BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi pada zaman sekarang telah menjadi kebutuhan bagi semua masyarakat, perkembangan teknologi yang pesat di dunia ini telah memberikan dampak yang besar terhadap keberlangsungan hidup manusia. Namun tidak dapat dipungkiri bahwa perkembangan teknologi pada zaman sekarang seperti pedang bermata dua, sebab selain memberikan dampak positif bagi manusia nyatanya juga memberikan dampak negatif yang tidak kalah penting untuk diperhatikan. Perkembangan teknologi membuka peluang untuk meningkatkan tindakan kejahatan siber atau bisa disebut sebagai *cybercrime.*

Cyber crime atau kejahatan siber merupakan tindak kejahatan yang dilakukan secara online melalui komputer atau perangkat jaringan, *cybercrime* sendiri terbagi menjadi beberapa jenis diantaranya, penipuan *Phishing*[1], *Website Defacement*[2], dan *Malware* atau *Ransomware*[3]. Berikut merupakan perbandingan

---

[1] Penipuan *Phishing* merupakan penipuan yang dilakukan dengan modus memancing korban dalam memberikan identitas serta informasi pribadinya dengan menaruh tautan palsu pada akun sosial media dengan ajakan atau iklan sederhana serta menggiurkan (Wibowo & Fatimah, 2017).

[2] *website defacement* atau *defacing* ini merupakan salah satu bentuk kejahatan siber yang berfokus terhadap perubahan tampilan pada sebuah web. Perubahan web yang terjadi meliputi seluruh halaman website untuk menunjukkan bahwa *attacker* atau *hacker* telah memasuki website tersebut untuk melakukan protes atau kritik yang dilakukan oleh para *hacktivist*, namun selain untuk melakukan protes biasanya *deface website* juga digunakan untuk menunjukkan kelemahan keamanan dalam website, yang digunakan untuk pengujian awal keamanan web, dengan tujuan untuk mengetahui apakah dalam website tersebut masih terdapat celah yang dapat digunakan para *hacker* untuk melakukan peretasan (KEMENKES RI, 2023).

[3] *malware* merupakan kejahatan siber yang dilakukan dengan merusak perangkat lunak (Panjaitan et al., 2022). Malware memiliki berbagai macam jenis salah satunya yakni *Ransomware*, ransomware merupakan salah satu jenis kejahatan malware dengan modus ancaman terhadap korban melalui pemblokiran akses data ataupun sistem penting, yang kemudian menggunakan strategi tebusan dibayar untuk mendapatkan datanya kembali (Panjaitan et al., 2022). Lihat juga (Microsoft, n.d.).

data kasus *cybercrime* di Indonesia dan Singapura, yang diperoleh dari laporan BSSN (Badan Siber dan Sandi Negara) serta badan CSA *(Cyber Security Singapore).* Jenis kejahatan siber yang dibandingkan yakni kasus *Phishing, Web Defacement*, dan *Malware.* Kejahatan siber *malware* kedua negara memiliki jenis yang berbeda-beda contohnya Singapura, Singapura kasus malware yang terjadi lebih condong terhadap *malware* jenis *Ransomware, Command and Control*, dan *Botnet Drones*, sedangkan Indonesia jenis *malware* yang lebih sering terjadi diantaranya *Trojan*, *AllAple, ZeroAccess*. Berdasarkan data di bawah telah menunjukkan beberapa dinamika berdasarkan tiga jenis kejahatan siber diatas.

Tabel 1.1 *Dinamika kasus Cyber crime Singapura dan Indonesia tahun 2016-2021.*

Laporan Kasus Cyber Crime	Singapura			Indonesia		
	Phishing	Web Defacement	Malware	Phishing	Web Defacement	Malware
2016	2.512	1.750	60	5.637	-	30.734
2017	23.420	2.040	3.850	68	879	36.423.773
2018	16.100	605	3.221	4.499	16.939	122.437.819
2019	47.500	873	2.865	12.579.480 (web defacement, phishing, infeksi malware)		105.154.900
2020	47.000	495	7.715	2.549	9.749	495.337.202
2021	55.000	419	8.237	3.816	5.940	1.637.937.022

Sumber : Diolah dari berbagai sumber.

Sesuai pada tabel 1.1, pada tahun 2016 berdasarkan laporan yang diberikan oleh CSA *(Cyber Security Agency of Singapore*), terdapat 550 serangan tiap harinya terkait Ransomware di Singapura, dengan meningkatnya kasus ransomware di Singapura ini SingCERT telah memberikan peringatan kepada masyarakat terhadap bahaya tersebut serta memberikan tindakan pencegahan. Terkait kasus Website Defacement Singapura di tahun 2016 telah terdeteksi

hampir 1.800 perusahaan mengalami perusakan situs web, perusakan situs web ini pelakunya termasuk para *hacktivist* yang ingin mempromosikan terkait ideologi mereka, untuk kasus Phishing telah terdeteksi di tahun 2016 lebih dari 2.500 kasus phishing dengan sektor Perbankan dan Keuangan yang lebih banyak dilakukan pemalsuan (Cyber Security Agency of Singapore, 2016). Pada tahun 2017 kasus Phishing telah terdeteksi sebanyak 23.420 URLs Phishing, dengan sektor teknologi yang menjadi sektor tertinggi dalam pemalsuan contohnya Microsoft, pada kasus Website Defacement di tahun 2017 telah tercatat 2.040 kasus perusakan web dengan target utama Usaha Mikro atau SME's (*Small and Medium-Sized Enterprises*) dari sektor manufaktur, teknologi informasi dan komunikasi serta manufaktur (CSA of Singapore, 2018). Menurut pengamatan yang dilakukan oleh CSA terdapat 3.850 kasus malware yang terjadi di Singapura, dari 3.850 kasus tersebut didalamnya terdapat sekitar 750 server C&C (*Command and Control)*, botnet, serta varian *malware* lainnya (Cyber Security Agency of Singapore, 2018). Di tahun 2018 kasus phishing mengalami penurunan sebanyak 30% dari tahun 2017 yakni sebanyak 16.000 URLs Phishing, tidak hanya phishing saja kasus kejahatan *website defacement* juga mengalami penurunan sebanyak 70% dari tahun 2017 yakni sebanyak 605 kasus (*Cyber Security Agency of Singapore (CSA)*, 2018). Hingga di tahun 2019 kejahatan siber phishing telah tercatat oleh CSA sebanyak 47.500 kasus, dengan urutan teknologi menjadi urutan pertama, email service providers pada urutan kedua serta pengambilan informasi seperti banking atau financial services berada di urutan ketiga (Cyber Security Agency of Singapore, 2019).

Jika dilihat berdasarkan tiga jenis kejahatan siber yang dijelaskan sebelumnya yakni kejahatan phishing, website defacement serta ransomware Singapura memiliki beberapa penurunan pada jenis phising, di tahun 2020 telah tercatat mengalami penurunan dari 47.500 kasus menjadi 47.000 kasus, namun menjadi kasus serangan siber dengan total tahunan tertinggi yang ditangani oleh SingCERT[4]. Selain itu, pada kejahatan siber jenis website defacement juga mengalami penurunan, berdasarkan pada laporan siber Singapura pada tahun 2019 hingga 2020 telah terdeteksi website defacement sebanyak 873 kasus, yang kemudian menurun di tahun 2020 menjadi 495 kasus. Namun di tahun 2021 kejahatan siber jenis phishing mengalami peningkatan dari 47.000 pada tahun 2020 menjadi 55.000 di tahun 2021 (Cyber Security Agency of Singapore, 2022). Pada umumnya masyarakat Singapura sangatlah bergantung terhadap teknologi dikarenakan teknologi sudah menjadi kebutuhan dalam aktivitas keseharian masyarakat pada umumnya. Mengingat kasus serangan siber yang datang silih berganti karena ketergantungan masyarakat akan komunikasi ini menjadikan keamanan siber merupakan hal yang penting bagi Singapura.

Di sisi lain, Indonesia juga menjadi salah satu negara anggota ASEAN yang merasakan bagaimana ancaman siber telah memberikan dampak yang besar terhadap keamanan nasional, berbagai macam upaya juga telah dilakukan oleh Indonesia dalam membangun kapasitas *cyber securitynya*. Sesuai pada tabel 1.1 berdasarkan laporan yang diterima oleh ID-CERT pada tahun 2016 terdapat laporan kasus phishing sebanyak 5.637 laporan, serta kasus malware sebanyak

[4] SingCERT sendiri merupakan *Singapore Cyber Emergency Response Team* atau Tim Tanggap Darurat Komputer di Singapura.

30.734 laporan. Sedangkan untuk kasus *website defacement* berdasarkan data yang dipaparkan oleh ID-CERT belum terdeteksi, di tahun 2016 laporan yang diterima oleh ID-CERT terkait kejahatan siber lebih kepada Komplain Spam, Malware, Network Incident, Spam, Spoofing/Phishing, dan IPR (*Intellectual Property Rights*) (*ID-CERT*, n.d.). Pada tahun 2017 berdasarkan pada monitoring yang dilakukan oleh Gov-CSIRT selaku Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah, kasus phishing yang terdeteksi yakni sebanyak 68 kasus, dengan kasus web defacement sebanyak 879 kasus, kemudian untuk kasus *malware* selama tahun 2017 berdasarkan pemantauan yang dilakukan oleh Id-SIRTII yakni sebanyak 36.423.737 serangan *malware* (*Laporan Kinerja Lembaga Sandi Negara Dan BSrE Tahun 2017*, 2018).

Pada tahun 2018 berdasarkan laporan yang diterima oleh BSSN melalui badan ID-SIRTII terdapat 2.885 laporan terkait serangan siber, salah satunya *malware* sebanyak 122.437.819 yang dilakukan pada website dan aktivitas *malware* pada honeypot (BSSN (ID-SIRTI/CC), 2018). Berdasarkan Laporan Tahunan Indonesia *Cyber Security* 2019 oleh BSSN, beberapa kejadian penting terhadap keamanan siber juga terjadi, salah satunya beberapa peretasan oleh website resmi di Indonesia pada rentang bulan September hingga Desember, diantaranya website DPR, website Kemendagri, Website KPAI, website BMKG, website Pengadilan Negeri Jakarta, website Bareskrim Polri serta website Bawaslu Jakarta Pusat (BSSN, 2019). Pada tahun 2019, telah terdeteksi serangan sebesar 12.579.480 terhadap web server yang dimana serangan tersebut termasuk dengan serangan web defacement, phishing serta infeksi malware, sepanjang tahun 2019 dari bulan Januari hingga Desember telah tercatat serangan malware sebesar

105.154.900 (BSSN, 2019). Kejahatan siber yang terjadi di Indonesia ini terus meningkat hingga di tahun 2020 saat Covid-19 memasuki negara Indonesia, pada masa pandemi ini internet menjadi sasaran empuk bagi para *hacker,* hal tersebut dikarenakan tidak sedikit masyarakat Indonesia yang melakukan WFH (Work From Home) dengan menggunakan internet sebagai media utama dalam membantu melaksanakan pekerjaan. Menurut laporan BSSN, pada bulan Maret 2020 terdapat 22 jenis serangan siber dengan faktor pandemi Covid-19 diantaranya adalah jenis *ransomware, trojan* dan *Covid 19 Tracker Apps* (BSSN, 2020).

Meski telah mengalami banyak ancaman dan serangan siber, Menurut data GCI (Global Cybersecurity Index) pada tahun 2020 keamanan siber di Singapura berada di posisi pertama Asia Tenggara dengan skor 98,52 dari skala 0-100 (Kusnandar, 2022). Singapura sebagai negara dengan posisi pertama di Asia Tenggara terhadap keamanan siber menunjukkan kekonsistenan serta keseriusan negara Singapura dalam menanggapi serangan siber. Sedangkan Indonesia berdasarkan data Global Cybersecurity Index (GCI) pada tahun 2020 Indonesia menduduki peringkat nomor tiga di Asia Tenggara dalam *cyber securitynya* dengan skor 94,88 dari skala 0-100, yang menunjukkan berada di bawah Singapura setelah Malaysia (Kusnandar, 2022).

Global Cybersecurity Index telah mengkategorikan negara-negara anggota yang berkomitmen terhadap keamanan siber kedalam tiga kategori berdasarkan Global Cyber Index mereka, diantaranya *Initiating* (tahap inisiasi) tahap yang menunjukkan skor GCI kurang dari persentil ke-50 yakni mulai membuat komitmen terhadap keamanan siber, *Maturing* (tahap pendewasaan) tahap yang

menunjukkan skor GCI antara persentil ke-50 serta ke-89 yakni mulai mengembangkan komitmen kompleks, serta terlibat dalam program keamanan siber maupun inisiatif, *Leading* (tahap terdepan) tahap yang menunjukkan skor GCI pada persentil ke-90 yakni menunjukkan komitmen tinggi terhadap lima pilar indeks (ITU-D, 2017). Berdasarkan Global Cybersecurity Index tersebut Singapura termasuk dalam negara *leading* dalam keamanan sibernya, sedangkan Indonesia masih masuk dalam kategori *maturing* yang berada dalam persentil ke-50 serta ke-89, dengan begitu maka Indonesia perlu mempelajari strategi serta upaya Singapura dalam meningkatkan keamanan sibernya.

Penulisan ini akan membahas lebih dalam terkait pembangunan kapasitas cybersecurity di negara ASEAN dengan mengkomparasikan antara negara Singapura dan Indonesia. Penulis akan mengaitkan penelitian ini dengan beberapa karya ilmiah terdahulu atau beberapa data yang berkaitan dengan penelitian ini sehingga dapat membantu penulis dalam melaksanakan penelitian. Adapun karya ilmiah dan data yang penulis gunakan yakni sebagai berikut :

Jurnal Milik I Wayan Midho, Yono Reksoprodjo, Hamzah Zaelani dengan judul : "PEMBANGUNAN KAPASITAS CYBER SECURITY DI NEGARA ASEAN: ANALISIS KOMPARATIF TERHADAP BRUNEI DAN INDONESIA" tahun 2020. Dalam jurnal ini membahas terkait analisis komparatif *cyber security* Indonesia dengan Brunei Darussalam, dalam jurnal ini bentuk pembangunan kapasitas *cyber security* Brunei Darussalam dilakukan melalui pembentukan badan di bawah Menteri Keuangan dengan nama ITSSD (Information Technology and States Stores Department), pada tahun 2004 Brunei Darussalam membentuk BruCERT (Brunei Computer Emergency Response Team) yang bertugas dalam

memberikan pengamanan terhadap ancaman siber, sedangkan Indonesia dalam pembangunan kapasitas cybersecuritynya melakukan pembentukan kebijakan dengan memberikan kepastian hukum melalui Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet serta melakukan pembentukan ID-SIRTII yang berfungsi untuk melakukan pemantauan, deteksi dini, koordinasi dengan pihak lain dalam melakukan pengamanan jaringan. Berdasarkan jurnal tersebut penulis menyimpulkan bahwa Indonesia masih perlu meningkatkan kapasitas cybersecuritynya salah satunya dalam kepastian hukumnya.

Dari adanya tinjauan pustaka diatas maka didapatkan persamaan serta perbedaan yang peneliti lakukan dalam meneliti. Letak persamaannya yakni sama-sama membahas terkait analisis komparatif *cyber security*, sedangkan penelitian ini akan membahas terkait analisis komparatif *cyber security* Indonesia dengan Singapura.

1.2 Rumusan Masalah

Mengangkat terkait upaya Singapura dan Indonesia dalam mengurangi kasus kejahatan siber, berdasarkan latar belakang yang telah diuraikan maka rumusan masalah dalam penulisan ini adalah “bagaimana upaya keamanan siber yang dilakukan oleh Singapura serta Indonesia pada tahun 2016-2021?”

1.3 Tujuan Penelitian

Tujuan dari penelitian ini untuk menganalisis bentuk keamanan siber Singapura dan indonesia sebagai upaya dalam menghadapi kejahatan siber, dengan

tujuan khusus untuk mengetahui dimanakah letak kekurangan Indonesia dalam meningkatkan keamanan sibernya.

1.4 Kerangka Pemikiran

1.4.1 Cyber Crime

Cyber crime merupakan kejahatan yang menjadikan teknologi sebagai alat atau sasaran dalam berlangsungnya kejahatan tersebut (Arifin, n.d.). Menurut Zaenal Arifin dalam modulnya yang berjudul Keamanan dan Ancaman pada Cyberspace ,terdapat beberapa ruang lingkup serta jenis dalam cybercrime, diantaranya, Komputer serta perangkat dan data-data yang ada dalam komputer digunakan sebagai objek penyalahgunaan seperti dimodifikasi, dihapus, diubah maupun diduplikasi secara tidak sah, komputer menjadi instrumen dalam melakukan tindak kejahatan seperti halnya pencurian, penipuan serta pemalsuan, Penggunaan data atau komputer secara ilegal atau tidak sah, pengungkapan, akuisisi, serta penyalahgunaan hak akses dengan cara yang ilegal.

Cybercrime juga dibagi menjadi beberapa jenis yakni cybercrime berdasarkan motif dan cybercrime berdasarkan sasaran, jika dilihat berdasarkan motif, cybercrime terbagi menjadi dua yakni sebagai tindakan kriminal murni yang dimana kejahatan tersebut dilakukan secara sengaja dengan memanfaatkan internet sebagai tempat kejahatan, sedangkan yang kedua cybercrime bisa dianggap sebagai tindakan kejahatan “abu-abu” yang mengartikan bahwa kejahatan tersebut masih sulit dikatakan sebagai tindak kejahatan kriminal karena kejahatan yang dilakukan motifnya belum tentu untuk berbuat kejahatan (Arifin, n.d.). Berdasarkan sasarannya jenis-jenis cybercrime terbagi menjadi tiga, cybercrime dengan sasaran hak cipta, cybercrime dengan sasaran hak cipta ini dilakukan

melalui penyerangan dengan tujuan materi atau non materi terhadap hasil karya dengan menggandakan, memasarkan, mengubah hasil karya. Cybercrime sasaran Individu, sasaran individu ini dilakukan dengan motif dendam seseorang yang bertujuan untuk merusak nama baik. Ketiga yakni cybercrime dengan sasaran pemerintah, cybercrime dengan sasaran pemerintah ini dilakukan dengan motif membajak, melakukan teror serta merusak keamanan dengan tujuan untuk menghancurkan citra institusi pemerintah (Arifin, n.d.).

1.4.2 Kebijakan Komparatif (*comparative policy*)

Kebijakan publik komparatif atau Comparative Public Policy merupakan bidang studi interdisipliner yang memanfaatkan kebijakan publik sebagai analisis utama untuk membandingkan antara sistem serta institusi yang berbeda, pada negara atau pemerintahan (Wong, 2016). Dalam kebijakan publik komparatif ini biasanya menanyakan terkait bagaimana, mengapa serta apa perbedaan pengaruh pemerintah dalam menerapkan kebijakan yang serupa maupun tidak serupa. Selain untuk membandingkan serta mengkategorikan kebijakan publik berdasarkan isinya, analisis kebijakan juga menyelidiki proses pembuatan kebijakan dalam upaya untuk membangun model teoritis terkait bagaimana kebijakan sebenarnya terbentuk (Krupavičius et al., 2013). Menurut Christoph Knill dan Jale Tosun (2011:375) dalam (Krupavičius et al., 2013) model utama yang ditemukan dalam literatur kebijakan publik ialah 1) rasional, 2) inkremental serta 3) model proses, model-model tersebut bersifat saling melengkapi dikarenakan model ini lebih berfokus terhadap berbagai aspek kehidupan politik serta berkonsentrasi terhadap karakteristik kebijakan yang berbeda. Kebijakan publik komparatif dengan politik komparatif merupakan bidang studi yang berbeda namun saling berkaitan karena

memiliki elemen yang bertumpang tindih (Wong, 2016) menurut salah satu ilmuwan politik Amerika Robert Dahl berpendapat bahwa inti dari politik komparatif yakni studi terkait distribusi kekuasaan dalam pengambilan keputusan, namun disisi lain menurut Jean blondel objek utama dalam politik komparatif adalah kebijakan publik maupun hasil dari tindakan politik (Krupavičius et al., 2013). Pada umumnya seluruh Negara menghadapi masalah yang sama, hanya saja yang berbeda yakni dalam merespons masalah tersebut. Suatu kebijakan juga dapat menimbulkan dampak yang berbeda dikarenakan tergantung terhadap tujuan, pendekatan, serta lingkungan yang diharapkan, menurut teori sistem menyatakan bahwa pembentukan kebijakan publik tidaklah dapat dilepaskan dari adanya pengaruh lingkungan (Mustari, 2015)

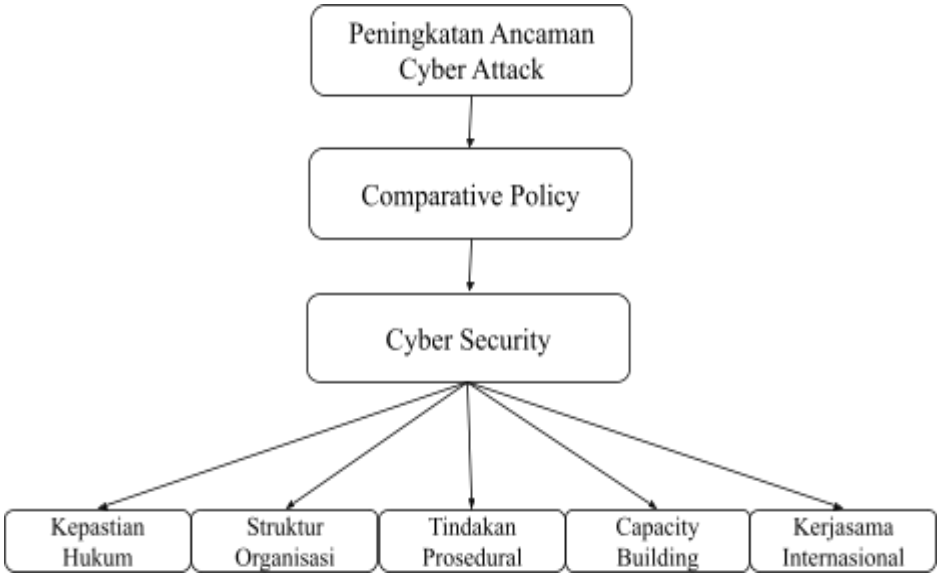
1.4.3 Cyber Security

Cyber security merupakan bagian dari keamanan informasi melalui perlindungan sistem yang terhubung dalam perangkat keras termasuk program, perangkat lunak serta data dari potensi serangan siber, cybersecurity memiliki peran yang besar dalam melindungi data yang bersifat informasi sensitif dalam bidang pemerintahan, militer, maupun perusahaan swasta (Arifin, n.d.).

Cyber security sendiri merupakan upaya dalam memastikan pencapaian maupun pemeliharaan sifat keamanan organisasi serta aset pengguna dalam Global cyber-security, Global *cyber security* sendiri dibangun diatas lima bidang kerja diantaranya Kepastian Hukum, Struktur Organisasi, Capacity Building, Kerjasama Internasional, dan Tindakan Prosedural (Ardiyanti, 2014). Pada bidang kepastian hukum dapat dilihat dari adanya Undang-Undang yang mengatur dalam kasus siber atau Undang-Undang *Cybercrime.* Pada bidang kerja struktur organisasi

dalam global *cyber security* sendiri dapat dilihat melalui struktur organisasi suatu negara terkait siber, adakah pembentukan lembaga negara yang mengatur terkait masalah *cyber* serta saling bertumpang tindih atau tidak. Bidang kerja capacity building, bidang ini dapat dilihat melalui bagaimana bentuk peningkatan kapasitas tiap negara terkait keamanan siber ini, bisa dilihat melalui program pelatihan serta pendidikan yang diberikan, kemudian pembentukan badan siber di tiap negara. Selanjutnya pada bidang Kerjasama Internasional, pada bidang ini dapat dilihat melalui langkah kedua negara melalui adanya kerjasama serta jaringan berbagi informasi dan yang terakhir yakni pada bidang tindakan prosedural, dalam bidang ini dapat dilihat melalui kerangka kerja ataupun strategi tiap negara terhadap keamanan sibernya (Ardiyanti, 2014).

1.5 Sintesa Pemikiran



Bagan 1.1 Sintesa Pemikiran
Sumber: Olahan Penulis

Semakin meningkatnya kejahatan siber dari tahun ketahun, kedua negara telah berupaya dalam meningkatkan keamanan sibernya. Dengan adanya upaya peningkatan keamanan siber kedua negara, penulis melihat upaya kedua negara dalam meningkatkan cyber securitynya melalui *comparative policy* yang dilihat dari bidang kerja kedua negara terhadap, Kepastian Hukum, Struktur Organisasi, Tindakan Prosedural, Capacity Building, dan Kerjasama Internasional. Dengan adanya komparasi politik berdasarkan lima bidang kerja ini dapat dilihat seberapa jauh kedua negara dalam meningkatkan keamanan sibernya.

1.6 Argumen Utama

Berdasarkan pada data serta pemikiran yang telah dianalisis sebelumnya, dengan begitu penulis menyimpulkan argumen utama dalam penelitian ini adalah dalam meningkatnya kasus kejahatan siber di negara ASEAN, Singapura dan Indonesia melakukan upaya yang besar dalam menciptakan keamanan siber. Jika dilihat berdasarkan lima bidang kerja sebelumnya yakni Kepastian Hukum (Undang-Undang *Cybercrime*), Struktur Organisasi, *Capacity Building*, Kerjasama Internasional serta tindakan Prosedural, kedua negara telah memenuhi lima bidang kerja diatas dalam meningkatkan keamanan sibernya. Perbedaannya, di Indonesia memiliki kelemahan pada 4 indikator diantaranya, dalam indikator Kepastian Hukum, kedua negara telah membentuk Undang-Undang terkait siber, namun Undang-Undang yang dibentuk oleh Indonesia lebih umum, dan masih berfokus terhadap tindak pidana kejahatan siber seperti halnya pencemaran nama baik, atau perjudian, berbeda dengan Undang-Undang yang dibentuk oleh Singapura lebih jelas dalam Bagian-bagiannya mencakup khusus terkait Keamanan Siber. Untuk

indikator Struktur Organisasi Indonesia juga masih bertumpang tindih, Tindakan Prosedural di Indonesia masih belum memberikan perhatian lebih terhadap perusahaan-perusahaan lokal maupun UKM, dan dalam pilar Capacity Building Indonesia masih melalui kegiatan webinar,seminar yang dilakukan dengan negara lain, Indonesia juga belum memiliki badan sertifikasi sendiri yang diakui oleh 30 negara untuk meningkatkan kapasitas SDM-nya. Sedangkan, dalam indikator Kerjasama Internasional, Indonesia sudah memenuhi dalam pelaksanaan kerjasama atau berbagi informasi.

1.7 Metode Penelitian

1.7.1 Tipe Penelitian

Tipe penelitian ini adalah deskriptif komparatif. Penelitian komparasi menurut Dra. Aswani Sudjud dalam buku (Anggara, 2015) merupakan penelitian yang dapat menemukan persamaan serta perbedaan tentang benda, orang, ide, prosedur kerja, serta kritik dalam kelompok atau prosedur kerja. Penelitian dengan deskriptif komparatif merupakan penelitian yang menggambarkan atau menerangkan gejala melalui variabel-variabel yang digunakan untuk mengetahui perbedaan (Saputra, 2016).

1.7.2 Jangkauan Penelitian

Dalam membatasi penelitian yang akan dijelaskan, jangkauan penelitian penulis membatasi bentuk *cyber security* Singapura dan Indonesia selama 2016-2021, dikarenakan pada tahun 2016 hingga 2021 kedua negara melakukan beberapa inisiasi dalam meningkatkan keamanan sibernya, salah satunya pada pembentukan badan siber serta pembentukan Undang-Undang. Pada tahun 2020

dan 2021 kedua negara melakukan pembaharuan terkait strategi cyber securitynya, khususnya Singapura melakukan pembaharuan strategi cyber security di tahun 2021 dan Indonesia di tahun 2020. Selain itu pada tahun 2021 merupakan tahun pasca COVID-19 terjadi, berdasarkan laporan tahunan kedua negara pada saat COVID-19 kejahatan siber menunjukkan peningkatan yang pesat. Sehingga penelitian ini dilakukan hingga tahun 2021 untuk mengetahui bentuk *cyber security* kedua negara pasca peningkatan yang pesat.

1.7.3 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini penulis akan menggunakan pengumpulan data dalam bentuk data sekunder dan primer, data sekunder yakni data yang telah tersedia sebelumnya melalui sumber tidak langsung atau tangan kedua, contohnya sumber tertulis milik pemerintah atau perpustakaan, sedangkan data primer merupakan data yang mengacu pada pengumpulan data secara langsung (Hardani et al., 2020, 401) dari website dan report resmi badan siber serta jurnal.

1.7.4 Teknik Analisis Data

Teknik analisis data dalam penelitian ini yakni analisis kualitatif, penulis menggunakan data-data terkait *cyber security* kedua negara yang didasari dengan pendekatan analisis kualitatif. Analisis data dilakukan dengan maksud untuk mengetahui bagaimana strategi kedua negara dalam meningkatkan cybersecuritynya yang kemudian hasilnya akan dikomparasikan dengan maksud untuk mengetahui dimanakah letak kekurangan Indonesia dalam meningkatkan cybersecuritynya. Data yang didapatkan melalui jurnal, penelitian, buku, media pemerintahan resmi, serta situs internet yang berkaitan dengan penelitian ini.

1.8 Sistematika Penelitian

Sistematika penelitian ini ditulis secara sistematis yang terdiri dari beberapa bab yaitu :

BAB I : Memuat Pendahuluan, Latar Belakang Masalah, Tinjauan Pustaka, Rumusan Masalah, Tujuan Penelitian, Kerangka Pemikiran, Sintesa Pemikiran, Argumen Utama, dan Metode Penelitian.

BAB II : Upaya Keamanan Siber Pemerintah Singapura pada tahun 2016-2021.

BAB III : Upaya Keamanan Siber Pemerintah Indonesia pada tahun 2016-2021.

BAB IV : Kesimpulan dan Saran.