BAB II

KAJIAN PUSTAKA

2.1 Penelitian Terdahulu yang Relevan

Dalam kajian pustaka ini peneliti mencantumkan hasil-hasil penelitian terdahulu sebagai berikut:

1. Jurnal oleh Jorge Izaguirre Olmedo, (2018) dengan judul "*Análisis de los Ciberataques Realizados en América Latina*". Menganalisis untuk menentukan tingkat risiko dan persiapan dalam pertahanan siber yang dimiliki kawasan sedemikian rupa sehingga pedoman dapat ditetapkan untuk memerangi ancaman di masa depan berbagai jenis serangan siber dan tingkat kerusakannya juga ditentukan[1]. Jurnal oleh Jorge Izaguirre dirujuk karena terdapatnya kekurangan-kekurangan yang ada di negara-negara kawasan berkenaan dengan mekanisme pertahanan terhadap serangan siber. Dengan adanya penelitian ini, dapat digunakan sebagai titik tolak untuk analisis spesifik masing-masing negara dan penentuan tujuan pertahanan yang akan dilaksanakan. Perbedaan dalam penelitian ini tidak terfokus pada suatu negara Meksiko dan Brasil dan isu serangan phishing yang tidak terdapat pada penelitian ini, tidak terdapat kebijakan pemerintahan, dan juga konsep yang digunakan dalam penelitian.
2. Buku oleh Boris Saavedra, (2015) dengan judul "*Cyber security in Latin America and the Caribbean*". Menganalisis Di Amerika Latin, dunia maya rapuh dan rentan dalam ketersediaan, kerahasiaan, dan integritas. Untuk mengembangkan sistem keamanan siber yang mampu memastikan kontrol negara yang dapat diterima atas domain ini, model kemitraan publik-swasta harus digunakan. Partisipasi teknologi yang luar biasa,

[1] Jorgez Izaguirre Olmedo, 2018. "Análisis de los Ciberataques Realizados en América Latina". Revista de la universidad internacional, Ekuador Vol. 3, No.9 Hal 180-189.

dukungan sumber daya manusia dan keuangan di sektor swasta akan sangat berperan bagi pengembangan kapabilitas sesuai dengan ancaman dan tantangan yang harus dihadapi. Kerjasama adalah alat utama yang harus diterapkan jika kita ingin memiliki dunia maya yang kokoh dan kuat[2]. Buku oleh Boris Saavedra dirujuk karena pada penelitian ini merupakan pentingnya melakukan analisis pengalaman yang dikumpulkan oleh negara-negara di Amerika Latin dan Karibia yang telah berada di garda depan dalam mengembangkan strategi dan kegiatan terkait keamanan siber dengan tujuan untuk mempercepat penerapan langkah-langkah oleh mereka yang belum memilikinya. alat tersebut. Perbedaan penelitian terdapat pada metode, dimana metode yang digunakan ialah kuantitatif, tidak membahas isu phishing disuatu negara, tidak terdapat kebijakan pemerintahan, dan juga konsep yang digunakan dalam penelitian ini.

3. Buku oleh Sebastian Floderus, Linus Rosenholm (2019), dengan judul "*An educational experiment in discovering spear phishing attacks*". Menganalisis orang normal sebuah perusahaan besar berada pada risiko yang lebih tinggi dibandingkan masyarakat pada umumnya, serangan ini bertujuan untuk melakukan kebocoran data suatu perusahaan yang dimana hal tersebut bisa menjadi tombak yang tajam bagi perusahaan yang mengalaminya[3]. Buku oleh Sebastian Floderus dirujuk untuk sebagai arahan betapa kita sebagai masyarakat ataupun negara haruslah bersiap dalam perkembaga era digital, sehingga kita para pengguna internet bisa lebih siap dan bijak dalam era ini. Perbedaan terdapat pada konsep, dimana penelitian tidak menggunakan

[2] Saaverda, Boris. Cybersecurity in Latin America and the Caribbean. Washington DC: Cebter for Hemispheric Defense Studies, 2015.
[3] Floderus, Linus Rosenholm. An educational experiment in discovering spear phishing attacks. Sweden: Blekinge Institute of technology, 2019.

konsep kepentingan nasional, dan tidak adanya kebijakan dari pemerintah Meksiko dan Brasil dalam penelitian ini.

Novelty peneliti berdasarkan penelitian terdahulu diatas adalah; pada 3 penelitian diatas tidak adanya satupun memfokuskan pembahasan penelitian terhadap suatu negara di Amerika Latin seperti contohnya Brazil dan Meksiko ini, kemudian tidak ditemukan secara spesifik studi kasus yang menyangkut terhadap kebijakan di negara atau wilayah tersebut. Peneliti melihat hampir dari ke-3 penelitian terdahulu melihat kesamaan, yaitu mayoritas dari penelitian terdahulu ini menggunakan teori sekuritisasi dan konsep kemanan. Tetapi terdapat perbedaan, dimana teori yang digunakan pada penelitian terdahulu lebih berfokus pada sekuritisasi politik. Sedangkan pada penelitian ini, peneliti menggunakan sekuritisasi internet.[4].

2.2 Konsep dan Teori

2.2.1 Konsep Keamanan *cyber security*

Konsep keamanan diselaraskan dengan perkembangan posisi teoritis utama Hubungan Internasional. Negara mempunyai monopoli atas penggunaan kekuatan, keamanan berputar di sekitar negara sebagai aktor kesatuan. Secara etimologis konsep keamanan (*security*) berasal dari bahasa latin "*securus*" (*se* + *cura*) yang artinya merupakan terbebas dari bahaya, terbebas dari sebuah ketakutan. Kata ini juga bisa bermakna sebagai dari gabungan kata *se* yang berarti tanpa dan *curus* yang artinya rasa gelisah. Sementara itu dalam ilmu hubungan internasional, para sarjana hubungan internasional berpendapat bahwa konsep keamanan adalah sebuah konsep yang diperebutkan (*contested concept*). Sebuah pendekatan tradisional yang didominasi oleh mazhab Realisme menyatakan konsep keamanan adalah

[4] Palfrey, John G. 2010, "Four Phases of Internet Regulation", *Social Research,* Vol. 77, No. 3, Hal. 981-996.

sebuah kondisi yang terbebas dari ancaman militer datau kemampuan suatu negara untuk melindungi negara-bangsanya dari serangan-serangan militer yang asalnya dari lingkungan eksternal[5]. Secara tradisional, konsep keamanan selama ini memang hanya merujuk pada sifat ancaman yang bersifat militer semata sehingga responnya hanya bersifat militer dan hanya memfokuskan pada unit atau aktor negara.

Arus teoretis dalam hubungan internasional yang berbeda dan kapasitas penjelasannya mengenai realitas dunia memungkinkan kita untuk memahami kemanan siber dari posisis epistemologis tertentu. Masing-masing dari mereka telah mempresentasikan konsepsi mereka tentang ancaman dunia maya dan bagaimana menanggapinya. Dunia maya menjadi sebuah skenario dunia internasional yang baru, interaksi anarkis antarnegara yang tujuan utamanya adalah pencarian kekuasaan. Oleh sebab itu, kemanan siber adalah sebuah mekanisme pertahanan terhadap kemungkinan serangan siber dari pelaku kejahatan dunia maya. Untuk bisa mengamankan ruang siber, dari posisi militer, negara sedang mengembangkan sistem pertahanan siber dan memasukan skenario serangan siber dalam rencana strategis mereka[6]. Realisme berpandangan bahwa tujuan dari ancaman ialah kedaulatan dan keutuhan negara sebagai aktor utama dan kesatuan.

konsep keamanan siber dan keamanan nasional tersebut menggabungkan berbagai ancaman siber dan risiko siber, termasuk perang siber, konflik siber, terorisme siber, kejahatan siber, dan spionase siber serta

[5] Perwita, Agung Banyu. 2009. Dinamika Keamanan Dalam Hubungan Internasional Dan Implikasinya Bagi Indonesia. Bandung: Universitas Katolik Parahyangan.

[6] Kremer, Jens. 2014. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. Information & Communications Technology Law vol 23 (3) hal. 220-237.

konten siber, sementara konseptualisasi yang lebih sempit berfokus pada aspek yang lebih teknis terkait dengan keamanan jaringan dan komputer.

Keamanan siber telah menjadi bagian integral dari kebijakan dan doktrin pertahanan nasional dan luar negeri serta keamanan pemerintah, yang berkontribusi pada pembangunan keamanan siber sebagai domain perang baru. Upaya untuk mengembangkan aturan jalan untuk dunia maya fokus pada penerapan hukum internasional yang ada, potensi kesenjangan, pengembangan norma, langkah-langkah membangun kepercayaan, dan postulasi postur pencegahan. Akibatnya, kompleks rezim keamanan siber telah berkembang, mencakup berbagai institusi regional dan internasional yang memainkan peran penting dalam membentuk respons kebijakan[7].

Teknologi baru melahirkan kejahatan baru. Oleh karena itu, dengan penemuan komputer, kejahatan komputer menjadi tersebar luas. Perlu dicatat bahwa kejahatan dunia maya tidak memiliki batas. Di tingkat internasional, penting untuk melakukan koordinasi dengan berbagai mitra.

Dengan memprioritaskan ide, kebutuhan untuk mengkonsolidasikan identitas yang memungkinkan untuk menumbuhkan budaya keselamatan, membangun ide, nilai, dan institusi baru yang berfokus pada pengurangan risiko dan ancaman dari aktor internasional yang terlibat dalam sistem ditetapkan. Selain itu, untuk salah satu perwakilan terbesar dari konsep keamanan *cyber security*, ancaman sosial yang akan mewakili pengaruh terhadap keamanan adalah interaksi antara aktor yang menjadi struktur dengan keabadian mereka dalam waktu. Pendekatan yang lebih tradisional

[7] Reus-Smit, Christian. 2005. En Theories of International Relations. New York: Palgrave Macmillan.

berdasarkan asumsi realistis atau liberal tidak memungkinkan penjelasan yang memadai tentang perilaku Negara. Dengan memiliki fokus pada ide, tidak hanya mungkin untuk menjelaskan perilaku aktor[8].

Keamanan merupakan bentuk pembangunan kemanan sosial dari praktik yang berfokus pada ide dan minat tertentu. Tanpa skenario di mana interaksi antar para aktor menimbulkan risiko atau ancaman tidak akan ada kebutuhan untuk mengimplementasikan agenda keamanan atau menjalankan proses sekuritas. Masing-masing ingin bertahan hidup dan memiliki kapasitas materi tertentu, tetapi keduanya tidak memiliki kewajiban biologis atau domestik untuk mencari kekuasaan, kemuliaan, oleh sebab itu tidak ada sejarah keamanan dan ketidak amanan diantara keduanya. Konsep keamanan *cyber security* dirujuk untuk usulan baru dalam memahami realitas, realitas berdasarkan interaksi sosial dan ide-ide yang dihasilkan berdasarkan konsep dalam ilmu hubungan internasional. Konsep keamanan *cyber security* digunakan dalam penelitian ini untuk melihat bagaimana masalah kejahatan phishing ini mempengaruhi stabilitas politik dan sosial. Konsep keamanan Buzan, Weaver dan De Wilde menilai segala sesuatu jenis kejahatan atau ancaman yang bisa menganggu stabilitas negara bukan hanya dari sisi militer, tetapi mengganggu di stabilitas kemanan politik dan juga masyarakat. Phishing yang terjadi di Meksiko dan Brasil merupakan masalah serius yang harus segera ditangani baik dari pemerintah ataupun organisasi eksternal guna membantu menekan kejahatan siber di kedua negara tersebut.

[8] Hurd, Ian. 2008. En The Oxford Handbook of International Relations. Nueva York: Oxford University Press.

2.2.2 Kepentingan Nasional

Dalam konsep kepentingan nasional, negara sebagai aktor yang melakukan pengambilan keputusan dan juga berperan penting dalam hubungan antar negara berpengaruh terhadap jumlah penduduk negara tersebut. Kepentingan nasional tercipta karena adanya kebutuhan negara. Kepentingan juga dilihat dari adanya kondisi internal, baik politik maupun ekonomi, militer dan sosial budaya.

Kepentingan Nasional' adalah konsep kunci dalam Hubungan Internasional. Semua bangsa selalu terlibat dalam proses pemenuhan atau pengamanan tujuan kepentingan nasional mereka. Kebijakan luar negeri setiap negara dirumuskan atas dasar kepentingan nasionalnya dan selalu bekerja untuk mengamankan tujuannya. Ini adalah hak yang diterima secara universal dari setiap negara untuk mengamankan kepentingan nasionalnya. Suatu negara selalu berusaha untuk membenarkan tindakannya atas dasar kepentingan nasionalnya. Perilaku suatu negara selalu dikondisikan dan diatur oleh kepentingan nasionalnya. Oleh karena itu penting bagi kita untuk mengetahui pengertian dan isi dari Kepentingan Nasional. Hans J. Morgenthau dalam konsep kepentingan nasional (***interest***) diartikan ke dalam suatu kekuatan.

Kekuatan dan kekuasaan merupakan alat penting dalam mencapai kepentingan nasional. Kepentingan itu merupakan kebijakan negara yang didasarkan pada kepentingan yang relatif berkelanjutan yang terdiri dari tiga faktor, yaitu sifat kepentingan nasional yang dilindungi, lingkungan politik dalam pelaksanaan kepentingan itu, dan yang terakhir adalah kepentingan rasional. Kepentingan setiap negara dalam menjalankan identitasnya berguna

dalam menunjukan kekuatan yang dimilikinya[9]. Konsep kepentingan nasional oleh Hans J. Morgenthau dirujuk karena Kepentingan nasional mencerminkan tujuan umum dan berkelanjutan yang menjadi tujuan suatu negara bertindak. Konsep diaplikasikan untuk melihat ratifikasi Undang-Undang dilakukan agar Meksiko dan Brasil menjadi anggota resmi konvensi Budapest, sehingga adanya organisasi eksternal wilayah yang ikut berkontribusi guna membantu menekan angka kejahatan.

2.2.3 Teori Sekuritisasi

Teori sekuritisasi menunjukan kepada masyarakat bahwa kebijakan keamanan nasional tidak muncul secara alami melainkan diberikan secara hati-hati ditentukan oleh para politis dan pembuat keputusan. Teori sekuritiasi berpendapat bahwa isu-isu politik dikonstitusikan sebagai isu keamanan ekstrim yang harus segera ditangani ketika di kategorikan sebagai ‘berbahaya’, ‘mengancam’, ‘mengkhawatirkan’, dan sebagiannya oleh ‘aktor sekuritisasi’ yang menjadi kekuatan sosial dan institusional untuk memindahkan isu di luar politik. Sehingga, masalah kemanan tidak hanya ‘di luar sana’ tetapi juga harus diartikulasikan sebagai masalah oleh aktor sekuritisasi. Teori sekuritisasi menantang pendekatan tradisional terhadap keamanan dalam Hubungan Internasional dan menegaskan bahwa masalah pada dasarnya tidak mengancam; melainkan dengan menyebut mereka sebagai masalah 'keamanan' maka mereka menjadi masalah keamanan[10].

[9] Hans J. Morgenthau, Politics among nations : the struggle for power and peace, Alfred A. Knopf, New York 1956, Hal 123-131

[10] Clara Eroukhmanoff, 2018. ”Securitisation Theory: An Introduction” melalui https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/ pada 17 November 2021.

Lene Hansen menyatakan dalam *The Copenhagen School* terdapat beberapa teori di dalamnya, diantara lain adalah *Regional Security Complex Theory, European Security, Relations between Regional and Security*[11]. *The Copenhagen School* ini merupakan konsep yang memiliki tujuan untuk berpikir secara kritis mengenai konsep keamanan. *The Copenhagen School* berawal dari Barry Buzan, Ole Weaver dan Jaap de Wilde, mereka mencoba memasukan unsur lain dalam keamanan[12]. Konsep keamanan tidak selalu mengenai atau bersangkutan dengan militer, yang dimana hal tersebut merupakan konsep keamanan tradisional, namun mereka memperluas konsep tersebut.

Definisi sekuritisasi mencakup elemen konseptual yang berbeda yang telah didefinisikan oleh Buzan, Waever dan de Wilde (1998). Untuk para penulis ini "definisi dan kriteria yang tepat dari sekuritisasi didasari oleh pembentukan intersubjektif dari ancaman eksistensial dengan proyeksi yang cukup untuk memiliki efek politik yang substansial"[13]. Untuk teori sekuritisasi, seperti untuk Konstruktivisme, intersubjektivitas menjadi elemen penting untuk memposisikan ide yang terbentuk secara sosial. Hanya ketika ada intersubjektivitas, ide-ide dapat diwujudkan dalam praktik nyata, dalam hal ini, dalam kebijakan keamanan.

Untuk teori sekuritisasi menurut Buzan, Waever dan de Wilde (1998), karakteristik khusus dari suatu ancaman memotivasi penerapan tindakan luar biasa yang dapat dihadapinya. Dalam hal ini dipahami sebagai tindakan luar

[11] Buzan, Barry, Ole Waever, y Jaap de Wilde. 1998. Security: A New Framework for Analysis. Cambridge: Lynne Rienner Publishers.
[12] Ibid hal 164.
[13] Buzan et al., Security and the environment, hal 526.

biasa terhadap tanggapan yang menyimpang dari keputusan kebijakan publik konvensional. Penulis memberikan contoh batasan khusus untuk warga negara yang, jika tidak ada ancaman, tidak akan berlaku. Proteksionisme atau mengerahkan polisi atau militer adalah contoh tindakan luar biasa yang dapat digunakan dalam menghadapi ancaman. Di ruang siber, pembatasan akses informasi atau kontrol negara atas telekomunikasi dapat dianggap sebagai tindakan yang luar biasa.

Aktor sekuritisasi dapat terdiri dari aktor yang mengamankan masalah dengan menyatakan sesuatu - objek referensi - terancam secara eksistensial. Mereka dapat menjalankan perannya sendiri-sendiri maupun bersama-sama, selain itu pada umumnya mereka adalah orang-orang yang memiliki kemampuan agar pidatonya dapat disebarluaskan dan diterima oleh khalayak. Teori Sekuritisasi diaplikasikan guna melihat kewenangan aktor-aktor yang berpengaruh dan hubungan kekuasaan mereka dengan masyarakat dan memungkinkan mereka untuk menjalankan proses sekuritisasi dan mengontrol hasilnya dengan lebih baik. Sehingga teori ini dipilih karena isu yang terjadi menggagu stabilitas politik dan masyarakat di Meksiko dan Brasil karena maraknya terjadi kasus kejahatan phishing ini.

2.2.4 Konteks Teori terhadap Isu Serangan Phishing

Pentingnya konteks dalam teori sekuritisasi diberikan oleh kemampuan dimensi konseptual dalam memodifikasi proses dan juga hasil sekuritisasi. Dimensi konseptual ini dapat merujuk pada dua elemen yang berbeda. Di satu sisi, konteks yang bisa identik dengan adanya ruang lingkup. Dengan kata lain hal ini merujuk kepada ruang-ruang yang bisa di sekuritisasi seperti politik, militer, sosial, dan lain-lain. Di sisi lain, konteks juga bisa

merujuk kepada semua kondisi yang bersifat historis yang terkait dengan ancaman dan yang membentuk karakteristiknya saat ini.

Konteks diberikan untuk kemampuan menghasilkan kondisi yang diperlukan bagi tindakan para aktor yang terlibat dalam sekuritisasi suatu fenomena. Inilah bagaimana konteks semakin menjadi elemen fundamental dalam memahami dimasukannya suatu isu ke dalam agenda kemanan suatu negara atau wilayah[14].

Teori sekuritisasi secara khusus menurut Hansen dan Nissenbaum haruslah memperluas dan menambahkan sektor baru, Hansen dan Nissenbaum secara ekstensif berpendapat untuk memasukan keamanan siber sebagai sektor baru dan berbeda dalam teori sekuritisasi. Keamanan komputer dengan cepat dikaitkan dengan pengembangan bidang kebijakan yang berkembang yang dikenal sebagai *cyber security*. Berasal dari bidang ilmu komputer dan informasi sebagai keamanan komputer teknis, hal ini merupakan sebuah konsepsi keamanan komputer yang sebagian besar mengacu pada keamanan umum komputer, dimana mayoritas ilmuwan komputer mengadopsi wacana teknis yang berfokus pada pengembangan sistem. Program dirancang dalam tujuan penciptaan kemungkinan serangan eksternal. Dengan menghubungkan keamanan nasional dan kepentingan nasional, banyak negara di dunia melihat peluang munculnya wacana sekuritisasi baru dimana mereka peduli dengan keamanan digital mengidentifikasikan masalah pada keamanan siber yang rumit. Melalui

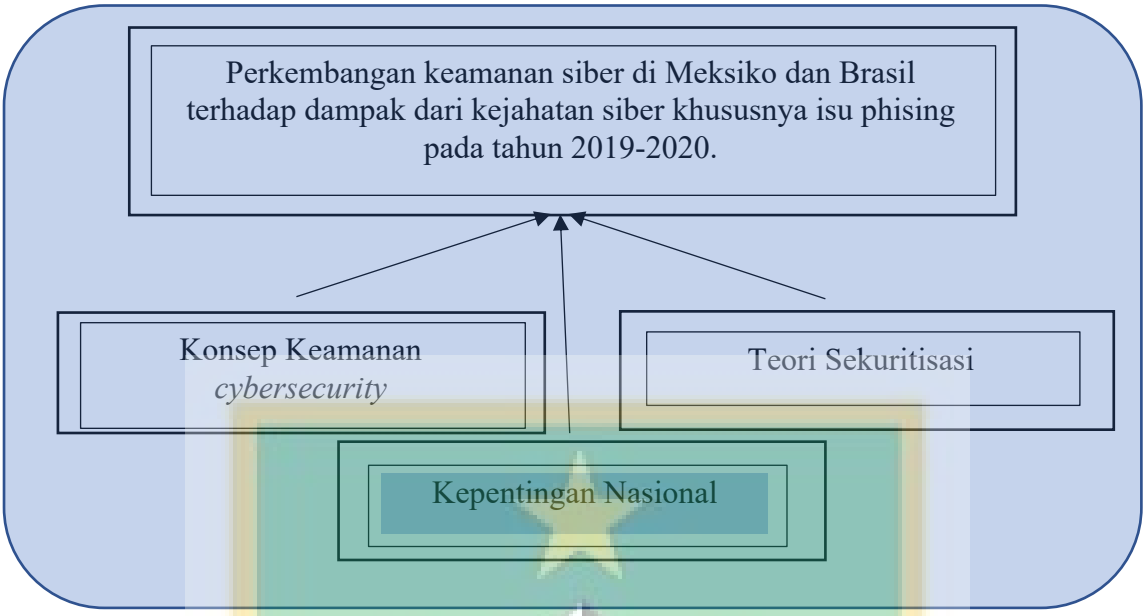
[14] Ibid.

berbagai dokumen kebijakan dan sumber lainnya, negara-negara di dunia semakin mengartikulasikan dan mengembangkan gagasan keamanan komputer sebagai keamanan siber, hal ini merujuk pada besarnya ancaman siber yang muncul melalui ketergantungan pada komputer sebagai aset publik dan juga swasta[15].

Meksiko dan Brasil merupakan negara yang menempati urutan 3 besar di wilayah Amerika Latin diikuti dengan selanjutnya yaitu kolombia, kedua negara ini sedang berproses dalam mengembangkan undang-undang dan juga perarturan mengenai kemanan di dunia siber (*cyber security*) hal ini dilakukan guna melindungi dan memberikan lapisan hukum apabila terjadi kejahatan dunia maya di kedua negara tersebut. Selain itu, visi eksternal memungkinkan mempertimbangkan pengaruh konteks dalam proses sekuritisasi, dalam aktor sekuritisasi, dalam subjek yang merujuk, dan dalam audiens. Dengan kata lain, melalui visi ini, konteks diberikan kemampuan untuk menghasilkan kondisi yang diperlukan bagi tindakan para aktor yang terlibat dalam sekuritisasi suatu fenomena. Inilah bagaimana konteks semakin menjadi elemen fundamental untuk memahami dimasukkannya suatu isu ke dalam agenda keamanan suatu negara. Kepentingan kedua negara membuat kebijakan juga didasari oleh keinginan setiap masyarakatnya memiliki hak perlindungan dari pemerintah saat mereka melakukan aktivitas di dunia internet.

[15] Nissenbaum, Helen. "Where computer security meets national security", Ethics and information technology (2005), hal. 63.

2.3 Kerangka Pemikiran



Dalam kerangka pemikiran, penulis akan menjelaskan mengenai bagaimana alur kerja dalam penelitian ini. Kerangka pemikiran dapat dilihat pada bagan di bawah ini. Dalam penelitian ini, penulis mengawali bagaimana Perkembangan keamanan siber di Meksiko dan Brasil terhadap dampak dari kejahatan siber khususnya pada isu phising pada tahun 2019-2020. Pada akhirnya aspek-aspek tersebut akan dianalisa dengan konsep dan juga teori yang telah ditentukan, yaitu konsep keamanan *cyber security*, kepentingan nasional dan teori sekuritisasi.