STRATEGI KEAMANAN SIBER SINGAPURA DALAM MENGHADAPI ANCAMAN KEJAHATAN SIBER

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Persyaratan Guna Memperoleh Gelar Sarjana (S-1) Dalam Bidang Ilmu Hubungan Internasional

Disusun Oleh :

TIARA ANJANI

07041181924031

JURUSAN ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS SRIWIJAYA

INDRALAYA

2023

HALAMAN PERSETUJUAN UJIAN SKRIPSI

STRATEGI KEAMANAN SIBER SINGAPURA DALAM MENGHADAPI ANCAMAN KEJAHATAN SIBER

SKRIPSI

Disusun Oleh :

TIARA ANJANI

07041181924031

Telah Disetujui oleh Dosen pembimbing untuk Diajukan dalam Ujian Akhir Program Sarjana

Pembimbing I

Dra. Retno Susilowati, MM.
NIP. 195905201985032003

Pembimbing II

Cynthia Azhara Putri, S.H., M.Kn.
NIDN. 0009029110

Disetujui oleh,
Ketua Jurusan,

Sofyan Effendi, S.IP., M.Si.
NIP. 197705122003121003

HALAMAN PERSETUJUAN PENGUJI SKRIPSI

STRATEGI KEAMANAN SIBER SINGAPURA DALAM MENGHADAPI ANCAMAN KEJAHATAN SIBER

SKRIPSI

Telah Dipertahankan di Depan Tim Penguji
Dan Dinyatakan Telah Memenuhi Syarat
Pada Tanggal..8/03/2023

TIM PENGUJI SKRIPSI

Pembimbing :

1. **Dra. Retno Susilowati, MM.**
   NIP. 195905201985032003

2. **Cynthia Azhara Putri, S.H., M.Kn.**
   NIDN. 0009029110

Penguji :

1. **Ganawan Lestari Elake, S.IP., MA.**
   NIP. 198405182018031001

2. **Abdul Halim, S.IP., MA.**
   NIP. 199310082020121020

Mengetahui,

Dekan FISIP UNSRI

Prof. Dr. Alfitri, M.Si

NIP. 196601221990031004

Ketua Jurusan

Sofyan Effendi, S.IP., M.Si.

NIP. 197705122003121003

LEMBAR PERNYATAAN ORISINALITAS

Saya yang betanda tangan di bawah ini :

Nama : Tiara Anjani

NIM : 07041181924031

Program Studi : Ilmu Hubungan Internasional

Menyatakan dengan sungguh-sungguh bahwa skripsi yang berjudul "Strategi Keamanan Siber Singapura dalam Menghadapi Ancaman Kejahatan Siber" ini adalah benar-benar karya saya sendiri dan saya tidak melakukan penjiplakan atau pengutipan dengan cara yang tidak sesuai dengan etika keilmuan yang berlaku sesuai dengan Peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 17 Tahuun 2010 tentang Pencegahan dan Penanggulangan Plagiat di Perguruan Tinggi. Apabila di kemudian hari, ada pelanggaran yang ditemukan dalam skripsi ini dan/atau ada pengaduan dari pihak lain terhadap keaslian karya ini, saya bersedia menanggung sanksi yang dijatuhkan kepada saya.

Demikian pernyataan ini saya buat dengan sungguh-sungguh tanpa adanya paksaan dari pihak manapun.

Indralaya, Maret 2023

Yang Membuat Pernyataan

Tiara Anjani

NIM. 07041181924031

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk kedua orang tua saya tercinta : Bapak Asmaja (Alm) dan Ibu Yahani dan ketiga kakak perempuan saya yang juga selalu memberikan dukungan kepada penulis selama menempuh masa perkuliahan. Semua perjuangan, pengorbanan, kasih sayang serta doa mereka tak pernah putus agar penulis dapat selalu dilimpahkan kelancaran untuk dapat meraih harapan dan cita-cita. Kemudian, teruntuk para teman-teman dekat yang senantiasa memberikan dukungan dan motivasi untuk menjadi lebih baik. Semoga Allah SWT selalu memberikan kesehatan serta perlindungan terhadap kedua orang tua saya, kakak-kakak saya serta para teman atau sahabat dekat saya.

ABSTRAK

Keamanan internasional semakin berkembang dan mengalami perubahan yang disebabkan oleh globalisasi dimana kemajuan teknologi dan informasi semakin berkembang pesat dan memudarkan batas-batas wilayah antar negara. Pembahasan terkait keamanan juga semakin meluas pada keamanan non-tradisional. Salah satu bentuk ancaman keamanan non-tradisional yang semakin marak terjadi adalah kejahatan siber. Untuk menghadapi ancaman kejahatan siber, sebuah negara tentunya perlu membuat strategi keamanan siber. Keamanan siber merupakan sebuah sistem dimana hukum, organisasi, kemampuan serta kerjasama harus sejalan agar menjadi efektif. Kawasan asia tenggara yang rentan mengalami kejahatan siber menjadikan Singapura sebagai target dari serangan siber dikarenakan Singapura adalah penguasa IT pada kawasan tersebut. Mayoritas masyarakat singapura yang kesehariannya sangat bergantung pada penggunaan internet pun membuat tinggi nya tingkat konektivitas dunia maya yang dimana akan membuat kejahatan siber juga meningkat. Penelitian ini bertujuan untuk menjelaskan bagaimana strategi keamanan siber Singapura dalam menghadapi ancaman kejahatan siber. Metode penelitian yang digunakan adalah metode kualitatif dimana sumber data yang akan dikumpulkan oleh penulis adalah data sekunder. Penelitian ini menggunakan konsep strategi keamanan siber internasional yang di populerkan oleh Mirko Hohmann tahun 2017 melalui 5 dimensi bidang kerja yaitu legal, technical, organizational, capacity building, dan international cooperation. Hasil penelitian ini menunjukkan bahwa strategi keamanan siber Singapura dalam menghadapi ancaman kejahatan siber yaitu dilakukan melalui 5 dimensi bidang kerja yang dikemukakan Mirko Hohmann yaitu Singapura membentuk aturan hukum terkait siber, adanya penerapan sistem teknologi yang baik dan pembuatan produk berlisensi untuk sistem komputer, terdapatnya juga koordinasi pembuatan kebijakan, pemberian edukasi tentang keamanan siber dari lingkup sekolah dasar hingga universitas, dan berbagai bentuk kerjasama internasional yang dapat digunakan sebagai cara dalam memerangi ancaman kejahatan siber.

Kata kunci : Keamanan Siber, Singapura, Strategi, Kejahatan Siber

Indralaya,

Mengetahui,

Pembimbing 1	Pembimbing 2
Dra. Retno Susilowati, MM.	**Cynthia Azhara Putri, S.H., M.Kn.**
NIP. 195905201985032003	**NIDN. 0009029110**

Disetujui oleh,
Ketua Program Studi

Sofyan Effendi, S.IP., M.Si.
NIP. 197705122003121001

ABSTRACT

International security is growing and experiencing changes caused by globalization where advances in technology and information are growing rapidly and fading boundaries between countries. Discussions related to security are also expanding to non-traditional security. One form of non-traditional security threats that is increasingly prevalent is cybercrime. To deal with the threat of cyber crime, a country certainly needs to create a cyber security strategy. Cybersecurity is a system in which law, organization, capabilities, and cooperation must align to be effective. The Southeast Asian region which is prone to cybercrime makes Singapore a target for cyberattacks because Singapore is the IT authority in the region. The majority of Singaporeans, whose daily lives are very dependent on the use of the internet, also result in a high level of cyber connectivity which will also increase cyber crime. This study aims to explain how Singapore's cybersecurity strategy deals with the threat of cybercrime. The research method used is a qualitative method where the data source to be collected by the author is secondary data. This study uses the concept of an international cyber security strategy which was popularized by Mirko Hohmann in 2017 through 5 work field dimensions namely legal, technical, organizational, capacity building, and international cooperation. The results of this study indicate that Singapore's cybersecurity strategy in dealing with the threat of cybercrime is carried out through the 5 dimensions of the field of work proposed by Mirko Hohmann namely Singapore establishes legal rules related to cyber, the implementation of good technology systems and the manufacture of licensed products for computer systems, there is also coordination of policy making, provision of education on cyber security from elementary schools to universities, and various forms of international cooperation that can be used as a way to combat the threat of cybercrime.

Keywords : Cyber Security, Singapore, Strategy, Cyber Crime

Indralaya,

Acknowledged By,

Advisor I	**Advisor II**
Dra. Retno Susilowati, MM.	**Cynthia Azhara Putri, S.H., M.Kn.**
NIP. 195905201985032003	**NIDN. 0009029110**

Approved By,
Head of Department
International Relations UNSRI

Sofyan Effendi, S.IP., M.Si.
NIP. 197705122003121003

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini dengan baik dan lancar. Penulisan skripsi ini dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar S-1 pada program studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Sriwijaya. Penulis menyadari bahwa selama proses penulisan skripsi ini tentunya bisa selesai dengan adanya bimbingan, dorongan dan arahan dari berbagai pihak yang selama ini telah memberikan bantuan. Oleh karena itu, pada kesempatan ini saya ingin mengucapkan terima kasih sebesar-besarnya kepada semua pihak yang telah membantu, sebagai berikut :

1. Orang tuaku tersayang bapak Asmaja (Alm) dan Ibu Yahani yang tidak pernah berhenti memberikan doa dan dukungan serta menjadi penyemangat dan motivasi selama penyelesaian skripsi ini.
2. Prof. Dr. Ir. H. Anis Saggaf, MSCE selaku Rektor Universitas Sriwijaya
3. Prof. Dr. Alfitri, M.Si. selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Sriwijaya
4. Sofyan Effendi, S.IP., M.Si. selaku Ketua Program Studi Ilmu Hubungan Internasional, Universitas Sriwijaya
5. Hoirun Nisyak, S.PD., M.PD. selaku dosen pembimbing akademik yang telah memberikan arahan dan bimbingan selama proses perkuliahan
6. Dra. Retno Susilowati, MM. selaku dosen pembimbing satu yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan dan membimbing saya selama penyusunan skripsi ini
7. Cynthia Azhara Putri, S.H., M.Kn selaku dosen pembimbing dua yang telah menyediakan waktu dan pikiran nya untuk mengarahkan dan membimbing saya selama penyusunan skripsi ini
8. Dosen penguji atau dosen pembahas ilmu hubungan internasional yang telah memberikan arahan dan masukkan yang sangat baik untuk penyusunan skripsi ini
9. Seluruh dosen, admin, dan civitas akademika fakultas ilmu sosial dan ilmu politik yang telah memberikan kelancaran dalam penyusunan skripsi ini

10. Serta semua pihak yang tidak bisa disebutkan satu persatu yang mana telah memberikan semangat dan dukungan dalam menyelesaikan skripsi ini

Indralaya,

Tiara Anjani

07041181924031

DAFTAR ISI

Daftar Tabel

DAFTAR GRAFIK

DAFTAR GAMBAR

DAFTAR SINGKATAN

APT : *Advanced Persistent Threat*

ASCCE *: ASEAN-Singapore Cybersecurity Centre of Excellence*

ASEAN : *Association of Southeast Asian Nation*

CERT : *Computer Emergency Responsible Team*

CII : *Critical Information Infrastructure*

CMA : *Computer Misuse Act*

CSA : *Cyber Security Agency of Singapore*

GCI : *Global Cybersecurity Index*

GCSOC : *the Government Cyber Security Operations Center*

IGCI : INTERPOL *Global Complex Innovation*

INTERPOL : *International Criminal Police Organization*

ITU : *International Telecommunications Union*

NCAP : *National Cybercrime Action Plan*

SICW : *Singapore International Cyber Week*

SITSA : *Singapore Infocomm Technology Security Authority*

SPF : *Singapore Police Force*

SNDGG : *The Smart Nation and Digital Government Group*

YCEP : *Youth Cyber Exploration Program*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Hubungan Internasional merupakan sebuah kajian ilmu politik yang dimana menelaah terkait sebuah kebijakan dan tindakan yang dilakukan baik oleh *state actor* dan *non-state actor* (organisasi, perusahaan multinasional dan kelompok) dalam lingkup internasional dengan tujuan untuk menyampaikan kepentingan masing-masing yang dimiliki para aktor-aktor tersebut (Prayuda, 2019). Dalam hubungan internasional, tentu nya terdapat beberapa aspek yang penting untuk negara melaksanakan seperti aspek ekonomi, keamanan, pendidikan, serta sosial budaya. Namun, aspek keamanan internasional (*international security*) saat ini menjadi sorotan bagi negara- negara di dunia. Setiap negara tentunya akan selalu berusaha untuk menjaga keamanan negara nya dikarenakan hal tersebut penting untuk dilakukan.

Seiring berjalannya waktu, konsep keamanan internasional semakin berkembang dan mengalami perubahan yang disebabkan oleh globalisasi dimana kemajuan teknologi dan informasi semakin berkembang pesat dan memudarkan batas-batas wilayah antar negara. Bentuk dari keamanan pun juga berkembang dari dimensi keamanan yang bersifat keamanan tradisional menjadi keamanan non-tradisional. Pembahasan terkait keamanan juga semakin meluas ke dalam hal non militer (Azizah, 2020). Salah satu bentuk ancaman kejahatan non-tradisional yang semakin marak terjadi adalah kejahatan siber atau *cyber crime.*

Untuk menghadapi ancaman kejahatan siber, sebuah negara tentunya perlu mengembangkan atau membuat strategi keamanan siber. Adapun pendapat para ahli

mengenai strategi dalam hubungan internasional adalah bahwa strategi merupakan sebuah rencana yang dirancang atau dibuat oleh suatu negara untuk dilaksanakan yang dimana strategi tersebut dibentuk dengan tujuan agar dapat meraih suatu hal. Strategi yang dibuat atau dirancang oleh suatu negara bersifat untuk jangka panjang (Wirtz, 2000). Keamanan siber merupakan sebuah sistem dimana hukum, organisasi, kemampuan, serta kerjasama (*cooperation*) harus sejalan agar menjadi efektif. Kehadiran organisasi internasional dan terjalinnya kerjasama dengan negara serta adanya juga peningkatan kapasitas siber menjadi hal-hal yang bisa dilakukan untuk membangun keamanan siber yang baik (Primawanti, 2020).

Adapun 3 macam tipologi ancaman terhadap keamanan siber yaitu *cyber crime, cyber war, dan cyber terrorism*. *Cyber crime* adalah semua bentuk tindakan yang dilakukan oleh suatu kelompok atau individu dengan memanfaatkan jaringan komputer sebagai sarana dalam melakukan tindak kejahatan. *Cyber war* yaitu bentuk perang yang dilakukan melalui dunia maya yang dimana biasanya melibatkan perusahaan, organisasi-organisasi, dan militer dalam mencoba melakukan perusakan terhadap sistem komputer negara lain. Sedangkan *cyber terrorism* adalah kegiatan untuk meretas atau melumpuhkan sistem perangkat lunak yang berisikan informasi serta data negara, dimana pelaku yang melakukan aksi nya tersebut berasal dari kelompok terorisme (Suharto, 2021).

Kawasan Asia Tenggara ternyata menjadi salah satu kawasan yang rentan mengalami kejahatan siber (Anshori, 2019). Keamanan siber di Kawasan Asia Tenggara juga dinilai belum sempurna dan masih perlu ditingkatkan dikarenakan tingkat keamanan siber akan berdampak juga pada perkembangan ekonomi digital di ASEAN sehingga negara lain yang berada di Asia Tenggara seharusnya tidak bisa mengabaikan hal tersebut begitu saja. Belum meratanya kemampuan teknologi

informasi pada negara-negara di Asia Tenggara menjadi sebuah permasalahan untuk menghadapi ancaman kejahatan siber. Ancaman siber yang terjadi tentu akan berdampak pada setiap negara di Asia Tenggara sehingga negara-negara tersebut sangat perlu untuk terus melakukan pengembangan teknologi yang baik agar dapat menghadapi dan mengatasi ancaman *cyber crime*. (Ramadhan, 2019).

Penguasaan IT (Teknologi Informasi) pada Kawasan Asia Tenggara diketahui dipegang oleh Negara Singapura dan menjadikan Singapura sebagai target dari serangan siber. Negara Singapura merupakan salah satu negara yang terletak di Wilayah Asia Tenggara dan dikategorikan sebagai negara dengan *cyber security* yang baik dibandingkan dengan negara lain di Asia Tenggara. Dalam *Global Security Index* yang dikemukakan oleh *International Telecommunications Union* (ITU) pada tahun 2022, Singapura berada pada peringkat pertama dengan nilai 98,52 dalam hal keamanan siber (Kusnandar, 2022). Pada tahun-tahun sebelumnya, Negara Singapura juga diketahui selalu mengalami kenaikan atau peningkatan terkait keamanan siber (*cyber security*). Walaupun Singapura telah memiliki nilai indeks keamanan siber yang tinggi dimana kecanggihan dan kemampuan teknologi yang sudah sangat baik dan memadai. Hal tersebut ternyata tidak menutup kemungkinan untuk Singapura tetap sering mengalami serangan siber tiap tahun nya

Serangan siber yang kerap terjadi dalam ruang siber di Singapura pun memiliki beberapa bentuk atau macam yaitu seperti *phishing* dan *ransomware* serta berbagai bentuk *online scam*. *Phishing* merupakan sebuah bentuk kejahatan dengan cara mengelabui korban untuk mendapatkan data vital seseorang seperti data finansial/ keuangan (*password* atau kata sandi rekening bank), data identitas diri (nama, usia, alamat), serta data akun social media (*username* dan *password*) dengan cara mengirimkan email yang berisikan link palsu. Kemudian, *ransomware* adalah tindak

kejahatan dengan cara menyebarkan virus pada sistem jaringan komputer dan biasanya pelaku akan meminta tebusan dari korban. (Ganesan, 2022) Beberapa bentuk kejahatan tersebut masih menjadi sebuah masalah yang sering terulang dan mengancam keamanan siber di Negara Singapura.

Pada bulan Juni tahun 2018, Pemerintah Singapura telah mengeluarkan hasil investigasi resmi kasus SingHealth. SingHealth adalah sebuah penyedia jasa kesehatan terbesar di Singapura, dimana sistem informasi SingHealth berhasil diretas dan pelaku peretas mencuri 2,5 juta data pribadi pasien termasuk data pribadi Perdana Menteri Lee Hsien Loong (Alijoyo, 2019). Menteri Komunikasi dan Informasi Singapura mengatakan, serangan itu kemungkinan berasal dari kelompok "*Advanced Persistent Threat*" (APT) yang biasanya terkait suatu negara (Hidayat, 2018).

Kemudian, pada tahun 2018 Singapura juga diketahui pernah mengalami kerugian dimana kurang lebih 19.000 data kartu kredit nasabah mereka bocor dan diperjualbelikan di internet. Di tahun yang sama, negara Vietnam dan Malaysia juga mengalami kasus kebocoran data akibat serangan siber. Pada tahun 2019, diperkirakan bahwa ancaman siber yang terus terjadi akan berpotensi menimbulkan kerugian sebesar 2,1 triliun miliar dolar AS. Saat ini, penguasaan teknologi informasi pada Kawasan Asia Tenggara memang telah dikuasai oleh Negara Singapura. Namun, kenyataan nya Negara Singapura juga menjadi salah satu target dari serangan siber meskipun Negara Singapura menjadi pusat teknologi informasi di seluruh Wilayah Asia Tenggara.

Pada bulan Juli tahun 2021, Badan Keamanan Siber (*Cyber Security Agency*) Singapura melaporkan bahwa 9.080 kasus serangan siber ditangani oleh Tim Tanggap Darurat Komputer Singapura pada tahun 2020 yang tercatat sebagai total tahunan tertinggi. Menurut badan tersebut, serangan terhadap sistem perangkat komputer mengalami peningkatan sebesar 154% dari tahun ke tahun. Hal tersebut sangatlah

mengkhawatirkan karena dapat memberikan dampak bagi perniagaan, usaha kecil dan menengah dalam berbagai industri seperti ritel, manufaktur dan perawatan kesehatan (Abke, 2021).

Mayoritas warga Singapura memang sangat bergantung pada teknologi karena dalam aktivitas keseharian nya sering memanfaatkan penggunaan internet. Adanya peningkatan konektivitas dalam dunia maya serta ketergantungan Singapura pada ruang siber akan membuat kejahatan transnasional berbasis siber tersebut semakin meningkat. Dengan adanya ketergantungan tersebut, maka hal terkait keamanan siber (*cyber security*) sangat penting bagi Negara Singapura. Keamanan siber sangat penting sebagai bentuk dalam menjaga dan mengantisipasi berbagai ancaman dari ruang siber serta sebagai cara untuk memfasilitasi serta mendukung keberhasilan terhadap berbagai inovasi yang dilakukan pada bidang-bidang infrastruktur di Negara Singapura yang sebagian besar memanfaatkan ruang siber (*cyber space*) (Luk, 2019).

1.2 Rumusan Masalah

Berdasarkan uraian penjelasan latar belakang di atas, dapat diketahui bahwa yang menjadi masalah dalam penelitian skripsi ini adalah: *"Bagaimana Strategi Keamanan Siber Singapura dalam Menghadapi Ancaman Kejahatan Siber" ?*

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis strategi keamanan siber Singapura sebagai sebuah upaya untuk menghadapi kejahatan atau serangan siber.
2. Menganalisis seperti apa kasus serangan siber yang menjadi sebuah bentuk ancaman kejahatan siber

1.4 Manfaat Penelitian

1.4.1 Manfaat Penelitian Teoritis

Menjadi bahan rujukan untuk penelitian selanjutnya maupun penelitian yang serupa agar penelitian ini bisa menjadi acuan dan sumber informasi bagi peneliti lainnya serta dapat memberikan kontribusi dalam pengembangan konsep mengenai kondisi-kondisi yang dapat berpengaruh bagi suatu negara dalam membangun atau membentuk strategi keamanan siber.

1.4.2 Manfaat Penelitian Praktis

Penelitian ini diharapkan dapat menjadi sarana yang memiliki manfaat dalam mengimplementasikan atau menerapkan pengetahuan tentang strategi keamanan dan kasus kejahatan siber

DAFTAR PUSTAKA

Buku

Bachri, B. S. (2010). Meyakinkan Validitas Data melalui Triangulasi pada Penelitian Kualitatif. *Jurnal Teknologi Pendidikan*, 54-55.

Hardani. (2020). *Metode Penelitian Kualitatif dan Kuantitatif.* Yogyakarta: CV.Pustaka Ilmu.

Hean, T. C. (2016). *Singapore Cyber Security Strategy* . Cyber Security Agency of Singapore.

Hohmann, M. (2017). *Advancing Cybersecurity Capacity Building.* Berlin: Global Public Policy Institute.

Loong, L. H. (2021). *The Singapore Cybersecurity Strategy.* Cyber Security Agency of Singapore.

Luk. (2019). *Strenghthening Cyber security in Singapore : Challenges, Responses, and The Way Forward.* Hershey: IGI Global.

Putra, K. I. (2019). *Belajar dari Tata Kelola Keamanan Siber Singapura.* Yogyakarta: Center for Digital Society.

Siyoto, S. (2015). *Dasar Metodologi Penelitian.* Yogyakarta: Literasi Media.

Sugiyono, P. D. (2012). *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta.

Wirtz, J. (2000). *Strategy In The Contemporary World.* Monterey, California: INSTITUTE FOR JOINT WARFARE ANALYSIS.

Yacob, H. (2018). *Cybersecurity Act 2018.* Government Gazette.

Jurnal

Aljunied, S. M. (2019). *The Securitization of Cyber Space Governance in Singapore. Asian Security*, 14.

Anshori, M. F. (2019). Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam *Singapore International Cyber Week. Padjajaran Journal of International Relations*, 40.

Azizah, R. Z. (2020). Mendefinisikan Kembali Konsep Keamanan dalam Agenda Kebijakan Negara-Bangsa. *Jurnal Diplomasi Pertahanan*, 97.

Ganesan, N. (2022). Singapore Faced More Cyber Crime, Phishing and Ransomware Threats In 2021. *Channel Newasia*.

Lubis, R. R. (2018). Sekuritisasi Isu Keamanan Maritim dalam Mendukung Diplomasi Pertahanan Indonesia di ADMM *Plus On Maritime Security*. *Jurnal Pertahanan dan Bela Negara*, 36-37.

Novitasari, I. (2017). Babak Baru Rezim Keamanan Siber di Asia Tenggara Menyosong ASEAN Connectivity 2025. *Asia Pacific Studies*, 222.

Prayuda, R. (2019). Diplomasi dan Power : Sebuah Kajian Analisis. *Journal of Diplomacy andInternational Studies*, 81.

Primawanti, H. (2020). Diplomasi Siber Indonesia dalam Meningkatkan Keamanan Siber melalui *Association of Southeast Asian Nation* (ASEAN) Regional Forum. *Jurnal Unfari*, 4.

Ramadhan, I. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber. *JurnalPopulis*, 501.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara : Self-Helpatau Multilateralism? *Jurnal Asia Pacific Studies*, 183.

Suharto, M. A. (2021). Konsep Cyber Attack, Cyber Crime, dan Cyber Warfare dalam AspekHukum Internasional. *Risalah Hukum*, 104.

Trihartono, A. (2020). Keamanan dan Sekuritisasi dalam Hubungan Internasional. Depok: MelvanaMedia.

Triwahyuni, D. (2016). Strategi Keamanan Siber Amerika Serikat. *Jurnal Ilmu Politik danKomunikasi*, 109.

Yanuar, A. P. (2021). Cyberwar : Ancaman Baru Keamanan Nasional dan Internasional. *JurnalKeamanan Nasional*, 31.

Website

Abke, T. (2021). Singapura dan A.S. Memperluas Kerjasama Keamanan Siber. *Indo-PacificDefense Forum.*

Alijoyo, A. (2019). Pembelajaran Kasus Serangan Siber SingHealth-Singapura. *Indonesia RiskManagement Professional Association.*

Andaya, B. W. (2022). Introduction to Southeast Asia. *Asia Society*.

Citiasianic. (2022). Smart City Framework : Singapore Smart Nation dan Telkom Smart City.

smartnation.id

CSA Singapore. (2021). Legislation on Cybersecurity, Personal Data Protection & Computer Misuse

Ganesan, N. (2022). Singapore Faced More Cyber Crime, Phishing and Ransomware Threats In2021. *Channel Newasia*.

Goh, C. (2022). Crimes Reported in Singapore rose 24 per cent in 2021, Full by steep Climb inScams. *todayonline*.

Hidayat, K. (2018). Serangan Siber Terbesar dalam Sejarah Menyerang Singapura.

investasi.kontan.co.id.

Kusnandar, V. B. (2022). ITU : Keamanan Siber Indonesia Kalah dari Singapura danMalaysia. *databoks.katadata.*

Permata, I. M. (2020). *The Securitization of Cyber Issue.* Padang: Universitas Andalas.

Pradistya, R. M. (2021). Teknik Triangulasi dalam Penelitian Kualitatif. *dqlab.id.*

Rosana, F. C. (2022). Perusahaan Keamanan Siber Asal Singapura Buka Kantor di Jakarta. *tempo.co*.

Sagar, M. (2019). Singapore Ministry of Defence Opens New Cyber Defence School. *opengovasia.com*

Shika. (2022). Cyber Security Metrics. *geeksforgeeks*.

Siregar, R. K. (2022). Perbedaan Hacker dan Cracker. *Kementerian Keuangan Republik Indonesia*

Syafnidawaty. (2020). Apa itu Cyber Crime?

*Universitas Raharja.*Wibowo, P. T. (2021).

Apa Itu Cybersecurity ? *Wartaekonomi.*