# BAB I

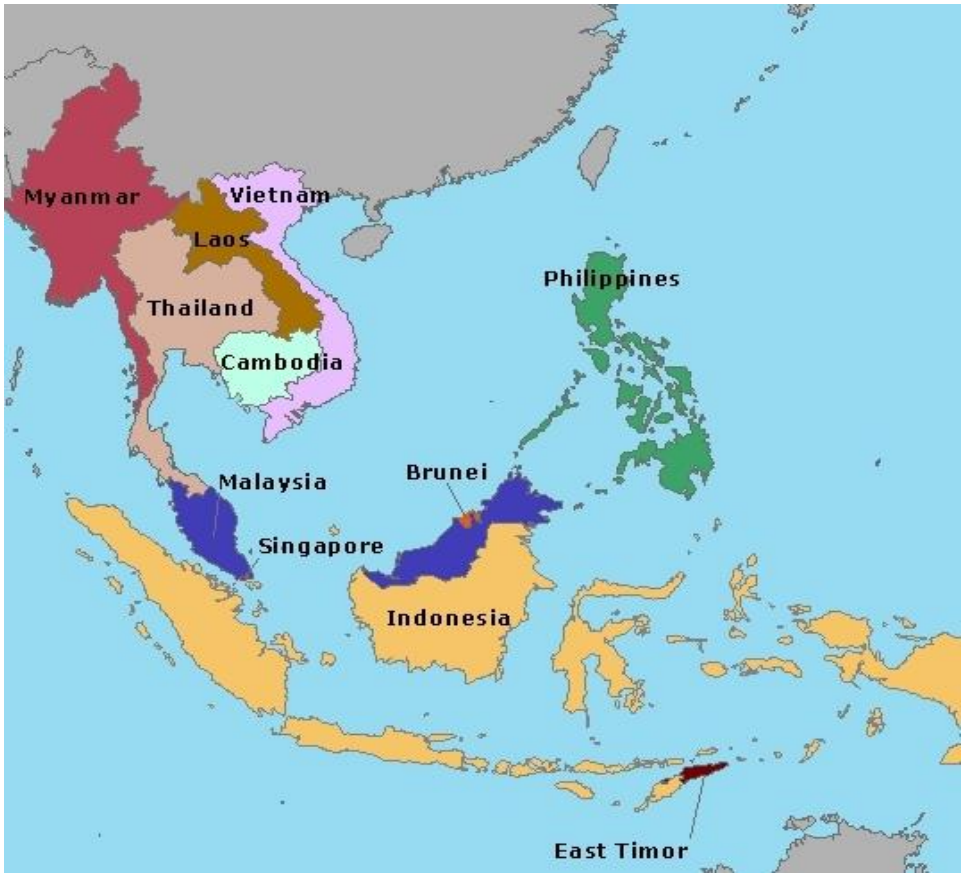
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Kejahatan siber atau *cybercrime* merupakan salah satu wujud dari ancaman non militer di bidang teknologi dan informasi. *Cybercrime* itu sendiri adalah jenis kejahatan yang tidak bisa dirasakan atau dilihat dampak nya secara fisik, dimana kejahatan satu ini bergerak dan menyerang di dunia maya. Kejahatan siber pada dasarnya tidak dilakukan untuk menggarap sebuah keuntungan bagi suatu pihak tertentu saja, kejahatan siber juga bisa dilakukan semata-mata hanya untuk merugikan atau menjatuhkan pihak yang lainnya. Hal ini berkenaan dengan pengertian kejahatan siber dari Wisnubroto yaitu semua tindak pidana yang dilancarkan dengan menggunakan teknologi komputer baik itu *software* atau *hardware* untuk alat objek baik bertujuan untuk memperoleh suatu keuntungan dari pihak tertentu atau sekedar merugikan pihak lain saja (Wisnubroto, 2010) *Cybercrime* itu sendiri hadir beriringan dengan berkembang nya teknologi dan komunikasi di dunia. Dengan bantuan perangkat komputer dan jaringan internet, *cybercrime* bisa dilakukan oleh sang penjahat tanpa memandang jarak dan waktu karena bisa dilakukan dan menyerang siapa saja, kapan saja dan darimana saja. Serangan ini dapat dilancarkan oleh *state actor* atau bahkan *non state actor*, di antar wilayah, antar negara, antar kawasan, atau antar benua sekalipun.

Meningkat dan semakin berkembangnya kejahatan siber yang terjadi di kawasan, tentu saja memunculkan suatu ancaman bagi kawasan Asia Tenggara itu sendiri. Kejahatan siber ini juga memiliki banyak sekali jenis dan bentuk nya, antaralain spionase dunia maya, pemalsuan / manipulasi data, konten-konten ilegal, propaganda terorisme, pembobolan ke sistem dan layanan komputer, *cyber stalking*, pelanggaran privasi, *cybersquatting* atau pemakaian nama domain internet dengan tujuan niat buruk, penipuan kartu kredit, *cracking* (Sukayasa & Suryathi, 2018) Ada pula disinformasi, pembajakan akun sosial media, pembobolan rekening bank, *web phising*, pemalsuan surat / dokumen penting, propaganda terorisme di

internet, pencurian data, penipuan pada transaksi perdagangan elektronik, serangan pembajakan pada situs web pemerintahan, dan masih banyak yang lainnya.




Gambar 1 Peta Kawasan Asia Tenggara

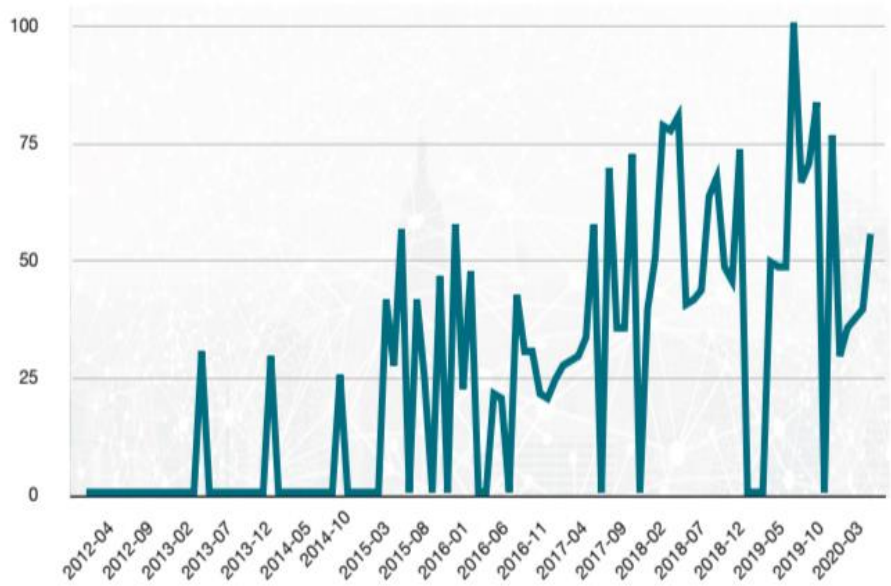
*Sumber : https://seasia.wisc.edu/southeast-asia-country-information-and-resources/*

Kawasan Asia Tenggara pada dasarnya tercipta melalui kondisi geografis dimana negara-negara di dalamya berada di satu lingkungan dan bahkan satu daratan. Kawasan itu sendiri merupakan negara-negara yang secara geografis berdekatan, berinteraksi, dan memiliki kesamaan pandangan pada berbagai fenomena (Thompson, 1973) Asia Tenggara memiliki beberapa persamaan sosial dan budaya, etnis, ras, sejarah, bentuk negara, dan banyak persamaan lainnya. Dari persamaan yang ada, timbulah kesadaran mengenai rasa solidaritas dari negara-negara di Asia Tenggara sehingga terbentuklah sebuah organisasi kawasan di Asia

Tenggara pada 8 Agustus 1967 yaitu *Association of Southeast Asian Nations* atau ASEAN yang di prakarsai oleh lima negara yaiu Thailand, Filipina, Singapura, Malaysia dan Indonesia. Lalu, (Acharya, The Evolution and Limitations of ASEAN Identity, 2017) mengungkapkan lima sumber identitas ASEAN yaitu agama, norma kultural dan model interaksi, regionalism, nasionalisme, orientasi pembangunan negara modern. Di kawasan Asia Tenggara sendiri seperti yang kita ketahui ancaman keamanan non militer telah terjadi sejak lama dan makin hari kejahatan masih meningkat di berbagai negara dan isu non militer ini akan selalu menjadi tantangan bagi stabilitas keamanan kawasan Asia Tenggara. Kondisi geografis negara di kawasan Asia Tenggara yang berdekatan bahkan satu daratan antar satu dan yang lain membuat isu ancaman non militer beredar di kawasan ini dengan mudah. Asia Tenggara dapat dikatakan sebagai kawasan dengan negara-negara yang sangat rentan terhadap permasalahan antar kawasan, seperti *human & drugs trafficking*, juga *cybercrime* (Daase & Friesendorf, 2010)

Timbulnya ancaman baru yang khususnya menyerang di dunia maya ini merupakan serangan yang *borderless* atau serangan yang tanpa melihat jarak, bisa terjadi dimana saja, kapan saja, menyerang siapa saja, dan bisa datang dari mana saja. Sehingga ancaman keamanan satu ini juga bisa dianggap sebagai ancaman global yang terbarukan. Jenis ancaman ini pun tergolong pada salah satu konsep ancaman dalam ilmu hubungan internasional yaitu ancaman non militer. Ancaman non militer juga secara luas bisa dipahami sebagai sebuah ancaman non militer yang hadir dengan tidak menggunakan kekuatan militer atau peralatan persenjataan yang apabila dibiarkan begitu saja akan menimbulkan bahaya keselamatan masyarakat, ataupun kedaulatan serta keutuhan wilayah negara walaupun tidak dengan kekuatan militer atau kekuatan persenjataan.

Berkaitan dengan kejahatan siber, seringkali kejahatan ini bersinggungan dengan "*darkweb"*. *Darkweb* itu sendiri merupakan kumpulan situs internet tersembunyi yang hanya dapat diakses oleh browser web khusus, yaitu *Tor Browser* yang dapat menyembunyikan alamat IP dan aktivitas penjelajahan Anda dengan mengarahkan lalu lintas web melalui serangkaian *router* berbeda yang dikenal sebagai *node*. (Kaspersky, n.d.)




Gambar 2 Jumlah artikel berita di Asia Tenggara yang menyebut *Darkweb* (Jan 2014 hingga Juli 2020)

*Sumber : Darknet Cybercrime Threats to Southeast Asia, UNODC 2020*

Jumlah artikel berita diterbitkan yang menyinggung tentang *Darkweb* sendiri meningkat sejak 2014 dibandingkan tahun-tahun sebelumnya. Data ini memberikan sebuah indikasi bahwa tren kejahatan siber mulai meningkat dan meningkat dari tahun ke tahun nya terutama di Kawasan Asia Tenggara itu sendiri. *Darkweb* juga digunakan sebagai jembatan anonim dari mana serangan siber itu dapat diluncurkan. (United Nations Drugs and Crime, 2020) Pelaku kejahatan siber dimotivasi oleh keuntungan seperti memperdagangkan informasi identitas pribadi dan keuangan yang dicuri dari individu dan bisnis di forum dan pasar *Darkweb*. Pelaku kejahatan siber menggunakan kredensial curian (seperti nama pengguna dan kata sandi) untuk mengakses layanan *online* dan kemudian mengeksploitasi informasi pribadi korban untuk penipuan.

Karena kredensial sering digunakan kembali tanpa disadari, satu kata sandi yang disusupi dapat menyebabkan penjahat mendapatkan akses ke layanan lain yang lebih berdampak seperti *PayPal*. Seorang warga negara Rusia ditangkap di Thailand pada tahun 2018 karena mengoperasikan pasar *Darkweb*, Organisasi *Infraud*, menjual informasi kartu kredit curian dan perangkat keras untuk

membahayakan ATM. Pasar tersebut memiliki 11.000 anggota yang memperdagangkan lebih dari 4,3 juta kartu kredit, kartu debit, dan rekening bank di seluruh dunia. Hal ini mengakibatkan kerugian lebih dari US$530 juta untuk pengguna dan bisnis yang sah. Dampak dari kerugian setengah miliar dolar terlihat jelas pada saat-saat terbaik, tetapi selama resesi ekonomi global terbesar dalam 50 tahun, dampak dari kerugian tersebut terhadap kemakmuran ekonomi, pemulihan dan kehidupan benar-benar fenomenal (United Nations Drugs and Crime, 2020) Contoh-contoh ini menunjukkan bahwa penjahat beroperasi di *Darkweb* Asia Tenggara.

Selain itu contoh kasus kejahatan siber yang terjadi di Kawasan Asia Tenggara adalah, pada tahun 2020 saat *lockdown* akibat Covid 19 berlangsung, terjadi kebocoran data 230.000 pasien di Indonesia. Data yang dikumpulkan dari para korban ditemukan diposting di forum *Darkweb* berbahasa Rusia dan Inggris. (CISOMAG, 2020) Lalu terjadi juga pelanggaran data di Indonesia yaitu *E-commerce* Tokopedia mengalami pelanggaran data besar-besaran setelah peretas membocorkan lebih dari 15 juta catatan pengguna. Juga ditemukan bahwa aktor ancaman menyimpan rincian 91 juta pengguna untuk dijual di darknet seharga US$ 5.000 dimana data yang bocor berisi nama, email, hash kata sandi, dan informasi pribadi lainnya.

Kejahatan siber yang marak di kawasan mengharuskan negara didalamnya untuk bekerjasama dalam mengkaji, mengatasi dan melakukan penanganan terhadap kejahatan siber itu sendiri. Karena benar adanya bahwa apabila tidak ada kerjasama di kawasan yang membahas tentang kejahatan siber, akan sulit stabilitas keamanan kawasan dicapai terutama dalam aspek siber. Salah satu upaya yang bisa dijalankan adalah dengan membentuk platform kerjasama keamanan siber di kawasan yang akan berfungsi sebagai sharing informasi serta koordinasi mengenai insiden siber antar negara di kawasan Asia Tenggara (Sunkpho, Ramjan, & Oottamakorn, 2018)

Badan Siber dan Sandi Negara atau BSSN sebagai lembaga yang bertugas melaksanakan keamanan siber negara Indonesia. BSSN sendiri didirikan pemerintah Indonesia pada 19 Mei 2017 sebagai pengganti Lembaga Sandi Negara.

Dasar hukum pembentukan dari BSSN sendiri adalah Perpres No. 53 Tahun 2017, Perpres No.133 Tahun 2017 (perubahan atas Perpres No.53 Tahun 2017) dan Perpres No. 28 Tahun 2021. Dengan itu, diharapkan BSSN dapat menjadi aktor yang dapat menangani marak nya kasus *cybercrime* yang ada baik di kawasan ataupun dalam negeri. BSSN juga bekerja sebagai badan yang akan meningkatkan kesadaran masyarakat terhadap *cybersecurity* (Kelleher, 2017) Karena seperti yang kita ketahui kejahatan siber memiliki jenis yang sangat beragam dan bisa langsung menargetkan seseorang, serta kejahatan jenis satu ini bisa datang dari berbagai belahan dunia sehingga *cybercrime* dapat dikatakan sebagai salah satu ancaman global bagi Indonesia dan juga kawasan Asia Tenggara.

Pemerintah Indonesia melalui BSSN dalam berupaya menangani kejahatan siber di kawasan Asia Tenggara melakukan beberapa upaya seperti pada tanggal 8 Oktober 2020 lalu, Deputi Bidang Proteksi BSSN menghadiri pertemuan Singapore International Cyber Week (SICW) Ministerial Roundtable bertema Adapting to the New Normal: Innovation, Opportunities, Cooperation yang juga merupakan penutupan Asean Ministerial Conference on Cybersecurity (AMCC) 2020 (BSSN, 2020) Dalam pertemuan tersebut, Akhmad Toha sebagai perwakilan Indonesia dari BSSN mendorong ajakan kerjasama antar professional teknologi informasi komunikasi dan siber di seluruh asia tenggara untuk mengatasi permasalahan siber yang meningkat terutama di masa pandemi Covid-19. Akhmad Toha juga menyampaikan bahwa diperlukan keserasian langkah ataupun pola pikir bersamaan dengan pengembangan kapasitas siber masing-masing negara termasuk mengenai regulasi, sumber daya manusia serta teknologi guna membangun serta memperkuat ketahanan siber di kawasan Asia Tenggara.

Selanjutnya, BSSN sebagai delegasi dari Indonesia menjadi pembicara dalam sebuah forum dialog kerjasama multilateral bertajuk 18th International Institute for Strategic Studies (IISS) Shangri-La Dialogue di Singapura pada tanggal 31 Mei-2 Juni 2019. Forum dialog yang didatangi oleh delegasi dari 30 negara ini mengambil fokus pembahasan mengenai Cyber-Capability Development: Defence Implications, yang juga membahas mengenai macam-macam tantangan keamanan baik regional ataupun global (BSSN, 2019) BSSN juga menyampaikan resiko dalam perkembangan teknologi di era revolusi industri yang

mengancam keamanan nasional seperti *cybercrime* dan terorisme. Dengan itu peningkatan pertahanan keamanan siber perlu dikembangkan lagi dengan memperluas kerjasama antar negara serta memanfaatkan aktor-aktor non negara untuk kolaborator demi terciptanya keamanan global terutama di bidang siber.

Lalu BSSN pada 6 Juni 2019 menggelar forum yang memfokuskan pada kerjasama negara-negara Asia Tenggara dengan Jepang di dalam bidang siber yaitu ASEAN-Japan Cyber Exercise. Dalam forum pertemuan yang dilaksanakan secara daring tersebut, BSSN sebagai aktor utama dalam perihal keamanan siber di Indonesia menanggapi pertemuan ini sebagai cara menjalankan kerjasama, mengumpulkan informasi serta menyuarakan aspirasi untuk membawa kepentingan Indonesia di kawasan Asia Tenggara dan Jepang di dalam aspek siber (BSSN, 2019) Melalui forum ini, BSSN bisa berkolaborasi untuk terus menghadapi perkembangan isu *cybercrime* dan kegiatan yang dilakukan seperti pertukaran informasi, pengembangan kapasitas, penindakan / penyelesaian insiden, dan yang terakhir Jepang dan masing-masing negara ASEAN bisa meningkatkan kepekaan keamanan informasi.

Berkaitan dengan upaya BSSN dalam menangani kejahatan siber di kawasan Asia Tenggara ini, ada sejumlah literatur yang penulis gunakan sebagai penelitian terdahulu untuk pendukung penelitian yang akan dilakukan. Pertama, (Sunkpho, Ramjan, & Oottamakorn, 2018) membahas tentang bagaimana keamanan siber dan bagaimana kebijakan mengenai keamanan siber di negara-negara Asia Tenggara ditetapkan. Dimana sebagian besar negara telah membentuk kebijakan untuk memerangi kejahatan dunia maya dengan memberikan undang-undang yang menghukum perbuatan salah di internet dan menjaga data pribadi warga negara dengan menyediakan hukum untuk menjamin privasi warga negara. Dan mengenai data pribadi ini (Rotenberg, 1998) menyatakan bahwa perlindungan data pribadi sudah diakui secara internasional dalam UDHR dan ICCPR, dimana privasi tersebut meliputi kehormatan, nama baik, rumah tangga, surat menyurat pribadi, dan informasi atau data pribadi.

Namun seperti yang kita ketahui, belum semua peraturan perundang-undangan mengenai kejahatan siber merata penerapannya di kawasan Asia

Tenggara. Penulisan terdahulu ini membantu penulis dalam memahami bagaimana sebagian besar negara di Asia Tenggara membentuk kebijakan dalam menangani kejahatan siber di masing-masing negara nya. Ada beberapa persamaan kebijakan dalam menangani kasus cybercrime misalnya kepemilikan undang-undang tentang kejahatan dunia maya, transaksi elektronik, perlindungan data, dan lain-lain.

(Kremling & Parker, 2017) menyatakan bahwa meningkatnya kompleksitas kejahatan siber dunia, negara-bangsa harus bekerjasama untuk mencapai keamanan nasional negara nya masing-masing dan pada saat yang sama ada juga ketidakpercayaan antar negara terkait tujuan politik dan penggunaan serangan siber. Berkaitan dengan itu, bagaimanapun juga untuk mencegah perang dunia maya maka kerjasama dan persamaan pola pikir diperlukan oleh negara-negara. Kerjasama dan berbagi informasi dibutuhkan oleh negara-negara Asia Tenggara untuk bisa menangani isu kejahatan siber di kawasan.

Dalam memahami pengertian serta jenis-jenis kejahatan siber, penulis mengambil referensi dari (Kremling & Parker, 2017) dan (Sukayasa & Suryathi, 2018) yang memiliki persamaan dalam pandangan mengenai jenis kejahatan siber yang paling marak dan serius yaitu spionase dunia maya, sabotase, terorisme, penggelapan, pemerasan, pemalsuan data, serta penipuan.

Dalam memahami tentang serangan *cybercrime* utama yang ditemui oleh negara-negara ASEAN, (Mizan, Ma'arif, Satar, & Shahar, 2019) memberi pedoman untuk membenahi sistem yang sudah ada. Dimana dikatakan bahwa keamanan siber Asia Tenggara hanya fokus pada beberapa tema saja yaitu serangan siber inovatif, strategi terhadap ancaman keamanan siber, kebijakan pemerintah dan perlindungan terhadap privasi, perlindungan terhadap infrastruktur komputer di pemerintahan, dan masalah hukum dan etika di dunia maya. ASEAN sebagai organisasi kawasan membutuhkan kerjasama penuh dari seluruh anggotanya. Isu dan tantangan ini tidak dapat ditangani dan dikelola dengan baik secara independen sehingga pencarian peluang dan peningkatan kerjasama diperlukan dalam upaya yang gigih untuk mencapai tujuan kestabilan keamanan siber di kawasan. Dan dari sini penulis juga menangkap bahwa diperlukan perluasan tema seperti untuk memasukkan kebijakan perlindungan sektor swasta dan infrastruktur perlindungan bagi masyarakat umum.

Selanjutnya ada yang didalamnya membahas tentang keamanan non militer di Asia yaitu karya (Anthony & Cook, 2013) yang mengartikan ancaman non militer sebagai sumber-sumber non militer seperti penyelundupan, penyakit menular, perubahan iklim, bencana alam, migrasi tak teratur, penipisan sumber daya serta degradasi lingkungan lintas batas, kekurangan makanan, perdagangan senjata illegal, perdagangan narkoba, penyelundupan orang, serta kejahatan siber yang hadir membawa tantangan pada kesejahteraan serta kelangsungan hidup masyarakat dan negara. Literatur kedua memiliki persamaan dengan penulisan ini dimana dijelaskan secara rinci apa itu ancaman non militer dan dijelaskan pula bagaimana isu ancaman non militer tersebut di kawasan Asia. Tetapi dalam penulisan ini hanya mengangkat kawasan Asia Tenggara saja tanpa membahas lebih lanjut atau lebih luas lagi.

Selanjutnya, (Primawanti & Pangestu, 2020) yang mengatakan bahwa masih banyak negara di Asia Tenggara yang belum membentuk kebijakan dalam negeri mengenai siber secara efektif seperti pembentukan lembaga khusus yang menangani *cybercrime* yang belum dimiliki oleh beberapa negara, sementara Indonesia sendiri telah membentuk BSSN. Apabila seluruh negara Asia Tenggara telah memiliki lembaga khusus yang memegang keamanan siber, kerjasama siber akan lebih mudah dijalankan nya, serta pertukaran informasim pemetaan jaringan serangan, serta pengambilan tindakan pun bisa dilakukan lebih mudah dan efektif. Berkaitan dengan lembaga khusus, penulis mengulik (Arianto & Anggraini, 2019) sebagai acuan untuk memahami bagaiamana penanganan keamanan siber yang mana sudah seharusnya melibatkan pemerintah sebagai pengatur, lembaga penegak hukum, lembaga intelijen, serta lembaga pertahanan dan keamanan. Penulis menganggap hal tersebut tidak hanya berlaku di Indonesia saja, tapi sudah seharusnya semua negara juga menerapkan hal yang sama, dimana harus adanya kesamaan dalam pemikiran serta bertindak dari tiap lembaga yang berwenang serta pemerintah di setiap negara di kawasan Asia Tenggara sehingga nantinya akan tercipta keselarasan yang mendukung keamanan di tingkat kawasan.

(Chotimah, 2019) yang membahas mengenai kerjasama dan diplomasi siber Indonesia serta peran BSSN dalam tata kelola keamanan siber Indonesia mengungkap bagaimana dan seberapa besar penggunaan internet serta kemajuan

teknologi informasi dan komunikasi di Indonesia yang menyebabkan besarnya kemungkinan ancaman siber yang terjadi di Indonesia. Dan dalam penulisan ini juga dibenarkan bahwa semakin banyak pengguna internet di suatu negara, maka semakin besar pula peluang ancaman yang akan datang. Sama seperti (Sudarmadi & Runturambi, 2019) yang membahas peran BSSN dalam mengahadapi ancaman siber di Indonesia, Dibahas pula mengenai bagaimana peran BSSN dalam menjaga keamanan siber Indonesia, tetapi penulis akan lebih berfokus pada peran BSSN dalam menanggapi ancaman keamanan siber di Asia Tenggara dan bukan hanya di lingkup nasional saja.

Dari literatur dan penelitian terdahulu yang penulis jadikan sebagai referensi untuk penulisan ini, penulis belum menemukan karya tulis yang secara rinci membahas mengenai upaya Indonesia melalui BSSN dalam menangani kasus kejahatan siber di kawasan Asia Tenggara. Sedangkan seperti yang kita ketahui BSSN adalah *leading sector* keamanan siber di Indonesia, tetapi sejauh ini penulis belum melihat ada penelitian lainnya yang membahas mengenai seberapa banyak atau seberapa efisien kah BSSN dalam menangani atau berkontribusi didalam keamanan siber di kawasan Asia Tenggara.

## 1.2 Rumusan Masalah

Berdasarkan lonjakan penggunaan *smartphone* dan internet yang menimbulkan maraknya kejahatan siber di kawasan Asia Tenggara, maka dapat dirumuskan pertanyaan "Bagaimana kerjasama siber pemerintah Indonesia melalui BSSN di Asia Tenggara pada tahun 2018-2020?"

## 1.3 Tujuan Penelitian

Tujuan Praktis :

Untuk menganalisis apa saja jenis kejahatan siber yang marak terjadi di kawasan serta membuktikan strategi Indonesia melalui Badan Siber dan Sandi Negara (BSSN) dalam menangani kasus kejahatan siber.

Tujuan Teoritis :

Untuk membuktikan efektivitas BSSN dalam memperkuat sistem keamanan nasional serta kawasan Asia Tenggara khusus nya dalam sektor keamanan siber dalam menghadapi ancaman global.

## 1.4 Manfaat Penelitian

Penelitian ini diinginkan bisa memberi informasi juga referensi baik untuk mahasiswa hubungan internasional ataupun masyarakat luas mengenai strategi Indonesia melalui BSSN dalam memperkuat keamanan nasional dan juga kawasan Asia Tenggara khususnya di sektor siber dari ancaman global. Hasil dari penulisan ini diinginkan bisa merefleksikan teori ilmu hubungan internasional yang ada dan memberikan andil pada kajian ilmu hubungan internasional sehingga penelitian ini bisa menghasilkan literatur baru.

## 1.5 Sistematika Penulisan

**BAB I PENDAHULUAN**

Pada bab pertama ada poin yang dikaji seperti, latar belakang masalah, rumusan masalah, tujuan praktis dan teoritis penelitian, manfaat yang dihasilkan dari penelitian ini serta sistematika dari penulisan. Bab ini adalah sebuah rangka awal dari seluruh proses penelitian.

**BAB II TINJAUAN PUSTAKA**

Pada bab kedua akan ada konsep dan teori yang digunakan pada penelitian dan juga kerangka pemikiran. Konsep serta teori-teori yang menjadi landasan penelitian akan dibahas guna menjelaskan temuan ataupun jawaban dari rumusan masalah.

**BAB III METODE PENELITIAN**

Pada bab ketiga ini penulis membahas tentang objek, pendekatan dan jenis penelitian, sumber data, teknik pengumpulan data, teknik analisis data dan tabel rencana waktu. Secara umum bab ini akan berisikan mengenai cara serta tahapan penulis dalam proses penelitian.

**BAB IV BSSN DAN TREN KEJAHATAN SIBER DI ASIA TENGGARA**

Bab kelima berisikan tentang penjabaran mengenai hasil dari penelitian yang penulis lakukan. Akan dibahas mengenai profil dari BSSN itu sendiri sebagai *Leading Sector* siber di Indonesia. Lalu akan dijabarkan apa saja dan bagaimana tren kejahatan siber di kawasan Asia Tenggara di tahun 2018-2020. Juga pada bab ini akan berisikan diskusi dan analisis data yang menjelaskan tentang temuan data penelitian yang nantinya dianalisis menggunakan teori-teori yang sudah digunakan.

**BAB V KERJASAMA SIBER INDONESIA MELALUI BADAN SIBER DAN SANDI NEGARA (BSSN) DI ASIA TENGGARA TAHUN 2018-2020**

Bab ini berisi tentang apa saja upaya yang dilakukan pemerintah Indonesia melalui BSSN dalam menanggapi maraknya kejahatan siber yang terjadi di Asia Tenggara pada tahun 2018-2020, mulai dari memperkuat pertahanan siber di dalam negeri sendiri sampai dengan kerjasama yang dilakukan antara negara-negara di kawasan Asia Tenggara dengan Indonesia.

**BAB VI KESIMPULAN DAN SARAN**

Di bab terakhir atau bab keenam penulis akan dibahas kesimpulan serta saran, baik saran praktis juga saran teoritis. Kesimpulan pokok dari seluruh pembahasan serta penelitian akan disampaikan pada bab ini. Usulan yang berguna untuk pemecahan masalah dari pun akan dijabarkan dalam bab terakhir ini.