BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan siber adalah tema sentral kebijakan internasional abad ke-20, dengan dampak yang kuat di berbagai bidang seperti keamanan nasional dan kebijakan luar negeri negara-bangsa. Keamanan siber telah melampaui batas-batas nasional dalam berbagai hal: Infrastruktur teknis internet memiliki cakupan global, tindakan ancaman yang berbasis di satu negara dapat menyamarkan identitas mereka dengan mengambil alih komputer di negara lain, bisnis global menjual perangkat lunak, perangkat keras, dan layanan keamanan yang dapat memperkenalkan atau memerangi kerentanan, dan konsekuensi dari serangan yang mengganggu dapat menyebar jauh melampaui korban awal. Bahkan negara yang paling paham dunia maya tidak bisa melindungi dirinya sendiri sepenuhnya terkecuali jika ingin memutuskan sambungan dari internet global dan secara ketat membatasi siapa yang dapat menggunakan teknologi informasi dan untuk tujuan apa di dalam perbatasannya sendiri. Dan tindakan ini tidak mungkin dilakukan karena akan mengakibatkan konsekuensi yang mengerikan bagi ekonomi nasional, militer, dan semua sistem lain yang bergantung pada teknologi informasi canggih. Kerja sama internasional untuk meningkatkan keamanan siber adalah jalan yang jauh lebih realistis dan layak[1].

Konsep keamanan telah diselaraskan dengan perkembangan posisi teoritis utama Hubungan Internasional. Beginilah, mulai dari posisi realistis dan neorealis, keamanan berputar di sekitar Negara sebagai aktor kesatuan. Dari perspektif ini, Negara memiliki

[1] Hitchens, Theresa, et,al. 2017. International cybersecurity infotmation sharing agreements. Maryland: center of international & security studies.

monopoli atas penggunaan kekuatan, yang melaluinya ia berhasil memenuhi kepentingannya dan menjamin kedaulatan atau kelangsungan hidupnya dalam sistem anarkis. Kekuatan memiliki hubungan langsung dengan kekuasaan dalam hal material; oleh karena itu, langkah-langkah rasional Negara akan diarahkan pada pengejaran kekuasaan dan, sebagai konsekuensinya, pada keamanan dalam istilah militer[2]. Ketidak seimbangan daya dalam sistem memberikan keamanan yang lebih besar untuk beberapa dan lebih sedikit untuk yang lain.

Konfigurasi tatanan internasional saat ini dan perilaku para aktor yang membentuknya telah mendorong topik studi baru yang menarik bagi Hubungan Internasional, keamanan dan hak asasi manusia. Kemajuan teknologi dan pesatnya perkembangan internet telah menciptakan skenario sibernetik yang di dalamnya terdapat ancaman dan risiko bagi mereka yang berinteraksi dengannya. Realitas ini tidak asing bagi Amerika Latin khususnya negara pada wilayah tersebutv yang masih minim perlindungan hukum di dunia maya seperti contohnya Meksiko dan Brasil ini. Negara-negara yang membentuknya harus melakukan langkah-langkah keamanan siber yang mengurangi cakupan ancaman yang luas dan keragaman sumbernya yang besar.

Perkembangan teknologi, perluasan Internet yang cepat dan peningkatan Teknologi Informasi dan Komunikasi (TIK), mendorong terciptanya ruang baru untuk interaksi sosial dan negara yang fondasinya dibentuk oleh hubungan antara komputasi dan jaringan. Dunia maya baru ini telah menjadi prioritas keamanan nasional bagi sebagian besar negara di dunia. Dunia maya atau *Cyberspace* menyediakan alat yang berfungsi sebagai mekanisme baru untuk melakukan tindakan terlarang atau kriminal,

[2] Morgenthau, Hans J. "Politics among nations: The struggle for power and peace". New York: A.A. Knopf, 1948.

menghasilkan ancaman signifikan terhadap keamanan negara. Sistem Internasional dan negara-negara yang menyusunnya telah, dalam beberapa kesempatan, menjadi saksi serangan terhadap keamanan suatu Negara melalui cara sibernetik.

Phishing atau pengelabuan merupakan sebuah jenis serangan rekayasa sosial yang sering digunakan untuk mencuri data pengguna, termasuk kredensial login dan nomor kartu kredit. Itu terjadi ketika penyerang, menyamar sebagai entitas tepercaya, menipu korban untuk membuka email, pesan instan, atau pesan teks. Penerima kemudian ditipu untuk mengeklik tautan berbahaya, yang dapat menyebabkan pemasangan perangkat lunak perusak, pembekuan sistem sebagai bagian dari serangan ransomware, atau pengungkapan informasi sensitif.

Sebuah serangan dapat memiliki hasil yang menghancurkan. Untuk individu, ini termasuk pembelian tidak sah, pencurian dana, atau pencurian identitas. Selain itu, phishing sering digunakan untuk mendapatkan pijakan di jaringan perusahaan atau pemerintah sebagai bagian dari serangan yang lebih besar, seperti peristiwa ancaman persisten tingkat lanjut [3].

Organisasi Perserikatan Bangsa-Bangsa telah memperlihatkan cakupan yang luas dari serangan yang bersifat sibernetik, ancaman aktual dan potensial terhadap keamanan informasi adalah beberapa masalah paling serius di abad ke-21. Ancaman berasal dari berbagai sumber dan bermanifestasi sebagai aktivitas destabilisasi yang ditujukan sama terhadap individu, bisnis, elemen infrastruktur nasional, dan pemerintah. Efeknya menimbulkan risiko yang cukup besar terhadap keamanan publik, keamanan negara dan stabilitas masyarakat internasional secara keseluruhan[4].

[3] Imperva, Phising Attack. Melalui https://www.imperva.com/learn/application-security/phishing-attack-scam/ pada 20 Maret 2022.
[4] PBB, 2010. ”Group of Government Experts on Developments in the Field of Information and Telecomunications in the Context of International Security”.

Ancaman dan kerentanan sosial dan negara yang bersifat sibernetik bukanlah kasus yang terisolasi. Negara-negara dengan pertumbuhan teknologi tercepat dan terpenting telah menjadi negara asal dengan jumlah serangan siber terbesar di dunia.

Di antara daftar negara asal serangan siber adalah Amerika Serikat, Prancis, Rusia, Cina, dan Argentina. Negara-negara ini jelas berbeda dalam aspek sosial, ekonomi atau budaya; namun, mereka menganggap pengembangan tindakan keamanan aktif dan reaktif penting dalam domain siber[5]. Demikian pula, kompleksitas yang dibenamkan dalam serangan siber terhadap keamanan nasional membuatnya perlu untuk memahami apa yang tercakup dalam ruang siber. Kemampuannya telah memungkinkan aktor publik dan swasta untuk memanfaatkan keuntungan relatif mereka untuk mempengaruhi keamanan siber di negara-negara kurang berkembang di bidang ini.

Mencegah adanya kejahatan siber merupakan sebuah bagian integral dari keamanan siber nasional dan informasi penting strategi perlindungan. Hal ini termasuk mengadopsi undang-undang yang sesuai di tingkat nasional serta di tingkat internasional. Di sebagian besar laporan, panduan atau publikasi *cybercrime* atau kejahatan dunia maya didefinisikan oleh istilah "kejahatan komputer" dan "kejahatan dunia maya". Istilah kejahatan siber memiliki arti yang sempit dibandingkan kejahatan yang berhubungan dengan komputer, karena harus melibatkan adanya jaringan komputer. Sedangkan kedua definisi dikembangkan melalui kongres Perserikatan Bangsa-Bangsa mengenai pencegahan kejahatn dan pelaku terhadap pelanggar[6]. Kejahatan dunia maya dalam arti sempit mencakup setiap perilaku yang ilegal yang diarahkan melalui operasi elektronik yang menargetkan kemanan sistem komputer dan

[5] Ibid.

[6] Gercke, M. 2012. Understanding cybercrime: Phenomena, challenges and legal response. The ITU publication.

juga sistem data telah diproses oleh pelaku kejahatan[7]. Kejahatan dunia maya mencakup setiap perilaku ilegal yang dilakukan dengan cara menawarkan atau mendistribusikan sebuah informasi melalui sistem komputer atau sistem jaringan. Adapun definisi umum yang menggambarkan kejahatan dunia maya sebagai aktivitas apapun dimana komputer atau jaringan menjadi alat, target, atau tempat aktivitas kriminal. Tetapi definisi tersebut memiliki masalah misalnya, akan mencakup kejahatan seperti pembunuhan jika mungkin pelaku menggunakan perangkat elektronik untuk menghabisi nyawa korban.

Manusia merupakan sumber atau sebab utama mengapa kejahatan dunia maya bisa terjadi sampai saat ini. Dan juga manusia merupakan pengguna utama dunia maya, apabila tidak ada manusia dunia maya hanyalah sebuah ruang kosong tanpa ada penghuni. Terkecuali ada hal lain seperti pengambilan alih pemeliharaan dan pengembangan infrastruktur dan konten siber, namun tetap saja itu masih membutuhkan adanya tenaga dari manusia, dalam dunia maya manusia merupakan indikator utama dan penggerak[8].

Kejahatan siber biasa terjadi pada setiap negara bagian di wilayah Amerika Latin yang membangun struktur pemerintahan yang terkomputerisasi. Pengejaran kriminal tersebut terutama tersebar di manajemen dan sistem industri, perbankan dan kegiatan yang berhubungan dengan layanan internet. Terdapat berbagai aktivitas dan hasil yang dihasilkan dari penggunaan teknologi komputasi secara ilegal. Tingkat kejahatan komputer akan lebih tinggi di negara-negara maju, negara-negara maju ini telah mengumpulkan lebih banyak pengalaman dalam memerangi kejahatan dunia maya, dimana tipologi kejahatan komputer serta orang-orang yang melakukan kejahatan

[7] Kaur, N. Prevention and Control of Cyber Crimes. Journal of Computer Science and Engineering, 2016, hal 37.
[8] *Ibid.*

dipelajari dan dianalisis bersamaan dengan mengembangkan metedologi untuk kemamanan terhadap kejahatan tersebut. Istilah kejahatan komputer dan kejahatan dunia maya pertama kali muncul di sumber-sumber ilmiah AS pada tahun 50-60an di abad ke 20[9]. Bisa disimpulkan bahwa komputer adalah dan merupakan alat universal terbaik untuk melakukan kejahatan yang dimaksudkan.

Dari sudut pandang penulis, norma hukum yang berkaitan dengan kejahatan komputer pertama dikembangkan untuk memastikan adanya perlindungan terhadap informasi. Norma yang mengatur aspek hukum dari pengoperasian teknologi komputer termasuk dalam berbagai ilmu hukum.

Berbagai posisi teoritis memungkinkan kita untuk menjelaskan perilaku aktor internasional dalam menghadapi ancaman keamanan siber. Oleh sebab itu, memungkinkan mereka untuk memusatkan perhatian pada studi kasus ini. Penelitian kualitatif berusaha untuk memahami dan menjelaskan bagaimana agenda keamanan siber dibangun di dua negara Amerika Selatan. Untuk mencapai tahap ini, perlu mengidentifikasi faktor-faktor proses sekuritisasi, seperti aktor nasional dan internasional dan kepentingan mereka dalam agenda keamanan negara, berdasarkan persepsi mereka terhadap ancaman siber.

Saling ketergantungan dalam hal teknologi dan konektivitas negara-negara kawasan meningkatkan kerentanan negara-negara tersebut terhadap ancaman dunia maya, menciptakan semacam efek domino. Karena alasan inilah promosi kerja sama antara entitas pemerintah, masyarakat, dan lembaga internasional, yang berupaya membangun ruang siber yang aman, mempengaruhi agenda keamanan kawasan.

[9] Wild, Ch, et,al. 2011. Electronic and mobile commerce law: an analysis of trade, finance, media, and cybercrime in the digital age. Hertfordshire: University of Hertfordshire press.

Pentingnya keamanan regional telah mendorong literatur yang berfokus pada negara-negara Latin. Alasan utama mengapa hal ini semua penting karena pada wilayah Amerika Latin kekurangan sistem informasi dihampir semua negara Amerika Latin, salah satu contohnya pemerintah mengalami kesulitan bagaimana mengimbau masyarakat dalam pintar dalam memilah langkahnya dalam dunia maya sehingga minism terjadi kasus phising pada Amerika Latin[10]. Namun, telah difokuskan pada ancaman terhadap keamanan negara dengan persepsi sosial yang lebih besar, seperti perdagangan narkoba, perdagangan manusia atau penyelundupan, dan bahkan terorisme. Sementara topik ini akan terus menjadi penting untuk penelitian akademis, kita tidak bisa melupakan bidang keamanan negara lainnya. Dunia maya telah menjadi skenario baru untuk melakukan kejahatan dan domain baru konflik internasional; oleh karena itu, penting untuk menghasilkan masukan di bidang keamanan nasional lainnya. Hal ini akan memungkinkan untuk menghindari efek pada ruang siber, yang ditimbulkan oleh ancaman yang menyebabkan dampak yang signifikan terhadap Negara, institusinya, dan penduduk sipil pada umumnya[11].

Menurut laporan yang diterbitkan bulan ini oleh *Organization of American States* (OAS) dan perusahaan keamanan perangkat lunak Symantec, penculikan data akibat dari kejahatan dunia maya pertama kali terdeteksi pada tahun 2012. Sejak itu, praktik tersebut telah meningkat secara mengejutkan 500% dalam insiden global pada tahun 2013, dengan peningkatan yang sepadan di Amerika Latin. Tingkat pengguna internet di Amerika Latin dan Karibia adalah yang tumbuh paling cepat di dunia, dengan peningkatan 12% selama setahun terakhir saja. Aktivitas gelap dan

[10] Mayo, 2009. "La seguridad social en América Latina y el Caribe: una propuesta metodológica para su medición y aplicación a los casos de Argentina, Chile y Colombia" melalui https://www.cepal.org/es/publicaciones/3731-la-seguridad-social-america-latina-caribe-propuesta-metodologica-su-medicion pada 13 Jun 2022.
[11] Ibid.

kecanggihan teknologi yang digunakan oleh para penjahat siber ini telah meningkat secara paralel. Serangan Ransomware telah berkembang dan teknologi yang muncul untuk pembayaran online telah memfasilitasi praktik kriminal. Di Amerika Latin, peningkatan kejahatan ini pada tahun 2013 menyebabkan pasukan polisi Meksiko dan Brazil mengeluarkan peringatan yang dimaksudkan untuk memperingatkan pengguna Internet tentang situasi tersebut. Bentuk kejahatan yang paling sering terhadap individu adalah phishing dan pencurian identitas, dengan tujuan melakukan penipuan keuangan atau untuk digunakan di jejaring sosial. Penipuan bank juga meningkat secara signifikan, yang telah menghasilkan kerugian jutaan dolar, melebihi apa yang dilaporkan.

Beberapa investigasi yang dilakukan oleh organisasi internasional seperti Organisasi Negara-negara Amerika atau Organisasi Perserikatan Bangsa-Bangsa mengungkap pertumbuhan yang mengkhawatirkan dalam jumlah serangan dunia maya yang bertujuan untuk mempengaruhi infrastruktur penting dari sebuah negara. Penyerangan tersebut dilakukan oleh pelaku kejahatan yang berusaha memperoleh keuntungan ekonomi atau oleh individu dengan agenda politiknya sendiri dan bertentangan dengan lembaga pemerintah atau swasta.

Minimnya akademisi yang mengangkat isu ini dari Amerika Latin mengenai *cyber security* mendorong studi agenda *cyber security* negara-negara Amerika Latin untuk memahami bagaimana negara-negara ini telah melindungi kepentingan nasional mereka dan telah berusaha untuk menjamin keselamatan warga negara. Pentingnya strategi dan rencana keamanan siber menjadikannya mekanisme mendasar untuk pencegahan, penanganan, dan solusi dari segala pengaruh yang ditimbulkan melalui ruang siber. Strategi-strategi ini berupaya menghadapi ancaman keamanan siber, yang

dapat berdampak pada masyarakat sipil, lembaga publik dan swasta, lingkungan, dan bahkan ekonomi.

- **Meksiko**

Meksiko adalah negara di Amerika Latin dan Karibia yang paling terpengaruh dan rentan oleh kejahatan dunia maya. Meksiko menempati urutan kesembilan dalam hitungan yag dibuat oleh *FBI* (*Federal Bureau of Investigation*). Dalam daftar yang dikepalai oleh Inggris, Meksiko mendapatkan 216.000 insiden berada di atas negara-negara seperti Belgia, Brasil, Filipina, Italia, Spanyol, Belanda, Nigeria, Pakistan, China, Kolombia, Dan Hong Kong. FBI menjelaskan bahwa tiga kejahatan besar seperti Phishing, Ransomware, *Denial of Service* (DOS) yang dilaporkan oleh korban di seluruh dunia dan yang menempati urutan teratas pada tahun 2020 adalah penipuan *phishing*, penipuan di mana diperoleh non pengiriman dan pemerasan[12].

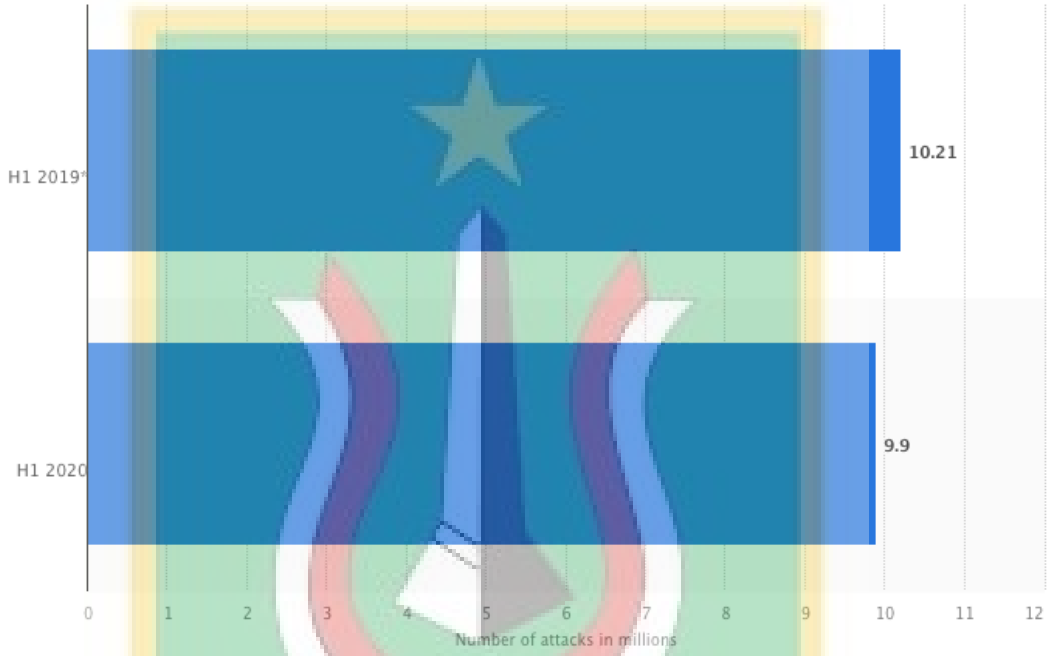
Di Meksiko ada lembaga yang bertanggung jawab atas keamanan yang memiliki area khusus untuk perhatian kejahatan dunia maya. Contohnya adalah Direktorat Ilmiah Garda Nasional. Juga di tingkat lokal, seperti halnya di Negara Bagian Meksiko, di mana Sekretariat Keamanan memiliki Polisi Siber yang bertugas mencegah dan menangani kejahatan siber. Namun, kurangnya kerangka hukum yang berfungsi untuk mengkoordinasikan kegiatan badan-badan tersebut dan yang menetapkan dasar untuk bertindak dalam kasus-kasus yang berbeda menyebabkan upaya-upaya tersebut menjadi terisolasi dan dilemahkan. Pada tahun 2020, Kamar Deputi mengumumkan bahwa undang-undang keamanan siber telah dibahas, tetapi sampai saat ini undang-undang tersebut belum dapat dilaksanakan[13]. Pada awal

[12] Adyrl Corral, 2021. "Mexico, en el top 10 de países victímas de ciberdelitos: ocupa el puesto 9, segun el FBI". Melalui https://www.milenio.com/policia/mexico-top-10-paises-victimas-delitos-ciberneticos-fbi pada 20 November 2021.

[13] Patricio garza, 2021. "La ciberseguridad en México: ¿una necesidad?". Melalui https://www.kas.de/es/web/mexiko/einzeltitel/-/content/la-ciberseguridad-en-mexico-una-necesidad pada 20 November 2021.

pertama tahun 2020, lebih dari 9,9 juta serangan komputer/jaringan di Meksiko. Namun jumlah ini menunjukan penurunan sekitar 3% dibandingkan dengan periode yang sama tahun sebelumnya, sekitar 10,2 juta serangan tercatat. Meksiko adalah salah satu negara dengan serangan siber terbanyak di Amerika Latin[14].

Gambar 1.1 Jumlah serangan di Meksiko 2019-2020



Sumber: https://www.statista.com/statistics/

- **Brasil**

Brasil merupakan rumah bagi berbagai kelompok penjahat dunia maya dengan taktik khusus, yang merupakan ancaman dunia maya yang dapat ditangani dengan spesialis pertahanan dunia maya dan respons insiden khusus Brasil. Target kejahatan dunia maya di Brasil tidak terbatas pada lembaga pemerintah dan organisasi besar. Warga biasa, pengunjung, dan usaha kecil dan menengah juga sering menjadi

[14] Statista Research Department, 2021. "Mexico: Registered number of malware attacks 2019-2020". Melalui https://www.statista.com/statistics/1179173/number-registered-malware-attacks-mexico/ pada 20 November 2021

sasaran.Pihak berwenang Brasil melaporkan lebih dari 100.000 kasus penipuan terkait internet pada tahun 2016, meskipun ini kemungkinan kecil.

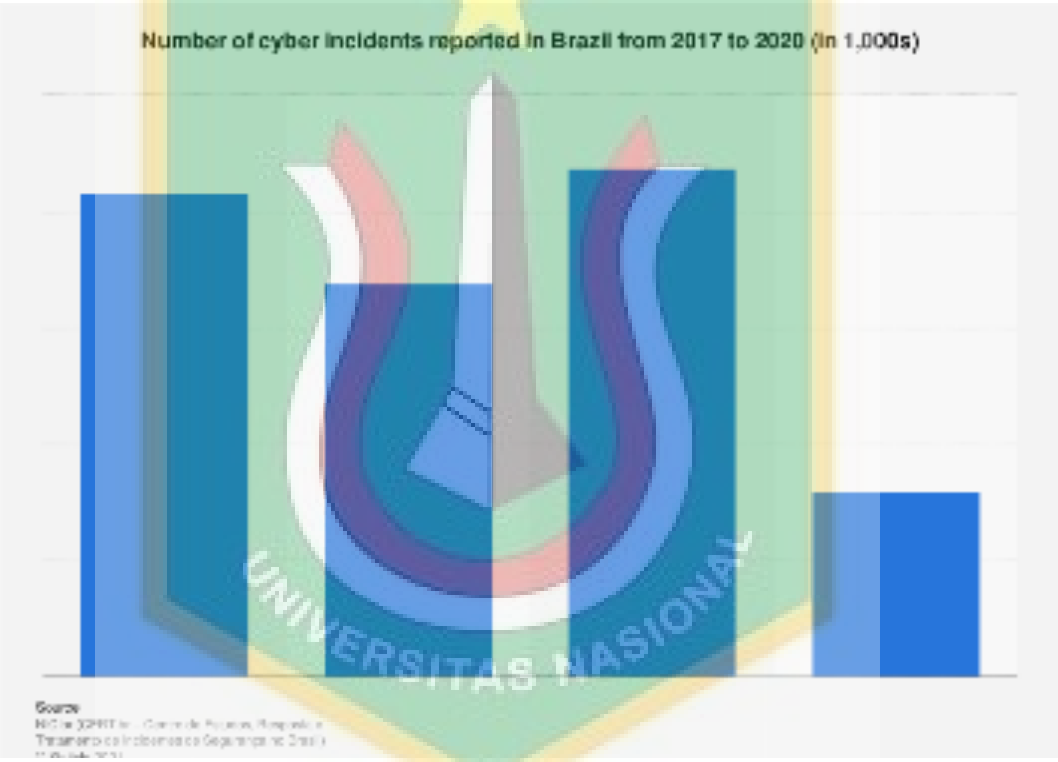
Menurut Federasi Bank Brasil, lebih dari 50% dari semua transaksi keuangan di Brasil dilakukan menggunakan perangkat yang terhubung ke internet, menghasilkan ruang lingkup yang signifikan untuk pencurian dunia maya. Brasil juga merupakan produsen dan pengekspor utama kejahatan dunia maya. Sebuah laporan baru-baru ini oleh *Symantec*, sebuah perusahaan keamanan siber, menempatkan Brasil di posisi ke-lima secara global setelah China, Amerika Serikat, Turki, dan Rusia dalam hal sumber malware, bot, spam, dan serangan phishing, dengan 5,4% deteksi ancaman global berasal dari negara tersebut[15].

Pemerintah Brasil mendiskusikan pembuatan strategi untuk mengatasi kejahatan di lingkungan digital. Presiden Federasi Bank Brasil (*Brazilian Federation of Banks*) Isaac Sidney, dan menteri kehakiman dan kemanana publik, Anderson Torres, memulai negosiasi untuk pembuatan strategi kejahatan dunia maya nasional. Idenya adalah untuk memperluas identifikasi dan penindasan para aktor yang bertanggung jawab atas kejahatan dunia maya. Dan tujuan lainnya adalah memperluas pengetahuan teknis pasukan keamanan Brasil dan mempromosikan kerjasama permanen antar agen publik dan swasta. Visi yang digariskan oleh asosiasi perbankan juga mencakup pengembangan bersama platform untuk berbagi data penipuan dengan cara digital dan mendukung pelatihan pasukan keamanan dalam masalah keamanan siber dan penipuan digital, dan menggunakan laboratorium kemanan siber. Rencana tersebut juga akan mencakup kampanye kesadaran tentang penipuan di dunia maya.

[15] Gabriel D. Lourenco, 2021. "Cybercrime in Brazil grow by 23% in 2021, research point out". melalui https://olhardigital.com.br/en/2021/08/31/seguranca/cibercrime-brasil-2021/ pada 9 November 2021.

Brasil menerbitkan kebijakan kemanan informasi nasional pertamanya pada tahun 2018. Srategi keamanan nasional untuk keamanan siber dan keamanan infrastruktur kritis diterbitkan pada tahun 2020 lalu[16]. Selama paruh pertama tahun 2020, warga Brasil melaporkan hampir 318.700 insiden siber. Hal ini kurang dari 37% dari 875.330 indsiden online yang tercatat sepanjang tahun 2019. Sumber lain memproyeksikan bahwa pendapatan *cyber security* di Brasil berjumlah lebih dari 4,7 miliar USD tahun 2020[17].

Gambar 1.2 Jumlah insiden siber Brasil 2017-2020



Sumber: https://www.statista.com/statistics/

Meksiko dan Brasil dipilih karena kedua negara tersebut merupakan negara dengan tingkat kriminalitas siber tertinggi di wilayah Amerika Latin, kemudian diikuti

[16] Angelica mari, 2021. "Brazil debates creation of national strategy to tackle cybercrime". Melalui https://www.zdnet.com/article/brazil-debates-creation-of-national-strategy-to-tackle-cybercrime/ pada 20 November 2021.
[17] Statista Research Department, 2021. "Brazil: Number of cyber incidents 2017-2020". Melalui https://www.statista.com/statistics/1225132/number-cyber-incidents-brazil/ pada 20 November 2021.

oleh Kolombia, data per-tahun 2021 Brasil mengalami serangan hampir 56%, kemudian Meksiko 27,8%. Selain phishing, ransomware, DoS dan DDoS (*Denial of Service*) dan serangan bertarget dengan malware juga merupakan ancaman yang mengkhawatirkan di kawasan ini[18]. Kedua negara ini juga sama-sama merupakan negara pengamat resmi pada konvensi budapest, kedua negara ini sedang berupaya agar Meksiko dan Brasil menjadi anggota Konvensi Budapest, tetapi saat ini kedua negara masih terhalang dalam penyesuaian undang-undang negaranya dengan undang-undang di Uni Eropa.

Munculnya dunia maya sebagai arena poltik internasional baru menyiratkan kemungkinan penggunanya untuk mengejar kepentingan tertentu Negara, aktor publik swasta atau individu melalui internet. Keamanan siber adalah isu baru yang menjadikannya penting dalam keamanan nasional dan politik internasional pada dekade terakhir abad ke-20. Sejak penciptaannya, pada tahun enam puluhan hingga tahun 2000, Internet dianggap sebagai ruang yang bebas dari campur tangan negara dan kebal terhadap kedaulatan yang akan mengubah arus informasi, mendemokratisasi pengetahuan, dan mengubah dinamika partisipasi warga. Periode ini yang mencakup tahun 1960 hingga 2000 didefinisikan sebagai fase akses terbuka dunia maya dan termasuk mempopulerkannya di masyarakat dan penggunaan yang semakin konstan dalam ekonomi, media, masalah pemerintah, dan bidang masyarakat lainnya.

Namun, dinamika yang berasal dari proses ini membuatnya menjadi area di mana campur tangan negara-bangsa tak terelakkan dan perlu[19]. Penting juga untuk dicatat bahwa selama tahun-tahun inilah Internet mengalami proses sekuritisasi, di

[18] MasContainer,2022. “Los países de Latinoamérica con más bajos estándares en ciberseguridad” melalui https://www.mascontainer.com/los-paises-de-latinoamerica-con-mas-bajos-estandares-en-ciberseguridad/ pada 13 Juni 2022.
[19] Palfrey, J. (2010). Four Phases of Internet Regulation. Social Research, 77(3): pp. 981-996.

mana negara-negara menekankan pada pembuatan definisi baru untuk membatasi kejahatan atau kegiatan terlarang yang dilakukan melalui platform ini atau digunakan untuk melakukannya.

Pada titik inilah dunia maya menunjukkan kapasitasnya untuk mengganggu keamanan publik dan kapasitasnya untuk berdampak pada keamanan nasional mulai dievaluasi, sehingga dianggap bahwa fase penolakan akses tidak menciptakan dengan demikian, tepi dan hambatan nyata pada Internet, tetapi itu mulai membatasi garis kontak geopolitik antara berbagai negara dalam kecenderungan politik, model ekonomi, dan kepentingan nasional mereka[20].

Penerapan luas internet telah menciptakan perkembangan positif dalam kehidupan sosial, seperti contohnya internet mampu menghubungkan satu daerah ke daerah lain meskupun memiliki jarak yang jauh. Namun dengan adanya internet ini hal tersebut bukanlah sebuah masalah lagi karena kita jadi mudah terhubung satu sama lain. Tampaknya mudah untuk memprediksi bahwa setiap orang akan memiliki kesempatan untuk menggunakan komputer dan jaringan global dalam waktu terdekat. Revolusi teknologi, tidak hanya mendorong kemajuan dalam masyarakat tetapi juga menjadi motivasi bagi proses dan perkembangan negatif yang sebelumnya tidak diketahui. Seperti banyak teknologi revolusioner lainnya, teknologi komputer memiliki potensi besar untuk kemajuan, serta penyalah gunaan.

Penggunaan teknologi informasi modern yang kompleks dan berskala besar membantu menggeser umat manusia ke tingkat perkembangan yang baru. Pada awalnya, komputer dimaksudkan sebagai gadget yang digunakan untuk tujuan

[20] Juan Manuel. 2021,"Challenge and opportunities in cybersecurity in latin america in the face of global context of cyberthreats to national security and foreign policy". Estudios Internacionales 198 (2021)–ISSN 0719-3769 • 169–197 Instituto de Estudios Internacionales–Universidad de Chile .

perhitungan dan komputasi. Namun, secara bertahap berubah menjadi alat yang unik dan luar biasa yang digunakan oleh umat manusia untuk memproses segala jenis informasi. Dunia modern menggunakan komputer untuk mengelola sistem perbankan, perusahaan, area pertahanan, pesawat ruang angkasa. Artinya tidak ada bidang kegiatan yang dijalankan oleh manusia tanpa menggunakan komputer. Ini adalah alat untuk membuat, mengumpulkan, menyimpan, memproses, dan mentransfer informasi.

Perkembangan komputer, teknik elektro dan globalisasi jaringan komputer yang berkelanjutan membawa banyak risiko sekaligus juga membawa manfaat. Jaringan komputer dan informasi elektronik juga dapat digunakan untuk melakukan tindak pidana dan bukti bahwa tindak pidana bisa disimpan disebuah jaringan. Masing-masing negara mengakui pentingnya kerjasama antar negara dan industri swasta dalam memperjuangkan melawan kejahatan dunia maya. Mereka percaya bahwa perjuangan yang efektif melawan kejahatan dunia maya membutuhkan kerja sama internasional yang mengikat[21].

1.2 Masalah Penelitian

Keamanan siber adalah tema sentral kebijakan internasional abad ke-20, dengan dampak kuat di berbagai bidang seperti keamanan nasional dan kebijakan luar negeri negara-bangsa. Kerja sama internasional untuk meningkatkan keamanan siber adalah jalan yang jauh lebih realistis dan layak. Perkembangan teknologi, pesatnya perkembangan Internet dan kemajuan Teknologi Informasi dan Komunikasi, mendorong terciptanya ruang-ruang baru untuk interaksi sosial. Dunia maya baru ini telah menjadi prioritas keamanan nasional bagi negara-negara di dunia. Dunia maya atau dunia maya menyediakan alat yang berfungsi sebagai mekanisme baru untuk melakukan tindakan terlarang atau kriminal, yang mengakibatkan ancaman signifikan

[21] Brenner, S. 2010. Cybercrime: Criminal threats from cyberspace. Santa Barbara: Praeger.

terhadap keamanan nasional. Meksiko dan Brazil adalah bukti nyata saat ini, kedua negara ini merupakan negara tertinggi kejahatan dunia maya di Amerika Latin. Oleh karena itu, kedua negara sedang mengembangkan undang-undang dan peraturan terkait keamanan siber.

1.2.1 Rumusan Masalah

Cyber security atau keamanan siber merupakan tema sentral kebijakan internasional abad ke-20, dengan dampak kuat di berbagai bidang seperti keamanan nasional dan kebijakan luar negeri negara-bangsa. Meksiko dan Brasil berada di peringkat 3 teratas di wilayah Amerika Latin dan diikuti oleh Kolombia dalam hal kejahatan dunia maya khususnya serangan *phishing*. Minimnya akademisi dari Amerika Latin meneliti terkait keamanan siber mendorong studi tentang agenda keamanan siber negara-negara Amerika Latin untuk memahami bagaimana negara-negara ini telah melindungi kepentingan nasional mereka dan berusaha memastikan keselamatan warganya. Kasus kejahatan siber ini marak terjadi di setiap negara di dunia yang baik masyarakat dan pemerintahnya terkomputerisasi, terkomputerisasi ini maksudnya ialah setiap aktivitas yang dilakukan dan didukung oleh teknologi, teknologi yang terhubung internet dan memungkinkan pengguna (manusia) bisa saling berinteraksi satu sama lain dengan mudah. Tetapi dari sisi positif yang dihasilkan, internet ini dimanfaatkan oleh orang yang tidak bertanggung jawab guna mendapatkan keuntungan yang mereka ingin capai. Dalam skripsi ini, penulis akan membahas kebijakan-kebijakan atau strategi dari wilayah Amerika Latin yang lalu kemudian strategi-strategi akan difokuskan ke negara Meksiko dan Brasil, strategi-strategi ini tercipta karena kejahatan siber merupakan

ancaman yang berpengaruh kepada keamanan nasional, oleh sebab itu penulis juga akan mengulas terjadinya kasus kejahatan siber di Meksiko dan Brasil pada 2019-2020 yang kemudian dianalisis menggunakan konsep keamanan dan teori sekuritisasi dan kepentingan nasional. Berdasarkan paparan diatas maka penulis merumuskan pertanyaan dalam penelitian skripsi ini sebagai berikut: **Bagaimana *cyber security* Meksiko dan Brasil berperan dalam menghadapi serangan phishing pada tahun 2019-2020?**

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian proposal skripsi ini, yaitu:

1.Mengetahui Mengapa Meksiko dan Brasil terjerat dari kejahatan di dunia maya, dan kebijakan apa yang akan mereka gunakan agar bisa meredam kasus kejahatan phishing akibat dari dunia maya?

1.4 Kegunaan Penelitian

Penelitian ini diharapkan memberikan manfaat baik secara teoritis maupun praktis, diantarannya sebagai berikut:

1.Sebagai pijakan dan juga refrensi pada penelitian-penelitian selanjutnya yang berkaitan dengan keamanan siber di wilayah Amerika Latin serta menjadi bahan kajian lebih lanjut.

2.Memberikan sumbangan pemikiran ilmiah dalam ilmu Hubungan Internasional, yaitu keamanan siber suatu negara atau wilayah.

3.Menambah wawasan tentang keamanan siber di wilayah Amerika Latin khususnya di negara Meksiko dan Brasil, serta mengetahui langkah-langkah yang dilakukan pemerintah dalam menangani kejahatan di dunia maya.

1.5 Sistematika Penulisan

Sistematika penulisan proposal skripsi ini dibagi menjadi beberapa tahapan-tahapan:

1.BAB 1: PENDAHULUAN

Bab ini berisi mengenai latar belakang penelitian ini, perumusan masalah, tujuan dari pelaksanaan penelitian dan juga sistematika penulisan proposal skripsi.

2.BAB II: KAJIAN PUSTAKA

Bab ini berisi tentang penelitian-penelitian terdahulu dari penelitian, pengertian kajian pustaka dalam penelitian, konsep kemanan, keamanan dalam Hubungan Internasional, teori dalam penelitian skripsi, dan juga kerangka pemikiran dalam penelitian skripsi.

3.BAB III: METEDOLOGI PENELITIAN

Bab ini berisi tentang pendekatan penelitian proposal, penentuan informan, teknik pengumpulan data penelitian, teknik pengolahan dan analisis data, dan lokasi dan juga jadwal penelitian.

4.BAB IV: PEMBAHASAN

Bab ini berisi pembahasan mengenai profil negara Meksiko dan Brasil, sejarah pembangunan internet di Amerika Latin, sejarah kejahatan siber, kejahatan siber dan keamanan siber, jenis-jenis kejahatan siber, keamanan siber dan hukum digital Amerika Latin, serta Meksiko dan Brasil dalam Konvensi Budapest.

5.BAB V: ANALISIS.

Bab ini berisi strategi keamanan Brasil dan Meksiko, kapasitas keamanan Brasil dan Meksiko, serta studi kasus pada tahun 2019-2020.

6.BAB VI: PENUTUP

Bab ini penulis akan mengemukakan kesimpulan dan saran yang diambil dari hasil penelitian untuk menjawab masalah dalam penelitian.