ANALISIS KEBIJAKAN SIBER INDONESIA TERKAIT ASEAN *CYBERSECURITY COOPERATION STRATEGY* (ACCS) TAHUN 2019 – 2022

(Skripsi)

Oleh

M. Rafly Ramadhan

1816071035

JURUSAN HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS LAMPUNG

2023

ABSTRAK

ANALISIS KEBIJAKAN SIBER INDONESIA TERKAIT ASEAN *CYBERSECURITY COOPERATION STRATEGY* (ACCS) TAHUN 2019 – 2022

Oleh

M. RAFLY RAMADHAN

Keamanan siber merupakan salah satu aspek yang perlu diperhatikan. Dikarenakan perkembangan teknologi informasi yang sangat pesat menciptakan kejahatan siber yang baru dan unik yang menjadi ancaman bagi negara hingga organisasi internasional. ASEAN yang merupakan organisasi regional kawasan Asia Tenggara memiliki kebijakan yang berisikan strategi dan program pengembangan keamanan siber di kawasan yaitu ASEAN *Cybersecurity Cooperation Strategy* (ACCS). Indonesia yang merupakan salah satu negara anggota ASEAN mengalami kejahatan siber besar sepanjang tahun 2019 – 2022. Penelitian ini bertujuan untuk melihat bagaimana keterkaitan dari implementasi kebijakan siber Indonesia dengan ASEAN *Cybersecurity Cooperation Strategy* (ACCS) pada tahun 2019 – 2022.

Penelitian ini merupakan penelitian kualitatif yang menggunakan teknik pengumpulan data berupa studi pustaka yang bersumber dari situs resmi ASEAN, dan lembaga resmi siber Indonesia yaitu BSSN. Penelitian ini menggunakan konsep *cyber security*, dan teori liberal institusionalisme untuk melihat bagaimana implementasi kebijakan siber Indonesia terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS) dapat membantu penanganan kasus kejahatan siber di Indonesia pada tahun 2019 – 2022.

Hasil penelitian menunjukan bahwa kebijakan siber yang telah dibentuk oleh ASEAN di dalam komunitas keamanan ASEAN *Political-Security Community* yaitu APSC Blueprint 2009 dan 2025, ASEAN *Cybersecurity Cooperation Strategy* (ACCS) 2017 – 2020 dan 2021 – 2025 dapat membantu Indonesia dalam penanganan kasus kejahatan siber yang terjadi dengan implementasi kebijakan tersebut oleh pemerintah Indonesia yang dibagi menjadi empat yaitu; pembentukan CERT serta lembaga siber terkait, pembentukan perundang – undangan keamanan siber, peningkatan kapasitas keamanan siber melalui kerjasama regional dan internasional, dan pembentukan laporan tahunan keamanan siber yang disusun badan siber Indonesia yaitu BSSN.

Kata kunci: Keamanan siber, ASEAN, Indonesia, Kejahatan Siber

ABSTRACT

ANALYSIS OF INDONESIAN CYBER POLICY RELATED TO ASEAN CYBERSECURITY COOPERATION STRATEGY (ACCS) 2019 – 2022

By

M. RAFLY RAMADHAN

Cyber security is one aspect that needs attention. Due to the enormous development of information technology, it creates new and unique cyber crimes which pose a threat to countries and international organizations. ASEAN, which is a regional organization in the Southeast Asia region, has a policy containing strategies and programs for developing cyber security in the region, namely the ASEAN Cybersecurity Cooperation Strategy (ACCS). Indonesia, which is one of the ASEAN member countries, experienced major cyber crimes throughout 2019 - 2022. This research aims to see how the implementation of Indonesian cyber policy is related to the ASEAN Cybersecurity Cooperation Strategy (ACCS) in 2019 - 2022.

This research is qualitative research that uses data collection techniques in the form of literature studies sourced from the official ASEAN website and the official Indonesian cyber institution, namely BSSN. This research uses the concepts of cyber security, and liberal institutionalism theory to see how the implementation of Indonesian cyber policies related to the ASEAN Cybersecurity Cooperation Strategy (ACCS) can help handle cyber crime cases in Indonesia in 2019 - 2022.

The research results show that the cyber policies that have been formed by ASEAN in the ASEAN Political-Security Community, namely the APSC Blueprint 2009 and 2025, the ASEAN Cybersecurity Cooperation Strategy (ACCS) 2017 – 2020 and 2021 – 2025 can help Indonesia in handling cyber crime cases that occur. with the implementation of this policy by the Indonesian government which consists of four parts, namely; the formation of CERT and related cyber institutions, the formation of cyber security regulations, increasing cyber security capacity through regional and international cooperation, and the formation of an annual cyber security report prepared by the Indonesian cyber body, namely BSSN (Badan Security dan Siber Negara).

Keywords: Cyber Security, ASEAN, Indonesia, Cybercrimes

ANALISIS KEBIJAKAN SIBER INDONESIA TERKAIT ASEAN *CYBERSECURITY COOPERATION STRATEGY* (ACCS) TAHUN 2019 – 2022

Oleh

M. RAFLY RAMADHAN

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA HUBUNGAN INTERNASIONAL

Pada

Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2023

Judul Skripsi	:	**ANALISIS KEBIJAKAN SIBER INDONESIA TERKAIT *ASEAN CYBERSECURITY COOPERATION STRATEGY* (ACCS) TAHUN 2019 – 2022**
Nama Mahasiswa	:	M. Rafly Ramadhan
Nomor Pokok Mahasiswa	:	**1816071035**
Program Studi	:	**Hubungan Internasional**
Fakultas	:	**Ilmu Sosial dan Ilmu Politik**

MENYETUJUI

1. Komisi Pembimbing

Gita Karisma, S.IP., M.Si.
NIP. 19870128 201404 2 001

Indra Jaya Wiranata S.IP., M.A.
NIP. 19921219 202203 1 011

2. Ketua Jurusan Hubungan Internasional

Simon Sumanjoyo H, S.A.N, M.P.A.
NIP. 198106282005011003

MENGESAHKAN

1. Tim Penguji

Ketua : **Gita Karisma, S.IP., M.Si.**

Sekretaris : **Indra Jaya Wiranata, S.IP., M.A.**

Penguji : **Hasbi Sidik, S.IP., M.A.**

2. Dekan Fakultas Ilmu Sosial dan Politik

Dra. Ida Nurhaida, M.Si.
NIP. 19610807 198703 2 001

Tanggal Lulus Ujian Skripsi : **07 November 2023**

PERNYATAAN

Dengan ini menyatakan bahwa

1. Karya tulis saya, skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana), baik di Universitas Lampung maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan komisi pembimbing dan penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan sebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah berlaku di Universitas Lampung.

Bandar Lampung, 07 November 2023

M. Rafly Ramadhan
1816071035

RIWAYAT HIDUP

Penulis dilahirkan di Bandar Lampung pada tanggal 28 November 2000 dari pasangan Sutrisno dan Meriyana sebagai anak terakhir dari tiga bersaudara. Penulis menempuh pendidikan formal pertama di SDN 2 Rawa Laut. Kemudian penulis melanjutkan pendidikan ke tingkat menengah pertama di SMP Kartika II-2 Bandar Lampung dan lulus pada tahun 2016, dan tingkat menengah atas di SMA Negeri 4 Bandar Lampung dan lulus pada tahun 2018. Kemudian penulis melanjutkan pendidikan ke perguruan tinggi Jurusan Hubungan Internasional, Universitas Lampung.

Selama menempuh pendidikan di perguruan tinggi, penulis aktif di organisasi kampus yaitu sebagai anggota bidang *Social and Environment* Himpunan Mahasiswa Jurusan Hubungan Internasional (HMJHI) Universitas Lampung. Pada tahun 2021 Penulis juga menempuh Program Kerja Lapangan di Sub Direktorat Pengelolaan Pinjaman Dan Hibah Luar Negeri, Direktorat Jenderal Sumber Daya Air, Kementerian Pekerjaan Umum dan Perumahan Rakyat selama dua bulan. Penulis juga aktif berwirausaha secara daring atau Online selama kuliah dengan membuka usaha *online* bernama Papi Store yang menjual beragam gadget dan perangkat lunak komputer.

MOTTO

"Dan aku menyerahkan urusanku kepada Allah"

QS. Al-Mu'min:44

"One day or day one"

M. Rafly Ramadhan

SANWACANA

Puji dan syukur penulis panjatkan sebesar-besarnya kepada Allah SWT. yang telah melimpahkan segala rahmat, hidayah, dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini.

Skripsi dengan judul *"***Analisis Kebijakan Siber Indonesia Terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS) Tahun 2019 – 2022"** merupakan salah satu syarat untuk menyelesaikan Program Sarjana Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Lampung.

Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan, kritik dan saran, serta nasihat dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa terima kasih sebesar-besarnya kepada:

1. Prof. Dr. Ir. Lusmeilia Afriani, D.E.A., I.P.M., selaku Rektor Universitas Lampung.
2. Dra. Ida Nurhaida, M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Lampung.
3. Simon Sumanjoyo H, S.A.N., M.PA. selaku Ketua Jurusan Hubungan Internasional sekaligus dosen yang senantiasa mendukung penulis dalam proses perkuliahan yang dijalani.
4. Bapak Indra Jaya Wiranata, S.IP., M.A. selaku Dosen Pembimbing Akademik yang telah membimbing penulis dalam menempuh perkuliahan.
5. Ibu Gita Karisma, S.IP., M.Si. dan Bapak Indra Jaya Wiranata, S.IP., M.A. selaku Dosen Pembimbing Skripsi yang senantiasa menuntun penulis dalam setiap proses pengerjaan skripsi.

6. Bapak Hasbi Sidik, S.IP., M.A. selaku Dosen Pembahas yang senantiasa memberikan kritik, saran, dan masukan kepada penulis dalam proses penulisan skripsi ini.
7. Dosen-dosen Jurusan Hubungan Internasional yang tidak dapat penulis sebutkan satu persatu yang telah memberikan ilmu dan manfaat yang sangat berharga bagi penulis baik dalam bidang akademik maupun non-akademik.
8. Sutrisno dan Meriyana selaku kedua orang tua, terima kasih karena selalu mengorbankan waktu, tenaga dan materinya, serta mempercayai penulis dalam setiap keputusan yang penulis ambil baik dalam perkuliahan maupun dalam kehidupan sehari-hari. Semoga segala keluh kesah dan keringat yang kalian keluarkan dibalas dengan Surga oleh Allah SWT.
9. Rio Jassica dan Willy Admajaya selaku kakak kandung yang selalu mendoakan dan mendukung penulis dalam setiap proses perkuliahan yang dijalani.
10. Diva Alisti Qhalos Hakiki, yang selalu sabar dalam mendengarkan keluh kesah dan menemani serta memberikan harapan kepada penulis untuk tidak menyerah dalam segala hal.
11. Syahfadh, Gerri, Alif, Hafizh, Ridho, Alif Irha, Arsy, Daffa, Bagus, Amar, Zani, Shendy, Aqshal, Adjie, Ino, Ikrom, Icad, Aul, Dum dum, dan Reza (Sinirumpad). terima kasih karena telah menjaga pertemanan kita hingga detik ini.
12. Ailsa, Yayas, Fabio, Hemas, Heza, Dani, Rehan, Tasya, Uti, Aldy, Safaana, Shaqilla, Elsa, dan Rara yang selalu menemani penulis dalam setiap perjalanan selama kuliah.
13. Teman-teman seperjuangan Jurusan Hubungan Internasional angkatan 2018 yang telah memberikan pengalaman kuliah terbaik yang sangat berharga bagi penulis.
14. Untuk saya yang sudah mampu sampai pada titik ini, terima kasih karena telah percaya pada diri sendiri dan tetap berjuang selepas banyak kesabaran yang dijalani.

Bandar Lampung, 07 November 2023

M. Rafly Ramadhan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

ASEAN	: *Association of Southeast Asia Nations*
ARPANET	: *The Advanced Research Projects Agency Network*)
APSC	: ASEAN *Political-Security Community*
ASC	: ASEAN *Security Community*
ACCP	: ASEAN *Cyber Capacity Program*
AMCC	: *ASEAN Ministerial Conference on Cybersecurity*
ACCBP	: ASEAN *Cybersecurity Capacity Building Programme*
ARF	: ASEAN *Regional Forum*
AEC	: ASEAN *Economic Community*
ASCC	: ASEAN *Socio-Cultural Community*
ACCS	: ASEAN *Cybersecurity Cooperation Strategy*
APJII	: Asosiasi Penyelenggara Jasa Internet Indonesia
ACCWP	: ASEAN *Cybersecurity Cooperation Work Programme*
AMS	: ASEAN *Member States*
ANSAC	: *ASEAN Network Security Action Council*
ADGMIN	: ASEAN *Directors-General of Immigration Departments*
ATRC	: ASEAN *Telecommunications and Information Technology Senior Officials Meeting and Related Meetings*
ASCN	: ASEAN *Smart Cities Network*
AJCCBC	: ASEAN-Japan *Cybersecurity Capacity Building Centre*
ASCCE	: ASEAN-*Singapore Cybersecurity Centre of Excellence's*
BSSN	: Badan Siber Dan Sandi Nasional
BGP	: *Border Gateway Protocol*

RCE	: *Remote Code Execution*
CENS	: *Center of Excellence for National Security*
CERT	: *Computer Emergency Response Team*
CSA	: *Cyber Security Agency of Singapore*
CII	: *Critical Information Infrastructure*
DDOS	: *Distributed Denial of Service*
GDP	: *Gross domestic product*
ICT	: *Information and Communications Technology*
IoT	: *Internet of Things*
ID-SIRTII/CC	: *Indonesia Security Incident Response Team On Internet Infrastructure / Coordination Center*
ISIS	: *Islamic State of Iraq and Syria*
KPU	: Komisi Pemilihan Umum
Kemenkominfo	: Kementerian Komunikasi dan Informatika
KIC	: *Katadata Insight Center*
LAN	: *Local Area Network*
POC	: *Point of Contact*
Pusopskamsinas	: Pusat Operasi Keamanan Siber Nasional
RSIS	: *Rajaratnam School of International Studies*
RUU KKS	: Rancangan Undang Undang Ketahanan dan Keamanan Siber
SOMRI WG-IMT	: *Senior Officials Meeting on Drug Matters Working Group on Illicit Manufacturing and Trafficking of Drugs*
TELMIN	: *Telecommunication and IT Minister Meeting*
USB	: *Universal Serial Bus*
UNGGE	: UN *Group of Governmental Expert*
UNODA	: *United Nations Office for Disarmament Affairs*
UU PDP	: Undang Undang Perlindungan Data Pribadi

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat cepat dan pesat menciptakan beberapa keuntungan dan juga kerugian. Dimana keuntungan nya ialah semakin berkembangnya teknologi maka akan semakin berkembang juga taraf hidup manusia dikarenakan dengan adanya teknologi kehidupan manusia akan menjadi lebih mudah dan juga efektif. Internet merupakan sebuah bukti perkembangan teknologi yang sungguh cepat. Internet merupakan singkatan dari Interconnected Network yaitu sebuah jaringan atau sistem komunikasi yang menyambungkan beberapa perangkat komputer dari satu ke yang lainnya secara global.

Dengan adanya internet berhubungan dari satu perangkat ke perangkat lainnya sangat lah mudah, praktis, dan juga cepat. Namun dari semua kemudahan yang diberikan oleh internet, lahirlah juga kerugian yang dapat terjadi oleh oknum – oknum yang tidak bertanggung jawab memanfaatkan internet untuk melancarkan tindak kejahatan. Kejahatan siber atau biasa disebut sebagai *cybercrime* merupakan sebuah tindakan kejahatan yang dilakukan melalui media internet atau biasa disebut juga sebagai dunia maya atau *Cyberspace*. *Cyberspace* atau dunia maya merupakan sebuah media elektronik yang berada dalam jaringan komputer yang digunakan untuk alat komunikasi satu arah maupun dua arah secara timbal balik atau *online* (Techterms, 2022) Kejahatan siber dilakukan untuk mendapatkan keuntungan atau meneror masyarakat dengan skala yang luas, dikarenakan kejahatn siber dilakukan di ranah internet yang dapat bersambung ke banyak pengguna sekaligus.

Terdapat beberapa jenis kejahatan siber mulai yang tradisional hingga modern, beberapa diantaranya adalah; Pencurian data pribadi, Pemalsuan data,

Ujaran Kebencian, Penyebaran pornografi, Jual – beli barang terlarang, dan masih banyak lagi. Kejahatan siber yang terkenal pada saat ini yaitu pencurian data dimana pencurian tersebut dilakukan oleh oknum atau kelompok siber yang meliputi data pribadi hingga data rahasia negara. Kejahatan siber memiliki sejarah yang cukup panjang dimulai pada tahun 1970 dimana pada saat itu terdapat proyek penelitian yang bernama ARPANET (*The Advanced Research Projects Agency Network*). ARPANET merupakan sebuah jaringan komputer luas pertama dengan kontrol yang terdistribusi dan menggunakan paket protokol TCP/IP (Markoff, 1999). Lalu seorang peneliti yang bernama Bob Thomas membuat sebuah program bernama CREEPER dimana program tersebut dapat memindahkan jaringan APRANET dengan minim jejak dan dapat memperbanyak programnya sendiri dengan otomatis. Maka dari itu CREEPER disebut sebagai virus komputer pertama di dunia (Cakrawala, 2021). Dari sejak itu *cybercrime* telah berkembang sangat pesat seiring dengan perkembangan teknologi komputer juga. Bahkan pada tahun 2017 terdapat salah satu kasus *cybercrime* terbesar sepanjang sejarah yaitu virus *wannacry*. *Wannacry* merupakan sebuah virus *ransomware* yang disebarkan melalui email dan menginfeksi komputer pengguna dengan menahan seluruh file yang ada dan meminta uang tebusan untuk membukanya kembali. Virus *wannacry* telah menginfeksi setidaknya 300.000 komputer dan 150 negara (Krisnadi, 2021).

Cybercrime dapat mengancam keamanan negara hingga keamanan kelompok negara secara regional maupun global. Karena ruang lingkup *cybercrime* yaitu *cyberspace* dimana memiliki ruang lingkup yang luas dan terhubung kepada pengguna di seluruh penjuru dunia. Pelaku cybercrime dapat melakukan aksi kejahatan nya yang bermacam – macam. Yang dikhawatirkan kejahatan *cybercrime* tersebut dapat melumpuhkan keamanan negara secara fisik maupun konstitusi dan akan menghancurkan suatu bangsa dan negara secara perlahan maupun cepat. Sehingga *cybercrime* tidak bisa dipandang remeh dikarenakan jangkauan resiko yang sungguh luas dan juga berkembang sangat cepat seiring perkembangan zaman.

ASEAN (*Association of Southeast Asian Nations*) merupakan sebuah organisasi geopolitik dan ekonomi di wilayah regional Asia Tenggara. Terbentuknya organisasi ini untuk menciptakan kawasan Asia Tenggara yang

damai, tentram, stabil, dan juga sejahtera (Pamungkas, 2022). ASEAN juga berfungsi sebagai pembantu dan juga jembatan kepada negara – negara anggota di Asia Tenggara untuk saling membantu dan bekerja sama satu sama lain ataupun ke pihak luar. Sehingga ASEAN memiliki kebijakan – kebijakan sebagai upaya dalam memenuhi tujuannya yaitu untuk mensejahterakan negara – negara anggota di Asia Tenggara. Salah satu kebijakan nya yaitu APSC (ASEAN *Political Security Community*) yang merupakan sebuah komunitas keamanan politik dan keamanan di kawasan Asia Tenggara. Komunitas ini dibentuk oleh ASEAN sebagai bentuk upaya dalam mewujudkan perdamaian antara negara anggota di kawasan Asia Tenggara serta mencegah tindak kejahatan yang dapat mengancam negara anggota ASEAN. Bentuk ancaman tersebut dapat bermacam – macam yaitu; terorisme, konflik antar negara, ancaman dalam dan diluar kawasan Asia Tenggara. Ancaman keamanan pun dibagi menjadi dua yaitu Ancaman keamanan tradisional dan Non tradisional. Pada ancaman kejahatan keamanan tradisional meliputi konflik militer, pertahanan nasional – regional, senjata nuklir, keamanan maritim, dan lainnya yang mana mengancam pertahanan secara langsung. Adapun keamanan non tradisional tidak secara langsung menyerang pertahanan militer, namun pada non tradisional keamanan dijelaskan secara lebih kompleks dengan menyangkut hal – hal seperti hak manusia, keamanan lingkungan, keamanan siber dan yang lainnya. APSC merupakan sebuah akar dari semua kebijakan yang membahas tentang keamanan dan politik di kawasan. Keamanan siber merupakan salah satu isu keamanan non tradisional yang dibahas pada APSC. (ASEAN, ASEAN Community, 2022)

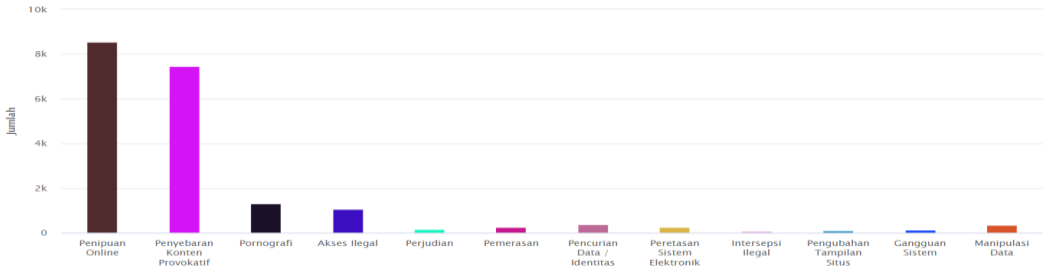
ASEAN dalam menanggapi isu keamanan siber yang merupakan bagian dari sektor keamanan ASEAN yaitu APSC menginisiasi sebuah kebijakan keamanan yang khusus menaungi di bidang siber yaitu ACCS (ASEAN *Cybersecurity Cooperation Strategy*). ACCS adalah salah satu strategi kebijakan keamanan yang berfokus pada keamanan siber yang dibentuk oleh ASEAN pada tahun 2010 dalam ASEAN Foreign Ministers' Meeting dengan 3 periode tahun yaitu 2011 – 2015, 2016 – 2020, dan 2021 - 20255. ACCS dibentuk dengan fokus cakupan diantaranya; kebijakan siber, undang undang yang mengatur tentang siber, pengembangan strategi, dan pembentukan tim respon insiden. Tujuannya yaitu meningkatkan kesadaran tentang tantangan keamanan siber, memanfaatkan kemampuan di antara

Negara Anggota ASEAN dan mitra eksternalnya, mengembangkan mekanisme dan solusi kooperatif secara terkoordinasi serta membangun kapasitas keamanan siber di negara – negara anggota ASEAN serta untuk meningkatkan pencegahan ancaman siber di daerah regional Asia Tenggara dan tentu saja membangun *cyberspace* atau duniamaya yang aman dan tangguh. Strategi ini melibatkan banyak pihak dari INTERPOL, akademisi dari institut *Center of Excellence for National Security* (CENS) di *S.Rajaratnam School of International Studies* (RSIS), *Cyber Security Agency of Singapore* (CSA) dan instansi terkait lainnya. ASEAN juga membagi beberapa badan sectoral khusus yang nantinya akan bertanggung jawab terhadap inisiasi program dari ACCS diantaranya ASEAN Digital Ministers' Meeting (ADGMIN), ASEAN Digital Senior Officials' Meeting (ADGSOM), ASEAN Regional Forum (ARF), ASEAN Ministerial Meeting on Transnational Crime (AMMTC), East Asia Summit (EAS), ASEAN Defence Ministers' Meeting (ADMM)-Plus, dan ASEAN Ministerial Meeting on Social Welfare and Development (AMMSWD). Pada ACCS sendiri berisi inisiasi dan program yang membahas tentang kerjasama dan peningkatan kapasitas keamanan siber di kawasan. (ASEAN, 2022) ASEAN *Cybersecurity Cooperation Strategy* (ACCS) yang dimana merupakan bagian kebijakan dari komunitas keamanan ASEAN yaitu ASEAN *Political Security Community* (APSC) berisi inisiasi – inisiasi yang bertujuan untuk meningkatkan keamanan siber yang disetujui dan disahkan oleh seluruh negara anggota ASEAN sehingga dapat diikuti dan diimplementasikan oleh semua negara anggota ASEAN dalam hal ini yaitu ASEAN Member States. Maka dari itu negara – negara anggota ASEAN dapat saling bekerja sama dan mengikuti program kerjasama yang terkoordinasi sehingga dapat menciptakan keamanan siber kawasan yang lebih baik.

Pada tahun 2019 hingga 2022, Indonesia mengalami banyak sekali serangan siber yang bermacam – macam. Mulai dari hacking, scamming, manipulasi data, pencurian data, pornografi, phishing, dan lain lain. Tahun 2019 – 2022 merupakan tahun yang sangat berat bagi keamanan siber di Indonesia, dikarenakan banyak sekali serangan siber yang diterima. Serangan siber tersebut disebabkan oleh aktivitas pengguna yang sangat banyak sejak awal pandemi Covid-19 sehingga membuka lahan untuk melancarkan *cybercrime* bagi *hacker*. Berdasarkan data

laporan data anomali trafik BSSN (2022), sepanjang tahun 2020, Indonesia mengalami serangan siber mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta.

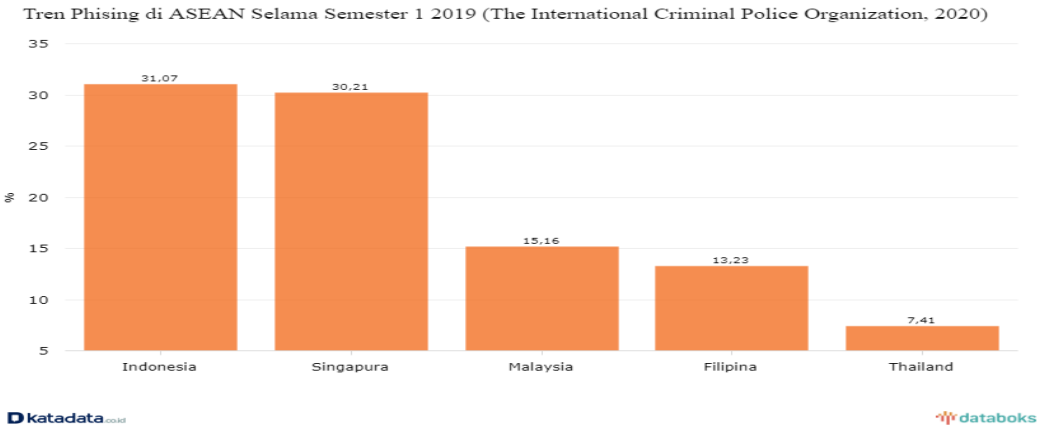
Gambar 1.1 Data jumlah dari setiap Kasus Kejahatan Siber tahun 2020



Sumber: (Patrolisiber, 2020)

Pada gambar 1.1 dijelaskan berapa jumlah kejahatan siber sepanjang tahun 2020 dikategorikan dari jenis – jenis kejahatan sibernya. Dapat dilihat bahwa Indonesia mengalami kejahatan siber jenis penipuan *online* atau biasa disebut sebagai *scamming* sebanyak 8.541 kasus yang merupakan tertinggi dibandingkan jenis kejahatan siber lainnya. Penipuan online yang dimaksud adalah transaksi yang dilakukan melalui basis dunia maya yang biasanya melalui *e-commerce* atau tidak melalui transaksi secara langsung. Seluruh kasus kejahatan siber yang terjadi tersebut, terhitung negara memiliki kerugian sebesar Rp. 5,05 Trilliun.

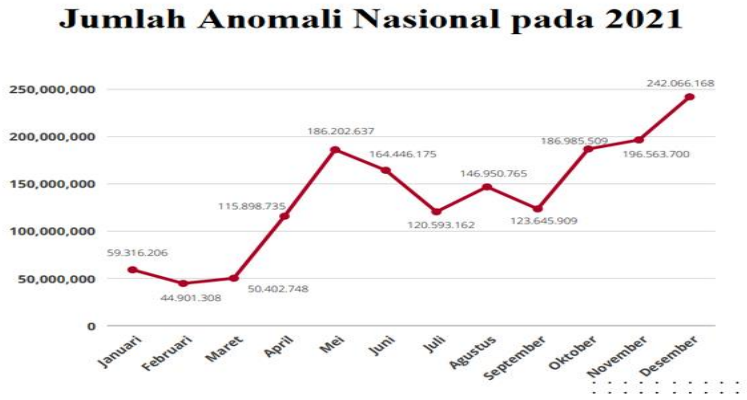
Gambar 1.2 Data Tren Phising di ASEAN Selama Semester 1 2019



Sumber: (Annur, Kataata, 2020)

Selanjutnya pada gambar 1.2, berdasarkan Laporan *The International Criminal Police Organization* (Interpol) 2020 menjelaskan bahwa Asia Tenggara merupakan region yang termasuk sasaran para penjahat siber dan Indonesia merupakan negara dengan target serangan siber (*Phishing*) tertinggi di ASEAN dengan persentase 31,07%. Maka dari itu tahun 2020 merupakan tahun dengan serangan siber terbanyak sepanjang sejarah Indonesia. Menurut BSSN, semua serangan siber di Indonesia disebabkan oleh masa pandemi yang menyebabkan penggunaan Internet atau dunia maya semakin meningkat serta Indonesia pun memiliki keterbatasan perundang – undangan kebijakan siber.

Gambar 1.3 Data Jumlah Anomali Nasional Sepanjang 2021



Sumber: Laporan tahunan "Monitoring Keamanan Siber" BSSN 2021

Sumber: (BSSN, BSSN, 2022)

Terakhir pada gambar 1,3, berdasarkan data jumlah anomali laporan tahunan yang dilaporkan oleh BSSN pada tahun 2021 menunjukan bahwa terjadi anomali trafik atau sebuah keadaan siber yang tidak normal yang mengalami serangan siber sebanyak 1,6 miliar lebih atau lebih tepatnya 1,637,973,022 serangan siber atau cybercrime. Terbanyak pada bulan desember yaitu sebesar 242 juta anomali. Angka yang sungguh fantastis dibandingkan pada tahun 2019 yang menerima serangan siber dengan jumlah sebesar 290 juta kasus *cybercrime*. Yang terbaru dan sedang hangat diperbicangkan yaitu seorang *hacker* atau peretas dengan kode nama *"Bjorka"* melakukan serangan siber besar – besaran ke Indonesia pada bulan agustus – september 2022. Setidaknya Bjorka telah meretas dan mengantongi data

pengguna Indihome, KPU, Kartu SIM, hingga surat rahasia presiden (Hardiansyah, 2022).

Jika kita lihat pada tahun sebelumnya jumlah kasus kejahatan siber yang terjadi di Indonesia tidak seburuk yang terjadi pada tahun 2019 – 2022. lebih tepatnya pada tahun 2020 dimana Indonesia menempati urutan ke 1 negara dengan serangan siber terbanyak di Asia Tenggara. Berdasarkan sumber – sumber media terpercaya di Indonesia bahwa pada dua tahun kebelakang yaitu 2017 dan 2018 serangan siber di Indonesia terklaim cukup tinggi di angka 205 juta (Damar, 2017) dan 225 juta (CNN, 2019) namun tidak ada kenaikan yang secara signifikan melambung tinggi. Pada tahun 2019 – 2022 barulah terjadi peningkatan angka yang sangat drastis hingga lebih dari 100% yang dimana secara bersamaan Indonesia mengalami pandemi Covid-19 menyebabkan masyarakat lebih banyak melakukan aktivitas secara WFH dengan media Internet. Jika divisualisasi data angka tersebut dalam info grafik, seperti berikut;

Gambar 1.4 Grafik Jumlah Kejahatan Siber Dari Tahun 2017 - 2022

Berdasarkan data – data yang telah dijabarkan diatas, bahwa Indonesia pada tahun 2019 - 2022 tidak sedang baik – baik saja. *Cyber security* 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 BSSN pada tahun 2017 yang merupakan lembaga pemerintah di Indonesia yang bertanggung jawab atas pengelolaan keamanan siber dan sandi (BSSN, Indonesia Cybersecurity Monitoring Report, 2019). negara Indonesia merupakan salah satu negara anggota dari ASEAN yang disebut ASEAN member state dan juga anggota komunitas keamanan ASEAN yaitu APSC. Dari kebijakan dilakukan Indonesia penulis tertarik untuk menganalisis pada keterkaitannya dengan kebijakan siber ASEAN yaitu ASEAN *Cybersecurity Cooperation Strategy* (ACCS).

ASEAN sebagai organisasi regional Asia Tenggara yang telah memiliki kebijakan keamanan siber yaitu salah satunya ASEAN *Cybersecurity Cooperation Strategy* (ACCS) dimana berisi strategi dan program dengan tujuannya yaitu untuk meningkatkan kapasitas keamanan siber di negara – negara anggotanya serta kawasan. Indonesia yang merupakan salah satu negara anggota ASEAN dan anggota komunitas keamanan APSC yang dimana merupakan negara dengan target serangan siber no. 2 pada tahun 2020 di Asia Tenggara (CNN I. , 2020). Pada tahun 2022 pun Indonesia meraih urutan pertama dengan ancaman siber terbesar di Asia Tenggara menyusul Vietnam yang awalnya peringkat 1 pada tahun 2020 (CNN, Ancaman Siber di RI Naik 22 Persen, Tertinggi di Asia Tenggara, 2022). sangat penting untuk melihat bagaimana keterkaitan Indonesia dengan kebijakan siber miliknya dengan ASEAN *Cybersecurity Cooperation Strategy* (ACCS) dalam penerapan kebijakan siber di Indonesia pada tahun 2019 - 2022. Dalam penelitian ini akan menganalisis keterkaitan kebijakan siber Indonesia dengan menggunakan teori liberal institusionalisme dan konsep keamanan, cyber security, regional organization dengan ASEAN *Cybersecurity Cooperation Strategy* (ACCS) yang merupakan kebijakan siber ASEAN bagian dari komunitas keamanan APSC dalam pada rentan tahun 2019 – 2022.

1.2 Rumusan Masalah

ASEAN dengan rangkaian kebijakan keamanan siber yang dimiliki yang melibatkan banyak sekali pihak, dinilai sangat baik untuk menciptakan keamanan

dan ketentraman keamanan siber di area Asia Tenggara. Dibalik hal tersebut terdapat beberapa negara anggota ASEAN yang mengalami serangan siber yang sungguh besar, terutama Indonesia sebagai target serangan siber no. 1 di Asia Tenggara pada tahun 2020. Sehingga kebijakan siber yang telah diciptakan oleh ASEAN yaitu ACCS atau ASEAN *Cybersecurity Cooperation Strategy* apakah dapat berpengaruh kepada kebijakan siber Indonesia tahun 2019 – 2022. Atas pertimbangan tersebut, penelitian ini memunculkan rumusan masalah:

"Bagaimana kebijakan siber Indonesia terkait ASEAN Cybersecurity Cooperation Strategy (ACCS) diimplementasikan pada periode tahun 2019-2022?"

1.3 Tujuan Penelitian

1. Mendeskripsikan kasus kejahatan siber yang terjadi di Indonesia dari 2019 – 2022.
2. Mendeskripsikan strategi pertahanan dan kebijakan mengenai keamanan siber di ASEAN.
3. Mendeskripsikan hasil Analisis kebijakan siber Indonesia terkait dengan ACCS yang diimplementasikan pada tahun 2019 – 2022.

1.4 Manfaat Penelitian

Adapun hasil dalam penelitian ini diharapkan memiliki manfaat bagi:

1) Teoritis

   Secara teoritis diharapkan penelitian ini dapat menghimpun informasi faktual dan sebagai penambahan pengetahuan studi mengenai analisis keamanan siber atau kebijakan keamanan ASEAN.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Penelitian terdahulu merupakan salah satu sumber penting dalam menganalisa suatu penelitian. Dikarenakan kita dapat melihat bagaimana peneliti – peneliti lain menganalisa sebuah subjek penelitian yang sama dengan kaca mata dan landasan teori yang berbeda – beda. Dalam hal ini subjek penelitian terdahulu yang dapat membantu penulis dalam menganalisa yaitu *Cyber Security* dan *Regional Organization* sehingga dapat memperluas serta mempertajam subjek analisa yang akan dianalisis oleh penulis. Berikut merupakan beberapa jurnal penelitian terdahulu yang memiliki kesamaan topik subjek penelitian dengan topik yang hendak dibahas oleh penulis.

Jurnal terdahulu yang penulis bahas yaitu skripsi dari mahasiswa hubungan internasional Universitas Sriwijaya yang bernama M Firly Fadilla yang berjudul Upaya Asean Dalam Meningkatkan *Cyber Security* Di Kawasan Asia Tenggara Melalui *Asean Regional Forum On Cyber security Initiatives*. Penelitian ini berfokus pada apa saja upaya ASEAN dalam peningkatan keamanan siber di Asia Tenggara. Mengingat bahwa ancaman siber terus meningkat dan melintasi belahan dunia yang tidak bisa dihindarkan. ASEAN melalui *ARF on Cybersecurity Initiative* berupaya meningkatkan keamanan siber di kawasan Asia Tenggara. Penelitian ini juga berfokus terhadap hasil peningkatan keamanan siber dari upaya – upaya yang dilakukan oleh ASEAN. Penelitian ini menggunakan teori Liberalis Institusional untuk melihat bagaimana peran organisasi atau institusi internasional sebagai aktor internasional yang berperan aktif dalam sistem internasional. Penelitian ini dilakukan berdasarkan peningkatan ancaman kejahatan siber yang meluas ke seluruh dunia. Dengan begitu penulis ingin menganalisa bagaimana upaya ASEAN sebagai institusi internasional daerah Asia Tenggara dalam meningkatkan

keamanan siber untuk mengatasi serta mencegah ancaman kejahatan siber yang dapat mengancam kedaulatan negara anggota ASEAN. Didalam penelitian ini juga memaparkan beberapa hasil dari hasil dari upaya peningkatan keamanan siber ASEAN melalui *ARF on Cybersecurity Initiatives* melalui tiga indikator liberalisme institusional yaitu menyediakan informasi dan kesempatan bernegosiasi, meningkatkan kemampuan untuk membuat kesepakatan dengan lebih dipercaya, dan juga meningkatkan kesolidan dari kesepakatan internasional. Dengan upaya – upaya tersebut menghasilkan peningkatan keamanan siber melalui peningkatan di global cybersecurity index tahun 2012 (Fadilla, 2021).

Selanjutnya terdapat jurnal penelitian yang ditulis oleh Adi Rio Arianto dan Gesti Anggraini dari Jurnal Pertahanan & Bela Negara berjudul Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui *Indonesia Security Incident Response Team On Internet Infrastructure* (ID-SIRTII). Jurnal ini merupakan penelitian kualitatif yang berfokus pada implementasi *Indonesia Security Incident Response Team On Internet Infrastructure* atau bisa disebut dengan (ID-SIRTII) sebagai bentuk langkah taktis yang dapat mewujudkan stabilitas informasi, perlindungan siber, dan segala bentuk ancamannya. Penelitian ini dilatarbelakangi Indonesia yang menjadi target kejahatan siber no 1 mengganti Tiongkok. Hal tersebut dianggap sebagai ancaman keamanan bagi pemerintah Indonesia sehingga harus membuat kebijakan yang dimana dapat mencegah sekaligus melindungi keamanan negara di ranah siber. Sebagai bentuk langkah taktis dari pemerintah Indonesia dalam melindungi keamanan sipil sekaligus militer dari kejahatan siber, pemerintah Indonesia akhirnya membentuk *Indonesia Security Incident Response Team On Internet Infrastructure* atau bisa disebut dengan (ID-SIRTII). Pada penelitian ini dibahas bahwa ancaman kejahatan siber di Indonesia sangatlah kompleks, terdapat 4 langkah bagaimana ID-SIRTII dapat beroperasi dengan baik yaitu; 1. Perlindungan segala aktivitas sipil di dunia maya, 2. ID-SIRTII harus terintegrasi dengan peran strategis institusi siber nasional, 3. ID-SIRTII perlu terintegrasi dengan institusi siber regional dan global, 4. Membentuk angkatan yang berfokus pada siber di militer yaitu angkatan darat, udara, dan air. Jika keempat langkah tersebut terpenuhi

penelitian ini dapat menyimpulkan bahwa dengan ID-SIRTII keamanan siber di Indonesia dapat meningkat jauh lebih baik dan efektif (Adi Rio Arianto, 2019).

Kemudian, jurnal penelitian yang berjudul *Cyber-Security* Dan Tantangan Pengembangannya Di Indonesia, ditulis oleh Handrini Ardiyanti dari Badan Riset Inovasi Nasional. Penelitian ini merupakan penelitian kualitatif yang berfokus pada bagaimana pemerintah indonesia menjalankan kebijakan keamanan siber dan bagaimana prospeknya. Penelitian ini dilatar belakangi oleh keadaan *cyber security* di indonesia yang sudah di tahap memprihatinkan, sehingga Indonesia perlu kebijakan keamanan siber yang komprehensif. Penelitian ini memaparkan bahwa Indonesia telah menjalankan kebijakan siber sejak tahun 2007 dimana dengan membentuk ID-SIRTII atau *Indonesia Security Incident Response Team on Internet Infrastructure* yaitu tim yang membantu Kementerian Komunikasi dan Informasi dalam menangani kasus kejahatan siber. Indonesia juga memiliki kerangka hukum yang mengatur kejahatan siber diantaranya UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Namun, agar kebijakan siber di indonesia dapat berjalan lebih efektif dan komprehensif peneliti menyarankan ke depan hendaknya dibangun atas lima bidang dasar yaitu adanya kepastian hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* & pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman siber) (Ardiyanti, 2016).

Tidak hanya jurnal penelitian atau tugas akhir lokal saja, selanjutnya terdapat juga jurnal penelitian internasional yang ditulis oleh Rudy Agus Gemilang Gultom, Asep Adang Supriyadi, dan Tatan Kustana yang berjudul *Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework*. Penelitian ini merupakan penelitian kualitatif yang berfokus pada kerjasama ASEAN dalam

penanganan kelompok siber teroris di Asia Tenggara. Penelitian ini dilatarbelakangi banyaknya kelompok radikalisme, ekstremisme, dan terorisme yang sudah memanfaatkan akses internet sebagai media dalam melancarkan aksi kejahatan seperti propaganda, serangan siber, dan yang lainnya. Hal tersebut merupakan suatu masalah yang dapat mengancam keamanan siber terutama di daerah Asia Tenggara. Penelitian ini menganalisa suatu kejahatan siber dimana sebuah organisasi terorisme yaitu ISIS yang melakukan kampanye bernama *One Billion Campaign*. Dimana kampanye tersebut mengajak masyarakat dalam berkontribusi menyumbang dalam rangka mendukung saudara dan saudari muslim. Penelitian ini juga memaparkan studi kasus sebuah kerangka kerja keamanan siber di Amerika Serikat yaitu *The NIST Cyber Security Framework* yang dibentuk tahun 2014 yang berisikan sebuah kebijakan untuk meningkatkan keamanan siber dengan strategi *Identify, Protect, Detect, Respond, dan Recover*. Kerangka kerja tersebut sangat efektif dalam meningkatkan keamanan siber di Amerika Serikat. Pada penelitian ini memaparkan dan menyimpulkan bahwa *The Six-ware Cyber Security Framework* akan sangat efektif diimplementasikan untuk negara – negara ASEAN mengingat bahwa ancaman kejahatan siber di wilayah Asia Tenggara sangat tinggi dan juga mayoritas negara – negara anggota ASEAN merupakan negara berkembang (Rudy Agus Gemilang Gultom, 2018).

Selanjutnya, jurnal internasional yang ditulis oleh Khanisa yang berjudul *A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation.* Jurnal internasional ini merupakan penelitian kualitatif yang berfokus pada kebijakan keamanan siber ASEAN pada tahun 2015. Dilatar belakangi persiapan keamanan siber ASEAN dalam menghadapi tahun 2015 dengan kerangka kerjasama yang baru. Penelitian ini berusaha melihat bagaimana kerangka kerja yang disusun dalam kebijakan kerjasama untuk meningkatkan keamanan siber di antara negara – negara anggota ASEAN. Penelitian ini memaparkan bahwa visi ASEAN dalam menciptakan Asia Tenggara sebagai region yang terkoneksi di dalam *ICT Infrastructure* tersebut sangat baik dalam mengembangkan negara – negara anggota ASEAN dalam hal ekonomi dan hubungan sosial. Dijelaskan juga bahwa rata – rata negara anggota ASEAN telah memiliki CERT team yang dapat berkembang dengan adanya kerangka kerjasama tersebut dan meningkatkan

keamanan siber di lingkup *cyberspace* Asia Tenggara. Namun yang dikhawatirkan yaitu masalah dalam membuat perjanjian kerjasama internasional mengenai meningkatkan keamanan siber, dikarenakan bahwa isu kejahatan siber bukan salah satu isu penting atau yang di prioritaskan (Krisman, 2013).

Terakhir, jurnal internasional yang ditulis oleh Nor Shazwina Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar, dan Siti Mariam Shahar yang berjudul *CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries*. Jurnal ini menggunakan metode penelitian kualitatif dengan fokus penelitian pada mengulas penelitian – penelitian terdahulu yang mengambil topik pada keamanan siber di ASEAN pada tahun 2014 – 2019. Dilatar belakangi dari keamanan siber yang belakangan ini merupakan sebuah isu keamanan kritis secara global. Penelitian ini berusaha melihat bagaimana masalah keamanan siber di negara – negara anggota ASEAN dan bagaimana langkah – langkah ASEAN dalam menangani masalah – masalah siber tersebut melalui penelitian – penelitian terdahulu. Penelitian ini menyajikan hasil dari penelitian – penelitian tersebut dan menyimpulkan bahwa untuk menghadapi masalah dan ancaman keamanan siber di Asia Tenggara, ASEAN perlu kerjasama penuh dari seluruh anggotanya dan memperluas kerjasama tersebut ke pihak negeri dan swasta sekalipun. Keamanan siber di ASEAN juga perlu lebih ditingkatkan mengingat ancaman kejahatan siber di cyberspace yang terus meningkat dengan pesat (Nor Shazwina Mohamed Mizan, 2019).

Tabel 2.1 Rangkuman Penelitian Terdahulu

Nama Penulis	Judul Penelitian	Metode Penelitian	Konsep dan Teori	Fokus Penelitian	Perbedaan Penelitian
M Firly Fadilla, Universitas Sriwijaya, 2021.	Upaya Asean Dalam Meningkatkan *Cyber Security* Di Kawasan Asia Tenggara Melalui *Asean Regional Forum On Cybersecu*	Pendekatan Kualitatif: Uji korelasi	*Cyber security Initiatives*, Teori Liberalis Institute	Upaya ASEAN dalam meningkatkan keamanan siber di Asia Tenggara melalui ARF atau biasa disebut sebagai *ASEAN Regional Forum on cyber security initiatives*	Penelitian menganalisis peran ASEAN dalam peningkatan keamanan siber pada *ARF on cyber security initiatives* yang menghasilkan peningkatan di global *cyber security* index tahun 2012

Nama Penulis	Judul Penelitian	Metode Penelitian	Konsep dan Teori	Fokus Penelitian	Perbedaan Penelitian
	rity Initiatives				
Adi Rio Arianto, Gesti Anggraini, Jurnal Pertahanan & Bela Negara, 2019.	Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui *Indonesia Security Incident Response Team On Internet Infrastructure* (ID-SIRTII)	Pendekatan Kualitatif: analisis studi Perbandingan	Teori Fungsionalisme dan Geometrik	implementasi *Indonesia Security Incident Response Team On Internet Infrastructure* atau bisa disebut dengan (ID-SIRTII) sebagai bentuk langkah taktis yang dapat mewujudkan stabilitas informasi, perlindungan siber, dan segala bentuk ancamannya	Penelitian ini menganalisis seberapa efektif implementasi ID-SIRTII sebagai kebijakan keamanan siber di Indonesia dan memberikan saran berdasarkan analisis tersebut.
Handrini Ardiyanti, Badan Riset Inovasi Nasional, 2014.	*Cyber-Security* Dan Tantangan Pengembangannya Di Indonesia	Pendekatan Kualitatif: Studi literatur dan uji relevansi	*Cyber security, capacity building*, dan Hukum Pidana	Penelitian tersebut berfokus pada bagaimana persiapan kebijakan keamanan siber di Indonesia dan prospek perkembangannya.	Penelitian tersebut memaparkan pemetaan bagaimana landasan kebijakan keamanan siber di Indonesia secara hukum dan kebijakan konstitusi serta memberikan rekomendasi untuk perkembangan keamanan siber dengan berlandaskan empat pondasi utama yaitu; perkembangan perangkat lunak (*software*) seperti sistem dan aplikasi dan perkembangan alat keras (*hardware*) perkembangan

Nama Penulis	Judul Penelitian	Metode Penelitian	Konsep dan Teori	Fokus Penelitian	Perbedaan Penelitian
					sarana dan prasarana teknologi informasi, manajemen isi *(content management), telecommunication and networking*, perkembangan internet serta perdagangan online atau melalui internet
Rudy Agus Gemilang Gultom, Asep Adang Supriyadi, Tatan Kustana, International Journal Of Management And Information Technology, 2018	*Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework*	Pendekatan Kualitatif : analisis studi Perbandingan dan uji korelasi	*Cyber Security Framework*, Perbandingan Politik.	Analisa upaya kerjasama ASEAN dalam penanganan kelompok siber teroris di Asia Tenggara dengan studi kasus perbandingan *The NIST Cyber Security Framework*	Penelitian ini berfokus pada usulan kepada ASEAN untuk mempertimbangkan *Cyber Security Framework* terhadap kebijakan keamanan siber ASEAN dalam peningkatan keamanan siber dengan perbandingan *The NIST Cyber Security Framework* yang merupakan kerangka kerja keamanan siber di Amerika Serikat.
Khanisa, Journal of ASEAN Studies, 2012.	*A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation*	Pendekatan Kualitatif : analisis studi literatur dan uji korelasi	Kerjasama Internasional, *Cyber, regional dan international organizat*ion	kebijakan keamanan siber ASEAN dalam menghadapi tahun 2015 dengan kerangka kerjasama yang baru	Penelitian ini berfokus pada analisis bentuk kerjasama ASEAN di dalam ICT Infrastructure apakah kerangka kerjasama tersebut dapat efektif meningkatkan keamanan siber di ASEAN mengingat

Nama Penulis	Judul Penelitian	Metode Penelitian	Konsep dan Teori	Fokus Penelitian	Perbedaan Penelitian
					bahwa isu tersebut dianggap bukan merupakan isu yang darurat maupun penting
Nor Shazwina Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar, dan Siti Mariam Shahar, International Journal of Advanced Trends in Computer Science and Engineering, 2019.	*CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries*	Pendekatan Kualitatif : analisis studi literatur	Kerjasama Internasional, *Cyber security*, dan *regional organization*	Penelitian – penelitian terdahulu yang membahas tentang keamanan siber di ASEAN pada tahun 2014 - 2019	Penelitian ini berusaha melihat bagaimana masalah keamanan siber di negara – negara anggota ASEAN dan bagaimana langkah – langkah ASEAN dalam menangani masalah – masalah siber tersebut melalui penelitian – penelitian terdahulu

Berdasarkan enam penelitian diatas terdapat beberapa kesamaan yang dapat dilihat, yaitu fokus isu dan latar tempat yang digunakan yaitu Keamanan siber atau *Cyber Security* dan juga Asia Tenggara. Beberapa penelitian diatas juga menggunakan aktor yang sama yaitu ASEAN dan Indonesia. Penelitian ini ditulis untuk memperbarui penelitian – penelitian yang telah ada dengan mengangkat fokus isu penelitian yang berbeda yaitu Analisis Kebijakan Keamanan Siber Indonesia terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS) Pada Kasus – Kasus Kejahatan Siber Di Indonesia.

2.2 Landasan Konseptual

2.2.1 *Cyber Security*

Cyber Security atau keamanan siber merupakan sebuah sistem keamanan yang melindungi jaringan atau sistem komputer dari kejahatan siber seperti virus, pencurian, peretasan dan yang lainnya. Mengamankan sebuah jaringan atau sistem

komputer merupakan sesuatu yang sangat vital dan penting, dikarenakan dengan mengamankan hal tersebut berarti mengamankan informasi penting dan rahasia yang dimiliki pengguna (Schatz & Bashroush, 2017). Menurut Barry Buzan yang merupakan salah satu ilmuwan HI yang mengemumkakan konsep keamanan. Beliau memperluas makna konsep keamanan menjadi dua yaitu keamanan tradisional dan non tradisional. Dimana keamanan non tradisional merupakan suatu situasi yang terbebas dari ancaman dan tantangan keamanan yang tidak hanya berasal dari konflik militer atau serangan langsung oleh negara-negara. Sehingga keamanan siber atau *Cyber Security* termasuk dalam keamanan non tradisional yang tidak secara langsung berasal dari konflik militer namun dapat mengancam keamanan individual maupun kelompok seperti aktor negara dan juga organisasi internasional (Buzan, Wæver, & Wilde, 1998).

Terdapat beberapa jenis aspek keamanan pada jaringan ataupun sistem komputer yang termasuk dalam *Cyber Security*, diantaranya sebagai berikut:

1. Kerahasiaan Data

   Dimaksudkan disini yaitu menjaga serta melindungi kerahasiaan informasi atau data yang ada pada suatu jaringan maupun sistem komputer. Sebagai contoh; Kata sandi, Data pribadi, dan yang lainnya
2. Verifikasi Data

   yaitu proses perlindungan data dengan cara verifikasi data untuk memastikan bahwa pengguna merupakan individu yang memiliki hak akses sah dan bukan robot atau yang lainnya.
3. Integritas

   Dimaksudkan disini yaitu sistem integritas yang melindungi data dari proses manipulasi, perubahan, penyisipan, pencurian, dan penghapusan yang dilakukan oleh pihak tidak dikenal dan tidak bertanggung jawab yang dapat merugikan pengguna

Dan masih ada aspek keamanan lainnya yang perlu disusun dan dibentuk dengan matang pada sistem keamanan siber atau *cyber security*. *cyber security* juga merupakan sistem keamanan yang melindungi banyak sekali jenis perangkat mulai dari komputer, ponsel, server, sistem elektronik hingga database. Sistem keamanan

tersebut dibagi menjadi beberapa kategori dimana mengklasifikasi jenis – jenis sistem keamanan komputer yang dibutuhkan, yaitu sebagai berikut:

1. Keamanan Perangkat Lunak

   Sebuah perangkat lunak atau biasa disebut sebagai *software* yang dibuat dengan memiliki satu tujuan yaitu melindungi sistem komputer dari serangan virus, retasan, pencurian dan yang lainnya. Sebagai contoh; *Antivirus, Firewall, Access Contro*l, dan yang lainnya.

2. Keamanan Jaringan

   Sistem keamanan yang bekerja untuk melindungi sebuah jaringan yang biasanya berada di *cyberspace* atau dunia maya menggunakan sarana internet, untuk melindungi dari serangan *breacher*, *malware*, dan yang lainnya.

3. Keamanan Informasi

   Susunan kebijakan keamanan yang melindungi data dan informasi privasi pengguna baik dalam saat digunakan, penyimpanan, dan perjalanan.

4. Keamanan Sistem Operasi

   Merupakan sebuah keamanan pada sebuah sistem operasi yang dijalani pada sebuah perangkat keras. Artinya sebuah sistem operasi harus memiliki sistem keamanan yang melindungi perangkat keras dalam menjalani program tersebut. sebagai contoh sistem operasi *Windows* dengan *Windows defender* sebagai sistem keamanan.

5. Mekanisme Keamanan *Hardware*

   Pada kategori ini terdapat beberapa perlindungan yang harus dilakukan untuk melindungi sebuah perangkat keras dari serangan fisik secara langsung seperti; USB *dongles* yaitu virus yang disalurkan melalui koneksi fisik USB atau *Mobile-enabled access devices* sebuah alat yang dapat mengoperasikan sebuah perangkat keras dari jauh dengan hanya menancapkannya saja.

6. Edukasi keamanan pengguna

   Yang terakhir yaitu edukasi tentang keamanan siber pada pengguna jaringan ataupun komputer. Dengan mengajarkan tentang beberapa virus berbahaya atau metode *hacking* dan *phising* yang beredar dapat mencegah kejahatan siber terjadi.

Tentu saja dari kategori – kategori tersebut terdapat ancaman – ancaman yang ada. Ancaman tersebut dinamai sebagai *Cybercrime* atau kejahatan siber yang dilakukan oleh pihak atau kelompok tidak bertanggung jawab dengan tujuan keuntungan pribadi atau hanya sekedar merugikan sebuah pihak. Ancaman tersebut dapat mempengaruhi dari yang paling kecil yaitu pengguna individu hingga keamanan negara sekaligus. Maka dari itu negara harus memiliki sebuah kebijakan keamanan siber yang melindungi dari ancaman *Cybercrime. Cyber security* juga harus memiliki susunan kebijakan dan hukum yang dibentuk oleh regulasi negara, organisasi regional, dan internasional. Karena pemerintah memiliki peran yang sangat penting untuk melindungi dari serangan - serangan *cybercrime* yang ada demi menjaga keamanan konstitusi negaranya.

Konsep ini dapat melihat bagaimana negara dapat mempersiapkan dirinya dalam mengembangkan keamanan siber untuk melindungi dirinya, dan bagaimana mengatur prilaku warga negara dalam menggunakan teknologi internet dalam negaranya. Dikarenakan *cyberspace* atau ruang dunia maya merupakan ruang terbuka dalam memproses informasi – informasi. Setiap negara harus memiliki strategi dan juga kebijakan dalam meningkatkan pertahanan dalam melindungi ICT atau *information and communications technology* sebagaimana merupakan infrastruktur yang melindungi database informasi disebuah negara.

Konsep *cyber security* yang digunakan pada penelitian ini akan membantu penulis dalam menjawab pertanyaan penelitian. Konsep ini dapat digunakan sebagai pandangan dalam melihat bagaimana kejahatan siber dapat mempengaruhi kebijakan keamanan siber di Indonesia, terutama dalam kaitannya dengan implementasi ASEAN Cybersecurity Cooperation Strategy (ACCS). Serta mengklasifikasikan dari kebijakan keamanan yang dibuat oleh Indonesia dan ASEAN, dimana dari sekian banyak kebijakan keamanan penulis dapat memilah satu persatu di antara kebijakan keamanan dimana yang berfokus dalam meningkatkan keamanan siber. Sehingga dapat dianalisis keterkaitan antara kebijakan keamanan siber Indonesia dengan ACCS atau ASEAN *Cybersecurity Cooperation Strategy.*

2.2.2 Liberal institusionalisme

Teori atau pendekatan liberal institusionalisme merupakan salah satu pendekatan utama dalam teori hubungan internasional yang menekankan peran institusi internasional, aturan, norma, dan kerjasama antar aktor negara dalam membentuk perilaku dan interaksi internasional. Teori ini menganggap bahwa institusi internasional / regional seperti PBB / ASEAN memainkan peran penting dalam memfasilitasi kerjasama antarnegara anggota. Institusi dapat menyediakan forum di mana negara-negara dapat berkomunikasi, bernegosiasi, dan mengembangkan aturan bersama. Liberal institusionalisme menekankan pentingnya norma dan aturan internasional dalam membentuk perilaku negara-negara. Institusi internasional berperan sebagai mediator atau perantara terhadap aktor - aktor dalam menjalankan kerjasama pada sistem internasional agar sesuai dan dapat mencapai tujuan bersama. Oleh karena itu institusi internasional merupakan hal penting dalam mencapai sistem internasional yang baik dan saling menguntungkan antara aktor – aktor internasional (Keohane, 1989).

Teori liberal institusionalisme sendiri dicetuskan oleh dua pemikir hubungan internasional yaitu Robert O Keohane dan Joseph Nye pada tahun 1970. Robert Keohane berpendapat bahwa teori ini muncul sebagai upaya untuk mendorong negara untuk bekerja sama, meningkatkan stabilitas keamanan, dan mengelola institusi internasional. Joseph Nye mengembangkan konsep soft power dan berkontribusi pada pemahaman tentang bagaimana aturan dan norma internasional mempengaruhi hubungan internasional (Nye, 2004). Dia juga berbicara tentang pentingnya peran institusi internasional dalam memoderasi perilaku negara-negara. Teori liberal instusionalisme memiliki asumsi enam asumsi dasar. Pertama adalah gagasan bahwa negara adalah aktor paling penting dalam hubungan internasional. Kedua adalah gagasan bahwa negara dianggap sebagai aktor rasional dalam hubungan internasional. Ketiga, masalah aksi bersama adalah masalah yang sering muncul dalam politik internasional (collective action problem). Keempat, struktur kepentingan negara menentukan politik internasional. Kelima, struktur anarki sistem internasional mempengaruhi politik internasional.

Keenam, struktur kepentingan negara dapat berdampak dari beberapa faktor, diantaranya; jumlah aktor, institusi internasional dan tingkat ketergantungan.

Robert Keohane menjelaskan institusi internasional dengan lebih spesifik yaitu Institusi Internasional atau organisasi internasional sebagai seperangkat aturan atau rezim (formal dan informal) yang saling berhubungan dan dapat menjelaskan pola tingkah laku suatu negara, aktivitas yang memaksa, dan bentuk – bentuk harapan. Institusi internasional diartikan menjadi tiga bentuk yaitu (Keohane, 1989):

1. Organisasi formal yang bentuk antara pemerintah negara ataupun negara non pemerintah sebagai organisasi yang memiliki tujuan khusus dan bersama. Organisasi yang dapat mengawasi aktivitas dan memberikan respon terhadap aktivitas tertentu. Organisasi ini biasanya dibentuk oleh negara – negara yang memiliki tujuan bersama, dan tidak memiliki intensi untuk menyerang satu sama lain.
2. Institusi bisa disebut juga dengan rezim karena memiliki peraturan eksplisit yang disetujui oleh negara – negara anggota institusi tersebut. Peraturan tersebut dibentuk dari beberapa isu – isu hubungan internasional.
3. Dalam teori sosial dan filosofi, konvensi didefinisikan sebagai institusi informal yang memiliki peraturan dan pemahaman yang implisit yang menentukan harapan para aktor. Tidak ada aturan yang jelas yang mengatur bagaimana aktor berinteraksi satu sama lain, jadi konvensi memungkinkan aktor berinteraksi satu sama lain. Sebagai contoh, prinsip kekebalan (imunitas) dalam diplomasi konvensional sudah ada sebelum ditetapkan dalam dua perjanjian internasional pada tahun 1960an.

Robert keohane juga menjelaskan bahwa institusi internasional memiliki beberapa peran penting yaitu:

- Sebagai sarana dalam menyediakan aliran informasi dan kesempatan bernegosiasi antara aktor internasional.
- Meningkatkan kemampuan pemerintah dalam memonitor kekuatan aktor lain dan dapat mengimplementasikan kebijakan atau rezim internasional pada aktor yang terlibat.

- Memperkuat harapan yang muncul dari aktor – aktor tentang kesolidan dari kesepakatan atau perjanjian internasional.

Tidak mudah untuk mencapai atau mempertahankan persetujuan internasional, liberal institusional mengklaim bahwa institusi menentukan kemampuan negara untuk berkomunikasi dan bekerja sama. Sama seperti realis, liberal menganggap negara sebagai inti dari pemahaman politik internasional. Namun, menurut liberal, baik aturan formal maupun informal dapat mempengaruhi tingkah laku negara. Sehingga rezim atau aturan yang dibentuk oleh sebuah institusi internasional akan mempengaruhi kerjasama dan juga kebijakan yang dibentuk oleh negara – negara anggota institusi tersebut.

Pada penelitian ini institusi internasional yang akan diteliti yaitu ASEAN yang merupakan institusi / organisasi regional wilayah Asia Tenggara. ASEAN juga memiliki beberapa norma dan aturan dasar yang perlu ditaati oleh negara – negara anggota ASEAN. Norma dan aturan tersebut dibentuk sebagaimana rupa dalam komunitas keamanan ASEAN yang dibagi menjadi tiga yaitu; ASEAN *Political-Security Community,* ASEAN *Economic Community*, dan ASEAN *Socio-Cultural Community*. Kebijakan ACCS atau ASEAN *cybersecurity cooperation strategy* merupakan kebijakan keamanan siber dibawah komunitas keamanan APSC yang dimana termasuk dalam aturan atau rezim internasional yang diciptakan oleh ASEAN sebagai organisasi regional atau bisa disebut juga institusi internasional

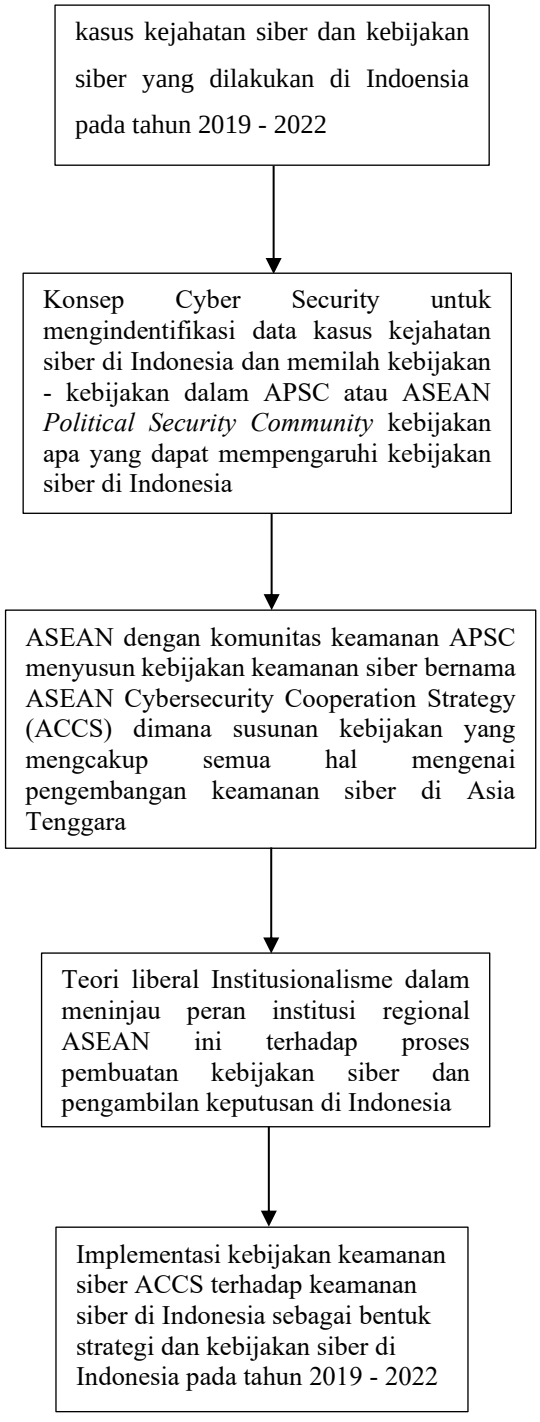
Teori liberal institusionalisme pada penelitian ini akan digunakan sebagai alat ukur untuk melihat bagaimana peran dari institusi internasional ASEAN dalam mempengaruhi kebijakan siber yang dibuat oleh Indonesia. Dari situ penulis dapat melihat apakah kebijakan siber yang dibuat ASEAN yaitu ACCS mempengaruhi pada implementasi kebijakan siber nasional yang dibentuk oleh Indonesia. Penulis juga dapat memahami yang lebih mendalam tentang Indonesia, berinteraksi dalam kerangka ACCS.

2.3 Kerangka Pemikiran

Keamanan siber atau *Cyber Security* merupakan sebuah aspek yang tidak dapat dihiraukan lagi. Semakin beragam dan berbahaya kejahatan siber atau *cybercrime* yang dapat dilakukan oleh oknum atau kelompok yang tidak bertanggung jawab. Hal ini merupakan ancaman bagi keamanan individu hingga keamanan internasional. Indonesia sebagai salah satu negara anggota ASEAN mengalami serangan siber terbanyak sepanjang sejarah. Hal ini merupakan hal yang sangat darurat dikarenakan keamanan suatu negara sudah terancam. ASEAN sebagai Regional Organization melakukan upaya untuk pengembangan *Cyber security* dan pencegahan *Cybercrime* terhadap negara – negara anggotanya.

Oleh karena itu, kerangka pemikiran ini dibuat sebagai alat bantu peneliti dalam menentukan alur penulisan dan menghasilkan jawaban dari pertanyaan penelitian yang telah dibuat. Dengan begitu kerangka pemikiran dengan menggunakan konsep *cyber security*, serta teori liberal institusionalisme diharapkan akan membantu peneliti dalam menganalisis keterkaitan kebijakan siber Indonesia dengan kebijakan siber ASEAN yaitu ACCS dalam implementasi kebijakan siber Indonesia pada rentan tahun 2019 – 2022. Setelah dianalisis dengan teori dan konsep tersebut akan menghasilkan bagaimana keterkaitan implementasi kebijakan siber Indonesia dengan ASEAN *Cybersecurity Cooperation Strategy* (ACCS) pada tahun 2019 – 2022.

Gambar 2.2 Kerangka Pemikiran



BAB III
METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Pada proses penelitian atau analisis sebuah isu atau topik diperlukan metode atau jenis pendekatan penelitian sebagai cara ilmiah dalam menjawab pertanyaan penelitian melalui pengumpulan informasi dan data. Pada Penelitian ini menggunakan pendekatan kualitatif dengan teknik analisis deskriptif. Pendekatan kualitatif merupakan strategi penelitian yang lebih menekankan pada kata – kata daripada data angka pada pengumpulan dan analisis data (Bryman, 2015). Ahli lain menjelaskan bahwa penelitian kualitatif merupakan sebuah proses analisis dengan cara pengumpulan informasi atas suatu isu atau fenomena yang timbul sebagai topik bahas dari sebuah penelitian (Arikunto, 1998).

Pada penelitian ini akan menggunakan metode penelitian kualitatif deskriptif sebagai alat bantu untuk peneliti dalam menganalisis dan mendeskripsikan bagaimana keterkaitan kebijakan siber Indonesia dengan kebijakan siber ASEAN yaitu ASEAN *Cybersecurity Cooperation Strategy* (ACCS) dalam mengatasi kejahatan siber di Indonesia dengan lebih terperinci. Data yang diperoleh berupa kata – kata berisi kebijakan keamanan siber ASEAN yaitu ASEAN *Cybersecurity Cooperation Strategy* (ACCS) secara terperinci dan hasil dari kebijakan keamanan siber tersebut terhadap kejahatan siber yang dialami di Indonesia pada tahun 2020. Konsep *Cyber Security*, dan teori liberal institusionalisme akan juga digunakan sebagai alat bantu dalam menggambarkan bagaimana keterkaitan kebijakan siber Indonesia dengan kebijakan ASEAN *Cybersecurity Cooperation Strategy* (ACCS).

3.2 Fokus Penelitian

fokus penelitian digunakan dengan tujuan membatasi tema atau topik penelitian yang telah dipilih untuk mempermudah peneliti dalam mengumpulkan data dan analisis data serta sebagai batasan penulis agar penelitian tidak terlalu luas. Sehingga pada penelitian ini memiliki fokus pada implementasi kebijakan siber Indonesia terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS). Penelitian ini menggunakan konsep *Cyber Security*, dan teori liberal institusionalisme sebagai alat bantu analisis. Latar tahun 2019 - 2022 dipilih disebabkan bahwa rentan tahun tersebut Indonesia mengalami serangan siber terbanyak sepanjang sejarah dan menjadi target serangan siber no. 1 di Asia Tenggara.

3.3 Jenis dan Sumber Data

Jenis data yang akan digunakan pada penelitian ini yaitu data sekunder. Data sekunder merupakan data yang diperoleh tidak secara langsung atau melewati orang lain atau sebuah media seperti buku, jurnal, situs, laporan, dan berita (sugiyono, 2013). Jenis data sekunder dipilih oleh peneliti disebabkan keterbatasan waktu dan lokasi untuk melakukan penelitian secara langsung. Pada penelitian ini data sekunder akan diperoleh dari situs resmi buku, artikel, jurnal, laporan, berita, dan situs internet resmi seperti ASEAN.org (situs resmi ASEAN), BSSN.go.id (situs resmi Badan Siber dan Sandi Negara Indonesia) dan lain lain. Lalu data tersebut akan diolah atau dianalisis dengan menggunakan konsep *Cyber Security*, dan teori liberal institusionalisme sehingga dapat menghasilkan data yang dibutuhkan oleh peneliti.

3.4 Teknik Pengumpulan Data

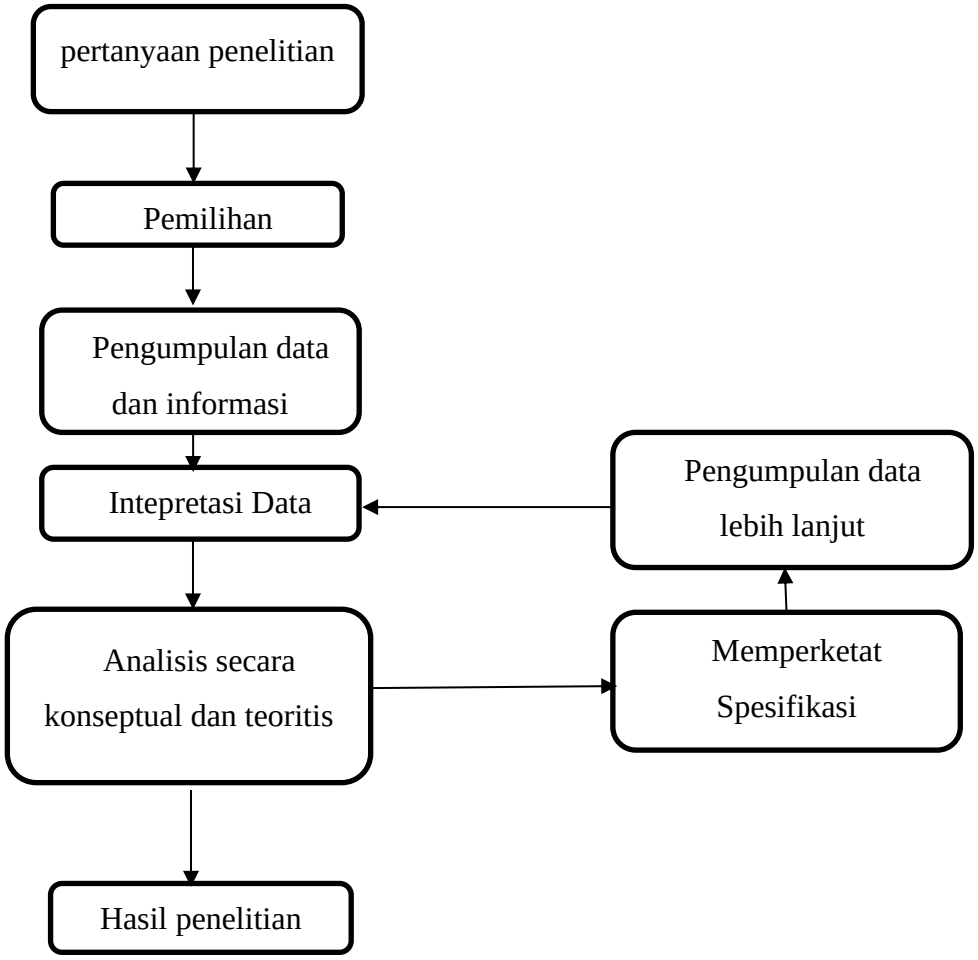
Teknik pengumpulan data merupakan cara atau strategi yang akan digunakan peneliti dalam proses pengumpulan data dan informasi yang berkaitan dengan topik atau isu penelitian. Peneliti akan menggunakan teknik studi literatur dan akan memperoleh data sekunder yang berasal dari jurnal, artikel, laporan organisasi,

website, dan buku yang memiliki keterkaitan dengan tema atau isu penelitan. Sebagian besar data yang dikumpulkan akan diperoleh berasal dari jurnal atau arsip artikel resmi dari lembaga terkait.

3.5 Teknik Analisis Data

Penulis mengacu pada teknik analisis data kualitatif yang dikemukakan oleh Alan bryman dimana terdapat beberapa tahapan yang perlu dilakukan dalam menganalisis sebuah data penelitian, gambaran nya sebagai berikut;

Gambar 3.1 Teknik Analisis Data oleh Alan Bryman



Sumber: (Bryman, 2015)

Berdasarkan buku dari Alan Bryman yang berjudul *Social Research Method* terdapat teknik penelitian kualitatif yang terdiri dari enam langkah. Langkah

pertama yaitu menentukan pertanyaan penelitian yang akan diteliti. Hal ini akan menjadi pondasi dasar dan penentu arah dari sebuah penelitian. Langkah kedua yaitu peneliti melakukan pemilihan subjek yang relevan terhadap tema dari penelitian itu sendiri sebagai variabel penelitian. Langkah ketiga yaitu proses pengumpulan data yang relevan terhadap topik peneltian. Data tersebut dibagi menjadi dua tipe yaitu primer atau sekunder. Dimana data primer dapat diperoleh secara langsung atau sekunder yang diperoleh secara tidak langsung yaitu melalui media terkait seperti buku atau jurnal. Langkah keempat yaitu interpretasi data. Langkah kelima yaitu analisis data secara konseptual dan teoritis, dimana data akan dianalisis menggunakan konsep dan teori yang relevan terhadap pertanyaan penelitian sebagai alat bantu untuk menghasilkan jawaban dari pertanyaan penelitian tersebut. Namun jika saat menganalisis data terdapat pertanyaan penelitian baru, peneliti harus memperketat pertanyaan penelitian dan mengumpulkan serta menginterpretasi data lanjutan. Langkah terakhir akan mendapatkan hasil penelitian yang dapat menjawab pertanyaan penelitian yang telah ditentukan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Keamanan siber atau *cyber security* merupakan sebuah aspek keamanan yang harus diperhatikan dari individu hingga tingkat internasional. Dimana teknologi informasi semakin berkembang sehingga terdapat ancaman – ancaman baru dan unik yang dapat menyerang individu hingga kelompok. Ancaman tersebut merupakan kejahatan siber atau cybercrime yaitu suatu aksi kejahatan yang dilakukan oleh pihak tidak bertanggung jawab dengan media internet dan teknologi. Maka dari itu sebuah negara hingga organisasi internasional harus menyiapkan sektor keamanan sibernya dengan lebih memadai sebagai bentuk pencegahan terhadap ancaman kejahatan siber. Hal tersebut dapat dicapai dengan kebijakan – kebijakan tertentu yang berisikan program serta strategi untuk meningkatkan keamanan siber. ASEAN yang merupakan organisasi regional dari kawasan Asia Tenggara memiliki banyak kebijakan – kebijakan sebagai upaya untuk mengembangkan kawasannya. Terdapat tiga kebijakan dan komunitas utama ASEAN yaitu *ASEAN Political-Security Community* (APSC), *ASEAN Economic Community* (AEC), dan *ASEAN Socio-Cultural Community* (ASCC). Dimana masing – masing kebijakan tersebut memiliki tujuan masing – masing. Keamanan siber merupakan salah satu aspek yang dibahas pada APSC dimana didalamnya menjelaskan bagaimana ASEAN meningkatkan keamanan siber di kawasannya.

Indonesia merupakan negara di Asia Tenggara dan merupakan salah satu anggota dari ASEAN atau biasa disebut dengan AMS atau ASEAN *member state.* Pada tahun 2019 – 2022 Indonesia mengalami serangan siber yang sangat masif dimana pada tahun 2021 Indonesia mengalami serangan siber terbesar sepanjang sejarah dengan angka 1,6 miliar kasus kejahatan siber. Melihat isu tersebut

kejahatan siber merupakan isu yang penting dan harus segera diatasi. Salah satu kebijakan siber yang dibentuk ASEAN yaitu ASEAN *Cybersecurity Cooperation Strategy* atau ACCS dimana berisi serangkaian program dan inisiatif terhadap bagaimana ASEAN mengembangkan keamanan siber dan mencegah kejahatan siber di kawasan. Maka dari itu dari kebijakan siber yang telah dibentuk oleh Indonesia dalam mengatasi masalah kejahatan siber sepanjang tahun 2019 – 2022 apakah berkaitan dengan kebijakan siber ASEAN yaitu ACCS. Secara dimana institusi internasional atau organisasi regional seperti ASEAN pasti berperan dan memberikan dampak pada pengambilan keputusan dalam pembentukan kebijakan di negara anggotanya yaitu Indonesia.

Dengan elaborasi konsep *cyber security,* dan teori liberal institusionalisme. Kebijakan siber yang telah dibentuk oleh ASEAN yaitu APSC Blueprint 2009 dan 2025, ACCS 2017 – 2020, ACCS 2021 – 2025 dengan berisikan berbagai strategi dan program. Penulis dapat melihat bahwa kebijakan – kebijakan keamanan siber yang diimplementasikan Indonesia yang berkaitan dengan ASEAN *Cybersecurity Cooperation Strategy* (ACCS) berperan dalam implementasi keamanan siber di Indonesia pada tahun 2019 – 2022. Disebabkan dengan adanya kebijakan – kebijakan siber ASEAN tersebut Indonesia dapat mengimplementasikan strategi dan program tersebut dalam kebijakan – kebijakan nasional dan internasional. Kebijakan siber ASEAN tersebut membantu Indonesia setidaknya dalam empat hal yaitu pembentukan lembaga siber nasional serta penggabungan dengan ASEAN - CERT, pembentukan perundang – undangan yang membahas keamanan siber dan kejahatan siber, peningkatan kapasitas keamanan siber dengan kerjasama regional dan internasional serta pembentukan laporan tahunan keamanan siber oleh BSSN atau Badan Siber dan Sandi Nasional yang merupakan badan siber Indonesia. lewat *security community*, APSC dengan berbagai kebijakan keamanan yang ada salah satunya *cyber security* yang telah dibentuk oleh ASEAN sebagai *regional organization* dapat membantu Indonesia sebagai salah satu anggota komunitas keamanannya pada bagian keamanan non tradisional yaitu keamanan siber dengan implementasi kebijakan siber ASEAN sebagai upaya dari penanggulangan kejahatan siber yang terjadi pada tahun 2019 – 2022. Walaupun memang secara

tidak eksklusif ASEAN turun tangan dan membantu Indonesia dalam penanganan kasus kejahatan siber di Indonesia.

5.2 Saran

Setelah melakukan analisis mengenai kebijakan siber Indonesia terkait ASEAN *Cybersecurity Cooperation Strategy* (ACCS) pada tahun 2019 – 2022, terdapat beberapa saran yang dapat penulis usulkan:

1. Indonesia seharusnya secepatnya men sahkan RUU ketahanan dan keamanan siber sebagai payung terhadap lembaga siber di Indonesia yaitu BSSN dalam melaksanakan program dan strateginya, serta agar penanganan dan pencegahan keamanan siber dapat lebih terkoordinasi. Indonesia juga merupakan salah satu negara di Asia Tenggara yang tidak memiliki undang – undang secara khusus membahas keamanan siber. Padahal pada APSC Blueprint ASEAN telah memberikan saran dan dukungan kepada seluruh AMS untuk membuat dan menguatkan hukum dan perundangan undangan yang membahas keamanan siber. Singapura merupakan salah satu negara yang implementasi kebijakan siber ASEAN tersebut dengan membentuk undang undang keamanan siber di negaranya.
2. Peneliti selanjutnya yang sekiranya tertarik untuk meneliti isu dan topik yang serupa dengan penelitian ini dapat menggunakan teori, konsep, dan kurun waktu yang berbeda agar dapat melihat secara lebih luas mengenai keamanan siber di ASEAN.

DAFTAR PUSTAKA

DAFTAR PUSTAKA

Adi Rio Arianto, G. A. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan dan Bela Negara*.

Annur, C. M. (2020, September 28). *Kataata*. Retrieved from Indonesia Menjadi Target Phishing Tertinggi di ASEAN: https://databoks.katadata.co.id/datapublish/2020/09/28/indonesia-menjadi-target-phishing-tertinggi-di-asean

Annur, C. M. (2023, mei 23). *Pandemi Mereda, Penggunaan Internet di Indonesia Turun pada 2022*. Retrieved from databooks: https://databoks.katadata.co.id/datapublish/2023/05/23/pandemi-mereda-penggunaan-internet-di-indonesia-turun-pada-2022

Ardiyanti, H. (2016). Cyber-Security Dan Tantangan Pengembangannya . *Badan Riset Inovasi Nasional*.

Arikunto, S. (1998). *Prosedur Penelitian Suatu Pendekatan Praktek.* Jakarta: Rineka Cipta.

ASEAN. (2009). *ASEAN Political-Security Community Blueprint.* jakarta: ASEAN Secretariat.

ASEAN. (2015, december 7). *Approach of the AEC Tops December "ASEAN Today"*. Retrieved from ASEAN: https://asean.org/approach-of-the-aec-tops-december-asean-today/

ASEAN. (2015). *ASEAN 2025: Forging Ahead Together.* Jakarta: ASEAN Secretariat.

ASEAN. (2016). *ASEAN Political-Security Community Blueprint 2025.* Jakarta: ASEAN Secretariat.

ASEAN. (2022, maret 06). *ASEAN Community*. Retrieved from Kementrian Luar Negeri Indonesia Untuk ASEAN : https://kemlu.go.id/ptri-asean/en/pages/komunitas_asean/965/etc-menu

ASEAN. (2022, Febuari). ASEAN CYBERSECURITY COOPERATION STRATEGY 2021 - 2025. *ASEAN Policy Draft*. Retrieved from ASEAN: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Asiatoday. (2020, mei 14). *In Southeast Asia, Indonesia Becomes the Number 2 Country Most Attacked by Hackers*. Retrieved from Asiatoday.id: https://asiatoday.id/read/di-asia-tenggara-indonesia-jadi-negara-nomor-2-paling-banyak-diserang-hackers

Bryman, A. (2015). *Social Research Methods(5th ed.).* New York: Oxford University Press.

BSSN. (2018). Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018 - 2019. *Rencana Strategis*.

BSSN. (2019). *Indonesia Cybersecurity Monitoring Report.* Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara.

BSSN. (2020). *Laporan Tahunan Monitoring Keamanan Siber Tahun 2020.* Jakarta: Badan Siber dan Sandi Negara.

BSSN. (2021). *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*. Jakarta: Badan Siber dan Sandi Negara.

BSSN. (2022, April 4). *BSSN*. Retrieved from Laporan Tahunan Monitor Keamanan Siber: https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

BSSN. (2022). *Lanskap Keamanan Siber Indonesia 2022.* Jakarta: Badan Siber dan Sandi Negara.

Buzan, B., Wæver, O., & Wilde, J. d. (1998). *Security : a new framework for analysis.* Boulder: Lynne Rienner Pub.

Cakrawala. (2021, Juni 26). *Infokomputer*. Retrieved from Bagaimana Cyber Security Bermula? Inilah Sejarah Awal Cyber Security: https://infokomputer.grid.id/read/122759088/bagaimana-cyber-security-bermula-inilah-sejarah-awal-cyber-security?page=all

CNN. (2019, Febuari 07). *225 Juta Serangan Siber Masuk Indonesia Sepanjang 2018*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20190207210646-185-367347/225-juta-serangan-siber-masuk-indonesia-sepanjang-2018

CNN. (2022, Mei 04). *Ancaman Siber di RI Naik 22 Persen, Tertinggi di Asia Tenggara*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20220426123543-192-789791/ancaman-siber-di-ri-naik-22-persen-tertinggi-di-asia-tenggara

CNN, I. (2020, mei 29). *RI Jadi Target Serangan Siber Terbesar Ke-2 di ASEAN Kala WFH*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20200512172258-185-502625/ri-jadi-target-serangan-siber-terbesar-ke-2-di-asean-kala-wfh

Damar, A. M. (2017, Desember 22). *Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017*. Retrieved from Liputan6: https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017

Deutsch, K. W. (1957). *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience.* Princeton: Princeton University Press.

Fadilla, M. F. (2021). Upaya ASEAN Dalam Meningkatkan Cyber Security di Kawasan Asia Tenggara Melalui ASEAN Regional Forum On Cybersecurity Initiatives. *Skripsi Universitas Sriwijaya*.

Fadjarudin, M. (2021, mei 31). *Indonesia Negara Nomor Tiga Terbanyak yang Dapat Serangan Siber*. Retrieved from suarasurbaya.net: https://www.suarasurabaya.net/kelanakota/2021/indonesia-negara-nomor-tiga-terbanyak-yang-dapat-serangan-siber/

Firmansyah, M. J. (2022, oktober 19). *UU PDP Disahkan, Pemalsu Data Pribadi Diancam Denda hingga Rp6 Miliar*. Retrieved from Tempo.co: https://nasional.tempo.co/read/1646858/uu-pdp-disahkan-pemalsu-data-pribadi-diancam-denda-hingga-rp6-miliar#:~:text=TEMPO.CO%2C%20Jakarta%20%2D%20Presiden,sisten%20elektronik%20atau%20PSE%20atau

Haftendorn, H. (1991). The Security Puzzle: Theory. Building and Discipline in International Security. *International Studies Quarterly*, 3 - 17.

Hardiansyah, Z. (2022, September 12). *Rentetan Aksi Hacker Bjorka dalam Kasus Kebocoran Data di Indonesia Sebulan Terakhir*. Retrieved from Kompas.com: https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all

Hardiyansyah, H. (2021, november 11). *Badan Kepegawaian & Pengembangan SDM Daerah Bangka Belitung*. Retrieved from Keamanan komputer dan jaringan: https://bkpsdmd.babelprov.go.id/content/keamanan-komputer-dan-jaringan

ID-SIRTII. (2022, september 26). *Singapura Resmikan Pembentukan ASEAN-CERT Sebagai Tim Keamanan Siber di Kawasan ASEAN*. Retrieved from ID-SIRTII: https://idsirtii.or.id/berita/baca/886/singapura-resmikan-pembentukan-asean-cert-sebagai-tim-keamanan-siber-di-kawasan-asean.html

kaspersky. (2022, june 08). *Phishing and Enterprises: Kaspersky Blocks 11M Malicious Mails in SEA 2021*. Retrieved from Cybersecurity ASEAN: https://cybersecurityasean.com/news-press-releases/phishing-and-enterprises-kaspersky-blocks-11m-malicious-mails-sea-2021

Keohane, R. O. (1989). *International Institutions and State Power (Essay in International Relations Theory)*. London: Westvie Press.

Krisman, K. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal Of ASEAN*, 41-53.

Krisnadi, J. J. (2021, Mei 7). *Kompasiana*. Retrieved from Lima Kasus Kejahatan Cybercrime Terburuk yang Pernah Ada di Dunia: https://www.kompasiana.com/nk7038/609563a28ede4817f80c3452/lima-kasus-kejahatan-cybercrime-terburuk-yang-pernah-ada-di-dunia

Kurtbağ, Ö. (2018). *Purposes and Roles of Regional Organizations in the International*. Eskişehir: Eskişehir: ANADOLU UNIVERSITY PRESS.

Markoff, J. (1999). An Internet Pioneer Ponders the Next Revolution. *New York Times*.

Mölder, H. (2006). NATO's Role in the Post-Modern European Security Environment, Cooperative Security and the Experience of the Baltic Sea Region. *Baltic Security & Defence Review*, 7.

Nor Shazwina Mohamed Mizan, M. Y. (2019). CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. *International Journal of Advanced Trends in Computer Science and Engineering*.

Nye, J. S. (2004). *Soft power : the means to success in world politics.* New York: Public Affairs.

P.H, L. (2002). Boomerang Effect: The Convergence of National and Human Security. *Securily DiRlogue*, 473-488.

Pamungkas, G. H. (2022, July 19). *CNBC Indonesia*. Retrieved from ASEAN: Pengertian, Negara Anggota, Sejarah dan Tujuan: https://www.cnbcindonesia.com/news/20220719171803-4-356822/asean-pengertian-negara-anggota-sejarah-dan-tujuan

Patrolisiber. (2020, desember 30). *Patrolisiber*. Retrieved from Jumlah data kasus kejahatan siber: https://www.patrolisiber.id/

Perwita, P. P. (2008). Dinamika Keamanan Dalam Hubungan Internasional dan Implikasinya Bagi Indonesia. *Universitas Katolik Parahayangan*, 6.

Putri, K. V. (2021). Kerjasama Indonesia Dengan ASEAN Mengenai Cyber security dan Cyber Resilience Dalam Mengatasi Cyber Crime. *Jurnal Hukum Lex Generalis*, 551.

Rudy Agus Gemilang Gultom, A. A. (2018). Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework. *INTENATIONAL JOURNAL OF MANAGEMENT AND INFORMATION TECHNOLOGY*.

Sandyryones Palinggi, S. P. (2020). Peningkatan Rasio Kejahatan Cyber dan Pola Interaksi Sosia Engineering pada periode akhir era Society 4.0 di Indonesia. *Jurnal Ilmiah Dinamika Sosial*.

Schatz, D., & Bashroush, R. W. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*.

Spandler, K. (2018). Regional Organizations in International Society: ASEAN, the EU and the Politics of Normative Arguing. *Palgrave Macmillan*.

sugiyono, P. D. (2013). *Metode penelitian pendidikan pendekatan kuantitatif, kualitatif dan R&D.* Bandung: CV. Alfabeta.

Techterms. (2022, agustus 16). Retrieved from Cyberspace Definition: https://techterms.com/definition/cyberspace

TEMPO. (2021, Oktober 21). *Global Firepower: Militer Indonesia Urutan Pertama Terkuat di Asia Tenggara*. Retrieved from Sekretariat Nasional ASEAN - Indonesia: https://setnasasean.id/news/read/global-firepower-militer-indonesia-urutan-pertama-terkuat-di-asia-tenggara#:~:text=Global%20Firepower%3A%20Militer%20Indonesia%20Urutan%20Pertama%20Terkuat%20di%20Asia%20Tenggara&text=TEMPO.CO%2C%20Jakarta%20%2D%20Halaman,

Union, I. T. (2020). Global Cybersecurity Index 2020. *Measuring commitment to cybersecurity*, 25 - 30.

Väyrynen, R. (2000). Stable Peace Through Security Communities? Steps Towards Theory-Building. *The Joan B. Kroc Institute For International Peace Studies*.

VOA. (2022, September 15). *UE Ingin Perketat Aturan Keamanan Siber untuk Perangkat Pintar*. Retrieved from VOA Indonesia: https://www.voaindonesia.com/a/ue-ingin-perketat-aturan-keamanan-siber-untuk-perangkat-pintar/6748577.html

Yinglun, S. (2022, agustus 16). *Xinhua*. Retrieved from 32nd ASEAN Summit concludes, rearffirming cooperation, common vision: http://www.xinhuanet.com/english/2018-04/28/c_137144125.htm