MUKADIMAH
Jurnal Pendidikan, Sejarah, dan Ilmu-ilmu Sosial
Program Studi Pendidikan Sejarah FKIP - Universitas Islam Sumatera Utara, Medan
e-Journal: http://jurnal.uisu.ac.id/index.php/mkd | e-mail: mukadimah@fkip.uisu.ac.id
ISSN: 2622-1373 (Online)
ISSN: 2614-1159 (Print)
Volume 5 | Issue 1
February 2021

ANALISIS KONTEKSTUAL PADA STRATEGI KEAMANAN SIBER MESIR 2017-2021 DALAM UPAYA PENGAMANAN SIBER NASIONAL

Dian Islami

Universitas Paramadina, Indonesia

Abstract

This study aims to understand and analyze Egypt's cybersecurity strategy in 2017-2021 related to the level of security and the role of each aspect of the cybersecurity strategy in the Egyptian state. This research was conducted because Egypt and Indonesia have several similarities, such as countries with a Muslim majority and fellow members in the Islamic Cooperation Organization, the Non-Aligned Movement, the G-20 developing countries, and the group of 8 developing countries. Qualitative methods are used to analyze the application of the concept of sovereignty theory which is exclusive or transfer, as well as aspects of cybersecurity which include infrastructure, application, and core (ideology). Meanwhile, quantitative methods are used to present the results of data analysis on Egyptian cybersecurity data relations and strategies with MAXQDA2020 and Gephi 0.9.2 applications. Based on the results of the analysis, the authors conclude that the context of Egypt's cybersecurity strategy has a tendency towards collaboration between state actors and non-state-actors based on aspects of national cybersecurity, cybersecurity awareness, cyberspace threats, international rules, laws and regulations, cyber crisis nation-wide. , cybercrime, and cyberinfrastructure. This aspect can be used in the formulation of Indonesia's national cybersecurity strategy policy in the coming year.

Keywords: Cybersecurity; Egypt; data relations.

Abstrak

Penelitian ini bertujuan untuk memahami dan menganalisis strategi keamanan siber Mesir pada 2017-2021 terkait tingkat keamanan dan peran tiap aspek strategi keamanan siber di negara Mesir. Penelitian ini dilakukan karena Mesir dan Indonesia memiliki beberapa berbagai kemiripan seperti negara dengan mayoritas muslim dan sesama anggota dalam Organisasi Kerjasama Islam, Gerakan Non-Blok, negara berkembang G-20 dan kelompok 8 negara berkembang. Metode kualitatif digunakan untuk menganalisa penerapan konsep teori kedaulatan yang bersifat *exclusive* maupun transfer, serta aspek keamanan siber yang meliputi *infrastructure*, *application*, dan *core* (*ideology*). Sedangkan metode kuantitatif digunakan untuk menyajikan hasil analisa data pola strategi dan relasi data keamanan siber Mesir dengan aplikasi MAXQDA2020 dan Gephi 0.9.2. Berdasarkan hasil analisis, penulis menyimpulkan bahwa konteks strategi keamanan siber Mesir memiliki kecenderungan arah pada kolaborasi antara *state-actor* dan *non-state-actor* berdasarkan aspek national *cybersecurity, cybersecurity awareness, cyberspace threats, international rules, laws and regulation, cyber crisis nation-wide, cybercrime, serta cyber infrastructure*. Aspek tersebut dapat digunakan dalam penyusunan kebijakan strategi keamanan siber nasional Indonesia di tahun mendatang.

Kata Kunci: Keamanan siber; Mesir; relasi data.

PENDAHULUAN

Era globalisasi merupakan salah satu faktor utama dalam transformasi banyak hal dalam memasuki era digital. Internet dan Teknologi Informasi Komunikasi (TIK) secara tidak langsung telah menghilangkan batas-batas teritorial antar satu negara dengan negara lainnya. Globalisasi juga telah mentransformasikan hubungan internasional antar negara secara tidak langsung dengan adanya diplomasi digital (Bjola & Pamment, 2018). Kemajuan teknologi yang bagaikan dua mata pisau ini tentu memiliki sisi positif maupun negatif. Pada satu sisi, mudahnya keterhubungan yang terjadi karena TIK telah memudahkan komunikasi dua arah. Namun, di sisi lain, muncul ancaman atau kerawanan dalam pengamanan informasi pada ruang siber. Oleh karena itu, dibutuhkan strategi yang

ARTICLE HISTORY: Submitted: 2021-02-01 | Revised: 2021-02-20 | Accepted: 2021-04-15 | Published: 2020-04-15
HOW TO CITE (APA 6th Edition):
Islami, Dian. (2021). Analisis Kontekstual pada Strategi Keamanan Siber Mesir 2017-2021 dalam Upaya Pengamanan Siber Nasional. *MUKADIMAH: Jurnal Pendidikan, Sejarah, dan Ilmu-ilmu Sosial*. *5*(1), 159-170.
CORRESPONDANCE AUTHOR: dianislami96@gmail.com | DOI: https://doi.org/10.30743/mkd.v5i1.3502

menjadi pedoman atau acuan dalam pengaturan aspek-aspek pertahanan dan keamanan siber dalam skala nasional, guna mencegah dan meminimalisir dampak negatif dari perkembangan dunia siber.

Mesir dan Indonesia memiliki beberapa berbagai kemiripan seperti negara dengan mayoritas muslim dan sesama anggota dalam Organisasi Kerjasama Islam, Gerakan Non-Blok, negara berkembang G-20 dan kelompok 8 negara berkembang. Selain itu, Mesir dan Indonesia juga merupakan *Board Committee* pada OIC-CERT (*Organization of the Islamic Cooperation – Computer Emergency Response Team*) sejak tahun 2013 (BSSN, 2018). OIC CERT merupakan *Computer Emergency Response Team* untuk negara-negara yang tergabung dalam Organisasi Kerjasama Islam (OKI) bertukar informasi dalam penanggulangan dan pemulihan terhadap serangan yang mungkin terjadi di masing-masing negara. Selain itu, OIC CERT juga merupakan platform yang dibentuk oleh OKI untuk mengembangkan dan mengeksplorasi inisiatif kerjasama yang mungkin dapat dijalin di ranah keamanan siber nasional (CERT, 2021). Dengan dipilihnya Indonesia sebagai *Deputy Chair* pada OIC-CERT pada tahun 2018, maka perlu adanya studi banding atau masukan dari negara-negara yang telah memulai berbagai upaya dalam mewujudkan keamanan siber nasional negaranya. Salah satu upaya yang dilakukan antara lain penyusunan dokumen strategi keamanan siber nasional. Mesir sebagai negara yang lebih maju dibandingkan dengan negara lainnya di benua Afrika, telah menyusun dokumen *National Cybersecurity Strategy* periode 2017-2021 (ESCC, 2018).

Tulisan ini bertujuan untuk memahami secara mendalam dokumen *Egypt National Cybersecurity Strategy* 2017-2021 dengan melakukan analisis kualitatif terhadap bangunan konteks dari dokumen tersebut melalui pendekatan terhadap konsep kedaulatan yang diatur serta aspek-aspek lainnya yang tercantum di dalamnya. Dengan memahami konteks yang terkandung, penulis kemudian berusaha untuk menjabarkan secara kuantitatif pola strategi, relasi data: aktor, hukum, politik, ekonomi, administrasi negara dan teknologi yang digunakan oleh Mesir guna mengamankan pertahanan dan keamanan siber nasional dari berbagai ancaman yang dapat mengganggu kedaulatan serta keamanan nasional. Melalui pendekatan kualitatif, penulis bertujuan untuk memperoleh gambaran besar tentang strategi keamanan siber Mesir dilihat dari sudut pandang konsep kedaulatan. Berikut *research question* dalam penelitian ini: (1) Aspek kedaulatan *(core, application, infrastructure; exclusive* atau *transfer)* mana sajakah yang menjadi fokus Mesir dalam mengatur keamanan siber negara? (2) Bagaimanakah cara Mesir melaksanakan strategi keamanan siber negara guna menghadapi berbagai ancaman siber (*cyber threats*)?

METODE

Analisis dilakukan dengan menguraikan secara rinci tentang strategi keamanan siber Mesir serta aspek-aspek yang diatur oleh otoritas setempat. Sistematika yang dibangun penulis adalah dengan mengurai dokumen *Egypt National Cyber Security Strategy* 2017-2021 menjadi unit gramatikal (satuan kalimat) yang selanjutnya disebut dengan *corpus*. *Corpus* yang diperoleh kemudian diklasifikasikan ke dalam *coding* {*Nation*, *Sovereignty*, dan *Aspects*}.

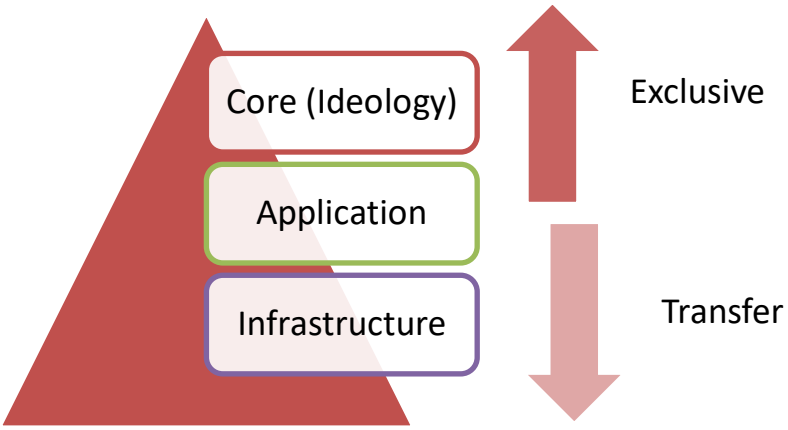
- *Code* {*Nation*} memiliki *sub-code* {*Core (Ideologi), Application,* dan *Infrastructure*}. *Code* ini menjelaskan tentang aspek kedaulatan yang diatur oleh dokumen *Egypt National Cyber Security Strategy* 2017-2021.
- *Code* {*Sovereignty*} berisi *sub-code* {*Exclusive* dan *Transfer*}. Keduanya merupakan sifat dari kedaualatan yang diatur oleh *Egypt National Cyber Security Strategy* 2017-2021.
- *Code* {*Aspects*} merupakan bagian penting dari analisis kualitatif terhadap dokumen *Egypt National Cyber Security Strategy* 2017-2021. Terdiri dari *sub-codes*: {*Collaboration/Cooperation, Society, Legal, Security/Defence, Cyber Threats, Technology Development, State Actor, Non-State Actor, Economic Development,* dan *Political Action*}.

Seluruh aspek tersebut merupakan substansi dari strategi, kendali, serta tata kelola Mesir terhadap keamanan siber yang secara kontekstual diperoleh penulis pada analisis kontekstual terhadap dokumen *Egypt National Cyber Security Strategy* 2017-2021 dengan menggunakan aplikasi

MAXQDA 2020 dan Gephi 0.9.2. Aplikasi MAXQDA merupakan *software* yang digunakan untuk analisis konten dari data yang tidak terstruktur seperti dokumen wawancara, artikel, media, survei, *tweet* dan sebagainya. Sedangkan Gephi 0.9.2 merupakan *software* analisis data yang menyajikan grafik interaktif dan analisis jaringan serta visualisasi yang memungkinkan penggunanya untuk mempelajari sifat-sifat grafik dan jaringan secara rinci, tanpa harus menulis kode apa pun (Pratama, 2018). Hasil analisis data kualitatif dari MAXQDA2020 dimasukkan ke dalam aplikasi GEPHI 0.9.2. untuk dianalisis lebih lanjut sehingga menunjukkan relasi data yang dihasilkan untuk setiap aspek. Relasi data tersebut akan menunjukkan keterhubungan dari berbagai aspek yang saling mempengaruhi dalam strategi keamanan siber Mesir.

KERANGKA TEORETIK DAN KONSEPTUAL

Maraknya ancaman dunia maya atau siber telah menjadikan upaya pengamanan siber merupakan salah satu urgensi bagi negara untuk menjadi prioritas dalam menjaga keamanan nasionalnya. Indonesia sebagai negara yang berkepentingan untuk menjaga keselamatan warga negaranya, turut mengikuti tren dengan melakukan diplomasi siber sebagai media pengamanan jagat siber (Adesina, 2017). Dalam memahami dokumen *Egypt National Cyber Security Strategy 2017-2021*, penulis menggunakan dasar-dasar dari teori kedaulatan yang membagi kedaulatan menjadi dua jenis, yaitu yang bersifat *transfer* (terbuka) dan *exclusive* (tertutup). Selain itu, digunakan juga piramida national *cyber security* yang terbagi menjadi tiga antara lain *core* (*ideology*), *application*, dan *infrastructure* (Yeli, 2017).



Gambar 1. Teori Kedaulatan dan Piramida *National Cybersecurity*

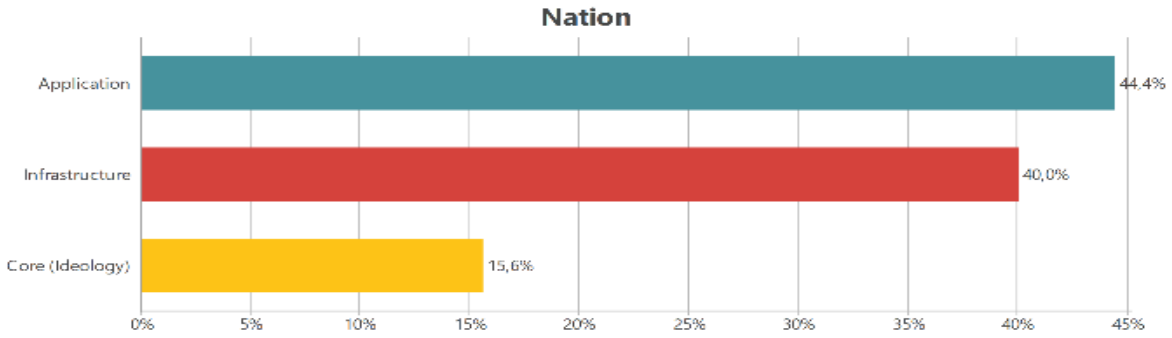
Selanjutnya, kedaulatan yang bersifat *transfer* dan *exclusive* ini akan menjadi dasar analisis penulis untuk memahami dan menguraikan strategi keamanan siber nasional Mesir selama 5 tahun ini yaitu 2017-2021. Selain itu, akan dilihat pula perkembangan teknologi informasi dan komunikasi (TIK) serta pemahaman negara Mesir terkait aplikasi dan infrastruktur yang digunakan dalam upaya pengamanan siber nasional. Karena saat ini, keamanan siber merupakan hal yang krusial dan menyangkut keamanan nasional dalam lingkup negara dan warga negara dalam lingkup yang lebih spesifik. Sebagai negara yang berkewajiban melindungi setiap masyarakatnya, maka strategi keamanan siber nasional merupakan urgensi bagi suatu negara. Hal itulah yang menjadi kerangka acuan penulis dalam melakukan analisis kualitatif terhadap strategi keamanan siber Mesir. 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 Mesir untuk mengimplementasikan strategi keamanan siber. Hasil analisis di setiap aspek keamanan siber Mesir periode 2017-2021 ditinjau lebih lanjut sebagai bahan masukan dalam penyusunan kebijakan strategi keamanan siber Indonesia di periode mendatang.

HASIL DAN PEMBAHASAN

Analisis dilakukan pada setiap aspek yang mempengaruhi strategi keamanan siber Mesir pada periode 2017-2021 mulai dari *Nation*, *Sovereignty*, dan *Aspects*. Nation terbagi atas tiga bagian yang meliputi *Application*, *Infrastructure*, dan *Core* (Ideologi). *Sovereignty* terbagi atas *exclusive* dan *transfer*. Sedangkan *Aspects* terdiri atas *Collaboration/Cooperation, Society, Legal, Security/Defence, Cyber Threats, Technology Development, State Actor, Non-State Actor, Economic Development,* dan *Political Action*.

Nation

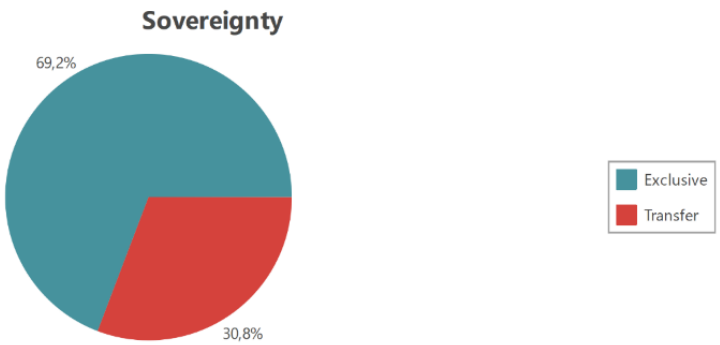
Temuan yang diperoleh penulis dari hasil olahan data menggunakan MAXQDA didapati bahwa kedaulatan yang diatur oleh Mesir dalam dokumen *Egypt National Cyber Security Strategy* 2017-2021 didominasi oleh pembahasan *Application* (44,4%) kemudian dijelaskan juga terkait *infrastructure* (40%), dan yang terakhir *Core* (*Ideology*) (15,6%). Berdasarkan data di bawah ini, dapat dilihat bahwa Mesir memiliki *concern* (perhatian) yang besar terhadap penggunaan TIK dalam penyusunan strategi keamanan siber nasional periode 2017-2021. Karena ranah aplikasi dan infrastruktur cenderung lebih banyak dibahas dalam rangka mewujudkan ketahanan dan keamanan nasional. Walau demikian, unsur ideologi negara tidak terlupakan, karena upaya pengamanan yang dilakukan semata-mata untuk melindungi negara.



Gambar 2. Persentase Piramida *National Cybersecurity*

Sovereignty

Setelah mengetahui besaran aspek kedaulatan yang diatur oleh otoritas Mesir yang tercantum dalam dokumen *Egypt National Cyber Security Strategy* 2017-2021, perbandingan antara sifat kedaulatan tertutup dan terbuka yang diatur oleh Mesir dapat dilihat pada diagram berikut ini:



Gambar 3. Persentase Pembahasan *Sovereignty*

Data di atas menyajikan fakta yang menarik. Walaupun pada Gambar 4 pembahasan terkait ideologi terlihat lebih sedikit dibandingkan dengan pembahasan infrastruktur dan aplikasi, namun berdasarkan teori kedaulatan, Mesir cenderung fokus pada kedaulatan yang bersifat *exclusive*

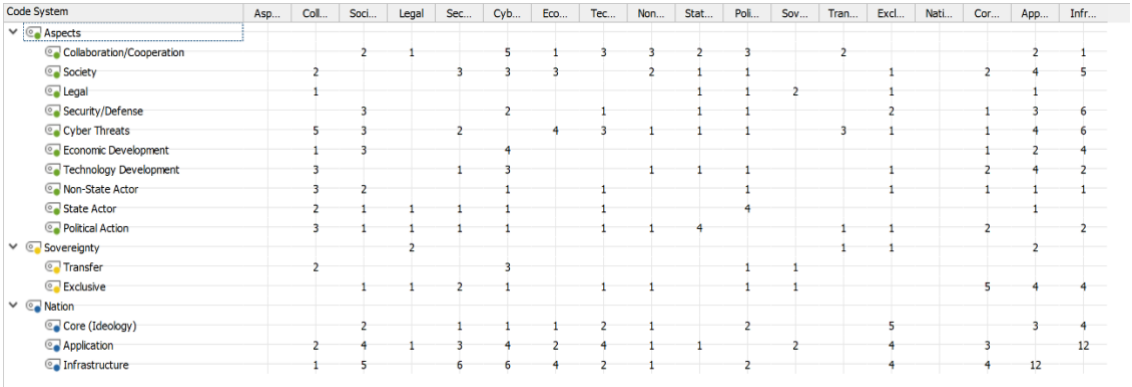
(tertutup) di internal negaranya. Hal ini menunjukkan bahwa, pada masa 2017-2021 ini Mesir lebih fokus pada aplikasi dan infrastruktur yang dikembangkan di internal negara Mesir terkait pengamanan siber nasional.

Aspects

Setelah mengetahui bahwa strategi yang dijalankan oleh Mesir dalam dokumen *Egypt National Cyber Security Strategy* 2017-2021 adalah dengan mengatur aspek kedaulatan Ideologi serta penetrasi terhadap kedaulatan yang sifatnya terbuka, maka perlu diketahui secara lebih lanjut unsur mana sajakah yang menjadi perhatian otoritas setempat dalam mengatur keamanan siber di wilayahnya.

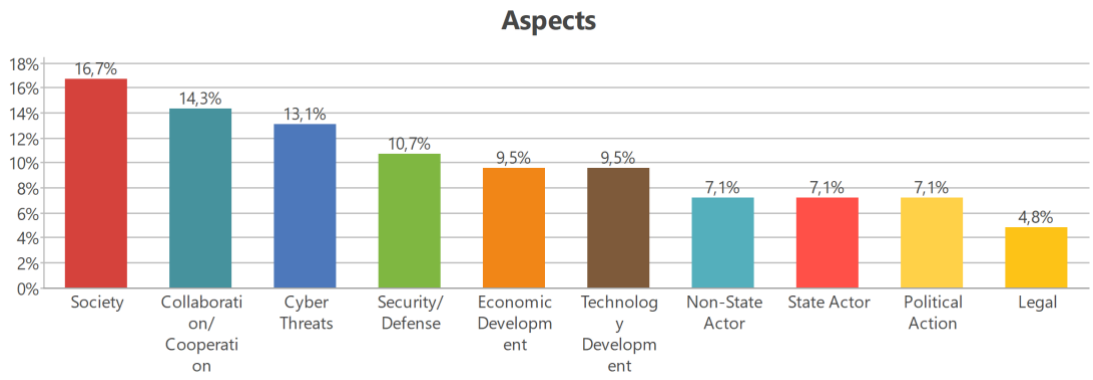
Poin ini menunjukkan data yang terbagi ke dalam kelompok *Collaboration/Cooperation, Society, Legal, Security/Defence, Cyber Threats, Technology Development, State Actor, Non-State Actor, Economic Development,* dan *Political Action*. Seluruh aspek tersebut merupakan isi dari *Egypt National Cyber Security Strategy* 2017-2021 yang secara kontekstual dituangkan oleh penulis ke dalam *Code* {Aspects} guna mengetahui seberapa besar pengaturan, kehadiran, ataupun interaksi negara Mesir dengan berbagai aspek tadi.

Penulis meyakini bahwa saat otoritas mengarahkan konten pengaturan *Egypt National Cyber Security Strategy* 2017-2021 ke dalam aspek kedaulatan Ideologi maka kehadiran lembaga-lembaga negara dalam tata kelola keamanan siber tentu akan dominan. Hal tersebut terlihat pada data di atas yang menunjukkan kehadiran masyarakat mendominasi seluruh aspek strategi keamanan siber Mesir. Akan tetapi, perlu diperhatikan pula bahwa Mesir memberikan ruang yang cukup besar bagi kolaborasi atau bentuk kerjasama antara negara dengan masyarakat dalam penanganan isu keamanan siber. Selain itu, hal yang cukup menarik adalah *aspect Legal* merupakan *aspect* yang persentase sangat kecil di dalam *Egypt National Cyber Security Strategy* 2017-2021. Pada konteks tata Kelola keamanan siber, hal ini menunjukkan bahwa masih lemahnya kebijakan atau peraturan terkait keamanan siber yang ada di Mesir saat dokumen tersebut disusun.



Code System	Asp...	Coll...	Soci...	Legal	Sec...	Cyb...	Eco...	Tec...	Non...	Stat...	Poli...	Sov...	Tran...	Excl...	Nati...	Cor...	App...	Infr...
Aspects																		
Collaboration/Cooperation			2	1		5	1	3	3	2	3		2				2	1
Society		2			3	3	3		2	1	1			1		2	4	5
Legal		1								1	1	2		1			1	
Security/Defense			3			2		1		1	1			2		1	3	6
Cyber Threats		5	3		2		4	3	1	1	1		3	1		1	4	6
Economic Development		1	3			4										1	2	4
Technology Development		3			1	3			1	1	1			1		2	4	2
Non-State Actor		3	2			1		1			1			1		1	1	1
State Actor		2	1	1	1	1		1			4						1	
Political Action		3	1	1	1	1		1	1	4			1	1		2		2
Sovereignty				2									1	1			2	
Transfer		2				3					1	1						
Exclusive			1	1	2	1		1	1		1	1				5	4	4
Nation																		
Core (Ideology)			2		1	1	1	2	1		2			5			3	4
Application		2	4	1	3	4	2	4	1	1		2		4		3		12
Infrastructure		1	5		6	6	4	2	1		2			4		4	12	

Gambar 4. Matriks Relasi Data

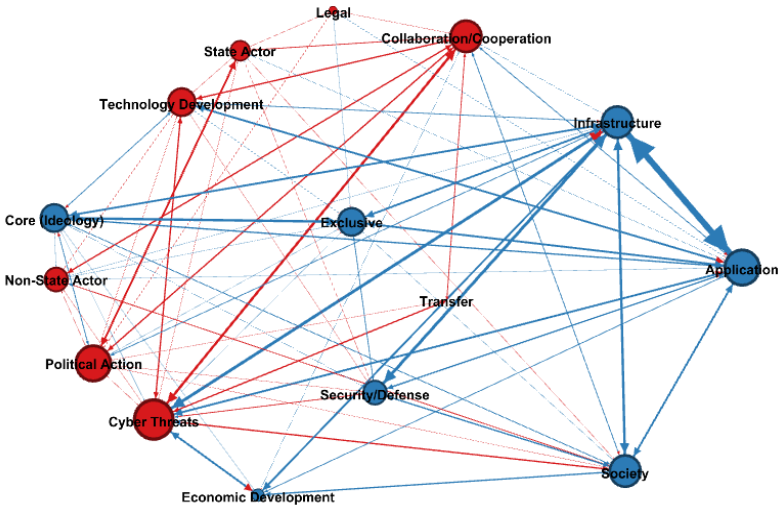


Gambar 5. Persentase Pembahasan *Aspects*

Pada Gambar 6 dapat dilihat bahwa *Application* dan *Infrastructure* merupakan fokus utama yang dimiliki oleh Mesir dalam penanganan *cyber threats*. Hal ini merupakan hal yang sangat realistis mengingat perkembangan teknologi yang kian pesat setiap harinya, maka pengembangan dan peningkatan terkait aplikasi dan infrastruktur TIK suatu negara merupakan ujung tombak dalam penanganan berbagai ancaman yang terjadi di ranah siber.

Relasi Data

Meskipun dari data-data sebelumnya telah diperoleh nilai dari berbagai aspek yang diatur dalam dokumen *Egypt National Cyber Security Strategy* 2017-2021, akan tetapi diperlukan analisis lanjutan guna memperoleh gambaran yang lebih komprehensif. Dalam tulisan ini akan menunjukkan relasi data yang timbul diantara satu aspek dengan aspek lainnya dapat dilihat dengan menggunakan analisis jaringan (*network analysis*) menggunakan GEPHI 0.9.2. Selain dipergunakan untuk melakukan analisis kualitatif, MAXQDA memungkinkan penulis untuk memperoleh data matrix dari relasi data yang terjadi. Matriks inilah yang kemudian dikonversi ke dalam bentuk sajian data analisis jaringan GEPHI 0.9.2.



Gambar 6. Relasi Data Utama GEPHI

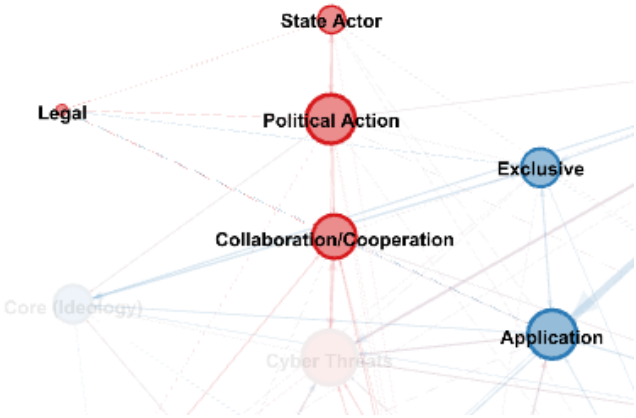
Gambar di atas menunjukkan bagaimana relasi data antara satu aspek dengan aspek lainnya menghasilkan dua *cluster* data besar: Merah dan Biru. Untuk memudahkan dalam menelaah relasi data, penulis melakukan penyesuaian terhadap tampilan data dengan menyematkan fitur tambahan pada pengaturan *layout* GEPHI 0.9.2. Temuan yang dapat diperoleh dari kedua *cluster* tersebut adalah sebagai berikut:

a. Cluster Merah [Q1] terdiri dari *nodes* : *Legal*, *Collaboration/Cooperation*, *State Actor*, *Technology Development*, *Non-State Actor*, *Political Action*, dan *Cyber Threats*.
b. Cluster Biru [Q2] terdiri dari: *Exclusive, Core/Ideologi, Transfer, Security/Defense, Economic Development, Society, Application,* dan *Infrastructure.*

Dengan demikian, dapat dipahami bahwa relasi data yang terdapat pada [Q1] merupakan aspek-aspek yang memiliki kaitan dengan pengaturan atau tata kelola keamanan siber yang bersifat lebih terbuka dibandingkan dengan relasi data [Q2] yang cenderung lebih eksklusif milik otoritas negara. Hal itu dapat dikonfirmasi bila melihat masing-masing *node* yang terkelompok pada [Q1] dan [Q2]. Untuk penjelasan yang lebih terperinci penulis menyajikannya pada poin-poin yang berpengaruh penting dan memiliki peranan dalam strategi keamanan siber Mesir, antara lain sebagai berikut:

Legal

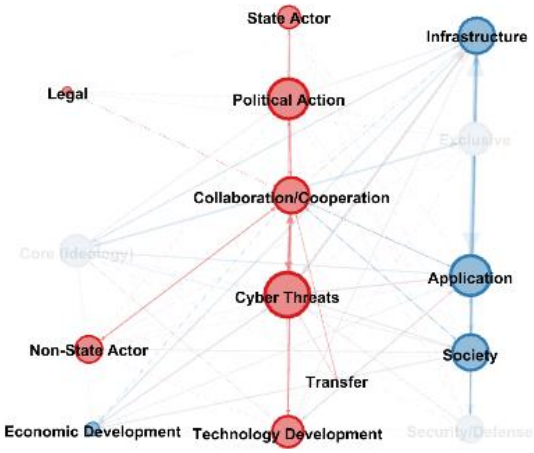
Pada gambar di bawah ini dijelaskan bahwa *aspect Legal* dipengaruhi dengan 3 *aspect* antara lain *state actor*, *political action*, *collaboration/cooperation*. Sedangkan berdasarkan konsep kedaulatan, menunjukkan bahwa *Legal* atau kebijakan, regulasi, dan peraturan sangat berelasi dengan kedaulatan *exclusive* yang penyusunan kebijakan sangat membutuhkan peran dari negara (Hanson, 2012). Selain itu, Legal juga berelasi dengan *application*, maka *application* juga merupakan *aspect* yang perlu diatur dalam kebijakan internal dalam menjaga keamanan siber nasional. Pada MAXQDA, *Legal* merupakan aspek yang memiliki nilai paling rendah yaitu 4,8% karena saat ini Mesir belum memiliki regulasi terkait pengamanan siber skala nasional.



Gambar 7. Relasi Data *Aspect* Legal

Collaboration/Cooperation

Kerjasama atau *aspects collaboration/cooperation* berelasi dengan *state actor, political action, legal, cyber threats, non-state actor, society, technology development, economic development*. Hal ini menunjukkan bahwa kerjasama atau kolaborasi dapat dilakukan hampir dalam segala aspects yang tercantum pada dokumen strategi keamanan siber nasional Mesir. Terutama terkait *Infrastructure* dan *Application* yang dapat diwujudkan dengan kolaborasi antara pemerintah dan *non-state actor*, atau bahkan dengan negara lain.



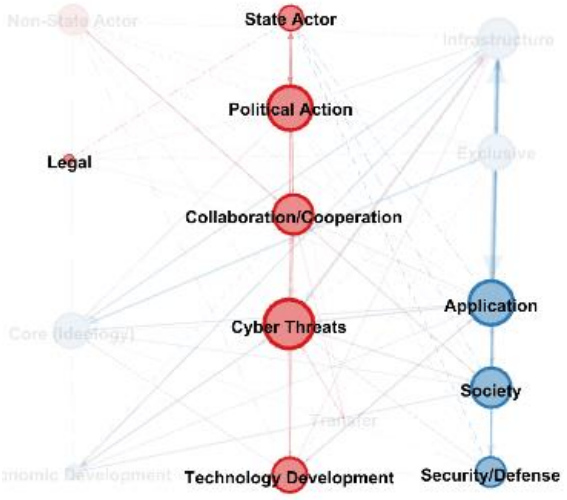
Gambar 8. Relasi Data *Aspect Collaboration/Cooperation*

Pada MAXQDA, *Collaboration/ Cooperation* merupakan *aspects* yang memiliki persentase nilai yang cukup tinggi yaitu 14,3%. Hal ini menunjukkan bahwa kerjasama yang dibangun oleh negara

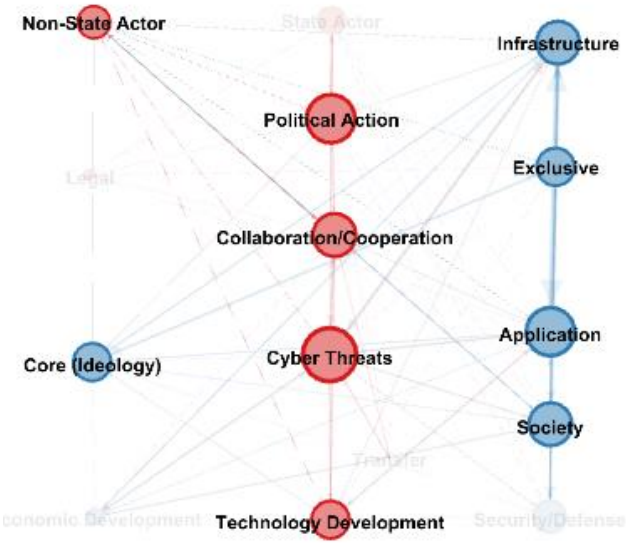
selaku *state-actor* dengan *non-state actor* merupakan salah satu *aspects* yang termasuk fokus dari negara Mesir.

Actor

Dalam *aspects state-actor* ini erat kaitannya dengan otoritas pemerintah yang berperan dalam pengambilan keputusan. Dengan demikian, dapat dilihat bahwa state actor berelasi dengan *aspects legal, political action, collaboration/cooperation, society, cyber threats, technology development, security/defense* dan *application. State actor* dapat mengambil langkah politik dengan menginisiasi penyusunan kebijakan keamanan siber dengan mempertimbangkan aspek-aspek yang berelasi.



Gambar 9. Relasi Data *Aspect State-Actor*



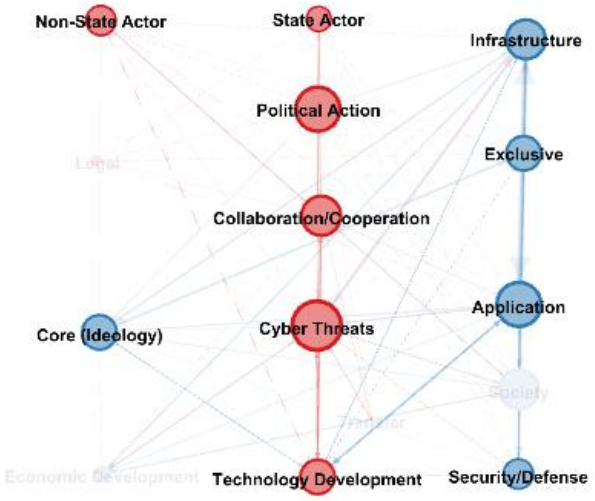
Gambar 10. Relasi Data *Non-State Actor*

Beda halnya dengan relasi yang terjadi dengan *state actor*, pada *aspects non-state actor* justru terjadi relasi antara *non-state actor* dengan kedaulatan yang bersifat *exclusive* (tertutup) atau internal di dalam negara Mesir, dan *Core (Ideology).* Hal ini merupakan hal yang menarik, karena berdasarkan dokumen *Egypt National Cyber Security Strategy* 2017-2021 memang negara lebih mengedepankan aspek kolaborasi dengan para *non-state actor* di dalam negeri seperti para *expert*, peneliti, dan pihak lain yang dapat berkontribusi dalam mewujudkan keamanan siber nasional.

Terlepas dari relasi antara *aspects* dan *actor*, hal yang menarik pada statistic MAXQDA menunjukkan bahwa baik *state-actor* maupun *non-state actor* memiliki persentase yang sama yaitu 7,1%. Hal ini menunjukkan kecocokan data antara *aspects collaboration/cooperation* dengan persentase peranan *actor* dalam strategi keamanan siber nasional, karena perlu adanya dukungan dari berbagai kalangan baik peran negara maupun peran masyarakat.

Technology Development

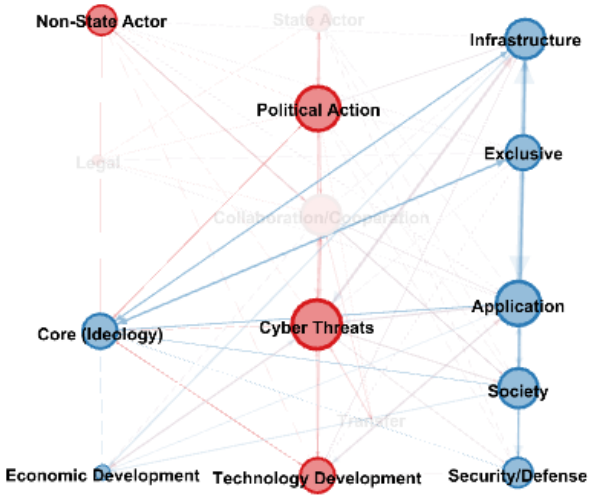
Aspects ini merupakan salah satu aspek yang memiliki relasi hampir dengan seluruh aspek yang ada, terutama pada *aspect* keamanan siber yaitu *core (ideology), application,* dan *infrastructure*. Hal ini menunjukkan bahwa perkembangan teknologi merupakan hal yang krusial dan menjadi ujung tombak dalam penyusunan strategi keamanan siber suatu negara (Pardini, 2017).



Gambar 11. Relasi Data *Aspect Technology*

Core (Ideology)

Pada penghitungan subcode *Core/Ideology* pada aplikasi MAXQDA, dapat kita lihat bahwa hal-hal terkait ideologi tidak sering disebutkan dalam *Egypt National Cybersecurity Strategy* 2017-2021. Namun, relasi data pada GEPHI menunjukkan bahwa *Core/Ideology* terhubung hampir ke semua aspects penilaian, antara lain *infrastructure, application, society, security/defense, technology development, economic development, cyber threats, political action*, dan *non-state actor*.



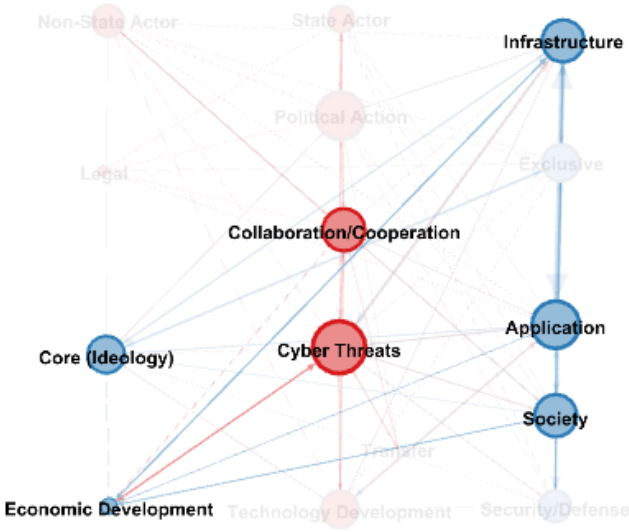
Gambar 12. Relasi Data *Core* (*Ideology*)

Selain seluruh *aspects* tersebut, tentu *Core/Ideology* juga berkaitan erat dengan kedaulatan yang bersifat *exclusive* karena berkaitan dengan nilai-nilau yang dimiliki Mesir secara internal.

Economic Development

Perkembangan ekonomi yang saat ini telah merambah dunia digital sangat rentan terhadap *cyber threats* (Teoh & Mahmood, 2017). Penggunaan *mobile banking, internet banking,* dan fitur-fitur lainnya yang terhubung dengan internet merupakan sasaran utama bagi para peretas (*hackers*) untuk melakukan berbagai ancaman seperti carding, phising, dan berbagai bentuk pencurian data lainnya (Siagian, 2018). Banyak pencurian uang terjadi karena explotasi data yang dilakukan oleh para peretas. Dengan demikian, antisipasi pengamanan dalam ranah siber merupakan langkah yang tepat oleh negara dalam mengembangkan perekonomian nasional.

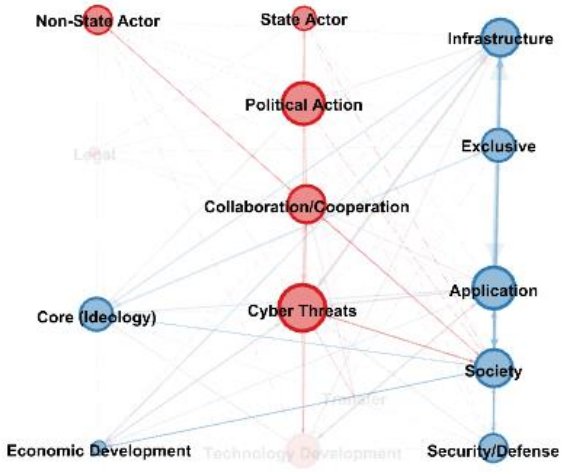
Pada gambar di bawah ini, dapat dilihat bahwa *economic development* dapat berkembang pesat dengan dipengaruhi oleh aspek-aspek lain terutama *application, infrastructure*, dan *collaboration/cooperation* yang dilakukan oleh *society* (masyarakat). Mesir yang memiliki strategi kolaborasi dengan masyarakat dalam penanganan *cyber threats*, sangat merangkul berbagai kalangan untuk dapat bekerja sama dengan harapan memperbaiki berbagai aspek lainnya, salah satunya adalah perkembangan ekonomi.



Gambar 13. Relasi Data *Aspect Economic Development*

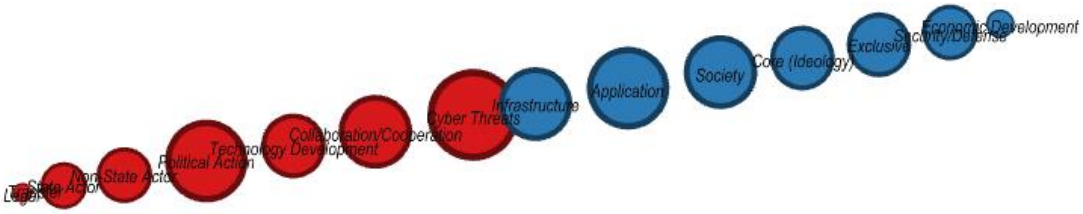
Society

Masyarakat merupakan komponen penting bagi Mesir dalam pembangunan strategi keamanan siber. Selain masyarakat sebagai pengguna, *awareness* masyarakat terkait keamanan informasi terutama informasi pribadi merupakan hal utama yang menjadi perhatian Mesir dalam pengamanan ranah siber di negaranya (Teoh & Mahmood, 2017). Selain itu, negara juga merangkul berbagai kalangan masyarakat dalam menyusun strategi keamanan siber, seperti para akademisi, pakar, dan komunitas yang bergerak di bidang TIK.



Gambar 14. Relasi Data *Aspect Society*

Dari dua aplikasi pengolahan data di atas, dokumen *Egypt National Cyber Security Strategy* 2017-2021 menunjukkan bahwa banyaknya *aspects* yang saling terhubung dalam menangani *cyber threat* menjadikan strategi yang disusun menjadi strategi yang komprehensif. Dapat dilihat bahwa terdapat relasi yang erat antara *cyber-threats* dan *infrastructure* untuk menghubungkan suatu aspek ke aspek lainnya. Hal ini menunjukkan bahwa Mesir mengedepankan peningkatan infrastruktur keamanan dalam menangani *cyber-threats*. Berikut hasil akhir dari pengolahan relasi data menggunakan GEPHI adalah sebagai berikut:

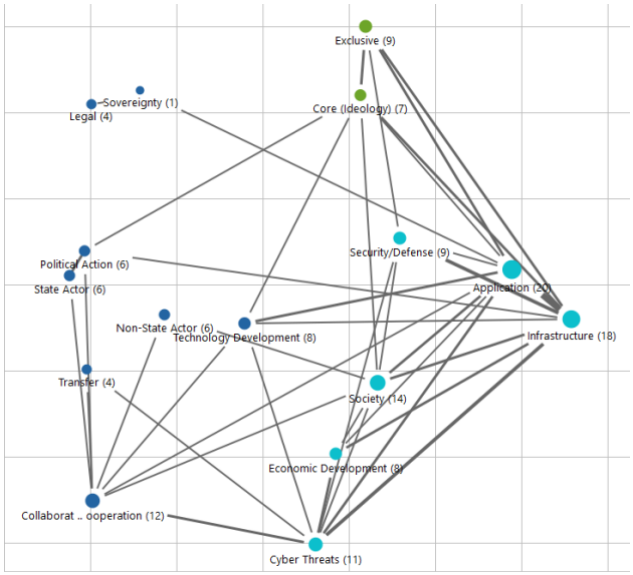


Gambar 15. Akumulasi Relasi Data GEPHI

SIMPULAN

Berdasarkan pertanyaan penelitian dan uraian berbagai *aspects* di atas, maka dapat disimpulkan hal-hal sebagai berikut. Mesir lebih fokus pada aspek kedaulatan yang bersifat *exclusive* terkait peningkatan dan pengembangan *application* dan *infrastructure* TIK yang berkembang di negaranya dalam penanganan *cyber threats*. Dari dokumen *Egypt National Cyber Security Strategy* 2017-2021 dan uraian relasi data di atas menunjukkan bahwa Mesir memiliki beberapa strategi pengamanan sebagai berikut: (a) Peningkatan dan pengembangan aplikasi dan infrastruktur TIK; (b) Kolaborasi antara *state-actor* dan *non-state actor* dalam peningkatan dan pengembangan aplikasi infrastruktur TIK. Negara merangkul para akademisi dan pakar di bidang *cyber security* untuk dapat bekerja sama dalam pengembangan teknologi; (c) Penyusunan *aspects legal* (regulasi) seperti peraturan atau kebijakan terkait *cyber security* karena saat ini Mesir belum memiliki peraturan yang menegakan hukum di ranah siber.

Berdasarkan relasi data yang didapatkan dari MAXQDA dan GEPHI, ditunjukkan bahwa dalam penyusunan strategi keamanan siber nasional, Mesir perlu melihat keterkaitan dari berbagai aspek secara keseluruhan, terutama *aspects* yang berkaitan dengan *nations* (*core/ideology, applications, infrastructure*) dan *sovereignty* baik yang bersifat *exclusive* (tertutup) maupun *transfer* (terbuka). Berikut hasil kesimpulan relasi data dari aplikasi MAXQDA.



Gambar 16. Relasi Data *Nation, Sovereignty, Aspects*

Hal ini dapat dijadikan bahan rekomendasi bagi Indonesia dalam meningkatkan strategi keamanan siber nasional di masa mendatang dengan perspektif kedaulatan. Indonesia yang saat ini memiliki Badan Siber dan Sandi Negara, dapat melakukan studi banding atau *benchmarking* dengan strategi keamanan siber nasional negara lain sebagai bahan masukan dalam perbaikan strategi keamanan siber nasional kedepannya. Indonesia yang saat ini sedang dalam tahap penyusunan Strategi Keamanan Siber Nasional dapat menyusun strategi yang meliputi peningkatan dan perbaikan infrastruktur TIK, mempererat kolaborasi antara *state-actor* dan *non-state actor*, dan penegasan dalam aspek legal di bidang TIK. Terutama Indonesia yang dipercaya sebagai *Deputy Chair* pada OIC CERT sejak tahun 2018, maka Indonesia perlu mengadaptasi atau melakukan studi banding dengan negara OKI lainnya yang pernah menjabat sebelumnya pada OIC CERT, salah satunya Mesir.

REFERENSI

Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences*, 1-13.

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

BSSN. (2018, April 9). Dampingi Oman, Indonesia Terpilih Menjadi OIC-CERT Deputy Chair 2018-2020. Diambil kembali dari Gov-CSIRT Indonesia: https://govcsirt.bssn.go.id/dampingi-oman-indonesia-terpilih-menjadi-oic-cert-deputy-chair-2018-2020/

CERT, O. (2021, April 9). Organisation of Islamic Cooperation - Computer Emergency Response Team. Diambil kembali dari Digwatch: https://dig.watch/actors/organisation-islamic-cooperation-computer-emergency-response-team

ESCC. (2018). *National Cybersecurity Strategy 2017-2021*. Cairo: ESCC.

Hanson, F. (2012, April 9). Baked in and Wired: eDiplomacy @ State. Diambil kembali dari In Foreign Policy at Brookings.: https://www.brookings.edu/research/baked-in-and-wired-ediplomacy-state/

Pardini, D. J. (2017). Cyber Security Governance And Management For Smart Grids in Brazilian Energy Utilities. Journal of Information Systems and Technology Management – Jistem USP, 385-400.

Pratama, F. Y. (2018). *Simulasi Jejaring Jalan Kota Pontianak dengan Betweeness Centrality dan Degree Centrality*. Tanjungpura: Universitas Tanjung Pura.

Siagian, L. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Peperangan Asimetris*.

Teoh, C. S., & Mahmood, A. K. (2017). National Cyber Security Strategies for Digital Economy. *JATIT LLS*, 6510-6522.

Yeli, H. (2017). A Three Perspective Theory of Cyber Sovereignty. *PRISM*, 109-115.