BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Saat ini, setiap negara di dunia harus menghadapi fenomena globalisasi yang tidak dapat dihindari. Globalisasi didorong oleh kemajuan teknologi yang berkelanjutan dan pertumbuhan yang cepat. Pengaruh globalisasi memiliki dampak yang signifikan dan meluas pada berbagai aspek kehidupan sehari-hari, termasuk interaksi sosial dan arus informasi. Revolusi digital atau "siber", di mana Teknologi Informasi dan Komunikasi (TIK) telah mengubah cara kita berinteraksi, bekerja, dan mengakses informasi, memiliki salah satu pengaruh terbesar yang dapat dirasakan saat ini.

Dalam konteks hubungan internasional, perkembangan teknologi telah membawa perubahan besar dalam interaksi hubungan internasional. Seiring dengan berkembangnya TIK, negara ataupun individu kini dapat terhubung secara lebih mudah dan cepat, hal ini membuat terjadinya perubahan dalam dinamika hubungan internasional. Seperti yang diketahui, studi hubungan internasional memiliki sifat yang sangat dinamis. Perkembangan teknologi yang terus menerus mengalami perkembangan merupakan salah satu faktor yang mempengaruhi sifat dinamis tersebut. Teknologi terus berkembang dan mempengaruhi cara negara-negara berinteraksi dan menjalin kerjasama.

Teknologi terus mengalami perkembangan dan menyebabkan terjadinya internetisasi dan digitalisasi dalam kehidupan, di mana segala aktivitas manusia saat ini secara keseluruhan menggunakan teknologi sebagai media utama. Hal ini dapat dilihat melalui munculnya sistem baru dengan pemanfaatan internet pada sistem kerja pemerintah *(e-government)*, pembayaran elektronik secara daring *(e-payment)*, transaksi daring *(e-commerce)*, sistem pembelajaran jarak jauh *(e-learning)*, perpustakaan berbasis daring *(e-library)* dan sebagainya.

Sejak terjadinya internetisasi dan digitalisasi dalam kehidupan, penggunaan teknologi telah menyebar ke seluruh dunia, dimana memungkinkan orang untuk terhubung dengan mudah satu sama lain melalui *handphone, email,* media sosial, dan aplikasi pesan instan. Hal ini membuat tidak ada lagi batasan geografis dalam berkomunikasi dan berinteraksi diseluruh dunia. Bahkan dengan saat ini informasi begitu mudah diakses dan dapat tersebar dengan begitu sangat cepat.

Dengan tidak adanya lagi batasan geografis dalam berkomunikasi dan berinteraksi di seluruh dunia, hal ini juga mengakibatkan interaksi antar aktor-aktor internasional yang kini tak lagi hanya terbatas pada ranah darat dan laut. Interaksi antar aktor juga terjadi di ruang maya atau disebut sebagai *cyberspace,* yang kini menjadi salah satu pilihan penting dalam mencapai suatu kepentingan negara. Perluasan ruang interaksi ini juga memperluas makna kekuasaan atau *power* dalam hubungan negara. Ukuran *power* dalam ranah darat dan laut lebih mudah untuk ditentukan dan diukur, namun hal ini tidak berlaku untuk *cyberspace*, yang justru mengaburkan standardisasi *power* tersebut. Dengan demikian, *cyberspace* telah

menjadi alat dan ruang baru dalam mencapai kepentingan yang disebut *cyberpower*. (Triwahyuni D, Yani Y. 2018)

Dalam konteks hubungan bilateral Tiongkok dan Amerika Serikat, peran dan pengaruh *cyberspace* telah menjadi salah satu elemen kunci yang memengaruhi dinamika hubungan mereka. Seiring dengan tidak adanya lagi batasan geografis dalam berkomunikasi dan berinteraksi di seluruh dunia, kedua negara telah memanfaatkan ruang maya atau *cyberspace* untuk mencapai berbagai tujuan nasional mereka. Di sinilah perdebatan seputar kebijakan terkait keamanan siber menjadi sangat relevan.

Hubungan bilateral antara Tiongkok dan AS telah menjadi topik yang menarik perhatian dunia internasional selama beberapa dekade terakhir. Sebagai dua negara dengan kekuatan ekonomi dan politik yang dominan, Tiongkok dan AS memiliki pengaruh yang signifikan dalam dinamika global terutama dalam bidang keamanan siber.

Kedua negara memiliki kepentingan dan ketergantungan yang saling berlawanan namun juga saling melengkapi dalam hubungan bilateral mereka. Kedua negara memiliki keterkaitan yang erat di sektor IT. Perusahaan-perusahaan teknologi terkemuka dari Tiongkok dan AS saling berinvestasi dan beroperasi di pasar masing-masing. Sebagai contoh, perusahaan AS seperti Apple, Microsoft, Intel, IBM, Qualcomm, dan CISCO memiliki kehadiran yang kuat di Tiongkok, sementara perusahaan Tiongkok seperti Huawei, ZTE, Xiaomi, dan Lenovo juga beroperasi di AS yang bahkan beberapa perusahaan elektronik Tiongkok telah

masuk sebagai daftar bursa saham elektronik terbesar di AS. (Triwahyuni D, Yani Y. 2018).

Selain itu, riset dan pengembangan serta inovasi teknologi juga menjadi bagian penting dari keterkaitan dalam bidang IT antara Tiongkok dan AS. Perusahaan-perusahaan teknologi AS melakukan riset dan pengembangan di Tiongkok, sementara perusahaan Tiongkok juga berkolaborasi dengan institusi dan perusahaan di Amerika Serikat untuk mengembangkan teknologi baru. Contohnya, perusahaan-perusahaan seperti Google dan Microsoft telah membuka pusat penelitian dan pengembangan di Tiongkok.

Meskipun terdapat keterkaitan dalam bidang IT antara Tiongkok dan AS, hubungan kedua negara seringkali terganggu oleh konflik yang menimbulkan ketegangan di antara mereka. AS telah menuduh Tiongkok melakukan serangan siber yang melibatkan pencurian data sensitif dan hak kekayaan intelektual dari perusahaan dan institusi AS. Pencurian ini diduga berpotensi dapat memberikan kerugian ekonomi bagi AS. Sementara itu, Tiongkok telah menolak tuduhan tersebut dan bahkan mereka menuduh kembali AS sebagai pelaku dibalik terjadinya serangan siber di Tiongkok.

Tiongkok dan AS juga memiliki perbedaan pandangan terkait keamanan siber mulai dari perbedaan ideologi dasar mereka. Dalam pandangan AS, internet yang ideal adalah platform yang terbuka dan aman, di mana akses dan kebebasan berekspresi diprioritaskan. AS mendorong nilai-nilai seperti transparansi, kebebasan bependapat, dan akses informasi yang tidak terbatas untuk semua individu. Mereka percaya bahwa internet harus menjadi alat yang dapat digunakan

oleh semua orang tanpa campur tangan atau kendali yang berlebihan dari pemerintah. (Kegley & Shannon, 2016).

Sedangkan Tiongkok menganggap keamanan siber sebagai bagian penting dari kedaulatan nasional dimana pemerintah memiliki kontrol penuh atas sumber daya siber di dalam negerinya. Pemerintah Tiongkok secara tegas mendukung prinsip kedaulatan siber yang menegaskan hak setiap negara untuk mengatur ruang siber mereka sendiri dan menolak campur tangan dalam urusan internal negara lain. Bagi Tiongkok, kedaulatan siber dilihat sebagai upaya untuk menjaga keamanan nasional serta melindungi kepentingan Tiongkok dalam dunia digital. Istilah ini juga disebut sebagai *cyber sovereignty* (Nigel Inkster, 2016).

Christensen dalam bukunya *"The China Challenge: Shaping of the Choices of a Rising Power"* menambahkan bahwasanya berbedanya pandangan antara Tiongkok – AS menyebabkan ketidakpercayaan dan kecurigaan strategis antara keduanya sehingga dapat meningkatkan kemungkinan terjadinya konflik.

"*Different definitions and prioritizations of national security interests, different threat perceptions, and different policies to protect these interests all contribute to a situation of strategic mistrust, even mutual suspicion, between Tiongkok and the United States. This clash of security architectures creates the potential for conflict that would be costly, dangerous, and counterproductive for all parties involved."* ("Perbedaan dalam definisi dan prioritas kepentingan keamanan nasional, persepsi ancaman yang berbeda, dan kebijakan yang berbeda dalam melindungi kepentingan tersebut semuanya berkontribusi pada situasi ketidakpercayaan strategis dan bahkan saling curiga antara Tiongkok dan Amerika Serikat. Benturan dari dua arsitektur keamanan ini menciptakan potensi konflik yang akan mahal, berbahaya, dan kontraproduktif bagi semua pihak yang terlibat.") (Christensen, 2015).

Hal ini menunjukkan kurangnya saling percaya antara kedua negara dan menghambat upaya untuk mencapai kesepakatan kerja sama dalam hal keamanan

siber. Kebijakan dan tindakan yang diambil oleh kedua negara dalam merespons serangan siber atau melindungi kepentingan negara akan terpengaruh oleh ketidakpercayaan tersebut.

Tiongkok mengeluarkan undang-undang keamanan siber atau *Cybersecurity Law* (CSL) yang disahkan dalam sesi pertemuan ke-24 dari Komite Tetap Kongres Rakyat Nasional ke-12 pada tanggal 7 November 2016, dengan jumlah 154 suara yang berjalan efektif pada 1 Juni 2017. (KPMG, 2017) CSL merupakan undang-undang pertama yang mengatur keamanan siber di Tiongkok secara menyeluruh dan sistematis.

Namun, jauh sebelum undang-undang tersebut diberlakukan, telah terjadi "keriuhan" besar di komunitas bisnis internasional. Dalam sebuah forum yang diselenggarakan di Hong Kong, Kepala Asosiasi Industri Sekuritas dan Pasar Keuangan Asia menyampaikan kekhawatirannya terhadap aturan dalam CSL. Undang-undang baru tersebut dikhawatirkan akan meningkatkan risiko pencuriaan kekayaan intelektual dan merugikan konsumen Tiongkok. (NY Times, 2016).

Hal lain juga dilakukan oleh lebih dari 46 kelompok bisnis termasuk AS, Eropa dan Asia melalui surat yang ditujukan kepada Perdana Menteri Li Keqiang, mereka menyatakan bahwa dengan diberlakukannya undang-undang ini akan menghalangi perusahaan asing dan pembangunan inovasi untuk masuk. (SCMP, 2016).

Cybersecurity Law Tiongkok (CSL) sendiri merupakan undang-undang yang mengatur berbagai aspek terkait keamanan siber dan penggunaan internet di Tiongkok. Beberapa aspek tersebut mencakup perlindungan data pengguna, konten

internet, keamanan jaringan, perlindungan konsumen, penegakan hukum, dan penyelesaian sengketa. (Digichina, 2017). Undang-undang ini dinilai memiliki cakupan yang luas dan berpotensi melebihi batas yang telah ditetapkan.

Sebagai peraturan pertama yang menyeluruh dalam hal privasi dan keamanan di dunia siber, undang-undang ini memberikan peningkatan perlindungan terhadap data dalam banyak aspek, namun juga menghadirkan tantangan kepatuhan komunitas global. Keadaan ini menjadi sangat menghawatirkan bagi entitas bisnis yang bergantung pada jaringan teknologi atau perusahaan yang mengandalkan lintas batas dan berbagi data bisnis. (Baker & Mckenzie, 2016).

Beberapa isi atau aspek dari CSL adalah:

- Mengharuskan operator infrastruktur informasi kritis melakukan penilaian keamanan sebelum memindahkan data keluar dari daratan Tiongkok, jika berisi informasi pribadi lebih dari setengah juta pengguna atau data yang memungkinkan dapat mempengaruhi keamanan nasional atau kepentingan publik sosial.
- Mengharuskan operator infrastruktur informasi kritis untuk menyimpan data pribadi dan data penting di dalam wilayah Tiongkok.
- Mengharuskan operator infrastruktur informasi kritis yang membeli produk dan layanan penting harus menjalani tinjauan keamanan nasional sebelum dijual di Tiongkok.

  (Digichina, 2017).

Konsep “infrastruktur informasi kritis” diperkenalkan dalam aturan CSL untuk pertama kalinya. Namun, CSL tidak menyebutkan penjelasan yang rinci dan jelas tentang apa saja yang termasuk dalam infrastruktur informasi kritis. CSL hanya memberikan definisi umum dan menyoroti beberapa industri dan sektor penting yang berpotensi sebagai infrastruktur informasi kritis. (Digichina, 2017). Dalam hal ini, pemerintah memiliki fleksibilitas yang cukup besar untuk memasukkan industri yang tidak secara eksplisit disebutkan dalam definisi ke dalam cakupan undang-undang di masa mendatang. Fleksibilitas ini memberikan dukungan bagi pemerintah terkhususnya Partai Komunis Tiongkok untuk tetap mempertahankan kendali.

Lalu beberapa hal yang menjadi perhatian lainnya dari CSL ialah ketentuan yang mewajibkan infrastruktur informasi kritis untuk menyimpan informasi pribadi dan data penting di dalam wilayah Tiongkok. Ketentuan ini dapat dipahami secara umum sebagai persyaratan bagi perusahaan asing untuk menyimpan server pengguna di Tiongkok dalam batas wilayah Tiongkok itu sendiri.

Untuk mematuhi ketentuan ini, perusahaan asing harus berinvestasi di server data baru di Tiongkok yang akan dikenakan pemeriksaan langsung pemerintah, atau mengeluarkan biaya baru untuk menyewa penyedia server lokal, seperti Huawei, Tencent, atau Alibaba. Perusahaan-perusahaan teknologi Tiongkok ini telah menghabiskan miliaran dalam beberapa tahun terakhir membangun pusat data domestik sebagai bagian dari Rencana Lima Tahun ke-12 Beijing (2011-2015). Investasi besar oleh perusahaan-perusahaan teknologi Tiongkok ini menunjukkan ambisi Tiongkok untuk meningkatkan kapasitas dan kompetensi teknologi

informasi dan komunikasi nasionalnya. Beberapa kritikus menganggap bahwa CSL sebagai bentuk proteksionisme yang dirancang untuk meningkatkan manajemen data domestik Tiongkok dan industri telekomunikasi terhadap pesaing global.

Persyaratan lokasi yang terlalu luas menghambat pertumbuhan ekonomi dan memisahkan Tiongkok dari ekonomi digital global. Posisi ini mendekatkan Tiongkok pada pencapaian *"cyber sovereignty"* yang diinginkannya, namun juga menimbulkan beberapa kekhawatiran bagi operator infrastruktur informasi kritis dengan biaya tambahan dan risiko adanya pencurian keamanan data.

Dalam demokrasi konvensional, umumnya terdapat batasan hukum yang mengatur aktivitas perusahaan terkait informasi serta batasan pemerintah dalam mengaksesnya. Namun, menurut seorang penulis dari beberapa buku dan artikel yang membahas tentang Tiongkok dan manajemen resiko, Daniel Wagner, *Cybersecurity Law* (CSL) dianggap dapat memberikan pemerintah akses yang tidak terbatas ke hampir semua data pribadi dan komersial. Kewenangan undang-undang memungkinkan Beijing untuk meminta akses ke kode sumber program komputer, yang biasanya hanya diketahui oleh pengembang perangkat lunak, dan tinjauan keamanan nasional (seperti yang terdapat dalam undang-undang CSL) juga dapat memberikan izin kepada Tiongkok untuk melakukan penyelidikan lebih mendalam ke dalam aset intelektual perusahaan. (Wagner, 2020).

Ketua Kamar Dagang Amerika Serikat di Tiongkok *(American Chamber of Commerce in China, AmCham China*) menyebutkan CSL yang luas sebagai tindakan yang membatasi inovasi di Tiongkok dan tidak memberikan kontribusi yang signifikan dalam meningkatkan keamanan. Ia juga mengkhawatirkan dampak

negatif CSL dapat mengurangi peluang untuk kerjasama siber yang lebih besar antara Tiongkok dan komunitas internasional terkhususnya Amerika Serikat itu sendiri. (Economist, 2016).

Cybersecurity Law (CSL) bertujuan untuk melindungi keamanan dan kedaulatan Tiongkok di ruang *cyber*. Salah satu faktor yang mempengaruhi pembuatan CSL adalah kepentingan nasional Tiongkok di *cyberspace*. Kepentingan nasional Tiongkok merupakan tujuan dan prioritas yang ditetapkan oleh pemerintah Tiongkok untuk menjaga kedaulatan, keamanan, dan kesejahteraan negara dan rakyatnya. Kepentingan nasional Tiongkok juga mencerminkan identitas, nilai-nilai, dan aspirasi Tiongkok sebagai negara besar yang memiliki sejarah, tradisi, ideologi, dan budaya yang khas.

Selain itu, kepentingan nasional Tiongkok juga dipengaruhi oleh kondisi dan tantangan yang dihadapi oleh Tiongkok di dalam dan luar negeri, seperti pertumbuhan ekonomi, stabilitas sosial, persaingan global, dan ancaman siber. Dengan memberlakukan CSL, pemerintah Tiongkok dapat melindungi dan memajukan kepentingan nasionalnya di *cyberspace.* Namun, CSL juga menimbulkan perbedaan pandangan antara Tiongkok dan negara-negara lain terkait dengan isu-isu keamanan siber, yang dapat mempengaruhi hubungan bilateral Tiongkok-AS di bidang ini.

Oleh karena itu, alasan peneliti memilih judul “Implikasi Kebijakan *Cybersecurity Law* Tiongkok Terhadap Hubungan Bilateral Tiongkok – Amerika Serikat (2017-2022)” adalah untuk untuk mengkaji kepentingan nasional Tiongkok dalam membuat kebijakan CSL tersebut dan implikasinya terhadap kebijakan CSL

terhadap hubungan bilateral Tiongkok – AS. Selain itu, topik ini menarik untuk diteliti karena hubungan kedua negara yang menjadi sangat penting dan kompleks. Tiongkok dan AS merupakan dua negara dengan ekonomi & *cyber power* terbesar di dunia dan memiliki pengaruh yang signifikan dalam politik global. Namun, hubungan bilateral antara kedua negara tersebut telah memburuk dalam beberapa tahun terakhir, khususnya terkait dengan isu-isu keamanan nasional, ekonomi, dan perdagangan.

Dari penelitian yang dibuat oleh Abdurahman Wahid dari Universitas Lampung tahun 2022 tentang "*Kebijakan Tiongkok dalam Menghadapi Cyber Warfare Pasca Serangan Amerika Serikat Tahun 2013"*. Penelitian ini menjelaskan bahwa terdapat 2 tahapan yang terjadi pada proses kebijakan Tiongkok dalam menghadapi *cyber warfare* itu sendiri, yang pertama melalui proses implementasi pembuatan kebijakan, dan yang kedua ialah dampak. Peneliti menemukan ada kesamaan dalam meneliti yaitu proses implementasi kebijakan Tiongkok itu sendiri. Perbedannya peneliti berfokus pada kebijakan siber Tiongkok melalui CSL tahun 2017. Sedangkan penelitian diatas berfokus pada kebijakan Tiongkok setelah peristiwa spesifik serangan Amerika Serikat pada tahun 2013 ke Tiongkok.

Dari penelitian yang dibuat oleh Fatihul Fikri dari Universitas Islam Indonesia tahun 2019 tentang "*Analisis Upaya Tiongkok untuk Menjadi Cyber Hegemon: Studi Kasus Alibaba Group*" Penelitian ini menjelaskan bahwa terdapat beberapa faktor yang mendasari ambisi Tiongkok untuk menjadi negara dengan *cyber hegemon*. Pertama, karakter dari pemimpin Tiongkok itu sendiri, Xi Jinping. Kedua, ekonomi Tiongkok yang kuat. Ketiga, faktor internal Tiongkok. Keempat,

faktor eksternal Tiongkok. Peneliti menemukan ada kesamaan dalam meneliti yaitu melihat potensi Tiongkok sebagai negara yang memiliki *cyber power* yang kuat. Perbedaannya peneliti lebih fokus pada kebijakannya. Sedangkan penelitian diatas berfokus pada upaya Tiongkok dalam ambisinya untuk menjadi negara *cyber hegemoni.*

Dari penelitian yang dibuat oleh Siti Annisa Meidiyani Gunawan dari Universitas Islam Negeri Syarif Hidayatullah Jakarta tahun 2022 tentang "*Diplomasi Tiongkok Terhadap Amerika Serikat Terkait Dunia Maya (Cyberspace)* tahun 2015-2019" Penelitian ini menjelaskan bahwa melalui diplomasi yang dilakukan oleh Tiongkok dan Amerika Serikat, mereka berhasil mencapai kesepakatan dasar dalam membangun dialog tentang keamanan siber dan menjaga hubungan bilateral yang stabil. Tiongkok mendorong pendekatan diplomasi siber untuk mencapai tujuannya menjadi "kekuatan siber" dan mempromosikan prinsip kedaulatan siber sebagai prinsip utama dalam tata kelola siber. Peneliti menemukan ada kesamaan dalam meneliti yaitu fokus dalam meneliti Tiongkok dengan prinsip keamanan sibernya *internet sovereignty*. Perbedaanya peneliti lebih fokus pada implikasi dari kebijakan yang diberlakukan Tiongkok melalui CSL terhadap hubungan Tiongkok – Amerika Serikat. Sedangkan penelitian diatas berfokus pada diplomasi Tiongkok ke Amerika Serikat.

Adapun mata kuliah yang telah mendasari penelitian ini yang sesuai dengan kurikulum Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia yaitu:

1. Hubungan Internasional di Asia Timur

   Mata kuliah HI di Asia Timur mempelajari tentang hubungan internasional di Asia Timur dan membahas berbagai negara di kawasan tersebut, termasuk Tiongkok yang terletak di Asia Timur. Mata kuliah ini telah membantu peneliti untuk memahami dan menganalisis kebijakan Tiongkok yang telah dilakukan sebelumnya dan yang sedang berlangsung.

2. Hubungan Internasional di Amerika Utara

   Mata kuliah HI di Amerika Utara mempelajari tentang hubungan internasional di Amerika Utara dan membahas berbagai negara di kawasan tersebut, termasuk Amerika yang berada di Amerika Utara. Mata kuliah ini telah membantu peneliti untuk memahami dan menganalisis kebijakan luar negeri Amerika Serikat yang telah dilakukan sebelumnya dan yang sedang berlangsung.

3. Politik Luar Negeri

   Mata kuliah politik luar negeri mempelajari tentang interaksi suatu negara dalam menjalankan hubungan dengan negara-negara lain di dunia melalui strategi dan kebijakannya. Mata kuliah ini telah membantu peneliti untuk menganalisa arah kebijakan luar negeri Tiongkok dan kepentingan Amerika Serikat melalui beberapa kebijakan siber yang telah dikeluarkan Tiongkok tersebut.

4. Studi Keamanan Internasional & Lanjutan

   Mata kuliah studi keamanan internasional dan lanjutan mempelajari tentang segala interaksi yang berkaitan dengan keamanan, baik yang bersifat nasional maupun internasional. Mata kuliah ini telah membantu peneliti untuk melihat kebijakan siber di Tiongkok melalui perspektif keamanan.

5. Keamanan Siber / *Cyber Security*

   Mata kuliah keamanan siber mempelajari tentang ancaman keamanan siber terhadap keamanan negara termasuk bagaimana tindakan negara dalam menangani kejahatan siber. Didalam mata kuliah siber juga mempelajari tentang bagaimana interaksi kerja sama internasional dalam mengatasi masalah siber. Mata kuliah ini telah membantu peneliti dalam menganalisis strategi keamanan Tiongkok dalam *cyber security.*

6. Hukum Siber / *Cyber Law*

   Mata kuliah hukum siber mempelajari tentang berbagai aspek hukum yang terkait dengan teknologi informasi dan internet. Mata kuliah ini telah membantu peneliti untuk menganalisa salah satu kebijakan siber yang dikeluarkan *China Cybersecurity Law.*

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Dengan berdasarkan latar belakang yang telah diuraikan sebelumnya, peneliti mengambil rumusan masalah utama yang akan diteliti dalam penelitian ini adalah sebagai berikut “Bagaimana kebijakan CSL Tiongkok dan implikasinya terhadap hubungan Tiongkok dan Amerika Serikat (2017-2022)?”

1.2.2 Rumusan Masalah Minor

Adapun rumusan masalah minor yang akan dirumuskan oleh peneliti, adalah sebagai berikut:

1. Apa kepentingan nasional Tiongkok dalam membuat kebijakan CSL Tiongkok tahun 2017?
2. Bagaimana perubahan keamanan siber di Tiongkok setelah diberlakukannya CSL tahun 2017?
3. Bagaimana respon Amerika Serikat terhadap diberlakukannya CSL Tiongkok tahun 2017?
4. Bagaimana hubungan Tiongkok dan AS setelah diberlakukannya CSL Tiongkok tahun 2017?

1.2.3 Pembatasan Masalah

Dengan berdasarkan latar belakang dan rumusan masalah yang telah diuraikan sebelumnya, peneliti menentukan jangka waktu yang akan diteliti dalam kurun waktu 6 tahun terakhir, yaitu tahun 2017 hingga 2022. Pembatasan waktu tersebut dipilih oleh peneliti karena *Cybersecurity Law* Tiongkok sendiri baru berjalan efektif pada 1 Juni 2017, sehingga dalam hal ini konteks penelitian akan fokus setelah CSL berjalan hingga 2022 untuk mengukur terkait sejauh mana dan respon AS terhadap diberlakukannya CSL. Oleh karena itu, membatasi penelitian pada periode tersebut dapat membantu dalam menganalisis dampak kebijakan siber Tiongkok terhadap hubungan Tiongkok-AS secara lebih komprehensif.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud dari penelitian ini adalah untuk mengetahui implikasi dari kebijakan *Cybersecurity Law* terhadap hubungan Tiongkok dan AS (2017-2022).

1.3.2 Tujuan Penelitian

Berikut adalah beberapa tujuan dilakukannya penelitian ini:

1. Untuk mengetahui dan menganalisa kepentingan nasional dalam membuat kebijakan CSL Tiongkok tahun 2017
2. Untuk mengetahui dan menganalisa bagaimana perubahan keamanan siber setelah diberlakukannya CSL Tiongkok tahun 2017

3. Untuk mengetahui dan menganalisa bagaimana respon Amerika Serikat terhadap diberlakukannya CSL Tiongkok tahun 2017
4. Untuk mengetahui dan menganalisa bagaimana hubungan Tiongkok dan AS setelah diberlakukannya CSL Tiongkok tahun 2017

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini diharapkan dapat memberikan konstribusi bagi pengembangan dan penalaran terkait keamanan siber dalam Ilmu Hubungan Internasional untuk membantu memahami dinamika hubungan bilateral antara dua negara besar yakni Tiongkok dan Amerika Serikat. Hal ini diharapkan dapat memberikan konstribusi pada pemahaman teoritis tentang bagaimana kebijakan domestik sebuah negara dapat mempengaruhi hubungan internasionalnya, terutama hubungan bilateral dengan negara lain.

1.4.2 Kegunaan Praktis

Kegunaan praktis penelitian ini untuk peneliti sendiri tentunya guna memperoleh gelar Sarjana S-1 (strata satu) pada Program Studi Ilmu Hubungan Internasional, Universitas Komputer Indonesia. Kegunaan praktis lainnya peneliti berharap dengan dibuatnya penelitian ini dapat membantu meningkatkan kesadaran tentang isu-isu keamanan siber yang terkait dengan hubungan Tiongkok-Amerika Serikat. Ini dapat mendorong diskusi publik yang lebih luas tentang isu keamanan

siber itu sendiri. Juga, penelitian ini diharapkan dapat memberikan beberapa rekomendasi yang dapat membantu meningkatkan kerjasama dan koordinasi antara Tiongkok dan Amerika Serikat dalam menangani ancaman-ancaman siber yang bersifat transnasional dan memerlukan respons kolektif.