JURNAL

JURNAL SOSIAL DAN SAINS

VOLUME 4 NOMOR 7 2024
P-ISSN 2774-7018, E-ISSN 2774-700X

Analisis Komparasi Kedaulatan Siber Negara-Negara Kawasan Asia Tenggara Australia dan New Zealand

Maruliana Sitanggang
Universitas Paramadina Jakarta, Indonesia
E-mail: maruliana.sitanggang@students.paramadina.ac.id

Kata Kunci:
Analisis Komparasi, Kedaulatan Siber, Asia Tenggara

ABSTRAK

Latar Belakang: Kedaulatan siber menjadi sangat penting bagi negara, karena dampak negatif apabila terjadi serangan, khususnya terhadap infrastruktur kritikal, dapat menggangu kelangsungan kehidupan masyarakat.

Tujuan: Penelitian ini bertujuan untuk melihat ketahanan kedaulatan siber negara-negara Kawasan Asia Tenggara, Australia dan New Zealand dibandingkan dengan Indonesia.

Metode: Penelitian ini menggunakan metode analisis komparatif (Comparative Analysis) dengan menggunakan pendekatan kuantitatif untuk mengetahui komparasi kedaulatan negara, peneliti melakukan teori perhitungan terhadap tiga komponen kedaulatan siber masing-masing negara berdasarkan *Theory of Three Perspectives*, terbatas pada sektor kritikal energi dan transportasi. Sumber data yang digunakan untuk mengetahui sejauh mana kedaulatan siber suatu negara suatu negara melalui cyber application, infrastruktur siber, dan data inti siber.

Hasil: Dalam penelitian ini terlihat bahwa ketahanan infrastruktur siber Indonesia dibandingkan dengan negara Kawasan Asia Tenggara, Australia dan New Zealand posisinya berada di level menengah (51%). Vietnam berada di posisi tertinggi (63%), diikuti Thailand (58%) dan Brunei Darusalam (58%).

Kesimpulan: Hasil olah data yang diperoleh, ketahanan infrastruktur siber Indonesia dibandingkan dengan negara Kawasan Asia Tenggara, Australia dan New Zealand pada penelitian ini posisinya merasa di level menengah, dan tidak lebih baik dengan Brunei Darusalam, Singapore, Vietnam**.** Namun demikian, tingkat keamanan siber untuk infrastruktur krititkal di sektor transportasi dan energi di negara-negara Kawasan Asia Tenggara, Australia dan New Zealand masih sangat perlu ditingkatkan. Hal tersebut karena angkanya yang masih belum mencapai 100%. Dengan demikian masih terdapat potensi kebocoran dan kerusakan jaringan dan aplikasi.

Keywords:
Comparative Analysis, Cyber Sovereignty, Southeast Asia

ABSTRACT

Background: *Cyber sovereignty is very important for the country, because the negative impact of attacks, especially on critical infrastructure, can disrupt the survival of people's lives.*

Objective *: This study aims to look at the resilience of cyber sovereignty in Southeast Asian countries, Australia and New Zealand compared to Indonesia.*

Method *: This study uses a comparative analysis method using a quantitative approach To determine the comparison of state sovereignty, the researcher conducted a calculation theory on the three components of cyber sovereignty of each country based on the Theory of Three Perspectives, limited to the critical energy and transportation*

sectors. Data sources are used to determine the extent of a country's cyber sovereignty through cyber applications, cyber infrastructure, and cyber core data.

***Results**: In this study, it can be seen that the resilience of Indonesia's cyber infrastructure compared to Southeast Asian countries, Australia and New Zealand is in a medium level (51%). Vietnam is in the highest position (63%), followed by Thailand (58%) and Brunei Darusalam (58%).*

***Conclusion** : The results of the data processing obtained, the resilience of Indonesia's cyber infrastructure compared to Southeast Asian countries, Australia and New Zealand in this study felt that its position was at a medium level, and not better than Brunei Darusalam, Singapore, Vietnam. However, the level of cybersecurity for critical infrastructure in the transportation and energy sectors in Southeast Asian countries, Australia and New Zealand still needs to be improved. This is because the number still does not reach 100%. Thus, there is still the potential for leaks and damage to networks and applications.*

PENDAHULUAN

Sistem sektor infrastruktur kritikal nasional seperti kelistrikan, transportasi, perbankan telekomunikasi dan lainnya menjadi sangat penting bagi fondasi kehidupan masyarakat secara luas (Astawa, 2019); (Cappur & Iswahyudi, 2019). Di era teknologi informasi saat ini, kerentanan dan acamannya ketahanannya semakin meningkat dan kritikal. Data dan informasi dari sektor kritikal yang ada di jaringan online dapat di-*hack*/diretas oleh pelaku kejahatan. Motifnya diantaranya untuk mengganggu sistem ketahanan negara di dunia siber, dimana bisa dilakukan oleh mata-mata negara, teroris, dan/atau individu.

Seiring dengan adanya pengaruh perkembangan teknologi informasi, terciptanya suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika (Setiawan et al., 2020). Indonesia sudah memiliki peraturan perundang-undangan yang mengatur persoalan berkaitan dengan ruang lingkup teknologi informasi, yakni Undang-Undang Nomor 11 Tahun 2008tentang Informasi dan Transaksi Elektronik, selanjutnya disebut sebagai UU ITE. Namun, peraturan tersebut belum mampu mengatur persoalan yang mencakup aspek cyberspace yang begitu luas (Rumlus & Hartadi, 2020); (Singgi et al., 2020).

Dikarenakan infrastruktur kritikal nasional sangat diperlukan oleh masyarakat, serangan terhadap infrastruktur kritial apabila terjadi dapat menggangu kelangsungan kehidupan masyarakat. Adapun insiden siber yang pernah terjadi dalam infrastruktur kritis yaitu serangan siber pembangkit listrik di Ukraina (Ali & Idris, 2022). Serangan tersebut menyebabkan pemadaman listrik masal, selanjutnya contoh lain yaitu serangan malwareStuxnet di Iran pada fasilitas nuklir dan ransomware di sistem rumah sakit yang mengakibatkan data seluruhnya terenkripsi dan tidak dapat digunakan, sehingga layanan secara keseluruhanpun terganggu.

Penelitian yang dilakukan oleh Ramadhan (2019) *Self-Help* Atau *Multilateralism*? Penelitian ini lebih fokus membahas membahas strategi seperti apakah yang paling tepat dalam menjaga keamanan cyberdi kawasan Asia Tenggara. Dalam menjawab research question, peneliti menggunakan pendekatan mainstreamseperti neorealism dan

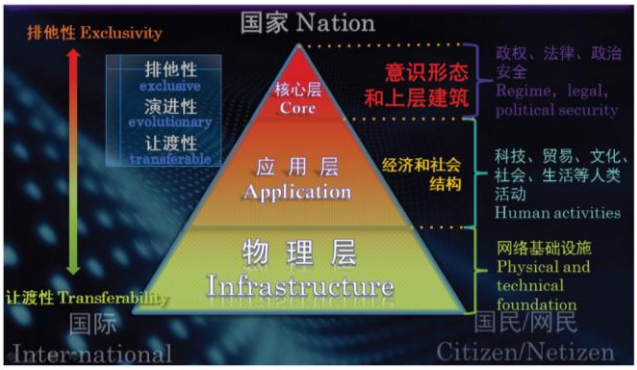
neoliberal. Pada intinya, negara yang tergabung sebagai anggota ASEAN perlu mengembangkan kemampuan power teknologinya tanpa mengesampingkan pentingnya kerja sama antar negara (Prawiyogi, 2023).

Dengan demikian, perlindungan ketahanan siber, khususnya infrastruktur kritikal nasional sangat diperlukan oleh sebuah negara negara. Langkah pertama yang dapat dilakukan adalah mengevaluasi ketahanan siber tersebut dengan melakukan penilaian. Penelitian ini dimaksudkan untuk menghitung level kedaulatan siber/*cyber sovereignty*, terbatas pada Kawasan Asia Tenggara, Australia, dan New Zealand; dan terbatas pada infrastruktur kritikal di sektor energi dan transportasi.

Tujuan penelitian untuk melihat dan membandingkan ketahanan kedaulatan siber negara-negara di Kawasan Asia Tenggara, Australia, dan New Zealand dengan Indonesia. Fokus analisis perbandingan dilakukan pada sektor infrastruktur kritikal energi dan transportasi. Manfaat penelitian ini memberikan gambaran dan pemahaman yang lebih komprehensif tentang posisi dan kondisi kedaulatan siber Indonesia dibandingkan dengan negara-negara lain di kawasan, mengidentifikasi area-area yang perlu mendapatkan perhatian dan peningkatan dalam upaya memperkuat kedaulatan siber Indonesia, terutama pada sektor infrastruktur kritikal energi dan transportasi. Dapat menjadi bahan masukan dan pertimbangan bagi pembuat kebijakan dalam merumuskan strategi dan langkah-langkah untuk meningkatkan ketahanan kedaulatan siber nasional.

METODE PENELITIAN

Penelitian ini menggunakan metode analisis komparatif *(Comparative Analysis)* dengan menggunakan pendekatan kuantitatif untuk menganalisis data yang dikumpulkan dan membandingkan tingkat kedaulatan siber negara-negara yang diteliti. Berdasarkan *A Three-Perspective Theory of Cyber Sovereignty* yang dibangun Yeli, dalam rangka menganalisis kedaulan siber sebuah negara, terdapat tiga komponen yang dilihat yaitu *infrastructure, application dan core* (Yeli, 2017). Core merupakan tingkat atas atau inti terdiri dari rezim, hukum, keamanan politik, dan ideologi, yang tidak dapat diganggu gugat dan mencakup yayasan yang mengatur dan mewujudkan kepentingan inti negara. Karena kondisi nasional yang unik, agama, dan latar belakang budaya, perbedaan yang sah memang ada di antara negara bagian. Keragaman adalah norma keberadaan manusia yang tidak dapat diformat menurut budaya tunggal mana pun. Perbedaan dan keragaman harus ditoleransi. Sedangkan aplikasi pada siber merupakan tingkatan menengah yang mencakup banyak platform internet dan operator internet di dunia nyata yang telah mengintegrasikan berbagai sektor seperti teknologi, budaya, ekonomi, perdagangan, dan aspek kehidupan sehari-hari lainnya. Pada level ini, derajat kedaulatan dunia maya harus disesuaikan dengan kondisi lokal, dengan tujuan mencapai keseimbangan dinamis, administrasi bersama multilateral, multi partai, serta keseimbangan antara kebebasan dan ketertiban. Pada tingkatan infrastruktur negara harus bersedia untuk secara kolektif mentransfer otoritas untuk kepentingan standardisasi dan interkonektivitas. Negara dengan kapasitas dunia maya yang berkembang dengan baik harus mengambil inisiatif untuk memperluas standardisasi dan konektivitas ke negara yang kurang mampu; negara maju harus mengekspor pencapaian mereka ke negara berkembang untuk menjembatani kesenjangan (Gioe et al., 2019).



Gambar 1. Pendekatan Layer dari Kedaulan Siber
Sumber: *A Three-Perspective Theory of Cyber Sovereignty* (Yeli, 2017)

Penelitian ini untuk melihat dari sisi ketahanan dari tiga komponen dimaksud. Pada level infrasturuktur yang dilihat apakah *domain source* tidak keluar dari domain utama. Pada level *application* yang dilihat apakah domain target tidak keluar dari wilayah negara. Selanjunya, level *core* untuk memonitor kebijakan masing-masing negara terkait siber. Ketiga komponen tersebut akan dibobot untuk memperoleh kedaulatan siber negara. Nilai bobot diberikan sesuai tingkat layer dari kedaulatan siber, dimana *core* > *application* > *infrastructure*. Angka pembobotan berdasarkan subjektif peneliti.

Cyber Core > Cyber Application > Cyber Infrastructure

5 > 4 > 3

Gambar 2. Angka Pembobotan Tingkat Layer Kedaulatan Siber

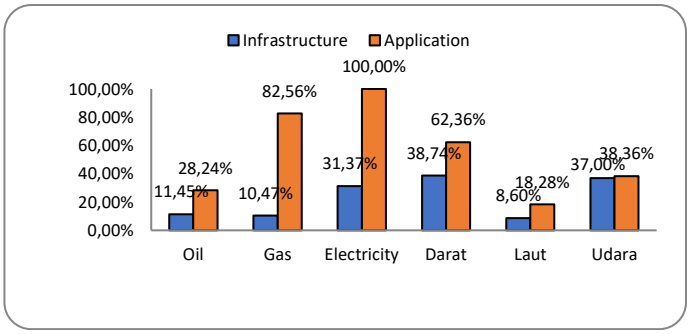
Entitas *cyber infrastructure, application* dan *core* yang dianalisis yaitu entitas yang memberikan pengaruh besar bagi kedaulatan siber setiap negara untuk melihat seberapa besar kedaulatan siber suatu negara (Wardani, 2021). Hasil dari perhitungan masing-masing entitas selanjutnya diagregasi untuk dapat mengambarkan secara nasional kedaulatan suatu negara. Berikut entitas dimaksud yang akan masuk di dalam perhitungan:

1. Perusahaan Nasional di sektor infrastruktur kritis pada sektor energi dan transportasi (Prabowo & Sihaloho, 2023). Sektor Energi terdiri dari Minyak, Gas dan Listrik. Sedangkan, sektor trransportasi: Darat, Laut dan Udara (Paminto, 2020).
2. Lembaga pemerintahan yang dapat mengeluarkan kebijakan siber antara lain *Cyber Authority, Police, Military, Ministry of Défense, Ministry of Communication, Ministry Of Home Affairs, Ministry Of Foreign Affairs, Minister of Political, Legal and Security Affairs,* dan *State Intelligence Agency,* and *National Planning Agency* (Pratiwi et al., 2021).

HASIL DAN PEMBAHASAN

Analisa Ketahanan Siber Setiap Negara

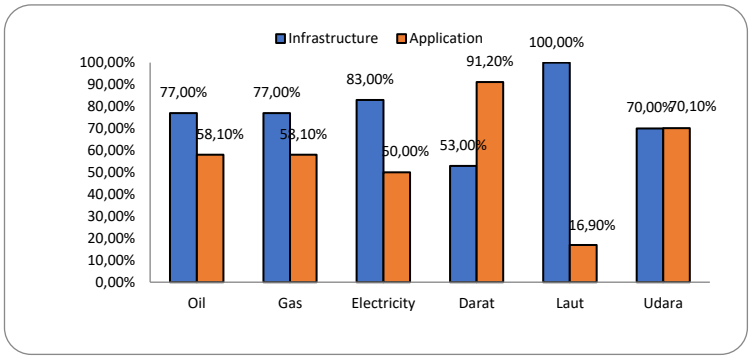
Berikut hasil olah data *Cyber infrastructure, Application, Core* dan *Sovereignty* untuk negara-negara di Indonesia dan Kawasan Asia Tenggara, Australia dan New Zealand.



Agregat	
Cyber Infrastructure	22.94%
Cyber Application	54.97%
Cyber Core	12.73%
Cyber Sovereignty	30.50%

Gambar 3. Ketahanan Siber Infrastruktur Kritis Negara Indonesia
Sumber: Olahan Penulis

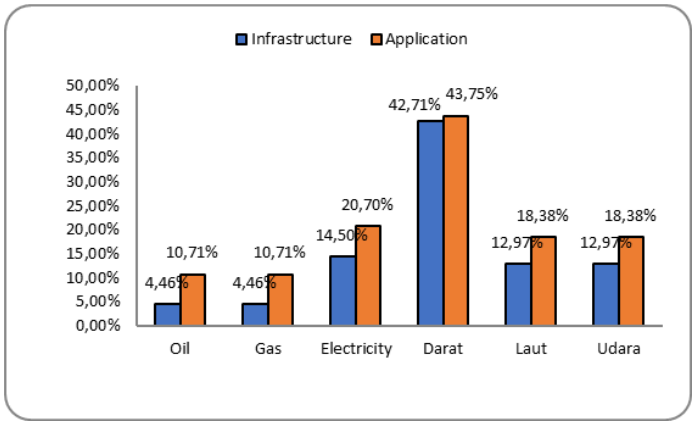
Dari gambar 3, terlihat bahwa ketahanan siber aplikasi lebih tinggi dibandingkan dengan siber infrastuktur, Dimana yang tertinggi di sektor Listrik. Meskipun demikian, angka secara agregat masih relatif rendah. Selanjutnya, melalui hasil pembobotan, *cyber sovereignty* Indonesia adalah sebesar 30,50%. Angka tersebut rendah, dengan demikian Pemerintah perlu mengambil kebijakan dalam rangka meningkatkan kedaulatan keamanan sibernya dari semua aspek (infrastruktur, aplikasi dan inti).



Agregat	
Cyber Infrastructure	76.67%
Cyber Application	57.40%
Cyber Core	10.25%
Cyber Sovereignty	57.60%

Gambar 4. Ketahanan Siber Infrastruktur Kritis Negara Brunei Darusalam
Sumber: Olahan Penulis

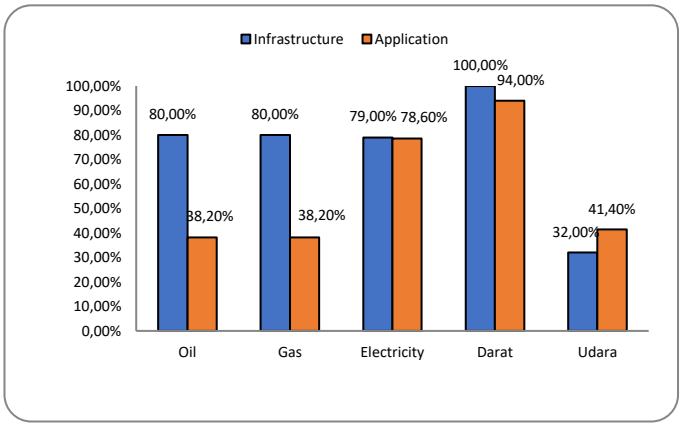
Dari gambar 4, terlihat bahwa ketahanan *cyber infrastructure* relatif baik (>77%), dimana yang tertinggi adalah sektor laut. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Brunei Darusalam adalah sebesar 57,60%, dimana *cyber core* merupakan bobot terendah yaitu 10,25%. Selanjutnya, secara agregat untuk semua sektor, *cyber core* yang memiliki angka terendah yaitu 10,25%. Dengan demkian, perbaikan keamanan siber, khususnya dari aspek inti sangat diperlukan.



Agregat	
Cyber Infrastructure	15.35%
Cyber Application	20.44%
Cyber Core	18.42%
Cyber Sovereignty	17.49%

Gambar 5. Ketahanan Siber Infrastruktur Kritis Negara Filipina
Sumber: Olahan Penulis

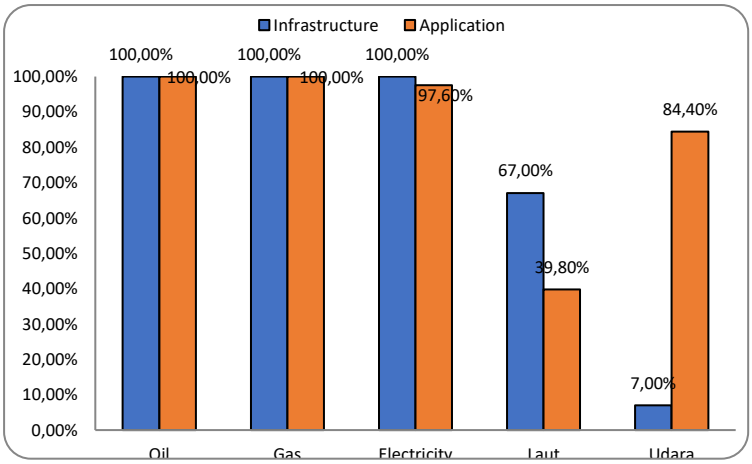
Dari gambar 5, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor transportasi darat merupakan yang tertinggi, namun demikian angkanya masih relatif rendah. Secara agregat *cyber infrastructure*, *application* dan *core* infrastruktur kritikal di Filipina, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Filipina adalah sebesar 17,49%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti masih sangat diperlukan.



Agregat	
Cyber Infrastructure	74.20%
Cyber Application	58.08%
Cyber Core	17.65%
Cyber Sovereignty	58.05%

Gambar 6. Ketahanan Siber Infrastruktur Kritis Negara Thailand
Sumber: Olahan Penulis

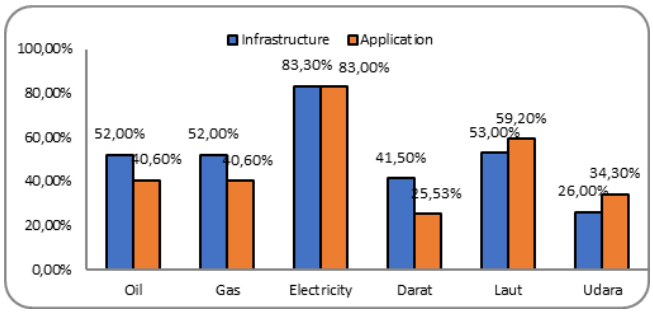
Dari gambar 6, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor transportasi darat merupakan yang tertinggi, namun demikian angkanya masih relatif rendah. Secara agregat *cyber infrastructure* dan *application*, angkanya relatif sedang. Disisi lain *cyber core* di Thailand, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Thailand adalah sebesar 58,05%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan.



Agregat	
Cyber Infrastructure	74.80%
Cyber Application	84.36%
Cyber Core	0.09%
Cyber Sovereignty	62.73%

Gambar 7. Ketahanan Siber Infrastruktur Kritis Negara Vietnam
Sumber: Olahan Penulis

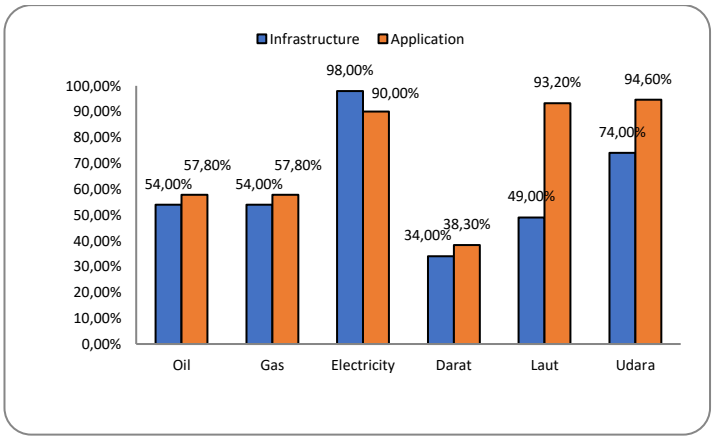
Dari gambar 7, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor transportasi sangat tinggi, namun dari sisi *cyber* core angkanya sangat rendah. Angka *cyber* core rendah, salah satunya dikarenakan berita terkait *cyber* masih kurang terpublikasi hasilnya di webite. Selanjutnya, melalui hasil pembobotan, *cyber sovereignty* infrastruktur Vietnam adalah sebesar 62,73%.



Agregat	
Cyber Infrastructure	51.30%
Cyber Application	47.21%
Cyber Core	0.12%
Cyber Sovereignty	39.84%

Gambar 8. Ketahanan Siber Infrastruktur Kritis Negara Singapura
Sumber: Olahan Penulis

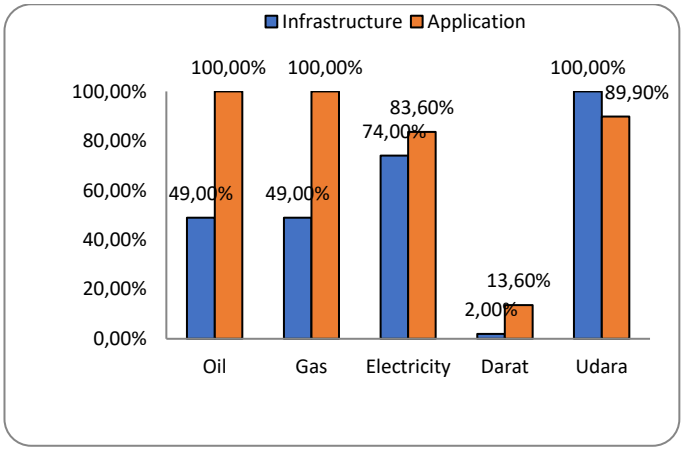
Dari gambar 8, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor Listrik merupakan yang tertinggi. Secara agregat *cyber infrastructure* dan *application*, angkanya relatif sedang. Disisi lain *cyber core* di Singapura, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Singapura adalah sebesar 39,84,05%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan.



Agregat	
Cyber Infrastructure	60.50%
Cyber Application	71.95%
Cyber Core	0.08%
Cyber Sovereignty	51.85%

Gambar 9. Ketahanan Siber Infrastruktur Kritis Negara Malaysia
Sumber: Olahan Penulis

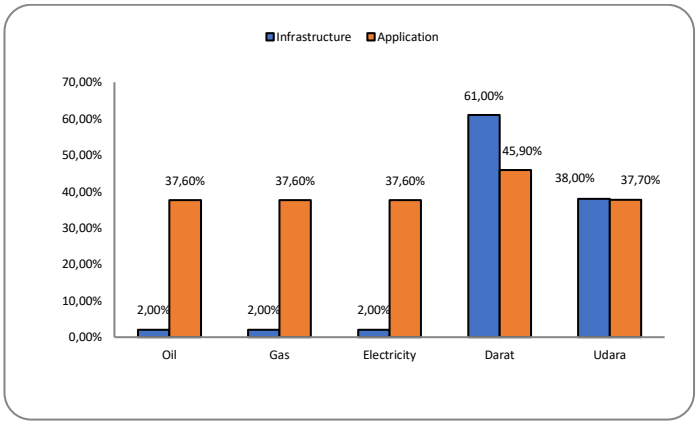
Dari gambar 9, Terlihat sektor yang paling baik ketahananya sibernya adalah kelistrikan, laut dan udara. Secara agregat *cyber infrastructure* dan *application*, angkanya relatif sedang. Disisi lain *cyber core* di Malaysia, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Malaysia adalah sebesar 51,85%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan, khususnya inti.



Agregat	
Cyber Infrastructure	54.80%
Cyber Application	77.42%
Cyber Core	0.06%
Cyber Sovereignty	50.64%

Gambar 10. Ketahanan Siber Infrastruktur Kritis Negara Laos
Sumber: Olahan Penulis

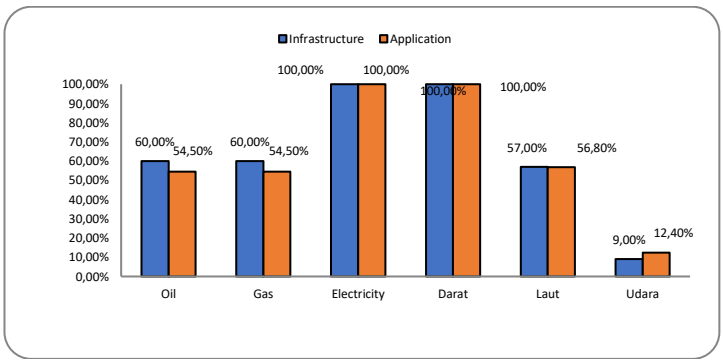
Dari gambar 10, terlihat bahwa ketahanan *cyber application* sektor energi dan transportasi angkanya tinggi, kecuali sektor darat. Disisi lain *cyber core* di Laos, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur kritikal Laos adalah sebesar 50,64%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan, khususnya inti.



Agregat	
Cyber Infrastructure	21.00%
Cyber Application	39.28%
Cyber Core	7.25%
Cyber Sovereignty	23.73%

Gambar 11. Ketahanan Siber Infrastruktur Kritis Negara Kamboja
Sumber: Olahan Penulis

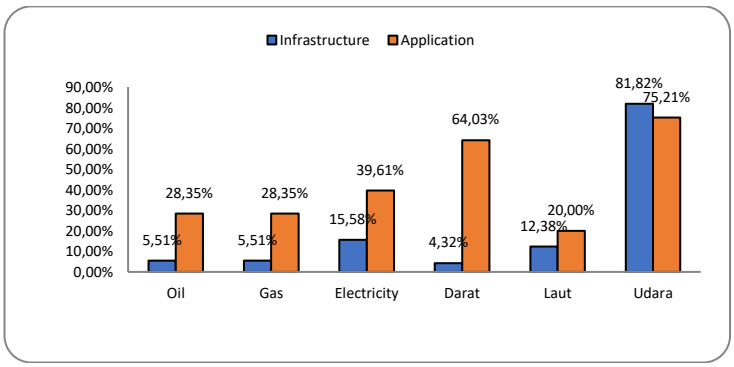
Dari gambar 11, Secara agregat *cyber infrastructure*, *application*, *core* di Kamboja, angkanya rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur adalah sebesar 23,73%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan, khususnya inti.



Agregat	
Cyber Infrastructure	64.33%
Cyber Application	63.03%
Cyber Core	0.05%
Cyber Sovereignty	51.09%

Gambar 12. Ketahanan Siber Infrastruktur Kritis Negara Myanmar
Sumber: Olahan Penulis

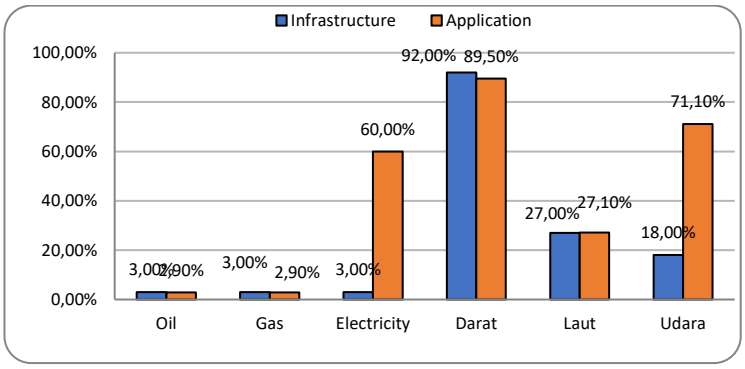
Dari gambar 12, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor transportasi darat merupakan yang tertinggi, namun demikian angkanya secara agregat adalah di tingkat menengah. Di sisi lain, *cyber core* Myanmar sangat rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Myanmar adalah sebesar 51,09%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan.



Agregat	
Cyber Infrastructure	20.85%
Cyber Application	42.59%
Cyber Core	17.47%
Cyber Sovereignty	26.70%

Gambar 13. Ketahanan Siber Infrastruktur Kritis Negara Australia
Sumber: Olahan Penulis

Dari gambar 13, terlihat bahwa ketahanan *cyber infrastructure* dan *application* sektor transportasi udara merupakan yang tertinggi, namun demikian angkanya masih relatif rendah. Secara agregat *cyber infrastructure* dan *application*, angkanya relatif sedang. Disisi lain *cyber core* di Australia, angkanya relative rendah. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur Ausralia adalah sebesar 26,70%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan.



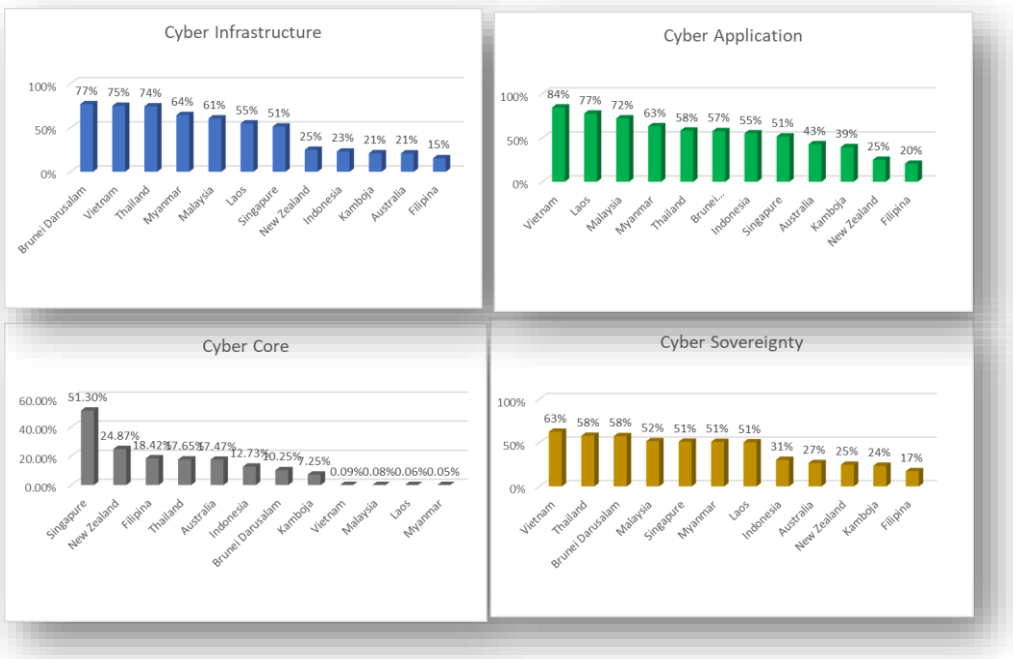
Agregat	
Cyber Infrastructure	24.33%
Cyber Application	42.25%
Cyber Core	0.13%
Cyber Sovereignty	24.87%

Gambar 14. Ketahanan Siber Infrastruktur Kritis Negara New Zealand
Sumber: Olahan Penulis

Dari gambar 14, terlihat bahwa ketahanan *cyber infrastructure* dan *application* relatif sedang secara agregat, namun *cyber core*-nya rendah. Sektor yang paling baik ketahannya sibernya yaitu darat. Melalui hasil pembobotan, *cyber sovereignty* infrastruktur New Zealand adalah sebesar 24,87%. Dengan demikian perbaikan di tingkat dasar, aplikasi, dan inti sangat diperlukan, khususnya inti.

Analisa Perbandingan Ketahanan Siber

Berikut hasil olah data perbandingan *Cyber infrastructure*, *Application*, *Core* dan *Sovereignty* dinegara-negara di Kawasan Asia Tenggara, Australia dan New Zealand.



Gambar 15. Perbandingan Ketahanan Siber Negara-Negara Kawasan Asia Tenggara, Australia dan New Zealand
Sumber: Olahan Penulis

Dari gambar 15 terlihat tingkat keamanan kritikal negara-negara Kawasan Asia Tenggara, Australia dan New Zealand masih perlu diperbaiki karena masih dapat dirusak ketahanannya. Dari sisi aspek keamanan infrastruktur yang paling baik adalah negara Brunei Darusalam, dan yang terendah adalah negara Filipina. Selanjutnya dari sisi aspek keamanan aplikasi, negara Vietnam berada di level tertinggi dan Filipina di level terendah. Dan dari sisi inti, negara Singapure yang tertinggi level-nya tertinggi dan yang terendah Myamar.

Indonesia berada di posisi tengah di antara negara-negara Kawasan Asia Tenggara, Australia dan New Zealand untuk tingkat keamanan jaringan, aplikasi dan inti siber (Bandono, 2020). Untuk level kedaulatan siber, Vietnam berada di posisi tertinggi, diikuti Thailand dan Brunei Darusalam. Indonesia berada di posisi 8, diantara 12 negara di Kawasan. *Range cyber sovereignty* yaitu 17% sd. 63%, Dimana Filipina adalah 17% dan Vietnam 63%.

KESIMPULAN

Keamanan siber merupakan hal yang sangat perlu diperhatikan oleh suatu negara, khususnya untuk infrastruktur kritikal karena yang terkait dengan masyarakat luas. Kelalaian suatu negara dalam memproteksi kedaulatan sibernya, dapat berakibat fatal, yang mengganggu kehidupan masyarakat. Dari hasil olah data yang diperoleh, ketahanan infrastruktur siber Indonesia dibandingkan dengan negara Kawasan Asia Tenggara, Australia dan New Zealand pada penelitian ini posisinya merasa di level menengah, dan tidak lebih baik dengan Brunei Darusalam, Singapore, Vietnam**.** Namun demikian, tingkat keamanan siber untuk infrastruktur krititkal di sektor transportasi dan energi di negara-negara Kawasan Asia Tenggara, Australia dan New Zealand masih sangat perlu ditingkatkan. Hal tersebut karena angkanya yang masih belum mencapai 100%. Dengan demikian masih terdapat potensi kebocoran dan kerusakan jaringan dan aplikasi.

Hasil penelitian ini, perbaikan ketahanan keamanan siber di Indonesia dan negara-negara Kawasan Asia Tenggara, Australia dan New Zealand perlu diperbaiki. Beberapa yang dapat direkomendasikan adalah pengawasan keamanan siber untuk Badan Usaha Milik Negara (BUMN) dan perusahaan-perusahaan swasta yang terkait dengan sektor-sektor infrastruktur kritial. Pemerintah perlu melakukan review secara langsung terhadap keamanan siber, dan mengatur lebih lanjut tingkat keamanan siber yang layak untuk BUMN dan perusahan dimaksud. Dalam rangka peningkatan ketahanan *cyber infrastructure* dan *cyber application*, ahli-ahli Teknologi Informasi dan *Cyber Security* sangat diperlukan. Dengan demikian, BUMN dan perusahaan hendaknya dapat merekruit ahli-ahli terkait *cyber security* yang unggul. Selanjutnya, Pemerintah perlu juga memberikan insentif kepada universitas-universitas yang membuka jurusan *cyber security*. Melakukan *sharing knowledge* dari negara-negara yang lebih unggul tingkat keamanan siber-nya sangat diperlukan. Mekanisme Kerjasama Kawasan, seperti ASEAN, ASEAN dengan Australia dan New Zealand, dapat dimanfaatkan dalam rangka *sharing knowledge*.

DAFTAR PUSTAKA

Ali, J. Y. S. T. Y., & Idris, A. M. (2022). Analisis Potensi Ancaman Asimetris Berdasarkan Kerentanan Keamanan Siber Sektor Industri Energi Baru Terbarukan (EBT). *Jurnal Kewarganegaraan*, *6*(2).

Astawa, I. M. M. K. (2019). Metodologi Penilaian Kerentanan Pada Infrastruktur Kritikal Nasional. *Seminar Nasional Aplikasi Teknologi Informasi (Snati)*.

Bandono, A. (2020). *Perkembangan Ancaman Islamic State (IS) di Asia Tenggara Analisis Perkembangan Dan Risiko Berbasis 3d Matrik Studi Kasus Jaringan Teror Di Wilayah Perbatasan Thailand, Malaysia, Filipina Dan Indonesia*.

Cappur, A. C., & Iswahyudi, D. (2019). Pengaruh Minimnya Infrastruktur Terhadap Pola Hidup Masyarakat. *Prosiding Seminar Nasional Fakultas Ilmu Pendidikan*, *3*, 74–82.

Gioe, D. V, Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy*, *4*(1), 117–137.

Paminto, A. K. (2020). Analisis dan Proyeksi Kebutuhan Energi Sektor Transportasi di Indonesia. *Jurnal Energi Dan Lingkungan (Enerlink)*, *16*(2), 51–54.

Prabowo, T. B., & Sihaloho, R. A. (2023). Analisis ketergantungan indonesia pada teknologi asing dalam sektor energi dan dampaknya pada keamanan nasional. *Jurnal Lemhannas RI*, *11*(1), 72–82.

Pratiwi, F. I., Ainnurrohman, B., & Wijaya, A. A. (2021). *Rethinking Indonesia's foreign policy: principles in evolving contemporary dynamics*. Airlangga University Press.

Prawiyogi, A. G. (2023). Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *4*(2), 119–127.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*, *3*(2), 181–192.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285–299.

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal USM Law Review*, *3*(2), 275–295.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339.

Wardani, D. E. K. A. K. (2021). *Penegakan Hukum Oleh Kepolisian Ri Terhadap Kejahatan Skimming Di Indonesia=(Law Enforcement By The Police Against Skimming Crimes In Indonesia)*. Universitas Hasanuddin.

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. *Prism*, *7*(2), 108–115.