PERAN ASEAN MELALUI CYBERSECURITY COOPERATION STRATEGY (ACCS) DALAM MENANGANI KEJAHATAN SIBER DI INDONESIA

Jonathan Manurung[1], Tom Finaldin[2]

Program Studi Hubungan Internasional,
Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Al-Ghifari Bandung
Email: jonathannurung28@gmail.com, finaldintom@gmail.com

ABSTRAK

Perkembangan dalam penguatan teknologi di masa kini tidak hanya menjadi pengaruh tutur cara dalam bersosial di masyarakat namun juga mempengaruhi sifat ancaman yang lebih modern dan kompleks yang berada pada domain virtual terhadap pertahanan dan keamanan suatu negara. Ancaman Siber saat ini tidak terbatas pada bentuk ancaman siber dengan motif ekonomi atau Sibercrime namun ancaman dalam bentuk Siber Keamanan yang dapat menjadi sifat pertahanan suatu negara, keamanan maupun kepentingan nasional suatu negara secara luas. Ancaman Siber Keamanan dianggap sangat berbahaya karena mampu mengakibakan kehancuran, gangguan, kerusakan jaringan infrastruktur militer maupun sipil yang sangat dibatasi serta diprediksi dampak dan ukurannya. Penelitian ini menganalisis terkait dengan perkembangan dan tindak lanjut ASEAN dalam memperkuat Kerjasama di bidang Siber Keamanan.

Kata Kunci: Keamanan Siber, Ancaman Siber, ASEAN.

A. PENDAHULUAN

Di era globalisasi, Cyber Space atau ruang siber telah menjadi kebutuhan dasar yang memungkinkan manusia terhubung tanpa batas fisik. Cyber Space mewakili era baru yang dihadirkan oleh internet (Zalesky, J., 1999). Ruang Siber adalah dunia virtual tanpa batas yang nyata meskipun tidak memiliki bentuk fisik. Konsep ini mencerminkan ide dari Borderless World, di mana ruang siber tidak terikat pada batasan negara, sehingga menghilangkan pembatasan dalam hal ruang, waktu, dan lokasi (Purbo, O. W., 2000). Bruce Sterling berpendapat bahwa meskipun tidak "nyata," Cyberspace adalah tempat yang memiliki konsekuensi nyata. Banyak orang mendedikasikan hidup mereka untuk layanan komunikasi publik melalui elektronik (Rizal, M., & Yani, Y. M., 2016).

Menurut Barrett, N. (1997), di balik keunggulannya, Cyber Space memiliki sisi gelap seperti akses ke konten pornografi dan berbagai kejahatan seperti penipuan, penyebaran informasi teroris, dan hacking. Kejahatan siber telah menjadi perhatian global, seperti yang dibuktikan dengan pembahasan di Kongres ke-10 PBB pada tahun 2000 di Wina, Austria. Namun, tidak semua negara memiliki regulasi untuk mengatur kejahatan siber dan tidak semua negara bersedia untuk secara serius mengatasi masalah Siber Crime, hanya negara maju dan beberapa negara berkembang yang terlibat dalam upaya tersebut.

Menurut Kongres PBB di Wina (Canton, H., 2021), kurangnya perhatian terhadap kejahatan siber bisa disebabkan oleh rendahnya partisipasi negara dalam komunikasi elektronik internasional, pengalaman penegakan hukum yang terbatas, dan estimasi kerugian masyarakat yang rendah akibat kejahatan siber. Sebagai negara berkembang, Indonesia menghadapi tantangan dalam penjagaan dan pengembangan teknologi informasi (Lakitan, B., 2013; Sabani, A., Deng, H., & Thai, V., 2019). Meskipun demikian, penggunaan teknologi informasi untuk tujuan merusak dapat menjadi ancaman bagi pertahanan nasional,

baik dalam bentuk militer maupun non-militer. Ancaman non-militer mencakup aspek ideologis, politik, ekonomi, sosial, dan budaya. Perkembangan teknologi diharapkan memengaruhi berbagai aspek kehidupan manusia, termasuk sosial, budaya, dan politik (Salehan, M., Kim, D., & Lee, J., 2018).

Sarjana hukum Ari Purwadi (Purwadi, A., 1993) juga mengakui bahwa teknologi mencerminkan sistem nilai tertentu karena merupakan produk dari budaya masyarakat. Secara umum, teknologi dapat diidentifikasi sebagai sumber potensial ancaman yang meliputi sumber internal dan eksternal, termasuk kegiatan intelijen, gangguan investigasi, organisasi ekstremis, peretas, kelompok kejahatan terorganisir, persaingan, permusuhan, konflik, dan teknologi itu sendiri (Grabosky, P., 2007). Menurut analisis ATKearney (Kearney, A. T., 2018), negara-negara di Asia Tenggara yang merupakan anggota ASEAN menjadi target utama serangan Siber karena beberapa alasan. Pertama, negara-negara ASEAN, terutama Malaysia, Indonesia, dan Vietnam, sering menjadi tempat tuan rumah untuk blokade aktivitas web yang mencurigakan secara global. Kedua, kebijakan regional, tata kelola, dan kemampuan keamanan siber di wilayah tersebut relatif rendah. Ketiga, terdapat kekurangan kemampuan dan keahlian di dalam negeri karena industri terfragmentasi dan kurangnya keterampilan yang memadai. Keempat, persepsi risiko Siber dari pihak korporasi dan pemangku kepentingan tidak memandang keamanan siber sebagai prioritas bisnis, yang mengakibatkan kurangnya pendekatan holistik terhadap ketahanan siber.

Gambar 1 Grafik Jumlah Serangan Siber di Indonesia 2017-2023

Sumber. Peneliti, 2023.

Berdasarkan data – data yang telah dijabarkan diatas, bahwa Indonesia pada tahun 2017 - 2023 tidak sedang baik – baik saja. Siber Keamanan merupakan hal yang sangat penting, mengingat bahwa teknologi semakin berkembang dengan sangat pesat yang membuat seiringnya perkembangan kejahatan. Indonesia sendiri telah melakukan beberapa bentuk kebijakan siber sebagai respon dalam penanganan kasus kejahatan siber yang terjadi di Indonesia. Salah satunya yaitu pembentukan Badan Siber dan Sandi Negara (BSSN) pada tahun 2017 yang merupakan lembaga pemerintah di Indonesia yang bertanggung jawab atas pengelolaan keamanan siber dan sandi (BSSN, Indonesia Cybersecurty Monitoring Report, 2019). Negara Indonesia merupakan salah satu negara anggota dari ASEAN yang disebut ASEAN member state dan juga anggota komunitas keamanan ASEAN yaitu Asean Political Security Society (APSC). Dari kebijakan dilakukan Indonesia penulis tertarik untuk menganalisis pada keterkaitannya dengan kebijakan siber ASEAN yaitu ASEAN Cybesecurity Cooperation Strategy (ACCS).
Berdasarkan data di atas, Indonesia selama paruh pertama 2023, ada 347 jutaan serangan siber yang terjadi di Indonesia, atau sekitar 1,9 juta serangan perhari, atau 22 serangan setiap detik. Data ini berasal dari laporan Ancaman Digital Semester 1 tahun 2023 dari AwanPintar.id. Dalam laporan tersebut terungkap

kalau selama enam bulan pertama tahun 2023 ini, serangan digital paling banyak terjadi pada bulan Mei. Jumlahnya mencapai 112 jutaan serangan dalam satu bulan. Padahal dari Januari sampai April 2023, jumlah serangan siber yang terjadi mengalami penurunan, dari 62 juta menjadi 36 juta. Baru melonjak drastis pada Mei, dan kembali turun pada Juni menjadi 37 juta. Untuk menjawab penelitian ini secara komprehensif, penulis memutuskan untuk memilih pertanyaan penutup mengenai masalah terkait yaitu *Bagaimana Kondisi Kerja Sama Indonesia-ASEAN terkait dengan kebijakan keamanan Siber dan ketangguhan Siber untuk menangani kejahatan Siber?* dan *Bagaimana Konsep Kerja Sama Indonesia-ASEAN terkait dengan kebijakan keamanan Siber dan ketangguhan Siber dalam usaha untuk menanggulangi kejahatan Siber?*

B. TINJAUAN TEORITIS

Hubungan internasional adalah bidang studi yang mengkaji interaksi antara negara, serta aktor lain seperti organisasi internasional, organisasi non-pemerintah, perusahaan multinasional, dan individu. Studi ini mencakup berbagai isu, termasuk pemerintahan global, diplomasi, keamanan internasional, ekonomi politik internasional, dan hak asasi manusia (Brown & Ainley, 2005). Salah satu tantangan utama dalam hubungan internasional adalah ancaman dan kejahatan siber. Keamanan siber mencakup langkah-langkah untuk melindungi dari serangan atau ancaman melalui elemen-elemen dunia maya seperti perangkat lunak, perangkat keras, dan jaringan komputer (Fischer, 2014). Fungsi keamanan siber meliputi memastikan sinergi kebijakan pertahanan siber, membangun tata kelola sistem, menjamin ketersediaan informasi, menanggulangi serangan siber, dan meningkatkan kesadaran serta riset keamanan siber (Kemenhan, 2014).

Kerja sama internasional terjadi ketika negara-negara atau aktor lain menyesuaikan perilaku mereka untuk mencapai kepentingan bersama dan mengatasi ancaman yang mengancam keamanan kolektif (Hadiwinata, 2013). Bentuk kerja sama ini meliputi kerja sama bilateral, regional, dan multilateral, yang semuanya penting untuk meningkatkan kesejahteraan ekonomi, mengurangi ancaman keamanan, dan meningkatkan efisiensi serta mengurangi kerugian akibat tindakan individu negara (Wicaksana & Rachman, 2018). Negara-negara perlu berkolaborasi dalam menghadapi tantangan global seperti kejahatan siber. Institusi internasional, seperti PBB dan ASEAN, memainkan peran penting dalam memfasilitasi kerja sama, menyediakan platform untuk komunikasi dan negosiasi, serta menetapkan aturan bersama untuk mengelola masalah global (Keohane, 1989; Ii & Pustaka, 2002).

Teori liberal institusionalisme menekankan pentingnya institusi internasional dan norma dalam membentuk perilaku negara serta mendorong kerja sama (Keohane, 2020; Nye, 2004). Dalam konteks keamanan siber, institusi seperti ASEAN memainkan peran kunci dalam memfasilitasi kerja sama regional. Kebijakan ASEAN Cybersecurity Cooperation Strategy (ACCS) adalah contoh konkret dari upaya ASEAN untuk membangun kerangka kerja sama keamanan siber di kawasan Asia Tenggara. Institusi ini menyediakan sarana untuk komunikasi, negosiasi, dan penguatan harapan tentang kesepakatan internasional (Keohane, 1989). Penelitian ini bertujuan untuk menganalisis bagaimana kebijakan siber ASEAN mempengaruhi kebijakan siber nasional Indonesia dan melihat bagaimana Indonesia berinteraksi dalam kerangka kerja sama regional ini.

C. METODE PENELITIAN

Metode penelitian yang dipakai oleh peneliti adalah metode penelitian kualitatif. Data- data dikumpulkan melalui wawancara dan studi literatur yang berasal dari berbagai sumber terutama buku dan jurnal penelitian ilmiah mengenai topik terkait kemudian menganalisanya dengan menggunakan teori/perspektif. Dengan demikian data yang berhasil dikumpulkan dapat dipahami secara lengkap dan menyeluruh. Sesuai dengan masalah pada penelitian ini yang akan menyoroti terkait masalah keamanan siber merujuk pada permasalahan yang di angkat serta variabel yang tersedia, maka peneliti melakukan analisa data

berdasarkan data- data serta informasi yang dikeluarkan olehsitus resmi ASEAN dan Badan Siber dan Sandi Negara (BSSN) kemudian diterapkan dengan teori-teori dalam kajian Hubungan Internasional.
Maksud dari metode ini adalah metode yang berusaha mengumpulkan, menyusun dan menginterpretasikan data yang kemudian diajukan dengan menganalisis suatu fenomena serta suatu metode dalam meneliti status kelompok manusia, suatu objek, dan suatu kelas peristiwa pada masa sekarang. Pengumpulan informasi aktual secara rinci yang melukiskan gejala yang ada, mengidentifikasi masalah yang sedang berlangsung akibat yang terjadi. Dalam penelitian ini dilakukan cara menganalisis data yang telah terkumpul melalui referensi buku yang berhubungan dengan masalah yang sedang diteliti dengan tujuan untuk mengumpulkan informasi dengan tepat mengenai Peran ASEAN melalui *ASEAN Cybersecurity Cooperation Strategy* (ACSS) dalam menangani Kejahatan Siber di Indonesia.

D. HASIL DAN PEMBAHASAN

Kondisi Indonesia dengan ASEAN Mengenai Kebijakan *Siber Keamanan* dan *Siber Resilience* dalam Mengatasi *Siber Crime*

Pembentukan ASEAN didasari pada prinsip bahwa stabilitas keamanan dan kelancaran pembangunan saling terkait. Indonesia, sebagai salah satu negara pendiri ASEAN, mengakui pentingnya kondisi aman dan stabil di tingkat regional untuk mendukung pembangunan nasional (Saptono, Y., dkk., 2023). Untuk melindungi dunia maya dari ancaman kejahatan siber, pemerintah Indonesia telah mengambil berbagai langkah. Salah satunya adalah dengan menerbitkan Undang-Undang Telekomunikasi tahun 1999 dan Undang-Undang Informasi dan Transaksi Elektronik tahun 2008 sebagai landasan untuk regulasi dan kebijakan keamanan informasi. Selain itu, pemerintah membentuk Badan Siber dan Sandi Nasional (BSSN) yang bertanggung jawab dalam mencegah serangan Siber dan memperkuat pertahanan negara serta meningkatkan kesadaran publik tentang keamanan siber (Mulyadi., & Rahayu, D., 2018). Hasil survei kebijakan keamanan dan ketahanan siber di enam negara ASEAN menunjukkan bahwa sebagian besar negara telah mengadopsi undang-undang dan kebijakan untuk menangani masalah siber, termasuk memberikan tanggung jawab kepada pemilik platform, mengatasi kejahatan siber dengan mengenakan hukuman kepada pelaku, dan melindungi data pribadi warga negara dengan regulasi yang mengatur privasi.

Gambar 1 Ratifikasi Kerja Sama ASEAN

	Openness of the Platform	Cybercrime Prevention	Privacy
Indonesia	Judicial System	No Specific cybersecurity laws; Information and Electronic Transaction Act (Law of the Republic of Indonesia No. 11 of 2008)	Data Protection Regulation (2016) -Personal Data Protection (Draft)
Malaysia	Notice and takedown	Computer Crime Act 1997	Personal Data Protection Act 2010 (PDPA).
Philippines	Judicial System	Cybercrime Prevention Act (2012)	Data Privacy Act (2012)
Singapore	Notice and takedown	COMPUTER MISUSE ACT (1993, amended 2017)	The Data Privacy Act of 2012
Thailand	Judicial System	Computer-Related Crime Bill (2007, amended 2017))	Sector specific approach such as National Health Service Act -Personal Information Protection Act (Draft)
Vietnam	Judicial System	Law on Cyber Information Security (Law No. 86/2015/QH13)	Law on Cyber Information Security (Law No. 86/2015/QH13)

Dari data yang disajikan, terlihat bahwa setiap negara memiliki tingkat perkembangan aturan yang berbeda-beda dan memiliki fungsi yang beragam. Hanya Singapura dan Malaysia yang memiliki prosedur Notice and Takedown dalam hal keterbukaan platform, sementara Indonesia, Filipina, Thailand, dan Vietnam tidak memiliki aturan serupa untuk melindungi hak cipta melalui sistem Notice and Takedown. Sebagai gantinya, pemegang hak harus menggunakan sistem peradilan untuk melindungi hak ciptanya. Sebagai contoh, pada tahun 2017, penelitian menemukan beberapa situs ilegal yang menyediakan unduhan buku secara gratis tanpa izin, seperti buku Negeri 5 Menara karya Ahmad Fuadi yang dapat diunduh secara gratis di www.rajaebookgratis.com dan kumpulan buku karya Raditya Dika yang tersedia di sebuah blog pribadi. Hal ini tentu merugikan para penulis yang tidak menerima royalti atas karya mereka yang dibajak. Selain itu, Indonesia adalah satu-satunya negara di antara keenam negara ASEAN yang tidak memiliki undang-undang khusus mengenai keamanan siber, hanya mengandalkan UU ITE. Begitu juga dengan perlindungan data pribadi, di mana baik Thailand maupun Indonesia belum memiliki hukum yang spesifik, sehingga penyelesaian pelanggaran data pribadi bergantung pada keputusan hukum yang berbeda-beda, meskipun keduanya sedang dalam proses menyusun undang-undang perlindungan data pribadi. Vietnam merupakan satu-satunya negara di ASEAN yang memiliki pengaturan hukum komprehensif untuk menangani keamanan dan perlindungan data pribadi dalam satu undang-undang tunggal. Permasalahan ini perlu ditangani melalui kerjasama dan pertukaran informasi antara negara-negara ASEAN, yang merupakan aspek kunci dalam memastikan keamanan dan ketahanan siber. Tanpa kolaborasi, ekosistem keamanan siber rentan terhadap gangguan. Karena kejahatan siber bersifat lintas batas negara, penting untuk memiliki perjanjian multilateral di tingkat regional dan internasional untuk mengatasi tantangan ini.

Kerja Sama Indonesia dengan ASEAN Mengenai Kebijakan Siber Keamanan dan Siber Resilience dalam Mengatasi Siber Crime

Keamanan siber adalah praktik yang melindungi informasi dan sistem komputer dari ancaman siber seperti virus, peretasan, dan pencurian data. Ini penting untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Di tingkat nasional, keamanan siber mengacu pada perlindungan aset negara dari ancaman siber, sementara ketahanan siber (siber resilience) mengacu pada pengembangan kekuatan siber yang seimbang dan terpadu untuk menjaga kesejahteraan dan keamanan negara. Indonesia mengelola keamanan sibernya melalui berbagai instansi pemerintah seperti Kementerian Komunikasi dan Informatika (Kominfo) dan ID-SIRTII, dan berkolaborasi dengan berbagai pihak seperti militer, sektor swasta, dan akademisi.

Kerja sama internasional sangat penting dalam keamanan siber, dan Indonesia telah terlibat aktif dalam kerjasama dengan ASEAN. ASEAN adalah kawasan dengan ekonomi yang cepat berkembang dan populasi besar, menjadikannya target potensial untuk kejahatan siber. Oleh karena itu, keamanan siber dan perlindungan infrastruktur informasi menjadi prioritas. Indonesia berkomitmen pada tiga pilar ASEAN: Komunitas Ekonomi ASEAN, Komunitas Sosial Budaya ASEAN, dan Komunitas Keamanan Politik ASEAN, serta telah bermitra dengan negara-negara seperti Malaysia dan Singapura untuk memperkuat keamanan siber regional.

Indonesia dan ASEAN telah bekerja bersama dalam berbagai inisiatif untuk mengatasi kejahatan siber, seperti partisipasi dalam ASEAN Forum Regional (ARF) yang fokus pada ancaman siber. Sejak tahun 2006, ARF telah menghasilkan berbagai pernyataan dan kesepakatan untuk memperkuat keamanan siber, termasuk pembentukan ASEAN-CERT pada tahun 2011. Melalui kerjasama ini, Indonesia terus mengembangkan dan meningkatkan keamanannya, menunjukkan komitmennya untuk menjaga keamanan siber di Asia Tenggara.

Analisis Kerja Sama Indonesia-ASEAN dari Perspektif Liberal Institusionalisme

Dalam konteks liberalisme institusional, kerja sama multilateral di kawasan Asia Tenggara, yang dipimpin oleh ASEAN, menjadi landasan utama bagi negara-negara anggota seperti Indonesia untuk mengatasi tantangan keamanan siber secara efektif (Acharya, 2004). Prinsip-prinsip kerjasama dan dialog yang ditanamkan oleh ASEAN dalam proses pembentukan kebijakan regional menciptakan lingkungan yang kondusif bagi negara-negara anggota untuk berkolaborasi dalam menangani ancaman siber yang semakin kompleks (Emmers, 2011). Menurut dari hasil wawancara dengan Mayor Jenderal TNI Dominggus Pakel, S.sos, M.M.Si., Kepala Deputi Bidang Operasi Keamanan Siber Dan Sandi (BSSN), melalui ACCS dan forum-forum lainnya, ASEAN telah berhasil membentuk struktur dan mekanisme yang memfasilitasi pertukaran informasi, koordinasi kebijakan, dan pembentukan inisiatif bersama dalam bidang keamanan siber. Hal ini memberikan landasan yang kokoh bagi negara-negara anggota untuk mengembangkan kapasitas dan respon kolektif terhadap serangan siber.

Selain itu, kerja sama ASEAN-Indonesia dalam keamanan siber juga berkontribusi pada pembentukan norma-norma baru dalam tata kelola keamanan siber di tingkat regional (Razak & Sulaiman, 2020), hal ini pun telah dikonfirmasi oleh pihak BSSN. Dengan pendirian ASEAN-CERT sebagai wadah untuk meningkatkan kerjasama dalam menanggulangi serangan siber, ASEAN dan Indonesia berkomitmen untuk mengintegrasikan praktik-praktik terbaik dalam penanganan kejahatan siber dan mempromosikan budaya keamanan siber di seluruh kawasan (Adler & Barnett, 1). Melalui dialog yang terus-menerus dan pertukaran informasi antar-negara anggota, norma-norma baru terbentuk yang menegaskan pentingnya kerjasama dan transparansi dalam menangani ancaman siber yang lintas batas (Wahyuni, R., Waluyo, S., & Simatupang, H, 2021). Dengan demikian, kerja sama ASEAN-Indonesia dalam keamanan siber tidak hanya memiliki dampak praktis dalam memperkuat infrastruktur teknis, tetapi juga membentuk fondasi yang kuat bagi tata kelola keamanan siber yang inklusif dan adaptif di kawasan Asia Tenggara.

Teori liberal institusionalisme memberikan kerangka untuk memahami kerja sama internasional antara Indonesia dan ASEAN dalam keamanan siber. ASEAN memfasilitasi komunikasi, negosiasi, dan pembentukan aturan bersama, yang penting untuk kerja sama yang efektif. Partisipasi Indonesia dalam berbagai inisiatif ASEAN menunjukkan komitmen terhadap norma dan standar regional, serta bagaimana kebijakan nasional dipengaruhi oleh kebijakan regional. Dengan demikian, kerja sama Indonesia dengan ASEAN dalam kebijakan dan ketangguhan siber menunjukkan pentingnya institusi internasional dalam membentuk perilaku negara dan meningkatkan keamanan siber di Asia Tenggara.

E. PENUTUP

Kesimpulan

Berdasarkan hasil penelitian di atas menunjukkan bahwa kerja sama antara Indonesia dan ASEAN terkait dengan kebijakan keamanan siber dan ketangguhan siber dalam mengatasi kejahatan siber telah menjadi fokus utama bagi kedua entitas. Langkah-langkah yang diambil oleh pemerintah Indonesia, seperti pembentukan Badan Siber dan Sandi Nasional (BSSN) dan pengadopsian undang-undang terkait keamanan informasi, menunjukkan komitmen untuk melindungi infrastruktur digital negara dan meningkatkan kesadaran publik tentang ancaman siber. Di tingkat ASEAN, hasil survei kebijakan keamanan dan ketahanan siber menunjukkan adopsi undang-undang dan kebijakan oleh sebagian besar negara anggota untuk mengatasi masalah siber, serta upaya untuk meningkatkan kerjasama lintas batas dalam pertukaran informasi dan pemahaman. Dari perspektif konsep kerja sama, ASEAN berperan sebagai platform untuk memfasilitasi dialog dan koordinasi antara negara-negara anggota dalam menangani ancaman siber. Melalui inisiatif seperti ASEAN-CERT dan pertemuan regional seperti ASEAN Forum

Regional (ARF), upaya telah dilakukan untuk meningkatkan keamanan siber di kawasan. Hal ini menunjukkan bahwa kerja sama Indonesia-ASEAN dalam keamanan siber tidak hanya terbatas pada aspek teknis, tetapi juga melibatkan pembentukan norma-norma baru dan pembahasan kebijakan yang bersifat inklusif. Dengan demikian, pembahasan di atas telah menjawab kedua pertanyaan dengan memberikan gambaran tentang kondisi kerja sama Indonesia-ASEAN dalam keamanan siber serta konsep kerja sama tersebut dalam usaha untuk menanggulangi kejahatan siber.

DAFTAR PUSTAKA

Barrett, N. (1997). *Digital crime: Policing the Sibernation*. London: Kogan Page.

Brown, C., & Ainley, K. (2009). *Understanding international relations*. Macmillan International Higher Education.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Keamanan: A new framework for analysis*. Lynne Rienner Publishers.

Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief.

Grabosky, P. (2007). The Internet, Technology, and Organized Crime. *Asian Journal of Criminology*, 2, 145-161. https://doi.org/10.1007/S11417-007-9034-Z.

Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*.

KEMENHAN 2014. RI, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber. Kementrian Pertahanan

Keohane, R. O. (2020). *International institutions and state power: Essays in international relations theory*. Routledge.

Lakitan, B. (2013). Menghubungkan semua titik: Mengidentifikasi tantangan “tingkat aktor” dalam membangun sistem inovasi yang efektif di Indonesia. *Teknologi dalam Masyarakat* , 35, 41-54. https://doi.org/10.1016/J.TECHSOC.2013.03.002 . Purbo, O. W. (2000). perkembangan teknologi informasi dan internet di Indonesia. *Jakarta: Kompas*.

Mulyadi., & Rahayu, D. (2018). Indonesia National Cybersecurity Review: Before and After Establishment National Siber and Crypto Agency (BSSN). *2018 6th International Conference on Siber and IT Service Management (CITSM)*, 1-6. https://doi.org/10.1109/CITSM.2018.8674265.

Nye, J. S. (2004). *Soft power: The means to success in world politics*. Public affairs.

Purwadi, A. (1993). KEBUTUHAN AKAN PERANGKAT HUKUM PERJANJIAN 01 BIOANG ALIH TEKNOlOGI.

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61-78.

Sabani, A., Deng, H., & Thai, V. (2019). Evaluating the Development of E-Government in Indonesia. *Proceedings of the 2nd International Conference on Software Engineering and Information Management*. https://doi.org/10.1145/3305160.3305191.

Salehan, M., Kim, D., & Lee, J. (2018). Are there any relationships between technology and cultural values? A country-level trend study of the association between information communication technology and cultural values. *Inf. Manag.*, 55, 725-745. https://doi.org/10.1016/j.im.2018.03.003.

Saptono[1], Y., Sumertha[2], G., Freddy, H., Alexandra[3], S., Widodo, P., , D., & Konflik, R. (2023). Strengthening Regional Keamanan Through The Establishment Of The Asean Counter Terrorism And Peacekeeping Task Force Led By Indonesia In Collaboration With The United States. *International Journal Of Humanities Education and Social Sciences (IJHESS)*. https://doi.org/10.55227/ijhess.v3i1.585.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of Siber Keamanan. *Journal of Digital Forensics, Keamanan and Law*, *12*(2), 8.

Slouka, M., & Andri, Z. (1999). Ruang yang hilang: pandangan humanis tentang budaya Siberspace yang merisaukan. *(No Title)*.

United Nations Office on Drugs and Crime, Crimes Related to Computer Networks - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

Zalesky, J. (1999). Spiritualitas Siberspace (Teknologi Komputer Mempengaruhi Kehidupan Keeragamaan Manusia). *Mizan, Bandung*.

Wahyuni, R., Waluyo, S., & Simatupang, H. (2021). STRENGTHENING THE SIBER DEFENSE CENTER OF THE MINISTRY OF DEFENCE OF THE REPUBLIC OF INDONESIA (PUSDATIN KEMHAN) TO SUPPORT THE INDONESIAN DEFENSE DIPLOMACY IN SIBER DEFENSE KEAMANAN COOPERATION IN ASEAN. *Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity*. https://doi.org/10.33172/jp.v7i3.747.