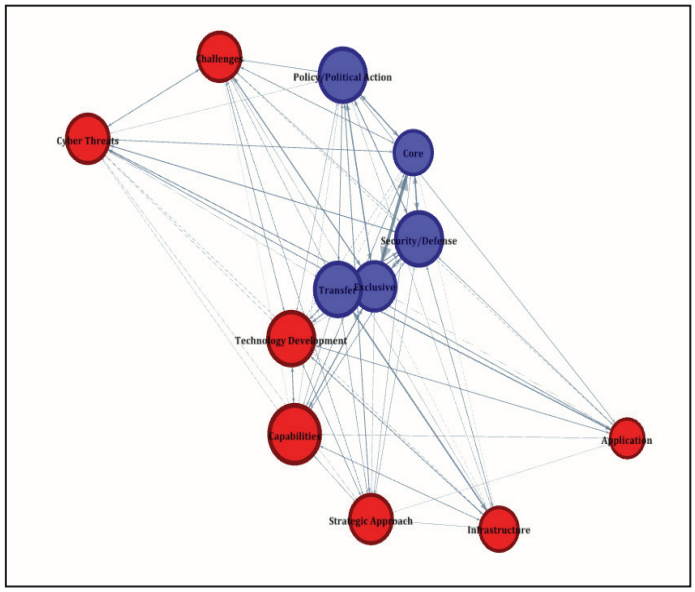
Gambar di atas menunjukkan bagaimana relasi data antara satu aspek dengan aspek lainnya menghasilkan dua *cluster* data besar: Merah dan Biru. Untuk memudahkan dalam menelaah relasi data, tampilan data dengan menyematkan fitur tambahan pada pengaturan *layout* GEPHI. Temuan yang dapat diperoleh dari kedua *cluster* tersebut adalah sebagai berikut:

a. Cluster Merah terdiri dari *nodes* (berurutan dari besar ke kecil)*: Application, Infrastructure, Strategic Approach, Challenges, Technology Development,* dan *Capabilities*.
b. Cluster Biru terdiri dari: *Security/Defense, Transfer, Policy/Political Action, Exclusive,* dan *Core/Ideology*.

Sehingga dapat dipahami bahwa relasi data yang terdapat pada [C1] merupakan aspek-aspek yang memiliki kaitan dengan kapabilitas pembangunan teknologi dalam tantangan ancaman siber, sedangkan [C2] berkaitan dengan keamanan dan pertahanan yang di dapat tidak hanya dari otoritas pemerintah namun kerja sama dengan pihak lain baik di dalam negeri maupun di luar. Langkah berikutnya adalah menambahkan *filter* untuk membaca relasi secara lebih mendalam dari bentuk layout radial axis dengan cara:

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

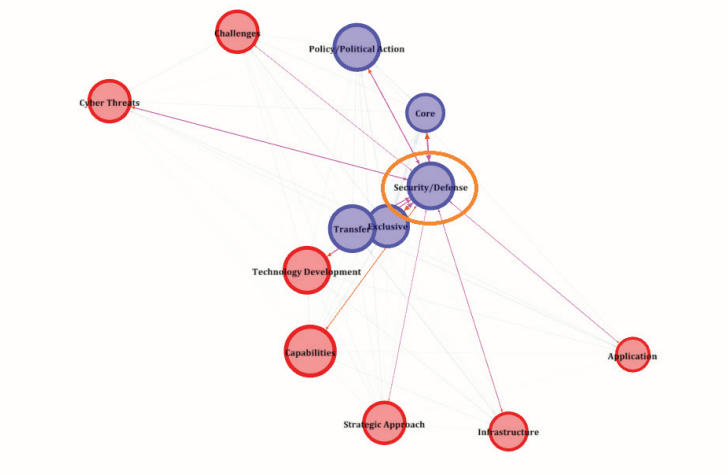
Setelah melakukan langkah-langkah tersebut, hasil yang diperoleh adalah sebagai berikut:



Gambar 7. Layout (spiral) radial axis pada Gephi

Untuk penjelasan yang lebih terperinci, maka menyajikannya pada poin-poin di bawah ini:

1. *Security/Defense*



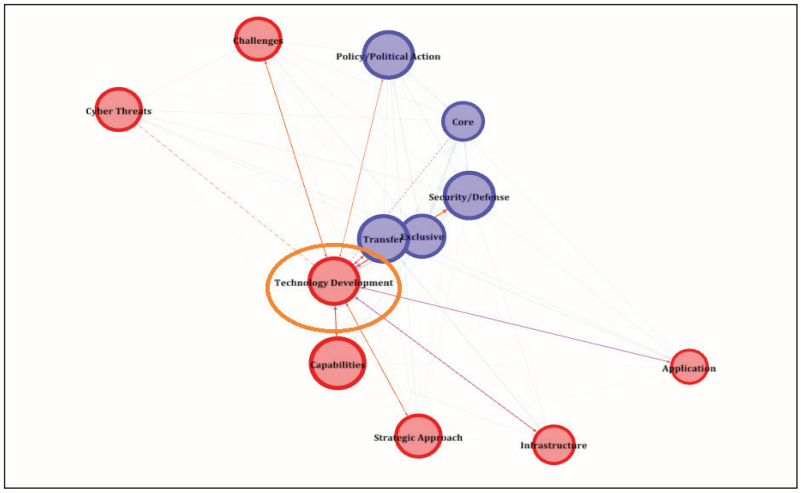
Gambar 8. Relasi Aspek Security/Defense

Keamanan dan ketahanan merupakan aspek paling tinggi yang difokuskan oleh pemerintah Qatar dalam QNCSS dengan nilai 22,2%. Dalam konteks relasi, seluruh aspek memiliki hubungan dengan aspek keamanan dan ketahanan tanpa terkecuali. Untuk mendukung upaya Qatar untuk menjaga jaringan dan masyarakat tetap aman serta untuk mengatasi ancaman dan risiko dunia maya saat ini dan yang muncul, QNCSS dikembangkan oleh *National Cyber Security Committe* dan dikembangkan oleh *the Ministry of Information and Communications Technology*, mengingat dorongan strategis dari Qatar's National ICT Plan 2015 untuk melindungi infrastruktur informasi kritis nasional dan untuk menyediakan lingkungan online yang aman dan terjamin untuk berbagai sector.

Kejahatan dunia maya mengancam keamanan seseorang atau negara dan kesehatan keuangan, dan tanggapannya biasanya merupakan yurisdiksi lembaga penegak hukum. Meski tidak ada yang pasti definisi doktrinal dari "*Cyberwarfare*" atau "*Cyberwar*," adalah dikonseptualisasikan sebagai "tindakan oleh negara-bangsa atau organisasi internasional untuk menyerang dan mencoba merusak komputer atau jaringan informasi negara lain melalui Motivasi taktis untuk perang dunia maya didasarkan pada keserakahan atau mendapatkan kekuasaan atau menyakiti secara emosional dan fisik. Salah satu kegunaan *cyberwar* adalah untuk membuat serangan konvensional lebih mudah dengan menonaktifkan pertahanan musuh sementara penggunaan lainnya perang dunia maya adalah mengirimkan propaganda untuk mendemoralisasi musuh dengan menyebarkan email atau menyebarkan berita palsu melalui orang lain Media internet.

Qatar telah menyaksikan banyak serangan dunia maya dalam beberapa tahun terakhir karena penetrasi internet dan transformasi cepat. Pada 2014, Qatar menduduki peringkat pertama di seluruh dunia dengan 91,5% orang menggunakan Internet di antara semua negara makmur, menurut State of Laporan Broadband edisi 2015. (Communication 2015) Pada tanggal 16 September 2014, Qatar mengumumkan hukum pencegahan kejahatan dunia maya untuk mencegah orang yang tidak berwenang pelanggaran data dan bentuk kejahatan dunia maya lainnya. Itu undang-undang termasuk beberapa hukuman terhadap individu yang melanggar privasi. (Tamimi 2014) Undang-undang tersebut mengatur secara eksplisit tentang online pelanggaran kekayaan intelektual, peretasan, pemalsuan dokumen elektronik, dan tidak sah lainnya akses ke sistem informasi, penipuan kartu kredit. Ini juga mencakup *cyberterrorism* dan pemalsuan melalui media online, pornografi anak dan pencemaran nama baik, pemerasan, pelanggaran privasi dan perilaku tidak masuk akal. (Group 2014)

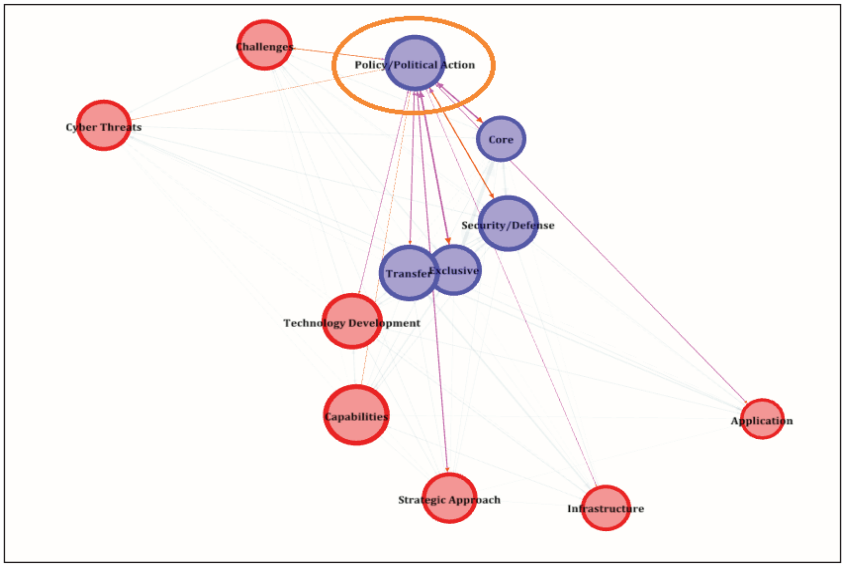
2. **Technology Development**



Gambar 9. Relasi Aspek *Technology Development*

Pengembangan teknologi dipengaruhi berbagai faktor, seperti ancaman siber dalam berbagai aspek yang juga mempengaruhi kehidupan sosial. Pengembangan teknologi pada data diatas, memiliki nilai yang cukup tinggi yaitu 17,9% dan cakupan relasi yang luas dengan aspek lainnya. Hal ini menggambarkan bahwa pengembangan teknologi menjadi kategori yang penting dalam keamanan siber. Teknologi siber Qatar merupakan proses pencapaian tujuan untuk mengamankan dan melindungi data siber yang dimiliki dari bagai kalangan, baik keamanan individu, kelompok, negara, atau entitas lainnya serta melindungi kepentingan nasional. Sehingga pengembangan teknologi menjadi fondasi dasar bagi negara untuk mengamankan keamanan siber di ruang yang bebas dan terbuka baik dengan inovasi yang dibuat oleh berbagai actor didalam negeri maupun melakukan kerangka kerja sama dengan negara lain. Menurut *Internet Corporation for Assigned Names and Numbers* (ICANN), *Qatar Domain Registry* (QDR) adalah yang pertama untuk mengadopsi standar baru dan untuk memulai DNSSEC proyek, Ekstensi Keamanan Sistem Nama Domain yang bertujuan untuk menjamin keamanan dan stabilitas Domain Qatar.

3. **Policy/Political Action**



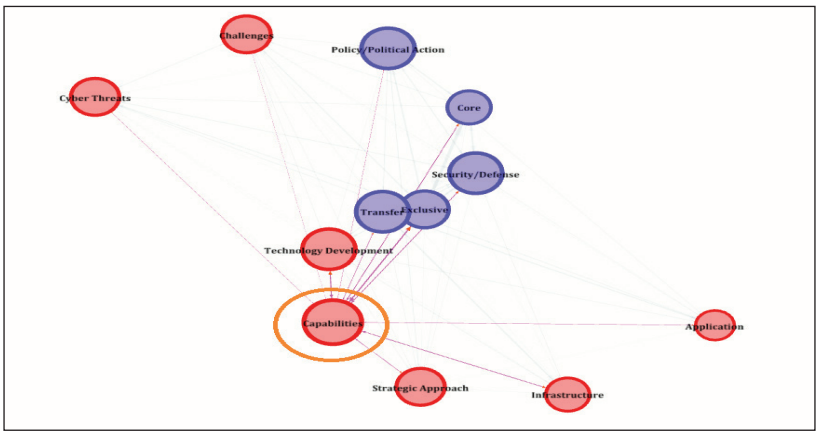
Gambar 10. Relasi Aspek *Policy/Political Action*

Pada aspek ini, kebijakan atau aksi politik memiliki nilai 15,5% yang menggambarkan bahwa negara memainkan peran penting dalam strategi keamanan siber Qatar, penguatan peran negara dalam kebijakan dan aksi politi juga merupakan hal yang penting bagi Qatar dalam mencegah potensi ancaman. Kebijakan atau aksi politik dalam konteks relasi juga merupakan aspek yang terhubung dengan hampir semua kode. Dengan relasi tersebut, peran negara menjadi sentral dalam pertahanan siber Qatar.

Mendukung serangan siber, file negara-negara di kawasan Teluk memutuskan hubungan politik dengan Qatar dengan memberlakukan blokade darat, udara dan laut yang parah pada mereka negara tetangga. Itu semacam perang dunia maya dengan Qatar melalui penyebaran pernyataan keliru yang diterima Qatar menjadi situasi menyedihkan yang membahayakan otoritas dan memimpin untuk keadaan yang tidak menguntungkan. Serangan ini dimaksudkan untuk merusak postur keamanan Qatar oleh negara lain. *Cybercrime* memiliki dampak sosial, ekonomi, fisik, politik dan dampak emosional pada hidup kita. Itu adalah risiko utama yang dihadapi oleh banyak organisasi bisnis di seluruh dunia yang membutuhkan biaya ekonomi global lebih dari 400 miliar dolar setiap tahun. Menurut sebuah perusahaan riset ekonomi siber, file Kerusakan akibat kejahatan dunia maya diperkirakan akan merugikan dunia sekitar $ 6 triliun pada tahun 2021 setiap tahun. (Cyber Crime Magazine - Cybercrime Damages $6 Trillion By 2021 n.d.) Serangan dunia maya dapat menyebabkan kerugian besar di tingkat negara, negara bagian, organisasi, dan individu. Terkadang penyerang mencuri informasi rahasia dari negara untuk

mengancam atau dengan motif lainnya. Jenis peretasan ini dapat digunakan sebagai jenis baru senjata untuk memulai perang atau memenangkan negara.

4. *Capabilities*

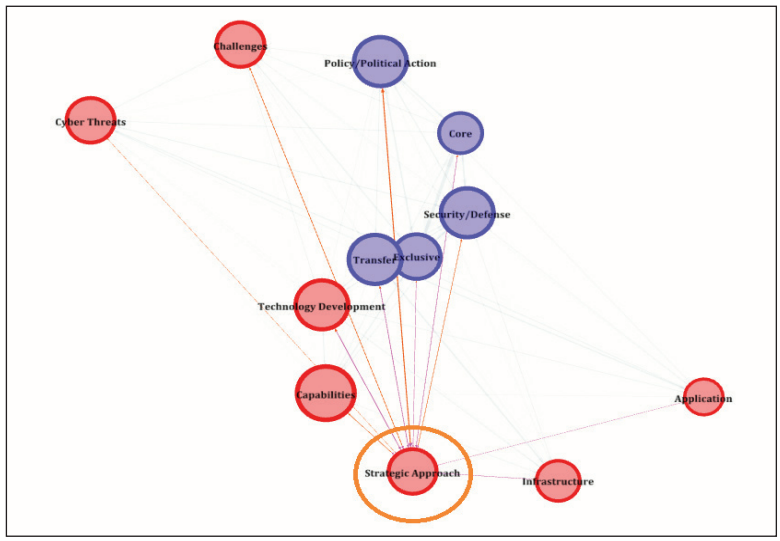


Gambar 11. Relasi Aspek *Capabilities*

Pada aspek ini, negara melalui kebijakan dan prinsip-prinsip mengembangkan kapabilitas dalam hal perwujudan ketahanan dan keamanan nasional. Kapabilitas negara dapat meliputi keamanan dan kesejahteraan dengan nilai 14,5% dalam QNCSS dan memiliki relasi yang cukup kuat dengan seluruh aspek. Kesejahteraan negara akan membantu menciptakan pertahanan dan keamanan yang sesuai dengan tujuan atau kepentingan nasionalnya. Peran pemerintah dan organisasi baik internal maupun eksternal turut mendukung kesejahteraan dan keamanan siber. Pembangunan jaringan internet, peralatan penting, tetapi aktor juga tak kalah penting. Sebagai contoh konkrit Perdana Menteri membentuk Komite Keamanan Siber Nasional untuk menangani agenda dunia maya di tingkat nasional untuk memastikan bahwa semua entitas publik dan swasta mengadopsi agenda dunia maya yang benar.

Pengetahuan dan pelatihan diperlukan untuk berperang ancaman, IctQATAR terorganisir dan juga bergabung dalam beberapa konferensi berfokus tentang masalah privasi kritis yang mempengaruhi wilayah Timur Tengah dan mengeksplorasi masalah global yang lebih luas di tingkat internasional. ictQATAR dan Q-CERT bekerja sama secara berdedikasi dengan lembaga pemerintah, sekolah dan organisasi dan warga Qatar untuk memahami dan mengelola potensi risiko.

5. *Strategic Approach*

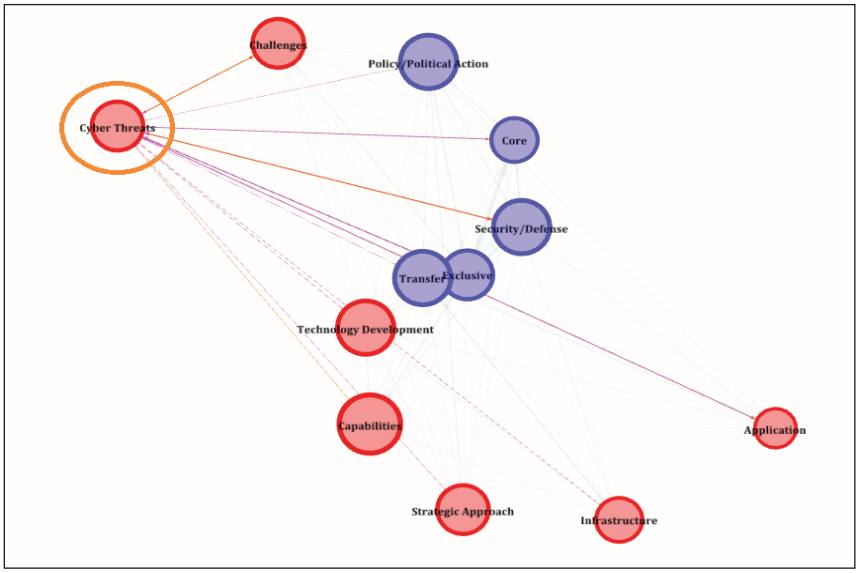


Gambar 12. Relasi Aspek *Strategic Approach*

Aspek pendekatan strategik dalam QNCSS seperti yang dibayangkan dalam visi nasional Qatar 2030, mewakili peta jalan menuju peningkatan keamanan dunia maya di Qatar. Selain itu, QNCSS memberikan rencana tindakan dengan detail lebih lanjut tentang rencana pemerintah Qatar untuk mencapai visi keamanan dunia maya Qatar selama periode 2014-2018. Rencana tersebut disusun berdasarkan tujuan dan mengharuskan berbagai pemangku kepentingan dari entitas dan lembaga pemerintah untuk bekerja sama dengan banyak pihak lainnya guna melaksanakan tujuan ini dan tindakan yang relevan untuk kepentingan Qatar. Dengan nilai 12,6%, pendekatan strategik merupakan hal yang penting untuk menilai focus pemerintah Qatar dalam mengambil kebijakan terkait *cyber security*. Terbukti, relasi pada aspek pendekatan strategik memiliki hubungan dengan hampir seluruh aspek yang ada pada QNCSS.

Bekerja sama dengan ITU-Arab Regional Office, ictQATAR dan negara GCC lainnya, menjadi tuan rumah Arab's Region CERTS setiap tahun untuk meningkatkan kemampuan komunikasi, membangun tim dan kemampuan respons ancaman siber, sambil mempertahankan upaya yang sedang berlangsung oleh *Arab Computer Emergency Response Teams* (CERT) di memerangi ancaman siber. *(Qatar to host fifth regional cyber drill 2017) Qatar National Research Fund* (QNRF) pada tahun 2006 dan Qatar Computing Research Institute (QCRI) pada tahun 2010 untuk mengintensifkan pendidikan dan penelitian di bidang ilmu pengetahuan dan keamanan, secara khusus berfokus pada keamanan siber. QCRI telah mengambil proyek sistem dan jaringan kendali industry arsitektur untuk melindungi jaringan ICS untuk air sistem pemurnian (Kahramaa), gas dan minyak industri.

6. *Cyber Threats*



Gambar 13. Relasi Aspek *Cyber Threats*

Ancaman siber yang dihadapi oleh Qatar saat ini meliputi *hacktivist, cybercrime syndicates, Trojans* dan virus-virus lainnya. Seiring meningkatnya ancaman siber yang menyerang Qatar, pemerintah menyusun *National Cyber Security Strategy* (NCSS) yang memiliki tujuan membangun dan memelihara dunia maya yang aman untuk melindungi kepentingan nasional serta melestarikan hak-hak dasar dan nilai masyarakat Qatar. Aspek ini memiliki cakupan relasi yang luas dengan aspek lainnya. Jika dilihat dari relasinya, seluruh aspek memiliki relasi dengan *cyber threats*. Dalam NCSS, aspek *cyber threats* memiliki nilai yang cukup tinggi yaitu 10,1% oleh karena itu pemerintah Qatar memfokuskan dokumen strategi siber pada *security/ defense*.

Pada 2014, Qatar menduduki peringkat pertama di seluruh dunia dengan 91,5% orang menggunakan Internet. Pernyataan ini adalah terbukti bahwa Qatar telah membuat kemajuan luar biasa di bidangnya tujuan telekomunikasi berteknologi tinggi, tetapi berbagai ancaman dunia maya paling mengkhawatirkan yang mengungkapkan kekurangan yang menakutkan dari negara ini. Jumlah pasti serangan siber tidak mungkin dikenal karena beberapa insiden siber tidak dilaporkan. Jadi, sedikit acara dicantumkan di sini untuk memahami potensi jebakan dan implikasinya. *Cyber Security Division in Qatar* merupakan member dari *Global Forum Of Incident Response and Security Teams* yang bertujuan memelihara, berbagi informasi ancaman, dan berkolaborasi dengan tim keamanan dan mitra di seluruh dunia. Qatar juga bermitra dengan Interpol untuk meningkatkannya berbagi informasi dan penegakan hukum untuk menyelidiki dan menuntut kejahatan dunia

maya. Qatar juga telah bekerja dengan *Interpol Global Complex for Innovation* (IGCI), yang menganalisis berbagai praktik keamanan siber negara dan kemampuan untuk menyelidiki dan menuntut kejahatan dunia maya.

7. **Challenges**

Gambar 14. Relasi Aspek *Challenges*

Qatar saat ini menghadapi banyak tantangan siber seperti keterampilan keamanan siber, konektivitas ICS, kendala berbagi informasi dan penyalahgunaan data pribadi. Meningkatnya penyalahgunaan informasi pribadi di dalam organisasi pemerintah dan di seluruh bisnis internasional, membuat Qatar terus memberlakukan dan memperbarui undang-undang privasi untuk melindungi individu dan datanya. Jika informasi pribadi tidak dilindungi dengan benar, organisasi menghadapi potensi risiko. Pada QNCSS aspek tantangan memiliki nilai 7,2%. Nilai tersebut didasari bahwa dokumen QNCSS membahas aspek tantangan dan kemampuan yang dapat dilakukan oleh pemerintah baik secara eksklusif maupun transfer untuk memenuhi tantangan tersebut.

Metode lain untuk meningkatkan tenaga kerja keamanan siber adalah memeriksa organisasi keamanan siber secara tepat kasus uji nonkonvensional. Agensi yang tidak memenuhi kriteria mekanisme keamanan mutlak harus disertifikasi oleh pemerintah. Proses audit internal yang kuat ini organisasi memastikan bahwa keamanan ada di tangan yang benar. Keamanan siber adalah tanggung jawab Bersama, oleh karena itu harus ada kerjasama erat antara pemerintah dan swasta lembaga untuk melawan serangan cyber. Di luar sertifikasi organisasi, suatu negara harus membangun keamanannya sendiri strategi alih-alih mengandalkan prosedur keamanan pihak ketiga. Praktik bergantung pada orang lain untuk melindungi suatu negara privasi

itu mahal dan tidak pasti. Jadi, keamanan siber yang profesional harus diberikan pelatihan yang dapat mengembangkan tim perlindungan siber yang waspada yang menganalisis, memantau dan mengurangi kemungkinan ancaman dunia maya melalui penelitian proaktif dan alat keamanan yang inovatif.

Penutup

Tata Kelola yang kuat diperlukan untuk menerapkan dan mengelola pelaksanaan QNCSS. Oleh karena itu, Qatar menetapkam prioritas untuk mempromosikan tingkat keamanan siber, memberikan arahan strategis untuk upaya keamanan siber dan bekerja sama dengan organisasi untuk memenuhi tujuan NCSS. Dapat disimpulkan berdasarkan Analisa kualitatif QNCSS bahwa konteks strategi keamanan siber Qatar paling besar mengacu pada kebijakan, pembangunan teknologi dan keamanan serta kapabilitas negara dalam mengelola keamanan dan potensi ancaman siber yang akan datang.

Qatar melakukan langkah progresif terhadap aspek pengembangan teknologi serta sistem informasi. Selain itu, kedaulatan negara yang bersifat eksklusif juga menjadi tolak ukur *nations*. Meskipun memiliki unsur kedaulatan eksklusif, namun Qatar tidak menutup diri untuk melakukan kerja sama dengan pihak ketiga untuk membangun infrastruktur yang akan meningkatkan keamanannya. Dengan mengimplementasikan QNCSS, tercatat bahwa Qatar telah menekankan bahwa serangan dunia maya mengancam keamanan, perdamaian dan stabilitas, bertepatan dengan peringatan tiga tahun kejahatan e-pembajakan yang menargetkan *Qatar News Agency* pada 23 Mei 2017. Sehingga pada aspek kedaulatan, Qatar lebih berfokus pada *Core* dan *Exclusive* yang artinya pemerintah lebih mendominasi pengamanan siber. Pada seluruh aspek, Qatar telah melakukan berbagai upaya untung mengamankan *cyberspace*-nya namun tetap memiliki tantangan yang akan dihadapi kemudian hari. Selain itu, pentingnya keamanan siber dan bahaya terkait penggunaan *Internet of Things* (IoT) adalah perlu diajarkan di lembaga pendidikan untuk meminimalkan terjadinya insiden.

Di dunia maya evolusi teknologi yang tak terbantahkan saat ini penggunaan tidak memiliki analisis hukum, hak atas privasi dan perlindungan data. Meskipun tindakan teknis terbukti berhasil membela serangan dunia maya, standar hukum tidak bisa dihindari mencegah penyerang sebelum berniat menargetkan negara mana pun. Kebijakan ketat harus dirancang untuk menghukum penjahat online sehingga serangan dimitigasi sepenuhnya. Setiap bangsa harus memulai dan memelihara hukum pengaturan mandiri prosedur untuk memerangi penyalahgunaan dunia maya di selanjutnya untuk mencegah dan menghalangi pertumbuhan yang cepat kejahatan dunia maya. Bagaimanapun, sistem seperti itu harus didukung oleh undang-undang internasional juga. Sejak kejahatan dunia maya melintas perbatasan semua negara bagian, penuntutan pelanggar sulit. Oleh karena itu dibutuhkan korporasi asing. Langkah-langkah ini tidak hanya bermanfaat bagi Qatar tetapi juga bermanfaat bagi setiap orang bangsa di dunia.

Pengalaman analisa yang mendalam dan *advance* ini didapatkan dari *software* MAXQDA yang mampu mengkategorikan seberapa besar prioritas yang ada bagi strategi keamanan siber Qatar. Analisis jaringan yang dimiliki Gephi juga menyusun konektivitas yang ada dalam unsur-unsur keamanan siber Qatar. Kombinasi analisa ini kemudian menjadikan data yang terpetakan dengan baik. Gambaran mengenai apa yang diperlukan bagi Qatar terhadap strategi keamanan sibernya serta faktor-faktor apa saja masuk dalam katergori keamanan siber telah teridentifikasi,

Daftar Pustaka

Aliya Tabassum, Mohammad Saleh Mustafa, Sumaya Ali Al Maadeed. "The Need for a Global Response Against Cybercrime: Qatar as a Case Study ." *Conference: 6th International Symposium in Digital Forensic and Security at Antalya Turkey*, 2018.

Al-Jaber, H., & Dutta, S. "Qatar: Leveraging technology to create a knowledge-based economy in the Middle East." 2008.

Arianto, Adi Rio. "Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21." *Jurnal PIR Vol.1 No. 2* (Jurnal PIR Vol.1 No. 2), 2017.

Chotimah, Hidayat Chusnul. "Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia." *Jurnal Diplomasi, Volume 7 No. 4*, 2015.

Communication, Ministry of Transport and. *Qatar Ranks First on Two Significant Internet Penetration Indicators in the State of Broadband Report 2015.* September 22, 2015. https://www.motc.gov.qa/en/news-events/news/qatar-ranks-first-two-significant-internet-penetration-indicators-state-broadband (accessed December 30, 2020).

Communications, Qatar's Ministry of Transport and. *Cyber Security.* n.d. https://www.motc.gov.qa/en/cyber-security.

Cyber Crime Magazine - Cybercrime Damages $6 Trillion By 2021. n.d. https://cybersecurityventures.com/annual-cybercrime-report-2017/.

Cyber Security. n.d. https://www.motc.gov.qa/en/cyber-security (accessed November 27, 2020).

Dutta, HESSA AL-JABER & Soumitra. "Qatar: Leveraging Technology to Create a Knowledge-Based Economy in the Middle East. ." 2020.

Forum, World Economic. *The Global Competitiveness Report 2015–2016.* Geneva: World Economic Forum, 2015.

Group, The CWB. *QATAR – ENACTMENT OF CYBERCRIME PREVENTION LAW.* December 19, 2014. https://www.cwblegal.com/qatar-enactment-of-cybercrime-prevention-law/ (accessed December 30, 2020).

Qatar National Cyber Security Strategy. Minister of Information and Communications Technology, 2014.

Qatar to host fifth regional cyber drill. March 07, 2017. https://www.qatar-tribune.com/news-details/id/51435 (accessed December 30, 2020).

Qatar, ICT. *SUPREME COUNCIL OF INFORMATION & COMMUNICATION TECHNOLOGY / ANNUAL REPORT.* ICT Qatar, 2012.

Q-CERT. *National Information Security Center.* n.d. https://www.qcert.org/activities-objectives.

Section, Public Key Management and Digital Identity. *Qatar National Cryptographic Standard.* Ministry of Transports and Communications, 2019.

Tamimi, Al. *LEXOLOGY - Cyber crime prevention law in Qatar.* October 29, 2014. https://www.lexology.com/library/detail.aspx?g=e9cd1a4e-e48d-481e-9372-0cfa39ecb42e (accessed 12 30, 2020).

Union, International Telecommunication. *Global Cybersecurity Index (GCI) 2017.* International Telecommunication Union, 2017.

Union, International Telecommunication. *Measuring the Information Society Report.* Geneva: International Telecommunication Union, 2016.

Winterfeld, Jason Andress & S. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners: Second Edition. ." 2013.

Yeli, Hao. "A Three-Perspective Theory of Cyber Sovereignty." *PRISM Volume 7, No 2*, 2017.