BAB I
PENDAHULUAN

A. Latar Belakang

Cybersecurity adalah praktik yang tidak bisa dilepaskan dari sejarah internet. Perkembangan internet tidak bisa lepas dari pengaruh hubungan internasional didalamnya. Kemunculan awal dari internet ketika terjadinya perang dingin Amerika Serikat dan Uni Soviet di tahun 1960 – an. Dalam perkembangan perang dingin ini, kedua Negara berlomba – lomba dalam mengembangkan system infomasi yang cepat untuk memenangkan perang (University System of Georgia, 2022). *Interconnection-networking* (Internet) merupakan sebuah sistem global jaringan komputer yang saling menghubungkan antara satu dengan yang lain di seluruh penjuru dunia dengan menggunakan *standart Internet Protocol Suite* (Naughton, 2016).

Didalam internet kita akan mengenal yang namanya big data, big data sendiri bisa didefinisikan data – data yang bersumber dari *people (Sosial media), Organizational – oriented* (data Pemerintah/ NGO, Perusahaan), *dan machine learning* yaitu sebuah Artificial intelegent yang mengolah data yang ada dengan algoritma ke dalam bentuk grafik yang kita inginkan. Big Data menjanjikan keuntungan informasi, baik itu dalam intelijen bisnis, intelijen negara, atau bentuk pengumpulan dan analisis data lainnya. Setidaknya secara teori, ia menawarkan kemampuan untuk menjadi sumber infomasi, sehingga bisa digunakan oleh bisnis, pemerintah, atau jaringan kriminal mana pun (Zwitter, 2015).

Kemunculan big data yang bisa diolah ini menjadi sebuah masalah dalam hubungan internasional, seperti contohnya adalah group teroris Al Qeda tahun 2003 yang mencoba merekrut anggotanya melalui media sosial. Meminjam istilah dari Joseph Nye bahwa internet yang memuat big data juga termasuk kedalam *cyberspace* memilik pengaruh negatif terhadap negara semisal *cyberattack* terhadap akun – akun resmi pemerintah maupun lembaga

keuangan, *cyberterorism* yaitu upaya yang di lakukan oleh kelompok organisasi teroris yang merekrut anggotanya melalui internet seperti kasus Al Qaeda, dan yang paling berbahaya adalah terjadinya *cyberwar* apabila negara – negara superpower secara tidak langsung melakukan kegiatan aktivitis internet dengan sentimen dalam internet bisa menyebabkan benturan masyarakat di dunia nyata (J. Nye, 2011).

Dari banyak praktek yang di lakukan oleh Negara – Negara dunia, tahun 2018 Amerika serikat secara mengejutkan menutup diri dari prinsip perdagangan bebas dengan menaikkan pajak masuk untuk produk produk China khususnya dalam bidang Teknologi. Di ketahui bahwa Amerika Serikat melakukan pelarangan masuk produk China seperti, Huawei, ZTE (Williams, 2020). Sejak menjabat menjadi Presiden AS, Januari 2017, Kebijakan "*America Firs*t" Presiden Trump telah mengakibatkan penarikan AS dari sejumlah besar perjanjian internasional dan strategi baru AS untuk partisipasi bersyarat dalam komitmen sekutu di Eropa dan Asia, yang membuat Washington tampak kurang kredibel bagi komunitas internasional. Lebih lanjut, pemerintahan Trump cenderung menerapkan pola pikir konfrontasi komprehensif ketika berhadapan dengan Beijing, yang dapat memperkuat persaingan Tiongkok-Amerika dan pada akhirnya mengarah pada Perang dingin baru (Arežina, 2019).

Amerika Serikat dibawah Pemerintahan Trump mulai menyatakan perang dagang dengan China Sejak tahun 2018 lalu, beberapa alasan kenapa Trump menggaungkan perang terhadap China. Terjadinya krisis di AS dan Eropa di tahun 2008 menjadikan China diuntungkan dari peristiwa ini. Pasca Perang Dingin hubungan kedua Negara berada dalam tahapan yang baik baik saja, karena adanya Globalisasi AS dan Negara – Negara barat memanfaatkan kebijakan China dalam hal ketenagaan kerjaan, dan lingkungan kebijakan yang longgar terhadap masuknya Investasi. Sebenarnya awalnya AS lah yang menjadi mentor China dalam menjalankan ekonomi dan masuk kedalam kancah politik internasional ini di tandai dengan masuknya China ke WTO (Sun, 2019).

Kemajuan teknologi China ini sebenarnya sudah di waspadai oleh Pemerintahan Obama dengan Pelarangan China berinvestasi dalam bidang semi – conductor. Namun tidak membuat perkembangan Teknologi dan Informasi China menurun, sehingga Pemerintahan Trump menyatakan untuk Perang dagang dalam bidang Teknologi.(Sun, 2019) Di tahun 2020, tepatnya bulan juli Pemerintah Amerika Serikat melayangkan gugatan kepada Pengadilan Amerika Serikat tentang pemblokiran Tik Tok beroperasi di Amerika Serikat (The White House, 2020). Kejadian ini di sebabkan karena, Tiktok diduga telah menjual data pelanggannya kepada Pemerintah China yang merupakan *national threat* untuk Amerika Serikat. Perang dagang antara Amerika China mengantarkan permasalahan ini, seperti apa yang di laporkan oleh Al Jazeera bahwa pemblokiran Tiktok merupakan salah satu imbas dari Perang dagang antara China – AS (Sukri, 2020).

Atas dasar Laporan dari Lembaga Riset Peterson Institute for International Economics yang menggambarkan TikTok sebagai masalah yang sama besarnya dengan Huawei yang juga menimbulkan ancaman keamanan nasional bagi Amerika Serikat (Biancotti, 2019). Aplikasi video pendek TikTok adalah aplikasi sosial media pertama yang lahir di luar AS yang secara signifikan menyaingi sosial media Amerika Serikat. Sejak menjadi sosial media yang paling diminati, TikTok mendapat banyak kecaman keras dari pemerintah di seluruh dunia, mengakibatkan larangan langsung di beberapa Negara (Press Information Bureau Delhi, 2020).

TikTok telah menjadi pesaing serius platform media sosial Amerika seperti Facebook, Instagram, dan YouTube. Sebelum TikTok, platform media sosial non-AS seperti WeChat (China), Line (Jepang), VKontakte (Rusia), dan Kaokao Talk (Korea Selatan) belum mencapai popularitas global, meskipun sangat sukses di dalam negeri dan di beberapa negara luar negeri . Dalam hal ini, kesuksesan TikTok dalam ekspansi global sangatlah luar biasa. Sejak 2018, TikTok telah menyaksikan peningkatan yang meroket: telah diunduh lebih dari 2 miliar kali secara global dan merupakan aplikasi yang paling banyak diunduh di App Store dan Google Play pada kuartal pertama tahun 2020 (J. Wang, 2020).

Anggota parlemen AS mempertanyakan apakah ByteDance, perusahaan pemilik TikTok, sudah cukup melakukan upaya dalam melindungi data pengguna dari campur tangan oleh negara China. Namun, praktik data TikTok tidak berbeda dengan aplikasi sosial media asal AS (Fowler, 2020) dan kontroversi atas kebangkitan TikTok di AS tidak dapat dijelaskan hanya dengan analisis teknologi, kebijakan, atau praktik perusahaan (Gray, 2021).

Pelarangan Tiktok ini dikhususkan karena Pejabat Pemerintah, Anggota Parlemen dan juga mereka yang termasuk personel angkatan bersenjata dapat disadap dan dapat dimanfaatkan untuk Pemerasan oleh Otoritas China. Ini diperkuat dengan dugaan bahwa Tiktok dengan kemampuannya dapat menyampaikan lokasi, gambar, dan data biometrik ke perusahaan induknya di China. Ini legal dilakukan secara hukum karena Perusahaan yang berasal dari China tidak dapat menolak untuk berbagi data dengan pemerintah China karena dibawah Undang-Undang Keamanan Internet China(Gray, 2021) .

Dengan demikian, beberapa hal di atas mendorong peneliti untuk melakukan penelitian ini akan lebih berfokus bagaimana Kebijakan Donald Trump dalam terkaitan upaya Pemblokiran Aplikasi Tiktok di tahun 2020, dengan melihat faktor-faktor pendorong utama, dampak serta tantangan yang cukup kompleks dari kebijakan pelarangan beroperasinya Tiktok di AS karena faktor keamanan siber.

B. Rumusan Masalah

Berdasarkan dari uraian latar belakang masalah tersebut diatas, maka penulis menentukan pokok permasalahan dalam penelitian ini yaitu : “Mengapa pemerintahan Presiden Donald Trump membuat kebijakan pemblokiran TikTok?”

C. Tujuan Penelitian

Dalam penelitian ini, penulis bertujuan untuk meneliti dan menganalisis mengenai pengaruh Keamanan Siber dalam perang dagang Amerika Serikat – China secara lebih spesifik di zaman Pemerintahan Donald

Trump untuk menunjang pandangan baru Pengetahuan bagi Mahasiswa hubungan Internasional tentang bagaimana Negara superpower tetap mempertahankan posisi politiknya dalam kancah dunia dengan cara – cara yang baru bahkan tidak sesuai dengan pengalaman politik luar negeri mereka selama ini.

D. Kajian Literatur

Untuk lebih memahami pokok permasalahan yang dibahas, penulis mengumpulkan berbagai macam sumber tulisan riset. Ini dimaksudkan agar menjadi awalan dalam mengembangkan penelitian. Penelusuran awal telah menghasilkan beberapa literatur sebagai berikut ;

Pertama , Jurnal berjudul *The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities* karya Tai Ming Cheung bahwa Kebangkitan negara China yang semakin mampu secara teknologi dan terobsesi dengan keamanan nasional, dimana industri keamanan siber merupakan komponen inti, memiliki komplikasi geopolitik dan geo-ekonomi internasional yang mendalam. Hasil peneltian adalah Pemerintahan Xi Jinping telah berusaha untuk mengukir peran yang lebih besar bagi China dipanggung dunia, yang mencakup upaya untuk merevisi norma dan aturan yang tidak disetujui (Cheung, 2018).

Kemudian China berupaya meletakkan fondasi jangka panjang keamanan sibernya salah satu tujuannya adalah menjadikan sektor keamanan siber domestik sebagai pengekspor utama produk dan layanannya. Selanjutnya, ketika China mendapati dirinya terlibat dalam persaingan strategis yang semakin intensif dengan AS, domain cyber akan menjadi salah satu arena utama kontes. Sebagian besar persaingan ini sudah terjadi dalam spionase dunia maya, tetapi juga mulai meluas ke bidang teknologi terkait lainnya. Undang-undang keamanan siber China, misalnya, menimbulkan kekhawatiran serius di antara beragam perusahaan, termasuk mereka yang terlibat dalam mendukung infrastruktur informasi penting serta perusahaan di sektor energi, transportasi, keuangan, dan lainnya yang mengumpulkan data informasi pribadi di China (Cheung, 2018).

Kedua, Jurnal berjudul *Critical Engagement on Digital Sovereignity in International Relations: Actor Transformation and Global Hierarchy* tahun 2019 yang ditulis oleh Adonis menjelaskan bahwa kedaulatan negara secara alami akan mengalami gangguan karena adanya teknologi sehingga perlu adanya tindakan yang nyata dari Negara untuk membuat sebuah kebijakan khusus tentang dunia digital. Untuk menjelaskan peran negara dalam kedaulatan siber bisa menggunakan dua pendekatan struktural dan saling terkait: transformasi aktor dan hierarki global (Adonis, 2019).

Pemahaman transformasi aktor berpotensi menjelaskan bagaimana aktor berperilaku sesuai dengan kekuatan, minat, sejarah, dan persepsi mereka. Ketika seorang aktor berinteraksi dengan aktor lain, ia secara otomatis membangun hubungan kekuasaan yang pada gilirannya menciptakan distribusi lanskap kekuasaan dan menghasilkan hierarki digital global di antara para aktor. Hirarki digital global ini muncul tidak hanya berdasarkan aktor, tetapi juga isu terkait kedaulatan digital. Dua pendekatan yang saling terkait yang Adonis usulkan ini dimaksudkan tidak harus secara ketat dianggap sebagai tawaran teoretis. Namun, itu lebih sebagai pajangan bahwa eksplorasi teorisasi kedaulatan digital masih banyak harus diteliti di masa depan (Adonis, 2019).

Ketiga, *Reading the Trump Administration's China Policy* oleh Fumiaki Kubo berbicara tentang Kebijakan terhadap China dibawah Administrasi Trump adalah kombinasi yang langka dan bagian terberat dari Partai Demokrat, yaitu perdagangan, dan dari Partai Republik, yang merupakan keamanan nasional. Strategi Keamanan Nasional oleh Pemerintahan Trump mendefinisikan China dan Rusia sebagai pesaing. Ini adalah pertama kalinya bagi Pemerintah AS untuk bersikap keras terhadap China dan Rusia (dahulu Uni Soviet) sejak akhir 1960 – an (Kubo, 2019).

Meskipun perdagangan sejauh ini merupakan aspek yang paling menonjol dari kebijakan konfrontatif Presiden Trump terhadap China, itu merupakan fakta pendekatan seluruh pemerintah atau penolakan yang dilakukan oleh pemerintah AS untuk kerjasama dengan Pemerintah Cina,

yang berarti bahwa tidak hanya Gedung Putih tetapi berbagai Departemen dan Badan Legislatif AS bersikap keras dengan China, berurusan dengan banyak masalah dari perdagangan hingga hak asasi manusia sampai keamanan nasional. Presiden mungkin sebenarnya menjadi figur yang paling lembut, hampir secara eksklusif berfokus pada perdagangan. Ini mungkin sebuah perubahan haluan bersejarah dalam kebijakan AS terhadap China (Kubo, 2019).

Keempat, Jurnal berjudul *Cybersecurity policy and the Trump administration* karya Jacov Shiverly dengan menggunakan Teori PET (*punctuated equilibrium theory*) Shiverly mengemukakan bahwa dengan studi kasus akan mengikuti salah satu dari tiga skenario yaitu Perhatian pemimpin yang berkelanjutan: eksekutif atau figur kebijakan lain yang menentukan harus memajukan atau mendukung perubahan kebijakan secara konsisten dari waktu ke waktu daripada kebijakan yang spontan karena keadaan mendesak. Perubahan teknologi sistemik: teknologi baru yang memengaruhi kapasitas interaksi antarnegara. Perubahan keamanan sistemik: persepsi ancaman antarnegara bagian dasar berubah karena masalah atau krisis yang muncul (Shively, 2021).

Hasil dari Jurnal ini adalah Tidak ada perhatian kepemimpinan yang berkelanjutan atau perubahan kondisi sistemik yang muncul. Sebaliknya, skenario dua dan tiga muncul: masing-masing, kebijakan yang disesuaikan dan perubahan besar yang gagal. Pemerintah pertama kali mengadopsi versi pendekatan Obama yang sedikit dimodifikasi untuk kebijakan keamanan siber. Kemudian, upaya selanjutnya untuk menerapkan kebijakan keamanan siber yang lebih ofensif mewakili modifikasi praktik yang ada daripada transformasi besar – besaran. Sepanjang 2017 dan 2018, kebijakan administrasi Trump memperlakukan keamanan siber sebagai masalah teknis manajemen risiko. Pendekatan berpusat pada prosedur dan praktik kelembagaan domestik. Ini membingkai ulang tetapi tidak secara mendasar mengubah pendekatan era Obama yang ada (Shively, 2021).

Pejabat Gedung Putih hingga presiden tidak memprioritaskan keamanan siber dibandingkan dengan kebijakan keamanan nasional yang lebih tradisional, seperti persaingan kekuatan besar dan rezim yang mengancam proliferasi nuklir. Namun, setelah tinjauan kebijakan, pemerintah pada 2018 mengadopsi kebijakan "*Defending Forward*". Ini dirancang pada tingkat taktis dan operasional untuk merespons secara proaktif terhadap ancaman. Menjelang pertengahan pemilu 2018, misalnya, kebijakan administrasi mendorong lembaga yang bertanggung jawab atas keamanan siber untuk mencari dan menghambat atau mencegah upaya penyebaran disinformasi atau menembus sistem pemilu AS. Mungkin yang terpenting, postur kebijakan ini melengkapi preferensi strategis pemerintah untuk retorika garis keras dan diplomasi "tekanan maksimal" (Shively, 2021).

Sepintas tampaknya ini merupakan pemutusan dengan kebijakan keamanan siber sebelumnya; namun, "*Defending Forward*" muncul sebagai modifikasi, daripada pemutusan dramatis dengan, kebijakan keamanan siber sebelumnya. Lebih jauh lagi, pemerintahan Trump mengaitkan pendekatan ini dengan upaya yang lebih besar untuk memfokuskan strategi besar AS pada aktor negara tradisional dan pesaing yang setara. "*Defending Forward*" bukanlah revolusi untuk kebijakan keamanan siber. Sebaliknya, bagi Trump dan pejabat seniornya, hal itu memberikan visi nasionalis yang lebih besar untuk strategi keamanan nasional (Shively, 2021).

Kelima, Jurnal *berjudul U.S.-China Relations Under the Trump Administration: Changes and Challenges* karya Sanja Arezina membahas hubungan AS – China sejak tahun 1970 – an hingga Pemerintahan Trump. Penelitian bertujuan untuk memberikan alasan dibalik perubahan besar Kebijakan Pemerintah AS terhadap China dengan menggunakan narasi "*China Threat*". Hasil penelitian ini adalah Sejak Presiden Trump menjabat, Amerika Serikat telah mundur sendiri dari sejumlah besar perjanjian internasional dan memulai strategi baru untuk partisipasi bersyarat dalam perjanjian dengan sekutunya. Jika kita melihat hubungan AS-China dibawah pemerintahan Trump, kita dapat menyimpulkan bahwa kepemimpinan China telah menunjukkan pendekatan yang jauh lebih kuat dan stabil daripada

Amerika dan sekutunya. Perubahan yang dilakukan oleh Pemerintahan Trump hanya akan menguntungkan Amerika Secara negara namun tidak pada kekuatan Geopolitik AS di dunia serta Negara – negara yang berhubungan baik dengan kedua negara dalam hal perdagangan (Arežina, 2019).

Keenam, Jurnal berjudul *The Securitization of China's Technology Companies in the United States of America* karya dari Giandi Kartasasmita menjelaskan bahwa Presiden Trump melakukan kebijakan sekuritisasi Perusahaan Hardware maupun software asal China dikarenakan itu akan membahayakan kepentingan nasional AS di masa depan. Pemerintahan Trump Juga dinilai berhasil meyakinkan publik Amerika Serikat dengan kebijakannya memblokir Tiktok dan We Chat karena dinilai mengumpulkan data pelanggan dengan illegal. Ini dibuktikan dengam jajak pendapat Pew Research Center 2020, 62 persen populasi AS percaya China sebagai ancaman bagi AS, naik 14 persen dari jajak pendapat (Kartasasmita, 2020).

Ketujuh, Jurnal berjudul *Trade regimes as a tool for cyber policy* karya Karl Grindal yang menjabarkan bahwa Selama ini, alasan ancaman keamanan dari rezim perdagangan selalu diusulkan sebagian besar ditentukan oleh pemerintah. Hasil penelitian menunjukkan bahwa sudut pandang rezim perdagangan bisa dianalisis bisa secara individual dan sebagian besar dilihat melalui lensa solusi potensial, proposal keamanan siber khusus perdagangan ini belum dilihat secara komparatif atau kritis. Melalui lensa ini, berbagai distribusi biaya dan manfaat bersama kepada negara bagian atas perusahaan atau konsumen membantu menunjukkan koalisi potensial mana yang mungkin mendukung kebijakan semacam itu (Grindal, 2019).

Hasil lainnya, CFIUS yang menjadi lembaga penilai investasi asing AS, terlepas dari fokusnya, menyebabkan beberapa perusahaan meninggalkan *Merger and Aquisition* mereka, bahkan tanpa instruksi. Ada ketegangan yang melekat antara persaingan geopolitik China – AS dan perdagangan ekonomi yang terkait erat. Ketegangan ini menantang rezim perdagangan CFIUS, tetapi ketegangan serupa ditemukan didalam WTO dan sehubungan dengan kebijakan lokalisasi. Sehubungan dengan keamanan

siber, perlindungan tingkat konsumen yang netral terhadap negara, persyaratan khusus untuk pembelian pemerintah, dan pembatasan perdagangan yang ditargetkan, hanya jika diperlukan, akan meredakan ketegangan geopolitik sambil meningkatkan keamanan dan memajukan perdagangan lintas batas. Usaha – usaha yang dilakukan Pemblokiran Perusahaan China yang membeli perusahaan Teknologi Amerika Serikat dikarenakan alasan Keamanan nasional Amerika Serikat (Grindal, 2019).

Kedelapan adalah *The geopolitics of 'platforms': the TikTok challenge* karya Joanne E. Gray, mengatakan bahwa upaya blokirnya Tiktok adalah TikTok tidak menimbulkan ancaman keamanan yang lebih besar bagi penggunanya daipada sosial media lainnya. Hampir semua platform digital yang paling banyak digunakan mengancam privasi dan keamanan pengguna, semuanya memiliki kapasitas untuk pengaruh ideologis yang sangat besar, dan mengeksploitasi data pengguna untuk keuntungan ekonomi (Gray, 2021).

Dari Literatur di atas penulis mengambil fokus topik penulisan Keamanan Siber seperti yang di jelaskan Giandi Kartasasmita yang mengatakan bahwa masalah Keamanan Siber (Sekuritisasi) di jadikan sebagai alasan AS dalam kebijakan penolakan teknologi asal China. Dan untuk fokus dalam Pemerintahan Trump terhadap kebijakan penolakan teknologi asal China, Penulis mengambil dua sumber dari Jurnal karya Jacob Shiverly dan Fumiaki Kubo tentang bagaimana Pemerintahan Trump yang pada akhirnya mengambil kebijakan yang selama ini tidak pernah berkonfrontasi langsung terhadap China secara langsung yang dipengaruhi kondisi Ekonomi Politik dalam Negeri dan juga posisi Amerika Serikat di kancah Internasional. Sedangkan untuk Fokus Tiktok, sebagian besar Penulis mengambil data dari jurnal Joanne E. Gray, namun perbedaannya adalah rentang waktu penelitian dimana penelitian ini tidak hanya tahun 2020 namun dari 2018 hingga 2020.

Kerangka Teori

a. Konsep Keamanan Siber dalam Hubungan Internasional

Spionase dalam dunia siber, serangan siber, hacktivisme, sensor internet, dan bahkan isu-isu teknis seperti netralitas internet kini menjadi berita utama di setap negara. Ruang siber telah menjadi ruang politik yang diperebutkan, dibentuk oleh kepentingan, norma, dan nilai yang berbeda. Akibat politisasi ini, para diplomat (Negara) tidak bisa tinggal diam saja. Jika dunia maya hanya domain untuk diskusi teknis di antara para spesialis teknologi informasi saja, era itu sudah pasti berakhir (Barrinha dan Renard, 2017).

Istilah *Cybersecurity* sebenarnya telah ada, ketika ARPA – NET masih secara aktif di kembangkan oleh Pemerintah Amerika Serikat. Tahun 1970-an ketika peneliti Bob Thomas menciptakan program komputer yang disebut Creeper yang dapat bergerak melintasi jaringan ARPANET, meninggalkan jejak virus di dalam elemen kontrol grafis yang digunakan sebagai bantuan navigasi di antarmuka pengguna dan di halaman web. Ray Tomlinson, penemu email, menulis program Reaper, yang mengejar dan menghapus Creeper. Reaper adalah contoh pertama perangkat lunak antivirus dan program yang mereplikasi diri sendiri, menjadikannya worm komputer pertama (Davies, 2021).

Jauh sebelum 1970 – an dunia mengenal dengan istilah *cybernetic* yang terkenal di tahun 1948, dimana saat itu terjadi perang dunia kedua. Penjelasan tentang *cybernetic* ini adalah studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat. Namun yang dibahas disini hanyalah sistem komputasi sandi yang seadanya belum terhubung dengan perangkat komputasi yang lain (Chotimah, 2019).

Istilah dari cybersecurity sendiri diperkenalkan oleh ilmuan komputer ditahun 1990an yang menunjukkan pada gangguan jaringan internet, namun berubah dari masalah teknis tersebut kepada seluruh aktivitas di internet yang menjadi ancaman kepada masyarakat secara keseluruhan. Pembelajaran yang paling berharga adalah ketika jaringan internet dipakai untuk kepentingan

teroris seperti yang terjadi di tahun 2001, ketika gedung WTC dihancurkan oleh Pesawat teroris yang menggunakan aktivitas mengancam negara (Hansen dan Nissenbaum, 2009).

Konsep *Cybersecurity* dalam hubungan internasional dapat kita temui dalam buku *International Relations Theory and Cyber Security* karya mengatakan bahwa kemungkinan ancaman dari digital dan teknologi yang telah terkomputerisasi adalah *cybersecurity* dalam Hubungan Internasional (Valeriano dan Maness, 2018).

Lebih lanjut dijelaskan bahwa security yang dimaksud disini sama dengan keamanan nasional pada umumnya, meminjam istilah Arnold Wolfers dalam buku *Security Studies chapter National Security As an Ambiguous Symbol* dari bahwa keamanan nasional adalah Tiga ciri penting dari pengertian tradisional itu adalah: pertama, identifikasi "nasional" sebagai "negara"; kedua, ancaman diasumsikan berasal dari luar wilayah negara; dan, ketiga, penggunaan kekuatan militer untuk menghadapi ancaman-ancaman itu. Tak heran jika Arnold Wolfers sampai pada kesimpulan , bahwa masalah utama yang dihadapi setiap negara adalah membangun kekuatan untuk menangkal (*to deter*) atau mengalahkan (*to defeat*) suatu serangan (Kusnanto, 2003).

Untuk perkembangan Negara – Negara dalam menghadapi perubahan Peradaban menjadi era digital udah menulisnya dalam bentuk buku yang berjudul *Cybersecurity and Threat Politics* tahun 2007 karya Myriam Dunn Cavelty, dimana Negara – Negara harus menyiapkan langkah – langkah dalam perubahan digital dunia dari mulai sosial, politik hingga ekonomi (Dunn Cavelty, 2007).

Sedangkan Joseph Nye menjelaskan cybersecurity dari penjelasan cyberspace terlebih dahulu karena cyberspace merupakan "bumi" dari dunia maya yang didalamnya terdapat cybersecurity. Lebih jauh dia menjelaskan bahwa cyberspace adalah "Domain siber adalah lingkungan buatan manusia yang kompleks. Tidak seperti atom, musuh manusia memiliki tujuan dan kecerdasan. Gunung dan lautan sulit untuk dipindahkan, tetapi bagian dari

dunia maya dapat dihidupkan dan dimatikan dengan menekan tombol. Lebih murah dan lebih cepat untuk memindahkan elektron melintasi dunia daripada memindahkan kapal besar jarak jauh melalui lautan (Joseph Nye, 2010)

Keamanan siber merupakan bagian dari kekuatan siber, dimana kekuasaan di peroleh berdasarkan sumber informasi. Kekuatan siber adalah ruang kasat mata, dimana domain operasional yang dibingkai oleh penggunaan elektronik untuk mengeksploitasi informasi melalui sistem komputer dan aplikasi penunjang. Kalau Kekuasaan pada dunia nyata bergantung pada konteks, sedangkan kekuatan siber bergantung pada sumber daya yang menjadi ciri domain dunia maya (Joseph Nye, 2010).

Difusi kekuasaan dalam domain siber diwakili oleh sejumlah besar aktor, dan pengurangan relatif perbedaan kekuasaan di antara mereka. Siapa pun mulai dari peretas remaja hingga pemerintah modern besar dapat melakukan kerusakan di dunia maya, dan seperti yang pernah dikatakan oleh kartun terkenal New Yorker, "di internet, tidak ada yang tahu bahwa Anda adalah seekor robot. Virus "*Love Bug*" yang terkenal yang dilepaskan oleh seorang peretas di Filipina diperkirakan telah menyebabkan kerusakan senilai $15 miliar (Joseph Nye, 2010).

Jaringan komputer yang penting bagi militer Amerika diserang ratusan ribu kali setiap hari. Kelompok penjahat dunia maya dikatakan telah mencuri lebih dari $1 triliun data dan kekayaan intelektual pada tahun 2008. Satu jaringan spionase dunia maya yang bernama GhostNet ditemukan menginfeksi 1.295 komputer di 103 negara, dimana 30 persennya merupakan target pemerintah bernilai tinggi. Kelompok teroris menggunakan web untuk merekrut anggota baru dan merencanakan kampanye. Aktivis politik dan lingkungan mengganggu situs web perusahaan dan pemerintah (Joseph Nye, 2010).

Apa yang membedakan kekuasaan dalam domain siber bukanlah bahwa pemerintah berada di luar gambaran seperti yang diprediksi oleh para penganut paham liberal siber awal, tetapi sumber daya yang berbeda yang dimiliki oleh aktor yang berbeda, dan penyempitan kesenjangan antara aktor

negara dan non – negara dalam banyak kasus. Tetapi pengurangan relatif dari perbedaan daya tidak sama dengan pemerataan. Pemerintah masih memiliki lebih banyak sumber daya. Di internet, semua tidak bisa diidentifikasi *(Anonimous*) (Joseph Nye, 2010).

Sehingga bisa kita simpulkan bahwa definisi dari Keamanan siber adalah Keamanan yang mengacu pada masalah keamanan informasi bagi pemerintah, organisasi – organisasi, dan individu yang berurusan dengan teknologi komunasi , dan khususnya dengan teknologi Internet. Bisa dilihat dari gambar dibawah :

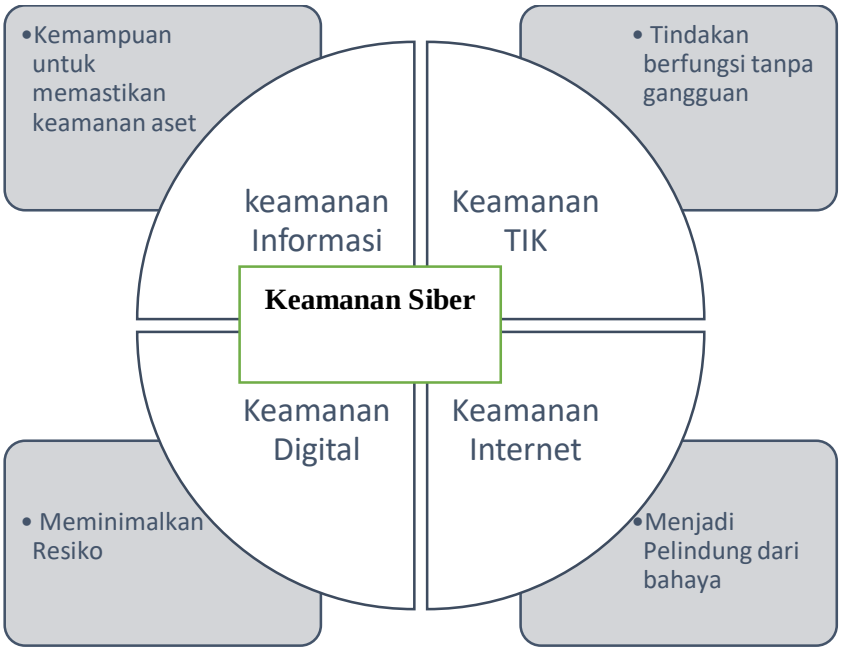
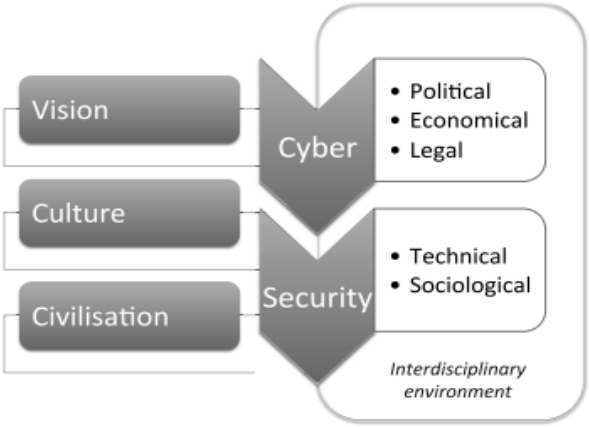


Diagram 1 1 Konsep yang berhubungan dengan Keamanan Informasi

Sumber dalam : (Ghernaouti, 2013, hal. 330)

Permasalahan tentang keamanan siber sendiri tidak hanya bisa ditangani oleh Negara namun diperlukan stakeholders lainnya. Semua cabang ilmupun di perlukan seperti teknologi, hukum, sosiologis, ekonomi, dan bidang politik, keamanan Teknologi Informasi sehingga pembahasan ini bersifat interdisipliner. Itu tidak hanya harus mencerminkan lokasinya, tergantung pada negara, dan nilai-nilai, budaya, dan peradaban bangsa itu, tetapi juga memenuhi kebutuhan keamanan khusus dari konteks lokal.



Gambar 1 1 Konsep Security adalah konsep yang bergantung pada hal lainnya

Sumber dalam :(Ghernaouti, 2013) hal 331

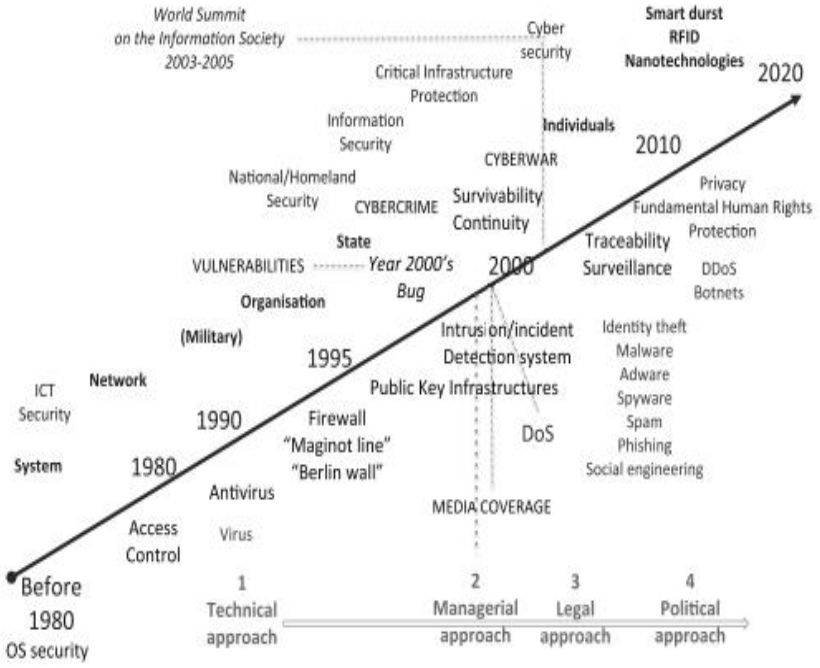
Dalam perkembangan nya teknologi internet yang berhubungan yang awalnya hanya di Sistem operasi (OS) pertama sudah termasuk mekanisme kontrol akses dan kriptografi, yang terutama disediakan untuk aplikasi penting dalam domain sensitif seperti militer, perbankan, dan keuangan umum. Keamanan jaringan merupakan bagian integral dari manajemen jaringan, disamping manajemen konfigurasi dan pemantauan kinerja. Namun, manajemen keamanan tidak dapat mengatasi kegagalan akibat masalah desain atau penyalahgunaan infrastruktur teknologi informasi dan telekomunikasi (TIK) secara kriminal. Penyadapan ilegal, penyusupan sistem, penyebaran malware, eksploitasi kerentanan; semua kegiatan ini menunjukkan pertumbuhan yang berkelanjutan. Keamanan informasi menyangkut organisasi mengenai perlindungan dan pertahanan aset dengan mempertimbangkan kerentanan intrinsik teknologi informasi dan ancaman kriminal terhadap strategi organisasi (Ghernaouti, 2013).

Kemudian yang menjadi masalah adalah bagaimana mencari Solusi keamanan dapat melindungi lingkungan tertentu dalam konteks tertentu, tetapi tidak dapat mencegah perilaku kriminal sama sekali. Lembaga hukum dan undang-undang harus ada untuk mencegah perilaku kriminal dan mengadili orang-orang yang melakukan tindakan ilegal. Karena keamanan TIK merupakan perhatian utama bagi pemerintah, diplomasi, dan isu militer,

dimensi politik melengkapi pendekatan teknis, manajerial, dan hukum keamanan informasi.

Sedangkan buku *Cyberpolitics in international relations* karya Nazli Chocri berperndapat bahwa segala bentuk ruang (fisik maupun siber) dalam hubungan internasional memberikan peluang untuk memperluas kekuasaan dan pengaruh dalam politik dunia. istilah "ruang" mengacu pada domain interaksi yang (1) menciptakan sumber kekuatan potensial, (2) menyediakan perluasan pengaruh dan , (3) memungkinkan layanan, sumber daya, pengetahuan, atau pasar baru, dan (4) mewujudkan potensi lebih lanjut bila diperkuat dan ditopang oleh kemajuan teknologi. Ketika aktivitas satu aktor mengancam kedaulatan, stabilitas, atau keamanan aktor lain, maka ruang menjadi variabel kritis dalam hubungan internasional. Secara tradisional, gagasan ruang sangat erat kaitannya dengan teritorial. Jelas, koneksi ini sudah tidak relevan

Keamanan siber juga menyangkut kedaulatan negara, keamanan nasional, dan keselamatan warga negara. Dalam arti yang lebih luas, ini mencakup perlindungan konsumen, perlindungan anak-anak, dan perlindungan kebebasan sipil dan demokrasi (Ghernaouti, 2013). Penjelasannya bisa kita lihat d bawah :



Gambar 1 2 Evolusi ICT Security

Sumber : (Ghernaouti, 2013).

Pembahasan tentang dunia siber, tak luput dari pengaruh internal maupun eksternal kepada dunia siber. Karena siber ini merupakan salah satu bagian dari teknologi. Faktor eksternal dari dunia siber adalah politik, atau kebijakan suatu negara, Perubahan arah kebijakan suatu negara bergantung dua kondisi yaitu Domestik dan juga politik Internasional (Dunn Cavelty dan Wenger, 2020). Untuk lebih jelasnya kita melihat diagram di bawah ;

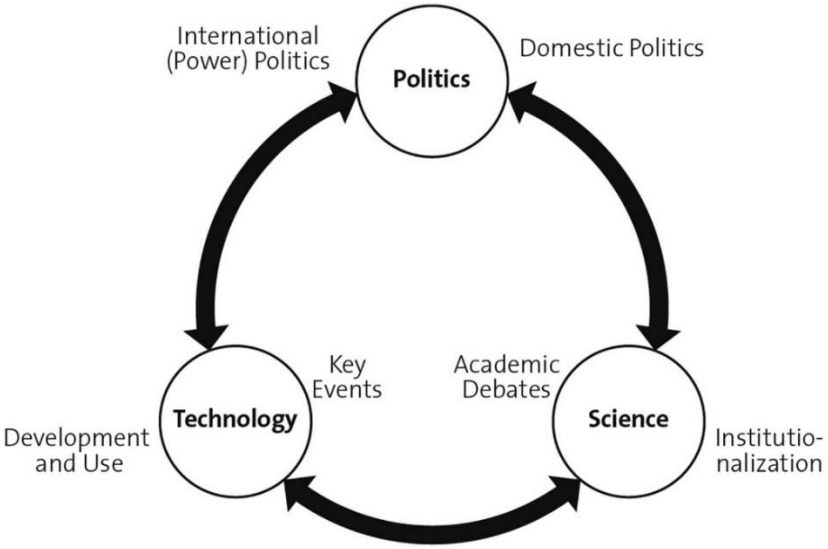


Diagram 1 2 Diagram kaitan antara Teknologi, Politik dan Ilmu Pengetahun

Penjelasan dari diagram di atas bisa kita lihat dari tabel di bawah ;

Bidang Bahasan	**Faktor Pendorong**	**Deskripsi**
Teknologi	Perkembangan dan Penggunaan Teknologi Digital Peristiwa Penting (yang berkaitan dengan Siber)	Teknologi dibentuk oleh ide-ide politik dan struktur kekuasaan dan membentuk kemungkinan tindakan politik pada gilirannya Peristiwa di luar dunia siber yang berpengaruh terhadap politik keamanan siber dan kejadian dari dunia siber berupa insiden siber
Politik	Politik (Kekuatan) Internasional	Keyakinan akan sumber kekuatan baru (“kekuatan dunia maya”) dan pola kerja

	Domestic Politics	sama dan konflik antara kekuatan besar Berpotensi konfliktual Proses negosiasi tentang peran dan tanggung jawab lembaga negara,ekonomi, dan masyarakat (nasional dan internasional)
Ilmu Pengetahuan	Debat Akademik Institutionalization	Tren ontologis dan epistemologis yang lebih luas yang membentuk disiplin Ilmu Hubungan Internasionadan Keamanan Peluang dan kendala bagi peneliti berupa jabatan, pendanaan, outlet publikasi, dan jaringan penelitian

Tabel 1 1 Penjelasan Kaitan antara Teknologi, Politik dan Ilmu Pengtahuan

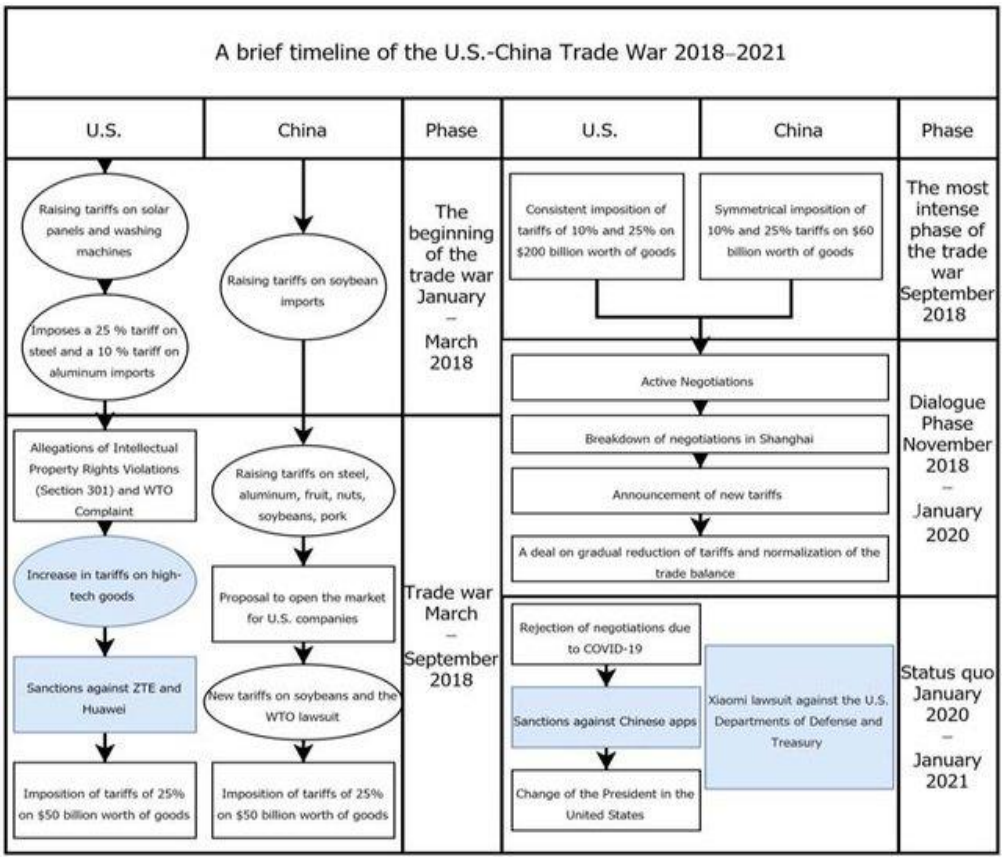
Sumber : (Dunn Cavelty & Wenger, 2020).

b. Keterkaitan Perang Dagang dan Kemanan Siber

Konsep dalam Hubungan internasional ada 3 level analisis pertama sistem : dimana negara yang menjadi aktor utamanya yang artinya Negara satu akan mempengaruhi negara yang lainnya. Level kedua adalah Level Negara, dimana penelitian lebih difokuskan kedalam level dalam Negeri sebuah Negara, dimana banyak kelompok kepentingan yang bermain dalam mempengaruhi kebijakan luar negeri, dan yang terakhir adalah level Individu

dimana yang diteliti adalah personal yang mempengaruhi kebijakan luar negeri sebuah negara seperti Presiden secara Individu (Mas'oed, 1990, hal. 119). Dari pengertian diatas bisa diambil kesimpulan bahwa menelaah Perang dagang dalam sebuah konsep bisa kita pakai dari level analisis sistem.

Perang dagang adalah situasi dimana suatu negara membalas tindakan proteksionis sepihak dari negara lain dengan kenaikan tarif serupa dan pembatasan impor lainnya. Konsep tersebut telah menjadi agenda internasional sejak pemerintahan Trump menaikkan tarif impor besi dan baja (25%) dan aluminium (10%) secara sepihak, menargetkan secara eksklusif barang-barang China dan Eropa pada 2018 (Serdaroğlu Polatay, 2020). China dan Eropa kemudian membalas dengan menaikkan tarif impor produk-produk Amerika. Dalam melihat bagaimana timeline trade war yang terjadi antara China dan US bisa kita lihat dalam gambar dibawah.



Gambar 1 3 Timeline US – China Trade War 2018 - 2021

Sumber : (Degterev dkk, 2021)

Dalam penjelasan dalam tulisan *An analysis of the China–US trade war through the lens of the trade literature* tentang penjelasan Trade war dari perspektif literatur perdagangan menyimpulkan bahwa masih perlu adanya penelitian lanjutan mengenai US – China Trade war dalam kacamata literatur perdagangan. Namun yang dibahas dalam penelitian tersebut variabel penelitiannya adalah *US – China Trade war, trade war, trade policy, dan trade theories* disebutkan bahwa potensi dari perang dagang bisa mencapai menular kebidang lainnya seperti kekuatan geopolitik, pasar dan juga tentang pasar bebas yang selama ini di anut oleh sebagian besar negara dunia (Qiu dkk, 2019).

Penjelasan lain tentang *Trade war* sebagai konsep, bisa di jelaskan dengan menggunakan teori perdagangan internasional. Dalam penjabaran Britanica tetntang *International Trade* menjelaskan bahwa perdagang internasional bisa kita katagerikan kedalam dua fase, yang pertama adalah tradisional dan yang kedua adalah modern. Dalam fase tradisional semua negara masih menganut mahzab Proteksionisme dalam perdagangan hingga muncullah teori dari Adam Smith tentang Perdagangan bebas terciptalah liberalisme. Di awal mula muncul fase modern, para ahli ekonomi sudah mulai mengajukan teori baru yaitu *comparative advantage* untuk menanggulangi ketidakadilan pasar bebas ala Adam Smith. Di Fase modern, fakta yang ada, adalah adanya sebuah organisasi Internasional yang di tunjuk untuk menjadi wasit dalam perdagangan internasional, yang di kenal sebagai WTO (Trend J. dkk, 2020).

Sedangkan dalam buku Liang dan Ding, 2020 di chapter 1 di jelaskan bagaimana menjelaskan trade war dari berbagai teori. Namun yang perlu dilakukan di awal adalah mengajukan 3 pertanyaan ; mengapa perang dagang terjadi?, Apa proses interaktif yang terjadi dan bagaimana itu mempengaruhi jalannya perang dagang?, apa dampak dari Perang dagang?

Dari sudut pandang praktis, ketiga pertanyaan tersebut saling terkait. Mengapa perang dagang terjadi adalah masalah ekonomi internasional tetapi juga terkait dengan hubungan internasional serta politik. Yang pertama

mencerminkan penyebab ekonomi dari perang dagang, sedangkan yang kedua meneliti interaksi politik antar negara dan di antara berbagai kelompok kepentingan dalam suatu negara. Melihat literatur perdagangan internasional, teori tentang tarif optimal, kebijakan perdagangan strategis dan pembuatan kebijakan perdagangan kooperatif dan nonkooperatif telah menjelaskan sifat interaktif pembuatan kebijakan perdagangan, termasuk melalui perang dagang yang ekstrem Mengenai dampak perang dagang, teori perdagangan konvensional menjelaskan dengan baik efek harga dan kesejahteraannya

Pertanyaan tentang bagaimana perang dagang dilakukan, mengapa pembalasan dendam terjadi dan apa yang menentukan hasilnya dapat dipelajari dengan bantuan alat analisis yang berguna dari *Game Theory* (Liang dan Ding, 2020). Sehingga dari penjelasan di atas kita bisa sederhanakan dengan bentuk diagram seperti di bawah :

Diagram 1 3 hubungan antara International Trade dan Trade war

Sumber : (Liang & Ding, 2020)

Centre for Economic Policy tahun 2009 menerbitkan kumpulan esai setebal 100 halaman tentang munculnya hambatan perdagangan dan

Perlindungan semu (setelah krisis keuangan AS 2008). Muncullah kata satu kata Teknologi dalam laporan ini. Teknologi informasi sering dilihat sebagai kisah sukses besar dalam perdagangan global, tetapi penyebarannya yang cepat telah menimbulkan resiko baru. Ekonomi modern, maju dan berkembang, semakin bergantung pada infrastruktur yang didukung TI untuk hampir setiap aspek kehidupan sehari-hari. Namun, seperti yang ditegaskan oleh tajuk utama, infrastruktur ini kurang aman, dan lanskap ancaman yang berkembang pesat membuat masyarakat yang bergantung pada risiko dramatis. Saling ketergantungan sistem dan institusi berarti bahwa kegagalan keamanan dapat memiliki konsekuensi yang mengerikan. proteksionisme semu) ("The Collapse of Global Trade, Murky Protectionism, and the Crisis: Recommendations for the G20," 2009)

Keterkaitan antara teknologi dan Perdagangan dan Perdagangan internasional dalam hal perangkat keras, perangkat lunak, dan data diperumit oleh tantangan keamanan siber. Peraturan dan penegakan domestik gagal ketika penjahat dan pemerintah asing berada di luar yurisdiksi mereka, dan teknologi tidak aman yang murah berkembang biak di seluruh dunia. Sementara itu, rantai pasokan global mengatur aliran segala sesuatu mulai dari senjata hingga mainan yang dilapisi cat bertimbal. Akibatnya, banyak pakar keamanan melihat pembatasan perdagangan sebagai mekanisme untuk mempromosikan keamanan siber domestik, atau untuk menerapkan beberapa bentuk kontrol senjata global (Grindal, 2019).

Pembatasan perdagangan digunakan untuk berbagai tujuan, termasuk mendorong industri yang sedang berkembang, melindungi sektor-sektor yang berpengaruh secara politik, dan mengendalikan penyebaran barang-barang berbahaya. Isu keamanan siber adalah topik yang sangat sulit untuk pembatasan perdagangan karena sebagian besar teknologi memiliki tujuan ganda (militer dan sipil). Misalnya, perangkat lunak yang mengganggu dapat digunakan oleh perusahaan untuk keamanan atau oleh pemerintah untuk pengawasan. Secara lebih luas, semua perangkat keras dan perangkat lunak mungkin mengandung kerentanan, dan perdagangan komoditas ini dapat

membahayakan integritas teknologi informasi dan komunikasi dan mengekspos kekayaan intelektual (Grindal, 2019).

Keamanan siber dimasukkan sebagai tujuan untuk meningkatkan perdagangan lintas batas, karena mekanisme untuk membatasi perdagangan bukanlah hal baru dan dibangun di atas organisasi dan proses yang ada. Sekarang ada perdebatan yang sedang berlangsung tentang berapa banyak ruang yang ada untuk menyerang masalah ini dan peran apa yang harus dimainkan oleh sistem perdagangan global dalam menguranginya. Empat rezim perdagangan di bawah ini tidak lengkap, tetapi digunakan atau mungkin digunakan untuk membatasi perdagangan produk keamanan siber atau teknologi informasi (TI) secara umum untuk alasan keamanan siber. Menyediakan berbagai mekanisme (Grindal, 2019).

Dalam melihat bagaimana Negara membuat kebijakan Pembatasan ekspor dan yang lainnya berdasarkan keadaan siber nya bisa di lihat dari tabel berikut.

Struktur untuk efek pengaturan keamanan siber melalui rezim perdagangan				
	Kontrol Ekspor	**Tarif**	**Pembatasan Investasi**	**Persyaratan lokalisasi**
Kemungkinan efek keamanan siber	Batasi proliferasi	Lindungi industri dalam negeri	Lindungi industri dalam negeri	Batasi spionase asing/aktifkan spionase domestik
Target Spesifik / umum	Umum	Umum	Spesifik	Umum/Spesifik
Menanggung sebagian besar biaya	Beberapa produsen dalam negeri	Semua produsen asing	Beberapa produsen asing	Semua produsen asing

Dampak terhadap konsumen Lokal	Tidak ada	Tinggi	Medium	Tinggi
Biaya administrasi per kasus	Medium	Low	High	Low
Risiko pembalasan	Low	High	Medium	Low
Fragmentation	Decreased	Increased	Increased	Increase

Tabel 1 2 Efek Pengaturan Keamanan Siber dengan Rezim Perdagangan

Sumber : (Grindal, 2019)

Efek keamanan siber yang diklaim dari kebijakan tersebut tidak mungkin secara langsung berlaku untuk konsumen. Daripada secara langsung memberikan jaminan informasi kepada konsumen atau perusahaan domestik, kebijakan yang ditargetkan pada rantai pasokan lebih cenderung membatasi proliferasi produk keamanan siber ke perusahaan yang sah, melindungi industri dalam negeri, atau menghambat spionase asing (Grindal, 2019). Konflik dalam dunia siber juga tidak bisa di hindari, menurut pendapat Nazli Choucri bahwa ada tiga tahapan konflik ;

Tipe	Contoh Kasus
Perselisihan atas tata kelola dan manajemen dunia siber	End-to-end argument Layers principle Network neutrality “ Code is Law ”
Konflik siber demi keuntungan politik dan finansial	Kekuasaan negara untuk kontrol politik Tantangan dunia maya bagi negara Politik kompetitif melalui tempat siber

	Kejahatan siber dan spionase siber
Siber menjadi ancaman Nasional	Militerisasi siber Perang Siber Ancaman Siber terhadap infrastruktur *Cyber terrorism*

Tabel 1 3 Tahapan Konflik dalam dunia siber

Sumber : Cyberpolitics in international relations oleh Nazli Choucri hal. 127

Perselisihan cyber jenis pertama terjadi atas arsitektur Internet dan aturan yang membentuk konteks cyber. Konflik-konflik ini berakar dan tergolong *low politics*. Namun, dalam beberapa tahun terakhir, mereka menjadi lebih dipolitisasi karena perselisihan baru muncul mengenai pengelolaan tempat-tempat dunia maya. Bermigrasi ke ranah *high politics*, konflik semacam itu memanfaatkan kekuatan dan pengaruh di ranah nyata untuk membentuk parameter dunia maya (Choucri, 2012, Chapter 6, hal 126).

Konflik siber tipe kedua adalah tentang penggunaan tempat siber untuk keuntungan politik dalam domain riil tradisional dan/atau untuk keuntungan dan keuntungan. Konflik-konflik ini biasanya didominasi oleh kekhawatiran citra kedua. Mereka menjadi internasional ketika penggunaan pengaruh dunia maya mengancam untuk mengubah distribusi kekuasaan (Choucri, 2012, Chapter 6, hal 127).

Konflik siber tipe ketiga berkisar pada masalah nasional keamanan. Ancaman tersebut terdiri dari ancaman terhadap dukungan dunia maya terhadap infrastruktur dasar dan terhadap kemampuan dunia maya, yang didefinisikan secara luas. Jenis konflik ini adalah masalah citra kedua yang jelas berbasis negara — dengan pengecualian terorisme, yang juga dapat dilihat sebagai aktivitas citra pertama dengan efek difusi (Choucri, 2012, Chapter 6, hal 127).

c. Big Data dan Politik

Dalam jurnal *Big data and Internasional Relations* karya Andrej Zwitter menjelaskan bahwa pengaruh Big data dalam ilmu hubungan internasional. Bila kita berbicara hubungan internasional maka aktor nya adalah negara, namun dalam perkembangannya tidak hanya negara namun perusahaan bahkan individu. Kaitannya dengan big data adalah perusahaan sosial media sekarang, masih kurangnya legislasi dalam menangani kejahatan siber baik nasional maupun nasional merupakan tantangan bagi setiap negara kedepannya (Zwitter, 2015).

Pengumpul Big Data seperti penyedia media sosial, mesin pencari, bank, dan perusahaan pemasaran dan Teknologi Informasi menentukan data mana yang dikumpulkan, apa yang disimpan dan bagaimana, dan untuk berapa lama. Dalam hal kualitas dan kebenaran data ini, pembeli—termasuk pemerintah—berada di tangan perusahaan penambangan data dan pialang data yang sama ini (Zwitter, 2015).

Big Data semakin penting di semua lini kehidupan sosial dan politik, yang menunjukkan perlunya tata kelola untuk mengurangi bahkan menghapus potensi penyalahgunaan. Dalam domain siber, para aktor menemukan ruang yang semakin besar untuk menghindari pembatasan yang diberlakukan oleh undang-undang nasional, contohnya adalah situs Silk Road yang baru-baru ini dibongkar, bagian dari apa yang disebut dark web, yang memperdagangkan senjata dan obat-obatan secara ekstensif. Big Data menonjolkan tren ruang yang tidak diatur ini, karena praktik seperti pengumpulan data dan penambangan data secara inheren dapat dijangkau secara global. Tidak mengherankan bahwa perusahaan dan gudang data menggunakan berbagai strategi untuk menghindari undang-undang nasional dan regional yang mungkin membatasi praktik ini (Zwitter, 2015).

Substansi dunia maya global semakin mengaburkan perbedaan antara internasional dan domestik, antara perdamaian dan perang, antara aktor negara dan non – negara, dan antara teknologi, politik, dan ekonomi. Dunia maya global , dan intensifikasinya melalui sifat Big Data dan *Internet of*

Things yang ada di mana-mana, menantang kita untuk memikirkan kembali gagasan mendasar tentang hubungan internasional dan kekuasaan—gagasan yang kita telah menerima begitu saja selama beberapa dekade (Frederik Kremer dan Muller Benedikt, 2014).

Pada akhirnya ketika mengembangkan kerangka hukum, sifat Big Data dan modus operandi para pelaku di ranah siber semakin menunjukkan bahwa prinsip-prinsip saat ini yang memandu undang-undang nasional dan internasional tidak mencukupi. Kelompok-kelompok akan semakin membutuhkan mekanisme perlindungan hukum mereka sendiri. Untuk mengurangi kerentanan yang disebabkan oleh Big Data pada masyarakat, pemangku kepentingan yang berpengetahuan luas perlu meningkatkan kesadaran orang-orang tentang jebakan yang dibawa oleh Big Data dan jejak digital mereka sendiri (Frederik Kremer dan Muller Benedikt, 2014).

Big Data tentu saja menjanjikan untuk meningkatkan kesejahteraan global, dan bahkan mungkin untuk mencegah konflik. Namun demikian, itu juga bisa menjadi sumber banyak kejahatan. Satu-satunya cara untuk mengendalikan penyalahgunaan Big Data adalah dengan menciptakan kesadaran global dan menggunakan alat yang ditawarkan Big Data sendiri—media sosial dan keterhubungan global—untuk memungkinkan masyarakat sipil menjadi pengawas publik di era Big Data (Frederik Kremer dan Muller Benedikt, 2014).

Aspek penting dari hubungan catatan adalah pengembangan *linkage record* otomatis melalui penggunaan algoritma yang menetapkan probabilitas bahwa record dari satu kumpulan data dapat dicocokkan dengan yang lain. Keterkaitan rekaman juga difasilitasi oleh teknik geocoding. Kecocokan harus membawa tingkat kesalahan pengukuran yang dapat diterima tetapi tidak harus sempurna. Misalnya, aktivitas politik dalam bentuk kontribusi kampanye dapat dikaitkan dengan karakteristik profesional dan demografis individu di sebagian besar profesi berlisensi (kedokteran, hukum, keperawatan) atau pekerjaan pemerintah negara bagian dan dalam beberapa kasus dengan data pendapatan (pegawai pemerintah negara bagian, termasuk

akademisi dan dokter di rumah sakit universitas). Dalam memanfaatkan big data di perlukan data accuracy dan data acces. Data accuracy merupakan keakuratan data, dan data acces adalah siapa yang bisa mengakses data , apakah pemerintah, perusahaan atau invidu (Atif Mian dan Howard Rosenthal, 2016).

Report Making *Data Portability More Effective for the Digital Economy : Economic Implications and Regulatory Challenges* karya Jan Kramer dkk 2020 mengatakan bahwa Data – data yang di kumpulkan oleh pemerintah akan membantu dalam perekonomian Negara sehingga Negara perlu membuat kebijakan yang mengatur tentang Proteksi data pribadi warganya.

Contoh dalam hal pemanfaatan big data dalam bernegara kita bisa melihat bahwa Sosial Media menyediakan platform untuk mengumpulkan data yang dapat melengkapi jajak pendapat, yang awalnya dianggap terbatas, mahal, dan memakan waktu. Pengumpulan data dari pengaturan dunia nyata - jejak digital. memungkinkan kita untuk menangkap berbagai reaksi manusia, yang sebelumnya di luar jangkauan, terhadap perkembangan politik antara lain. Pilihan Inggris yang keluar dari Uni Eropa telah di dasarkan pada olahan big data sehingga Inggris tidak akan merugi terlalu banyak ketika dia keluar dari Uni Eropa (Georgiadou dkk., 2020).

Lebih lanjut di jelaskan dalam laporan yang di tulis oleh (Jacobson dkk., 2018) yang berjudul *Data Diplomacy - Updating diplomacy to the big data era* tentang pemanfaatan big data oleh Pemerintah di banyak negara untuk membuat kebijakan yang sesuai dengan kepentingan nasional dan tidak bertabrakan dengan norma internasional. Big data memiliki potensi untuk berkontribusi pada diplomasi dalam berbagai cara yang berbeda. Untuk fungsi inti dari diplomasi , pengumpulan informasi dan pelaporan diplomatik, negosiasi, komunikasi dan diplomasi publik, dan urusan konsuler , big data memiliki potensi untuk berkontribusi dengan wawasan dan membuat proses tertentu lebih efektif dan efisien. Namun, relevansi big data di bidang ini sangat bergantung pada sejauh mana proses ini dipandu terutama oleh atribut

manusia, seperti hubungan interpersonal, empati, pengalaman, dan pengetahuan ahli. Dalam semua kasus, big daa mendukung proses dan aktivitas tetapi tidak mengubahnya secara mendasar (Jacobson dkk., 2018).

E. Argumen

Dari Latar belakang dan penjabaran yang telah di sampaikan di atas maka penulis menarik argumen sebagai berikut :

- Kebangkitan China sebagai negara *superpower* mengharuskan Amerika Serikat berbenah dengan melakukan kebijakan isolasionis terhadap barang barang China yang kita kenal sebagi perang dagang. Kebijakan Trump dalam melakukan pemblokiran Tiktok di tahun 2020 menjadi salah satu faktor eskalasi Perang Dagang Amerika Serikat dan China.
- Terkait pemblokiran tiktok, Pemerintahan Trump menginginkan data masyarakat AS tidak di manfaatkan oleh kepentingan China. Selain itu big data, yang juga berasal dari sosial media menjadi pertarungan penting dalam pengaruh geopolitik kedua negara. Siapa yang menguasai big data akan menguasai ekonomi dunia di masa depan, ini juga karena peralihan keuangan ril menjadi uang digital.
- Kebijakan ini juga sebagai salah satu upaya pemerintahan Trump dalam menjaga industri teknologi dalam negeri Amerika serikat supaya tetap maju dan tetap menghegemoni. Meskipun kasus ini belum sepenuhnya diselesaikan di bawah Presiden Trump, pemerintahan Biden akan tetap dan terus mencari cara untuk menjaga TikTok memegang kendali di Amerika Serikat secara legal.

F. Metode Penelitian

Dalam penelitian ini, penulis mengunakan metode deskriptif - Kualitatif. Untuk mencari pengaruh keamanan siber terhadap perang dagang khususnya TikTok secara sistematis, penelitian ini melibatkan analisis konten kualitatif dengan menggunakan dokumen pemerintah AS dan China yang dikeluarkan antara April dan Agustus 2020 (periode di mana pemerintahan Trump secara aktif mengejar regulasi TikTok), serta data jurnal terkait dengan tema Perang dagang dan keamanan siber. Menggunakan pencarian

kata kunci dari situs web dan database pemerintah, 27 dokumen dikumpulkan di mana pernyataan dibuat tentang TikTok oleh pejabat negara AS dan China yang kemudian Penulis jadikan sebagai sumber Primer. Sumber AS termasuk dokumen yang diterbitkan oleh whitehouse.gov.

Sumber resmi Pemerintah China termasuk delapan transkrip bahasa Inggris dari konferensi pers yang diterbitkan oleh Kementerian Luar Negeri Republik Rakyat China: tiga oleh Juru Bicara Zhao Lijian dan lima oleh Juru Bicara Wang Wenbin. Bersama-sama, sumber-sumber ini berisi posisi politik dan tanggapan aktor negara AS dan China selama periode di mana pemerintahan Trump secara aktif mengejar regulasi TikTok dan, terutama, mereka menyajikan posisi yang sangat konsisten tentang TikTok untuk kedua negara bagian. Dokumen perusahaan mencakup empat belas pernyataan resmi yang dikeluarkan oleh eksekutif TikTok dan satu pernyataan resmi oleh Microsoft Inc.

Dari sumber saluran berita dari AS dan China, penulis mengumpulkan berita tentang perang dagang dan pelarangan tiktok di AS di CNN, Reuters, Al – Jazeera, South China Morning Post, Time, Globaltimes, Guardian, VoxEU, thediplomat sebagai rujukan utama, selain dari saluran berita online yang lain juga.

G. Sistematika Penulisan

Bab 1 berisi tentang Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Kajian Literatur Kerangka Teoritik, Hipotesis, Metodologi Penelitian serta Sistematika Penulisan. Pemaparan pada bab ini di harapkan menjadi awalan untuk pembahasan pada bab selanjutnya.

BAB II, memberikan penjelasan tentang hubungan dagang AS – China dari segi historis dan juga perjalanan dari hubungan dagang kedua negara hingga Pemerintahan Trump. Kemudian akan di jelaskan bagaimana hubungan dagang keduanya dalam beberapa periode pemimpin kedua negara dan Dinamika Hubungan Dagang berubah menjadi konflik yang pada

akhirnya menjadi Penyebab Perang Dagang serta bagaimana dampaknya terhadap masyarakat internasional.

BAB III, memberikan penjelasan tentang Perang Teknologi AS – China yang di mulai dari perang dagang. Kemudian penjelasan tentang Hubungan Siber AS – China lebih khusus di masa pemerintahan Trump, serta dinamika keduanya dalam dunia siber. Bab ini juga akan di paparkan bagaimana kekuatan siber AS dan China dan bagaimana keduanya mempengaruhi bisnis teknologi global.

BAB IV, Bab ini menjelaskan bagaimana Kebijakan Pemblokiran Tiktok oleh Donald Trump Sebagai Bentuk Perlindungan Keamanan Bisnis Teknologi Amerika Serikat. Dan juga akan menjelaskan tentang bagaimana pengaruh upaya pemblokiran tiktok terhadap perang dagang Amerika Serikat dan China.

BAB V, merupakan Kesimpulan membahas kesimpulan dari seluruh pemaparan yang telah dibahas dan dipaparkan dari bab – bab sebelumnya.