BAB I

PENDAHULUAN

1. Latar Belakang Penelitian

Hubungan internasional merupakan sebuah studi tentang interaksi yang terjadi di antara negara-negara berdaulat. Namun tidak hanya hubungan antar negara, hubungan internasional juga berkaitan dengan pelaku-pelaku non negara (*non states actors*) Aktor dalam hubungan internasional (HI) meliputi, negara, International *Non-Governmental Organization*, *International Organization*, perusahaan multinasional, dan bahkan individu dapat menjadi aktor dalam hubungan internasional. Menurut Darmayadi dkk (2015:25)

Dalam studi hubungan internasional sendiri, terdapat beberapa elemen penting yaitu aktor internasional, kepentingan nasional dan kekuasaan, beberapa hal tersebut dapat membantu untuk menjelaskan mengapa setiap negara saling berinteraksi. Setiap negara dalam kaitannya dengan negara lain tentu memiliki sebuah tujuan, dan tujuan tersebut yang mengarah pada terciptanya kepentingan nasional.

Kepentingan nasional ini menjadi formula bagi setiap negara untuk membuat sebuah kebijakan luar negeri terhadap negara lain. Pada dasarnya, kepentingan nasional didasarkan pada keputusan negara yang didasarkan atas kesejahteraan rakyatnya, dalam hal ini kita dapat mengajukan pertanyaan dengan menjelaskan apa yang kita inginkan dari sebuah negara, dan setidaknya ada lima

dasar nilai yang kita ingin negara melakukannya, yaitu keamanan, kebebasan, pemerintahan, keadilan dan kesejahteraan (Jackson & Sorensen, 2010).

Hubungan Internasional berjalan dengan sangat dinamis, dimana mengalami perubahan dan perkembangan dari waktu ke waktu di mulai dari perubahan dalam sistem kenegaraan, perkembangan teknologi hingga peran negara tidak hanya melibatkan dominasi negara barat namun melibatkan juga negara berkembang. Perkembangan teknologi informasi dan komunikasi khususnya internet telah menciptakan sebuah dunia baru yang menghilangkan batas ruang dan waktu yang disebut dengan *cyberspace* (dunia maya), yaitu sebuah dunia komunikasi berbasis ranah jaringan komputer (dan pengguna di belakangnya) dimana informasi disimpan, dibagi, dan dikomunikasikan secara online.

Pemanfaatan teknologi mengubah cara pandang negara – negara di dunia internasional. Situasi di berbagai aspek kehidupan seperti politik, sosial, keamanan secara otomatis berubah dan dihadapkan pada komputer dan internet. Maka dari itu *cyberspace* dianggap sebagai interkoneksi manusia melalui komputer dan telekomunikasi, tanpa memperhatikan geografi fisik, yang artinya tanpa mengenal batasan-batasan antar negara sekalipun. Tidak ada batas-batas wilayah kedaulatan negara dalam *cyberspace*, tidak seperti dalam dunia nyata ada batas wilayah fisik kedaulatan sebuah negara.

Selain memberikan banyak manfaat yang positif dalam kehidupan manusia, *cyberspace* pun memberikan peluang bagi penggunanya untuk

melakukan tindakan-tindakan dengan akses yang ilegal seperti manipulasi atau mengambil data rahasia dari sistem informasi atau penyimpanan data atau penyusupan ke dalam sistem penyimpanan informasi dan atau masuk ke dalam sebuah sistem informasi, dimana hal tersebut dapat membahayakan kehidupan manusia pada tingkat individu dan membahayakan kelangsungan hidup sebuah negara. Apabila tidak mendapatkan perhatian serta penanganan yang tepat Kondisi pun dapat menimbulkan potensi ancaman pada ruang siber. Terlebih bagi negara-negara maju dimana seluruh kegiatan dan aktivitas pemerintahan dan ekonomi telah terintegrasi dalam *cyberspace* maka setiap ancaman akan menjadi gangguan serius bagi keamanan nasional sebuah negara.

Cyberspace sendiri memberikan peluang terhadap ancaman *cyber attack* yang berbahaya. Ancaman tersebut bagi keamanan siber dapat dikategorisasikan berdasarkan kepada aktor dan motivasi. Juga masalah-masalah yang terjadi karena adanya kebebasan ruang maya. Salah satunya adalah *cyber attacks* atau penyerangan siber.

Cyber attacks dapat mengganggu aktivitas jaringan informasi berupa digital yang gunakan oleh individu, perusahaan, atau bahkan sekelas pemerintahan pun dapat terserang. *Cyber attacks* menimbulkan berbagai konflik mengenai dunia *cyberspace* antara negara yang mempunyai power, dan pada akhirnya menimbulkan rasa ketidakpercayaan dan kewaspadaan yang serius tentang bagaimana masing-masing negara mempersiapkan bagaimana pertahanan negara sendiri untuk memenuhi kepentingan nasionalnya.

Cyberpower saling berkorelasi antara *cyber attack* dan *cyberspace*, konsep dari *cyberpower* sendiri menjelaskan kapabilitas suatu negara untuk dapat melakukan aksi atau memiliki pengaruh dalam *cyberspace*. *Cyberpower* kemudian menjadi alat bagi negara untuk menjalankan *cyber warfare.*

Saat ini, Tiongkok memang mengalami pertumbuhan yang besar dalam perkembangan industri teknologi cyber. Perkembangan dari teknologi cyber menjadi salah satu pertimbangan dalam konflik masa depan melalui cyberspace. Pada awalnya, Tiongkok mengembangkan teknologi cyber agar membawa modernisasi di Tiongkok, terutama sebagai support dalam pertumbuhan perekonomian nasional. Tapi, teknologi cyber dalam dunia internasional telah mengalami perluasan yang dimanfaatkan oleh negara-bangsa sebagai kegiatan defense atau offensive pada saat terjadinya perang/konflik. Alasan tersebut berdasarkan pada peningkatan dalam penggunaan teknologi cyber yang dimanfaatkan untuk modernisasi militer melalui penggabungan teknologi informasi dan militer. Presiden Xi Jinping bahkan mendorong tentaranya untuk mengubah pola pikir tentang perang konvensional menjadi perang informasi seperti yang dihadapi oleh Tiongkok dan negara lain. Fokus utama pemerintah Tiongkok adalah melakukan Peningkatan kapabilitas *cyberpower* untuk menjaga stabilitas sosial, ekonomi, dan politik negaranya dari pengaruh negara lain. Tiongkok gencar meningkatkan kapabilitas *cyberpower* negaranya terlihat dari upaya yang secara signifikan merekrut tentara siber untuk mengamankan sistem pertahanan teknologi Tiongok yang disebut dengan *online blue army* serta

pengembangan *Teknologi Anti Satellite* (ASAT) dan juga pembentukan *Computer Network Operation* (CNO).

Tiongkok mengembangkan teknologi anti satelit (Anti-Satellite). *Teknologi Anti Satellite* (ASAT) merupakan teknologi senjata antariksa yang digunakan dan memiliki kapabilitas untuk mengganggu satelit lain, serta dapat menghambat kemampuan sebuah negara untuk mendapatkan informasi rahasia atau dapat menyerang langsung satelit yang berada di orbit. Teknologi ASAT dapat dimanfaatkan sebagai persenjataan yang dapat menghancurkan satelit ataupun persenjataan musuh yang dapat menjadi ancaman bagi keamanan negara.

Selain membangun Teknologi Anti Satellite (ASAT) , Penguasaan Teknologi Informasi membawa fase baru pada Tiongkok dengan memanfaatkan *cyberspace* sebagai keuntungan nasional. Peningkatan kemampuan dalam teknologi *cyber*, Tiongkok mulai melaksanakan serangan cyber keberbagai Negara. Pasca pembentukan *Unit 61398* dan *Online Blue Army*, Tiongkok mulai mengembangkan *cyber operation* sebagai langkah awal untuk melaksankan *cyber warfare*. Chinese People's Liberation Army (PLA) melakukan investasi dalam *electronic countermeasure*, pertahanan dalam serangan elektonik (seperti: perangkap elektronik dan inframerah, angle reflector dan false target generator) dan *computer network operation* (CNO). *Computer network operation* (CNO) merupakan bagian paling utama dalam melaksanakan aktifitas *cyber operation* dan Chinese People's Liberation Army (PLA) bertanggungjawab dalam pelaksaaan *computer network operation* (CNO) tersebut.

Selain membangun Teknologi Anti Satellite (ASAT) dan pembentukan *computer network operation* (CNO), Tiongkok juga membentuk *Online Blue Army* yang merupakan bentuk realisasi dari peningkatan *cyber* teknologi Tiongkok. *Online blue army* berada di bawah angkatan darat Chinese People's Liberation Army (PLA) yang dipersiapkan untuk memperkuat cyber security Tiongkok dari serangan siber negara lain. Pada era digital saat ini, Tiongkok sangat bergantung pada *cyberspace* dalam menjalankan kegiatan di sektor ekonomi, politik, militer dan juga hubungan antar negara yang dijalin. Peningkatan terhadap penggunaan teknologi *cyber*, menjadi bagian penting dari sendi kehidupan di Tiongkok. Pendirian *Online Blue Army* disiapkan dalam menghadapi ancaman *cyber attack*, khususnya saat terjadinya *cyber war*. Saat ini, negara-negara mulai mengembangkan TI untuk meningkatkan kemajuan negara tersebut. Negara-negara yang menguasai teknologi siber yang tinggi akan menggunakan kemampuan dari efektifitas TI untuk melancarkan *cyber threat* melalui jaringan *cyberspace* ketika terjadi perang.

Dari munculnya ketiga fenomena tersebut membuat keresahan serta ancaman bagi negara lain khususnya negara yang menjadi satu kawasan dengan Tiongkok tersebut, pada dasarnya bahwa Asia Timur merupakan suatu kawasan yang memiliki berbagai macam potensi sumber daya alam. Potensi yang dimiliki mengakibatkan negara-negara di Asia Timur saling berkompetisi melakukan aksi klaim atas wilayah yang menjadi primadona akan kekayaan sumber daya yang dimiliki, contohnya yakni Laut Tiongkok Selatan.

Kemampuan yang kuat secara ekonomi dan militer, membuat posisi diplomatik Tiongkok sangat berpengaruh di dalam kawasan Asia Timur. Semua ini membuat cemas negara-negara di kawasan itu seperti Jepang, Taiwan dan Korea Selatan. Perkembangan terbaru menunjukkan bahwa Tiongkok sudah mengungguli Jepang dalam hal cadangan devisa dan hal itu membuat perekonomian Tiongkok semakin kuat sehingga Tiongkok telah menaikan anggaran pertahanannya dan terus membangun sistem pertahanan dalam bidang cyber. (Erwinsyah, 2011)

Jepang menanggapi ancaman siber dari Tiongkok melalui postur keamanan siber nasionalnya saat ini berimplikasi pada hubungan yang kompleks antara Jepang dan Tiongkok. Sikap Jepang terhadap Tiongkok di dunia maya adalah perpanjangan dari kegiatan keamanan dunia maya yang ada di negara itu, yang telah berkembang selama dua dekade terakhir. Pada masa ini yang bertanggung jawab dan berwewenang perihal keamanan siber Jepang pada tingkat nasional dialokasikan dan dilakukan pembagian di beberapa kementerian yang berbeda dan beberapa divisi pada pemerintahan seperti Kementerian Pertahanan, Kementerian Luar Negeri, dan Badan Kepolisian Nasional. Pusat Kesiapan Insiden dan Strategi Nasional untuk Keamanan Siber (NISC) memiliki tindakan selaku badan yang melakukan pengkoordinasian terhadap keamanan siber di seluruh pemerintahan, meliputi tim tanggap darurat komputer nasional (CERT) serta menciptakan berbagai strategi, standar, dan rencana keamanan siber.

Untuk meminimalisasi ancaman siber Tiongkok pada bidang militer, Kementerian Pertahanan Jepang telah melakukan penekanan terhadap peningkatan dan koalisasi kemampuan keamanan siber Pasukan Bela Diri Jepang melalui Komando Pertahanan Siber baru dengan memberikan investasi senilai 35,7 miliar yen yang setara dengan $341 juta untuk pelatihan dan teknologi keamanan siber yang lebih baik. Pada tahun 2021, kemampuan keamanan siber tersebut mengalami peningkatan yang signifikan sebesar 39,4 persen dari tahun 2020. Namun, Pasal 9 dan 21 dari konstitusi pasifis Jepang pascaperang mencegah SDF untuk terlibat dalam perang pre-emptive dan pengawasan domestik masing-masing. Ini membatasi pengembangan dan penerapan strategi keamanan siber holistik Kementerian Pertahanan terhadap Tiongkok yang akan mencakup kapasitas intelijen siber dan domestik ofensif.

Implikasi terhadap hubungan Jepang dengan Tiongkok pada tingkat politik, ketegangan yang lebih besar antara Jepang dan Tiongkok di dunia maya sepertinya tidak akan memperburuk hubungan bilateral saat ini secara signifikan. Begitu juga dengan sebaliknya, konflik yang terjadi pada ruang siber memiliki kemungkinan akan menjadi produk cadangan dari ketiga masalah geopolitik utama yang terjadi antar kedua negara jika masalah tersebut mengalami peningkatan. Masalah yang pertama adalah Tiongkok terus melakukan penentangan terhadap tuntutan kedaulatan Jepang pada wilayah tertentu di Laut Tiongkok Timur, melalui serangan secara berulang ke kawasan maritim Jepang. Kedua, sikap Tiongkok yang semakin agresif terhadap Taiwan sudah menjadi pendorong Jepang untuk mengemukakan komitmen negaranya terhadap

keamanan pulau Okinawa tersebut. Ketiga, apabila terjadi perang antara Tiongkok dengan Amerika Serikat, yang akan menjadi target utama militer Tiongkok adalah negara Jepang. Hal tersebut terjadi karena Jepang akan menjadi titik konsentrasi terbesar pasukan militer Amerika Serikat di Asia-Pasifik, termasuk pangkalan pulau Okinawa yang tidak jauh dari Taiwan.

Di bidang ekonomi, kondisi keamanan siber yang dimiliki Jepang dapat merusak hubungan perdagangan yang berjalan dengan baik dengan Tiongkok. Kebijakan yang tersedia untuk menanggulangi rasa khawatiran terhadap keamanan cadangan baik perangkat lunak maupun perangkat keras, investasi asing, serta pemindahan teknologi sudah menjadi paksaan terhadap perusahaan Jepang untuk memodifikasi industri manufaktur, distributor, dan kegiatan investasi Jepang dari Tiongkok. Hal tersebut menjadi penyebab Tiongkok membalas dengan melakukan peningkatan terhadap pengawasan pada investasi dan operasi asing. (Kompas,2021)

Terlepas dari upaya pemisahan yang dilakukan oleh Jepang, Tiongkok masih merupakan pasar utama untuk ekspor Jepang, yang lebih sulit untuk menggantikan perusahaan Jepang daripada pemasok. Begitu juga dengan Tiongkok yang sudah jelas memberi pernyataan terhadap niat negara tersebut untuk melakukan pengembangan ekonomi domestik yang mandiri sekaligus mendorong ketergantungan asing yang lebih besar pada Tiongkok dalam rantai cadangan negara Tiongkok di bawah strategi Made in Tiongkok 2025. Apabila dilihat secara keseluruhan dari hubungan perdagangan yang memburuk antara

Jepang dan Tiongkok, tentu Jepang kehilangan lebih banyak kerugian secara ekonomi dibandingkan dengan Tiongkok sebagai akibat dari respons keamanan siber yang lebih eksplisit, yang melibatkan kebijakan untuk melakukan pembatasan terhadap pertukaran komersial (Matsubara, 2021).

Jepang pada dasarnya memiliki keinginan untuk meningkatkan kerja sama bilateral dengan Korea Selatan dalam menghadapi tidak pastinya atas perkembangan Tiongkok dan Korea Utara. Namun Korea Selatan tidak menunjukkan keinginan yang sama, pasalnya Korea Selatan tidak memiliki anggapan ancaman yang sama terhadap Tiongkok. Korea Selatan melihat bahwa meningkatkan hubungan dengan Tiongkok merupakan pilihan yang tidak dapat dihindarkan demi menghadapi isu nuklir dari Korea Utara. Hal ini kemudian yang membuat PM Shonzo Abe lebih dominan kepada Amerika Sentris daripada Asia Sentris. Pemerintahan Jepang pada masa ini lebih meningkatkan hubungan dengan Amerika Serikat dalam berbagai bidang terutama keamanan Kedua negara bersepakat untuk bertukar pandangan mengenai isi dari kesepakatan keamanan informasi (Ministry of Japan, 2015).

Pada bulan Oktober tahun 2014 Jepang dan Korea Selatan datang dalam acara Seoul Defense Dialogue yang diadakan di Korea Selatan. Pada bulan April 2015 telah diselenggarakan pembicaran mengenai dialog keamanan dalam hal kebijakan keamanan serta kebijakan pertahanan pada tingkat working – level antara kedua negara sebagai yang pertama dalam lima tahun terakhir. Di perairan barat Kyushu, Japan Maritime Self Defense Force (JMSDF) mengadakan latihan

bilateral penyelamatan (search and rescue bilatiral exercise) pada bulan Desember 2013, yang kemudian meningkatkan koordinasi anatara JMSDF dengan Angkatan Lut Korea Selatan (Mus,A, 2014).

Dalam menanggapi kebijakan Air Defense Identification Zone (ADIZ) Tiongkok, Jepang melakukan patrol udara di Laut Tiongkok Timur begitu pula dengan Korea Selatan yang juga melakukan patrol udara, serta membeli sejumlah drone, atau pesawat militer tanpa awak untuk memantau situasi di kawasan dan tank amfibi (Mus,A, 2014).

Sama halnya Jepang dan Korea Selatan dalam menghadapi tidak pastinya atas perkembangan Tiongkok dan Korea Utara. Pemerintah Taiwan mendesak rakyatnya untuk waspada terhadap "Inflitrasi di mana-mana dari Tiongkok". Infiltrasi tersebut melibatkan mulai dari kampanye media yang didukung Tiongkok hingga serangan dunia maya. "Kelompok peretas Tiongkok telah menyusup ke lembaga pemerintah dan penyedia layanan informasi untuk waktu yang lama," kata wakil direktur Kantor Investigasi Keamanan Siber Biro Investigasi Taiwan, Liu Chia-zung. Liu menambahkan kelompok peretas tersebut bertujuan untuk mendapatkan dokumen dan data penting pemerintah.

Liu mengatakan Taiwan yakin dua kelompok peretas yang melakukan serang siber yakni Blacktech dan Taidoor didukung oleh Partai Komunis Tiongkok. Serta menambahkan penargetan celah dalam sistem yang disediakan oleh penyedia layanan informasi pemerintah Taiwan.

Dan upaya-upaya modernisasi militer Tiongkok ini memberi ancaman kepada negaranegara Asia Timur dan *deterrent effect* itu membuat negara-negara tetangganya ikut memperkuat militer mereka sebagai upaya mempertahankan diri (*self-defense*). Ini tentunya membuat suasana menjadi panas dan secara tak langsung Tiongkok telah membuat instabilitas, padahal stabilitas sebuah kawasan adalah kunci untuk meningkatkan pertumbuhan ekonomi secara regional. (Erwinsyah, 2011)

Melihat laju modernisasi Tiongkok yang sedemikian pesatnya, tentu negara-negara tetangganya akan mempersiapkan segala kemungkinan terburuk apabila suatu saat Tiongkok berubah haluan menggunakan kekuatan militernya dari yang awalnya untuk tujuan defensif menjadi ofensif. Misalnya seperti apa yang dilakukan Korea Utara dengan program pengembangan senjata nuklir dan teknologi rudalnya, dan Taiwan yang juga mulai meningkatkan pertahanan dalam negerinya dengan mempertimbangkan juga permasalahan dengan Tiongkok yang tidak kunjung selesai, karena tidak adanya kesepakatan untuk saling mengendurkan tensi mengenai status Taiwan yang masih ditentang Tiongkok. Faktorfaktor itulah yang mempengaruhi stabilitas keamanan dan perdamaian di Asia Timur, dan membuat kondisi keamanan di kawasan tidak kondusif.

Peneliti memilih judul ini untuk mengetahui dan menganalisa apa kepentingan Tiongkok dalam menjadi *cyber power* di kawasan Asia Timur. Serta motivasi apa yang menjadi dorongan yang kuat Tiongkok dalam peningkatan cyber pada kawasan Asia Timur. Dan pemaparan diatas menjadi pendorong untuk

peneliti supaya mengkaji lebih dalam dan mengembangkan pengetahuan studi Hubungan Internasional.

Dari penelitian yang dibuat oleh Guntomo Raharjo dari Universitas Islam Negeri Syarif Hidayatullah Jakarta tahun 2016 tentang "Strategi Amerika Serikat dalam Menghadapi Eskalasi Cyber Power Tiongkok 2011-2015". Peneliti menemukan kesamaan dalam meneliti yaitu kesamaan konsep-konsep yang digunakan. Seperti *cyberpower* serta kebijakan yg dikeluarkan oleh Tiongkok. Tetapi perbedaannya peneliti meneliti terkait kepentingan Tiongkok dalam menjadi *cyberpower* di kawasan Asia Timur sedangkan peneliti diatas meneliti terkait serangan Amerika Serikat dan Tiongkok dan melakukan kembali Perjanjian Siber tersebut di 2015.

Penelitian karya tulis akhir yang dilakukan oleh Kukuh Ugie Sembodho tentang "Keterbatasan Amerika Serikat Terhadap Serangan Siber Korea Utara". Peneliti menemukan kesamaan konsep ditemukan ialah, Seperti *cyber attack* dan *cyber security*. Tetapi perbedaannya peneliti meneliti terkait kepentingan Tiongkok dalam menjadi *cyberpower* di kawasan Asia Timur sedangkan peneliti diatas meneliti terkait Penelitian bagaimana pergeseran konsep keamanan dalam ruang siber dan bagaimana penerapanya dalam kasus Amerika Serikat dan Korea Utara.

Dari penelitian yang dibuat oleh Nadya Vira Meisitha tentang "Motivasi Tiongkok Menguasai Cyber Teknologi" Peneliti menemukan kesamaan dalam kepentingan serta motivasi Tiongkok dalam menguasai cyber teknologi. Tetapi

perbedaannya peneliti meneliti motivasi Tiongkok dalam menguasai cyber teknologi pada kawasan Asia Timur. Sedangkan peneliti diatas meneliti terkait motivasi Tiongkok untuk menguasai cyber teknologi di Taiwan.

Alasan dalam pemilihan topik ini yakni temuan awal mengenai aktivitas siber Tiongkok yang terus berkembang serta mengalami kemajuan yang signifikan tentunya hal ini membuat penulis ingin meneliti lebih lanjut perihal motivasi di balik perlakuan Tiongkok tersebut. Hal ini yang mendorong peneliti untuk tertarik meneliti dengan judul "Dampak Pembangunan Cyberpower Tiongkok di Kawasan Asia Timur" dengan tujuan mengetahui dan menganalisa apa kepentingan Tiongkok dalam menjadi *cyberpower* di kawasan Asia Timur. Serta motivasi apa yang menjadi dorongan yang kuat Tiongkok dalam meningkatan cyber pada kawasan Asia Timur.

Penelitian ini berdasarkan pada beberapa mata kuliah dalam kurikulum Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia yaitu:

1. Pengantar Hubungan Internasional, mengantarkan peneliti untuk memahami konsep dasar dari hubungan internasional khususnya yang terjadi diantara negara Tiongkok dengan negara di kawasan Asia Timur.
2. Regionalisme, memberikan sumbangan keilmuan mengenai dasar-dasar kajian negara pada kawasan tersebut. Kemudian mata kuliah Regionalisme memberikan gambaran dinamika serta membantu peneliti untuk mengetahui arah kebijakan luar negeri Tiongkok pada masa lampau dan

masa sekarang yang telah terjadi sebagai landasan dalam memahami latar belakang kawasan tersebut.

3. Keamanan Siber, memberikan pemahaman mengenai keamanan baru dan konsep kejahatan baru dalam hubungan internasional dengan menggunakan teknologi yang menyerang komputer target serangan siber, yang menjadi fokus utama dalam penelitian ini.
4. Politik Luar Negeri, Mata kuliah ini membantu peneliti untuk menganalisa arah politik luar negeri yang dilakukan Tiongkok, bagaimana Tiongkok melakukan kebijakan untuk meningkatkan kerjasama cyber di kawasan Asia Timur.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Berdasarkan latar belakang diatas, peneliti merumuskan masalah utama dari penelitian ini adalah sebagai berikut "Bagaimana dampak pembangunan *cyberpower* Tiongkok di kawasan Asia Timur."

1.2.2 Rumusan Masalah Minor

1. Apa kepentingan pembangunan *cyberpower* Tiongkok?
2. Bagaimana respon kawasan Asia Timur dalam pembangunan cyberpower Tiongkok?
3. Bagaimana dampak pembangunan *cyberpower* Tiongkok berpengaruh terhadap sektor ekonomi dan stabilitas keamanan kawasan Asia Timur?

1.2.3 Pembatasan Masalah

Berdasarkan yang penulis telah diuraikan dalam latar belakang dan rumusan masalah, maka penulis membatasi masalah dengan mengarah pada upaya apa yang telah dilakukan oleh Tiongkok terhadap cyber teknologi pada negara kawasan Asia Timur,serta respon negara yang berada di kawasan asia timur dalam menghadapi pembangunan cyberpower Tiongkok. Dan dampak dari pembangunan cyberpower Tiongkok dalam sektor ekonomi dan stabilitas keamanan kawasan Asia Timur. Penulis juga membatasi masalah dengan kurun waktu 2011 hingga 2021 untuk meneliti Pembatasan masalah diteliti hanya 10 tahun mengingat pada tahun 2011, Tiongkok mengalami penyerangan pengguna internet diserang oleh malware (termasuk virus dan trojan horse) yang menyebabkan kerugian negara puluhan miliar yuan.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud dari penelitian yaitu untuk mendapatkan informasi mengenai kepentingan Tiongkok menjadi *cyberpower* di kawasan Asia Timur.

1.3.2 Tujuan Penelitian

Tujuan penelitian mengenai Dampak pembangunan cyberpower Tiongkok di kawasan Asia Timur, yaitu :

1. Untuk mengetahui dan menganalisa motivasi Tiongkok menguasai cyber teknologi.

2. Untuk mengetahui dan menganalisa respon kawasan Asia Timur dalam pembangunan cyberpower Tiongkok
3. Untuk mengetahui dan menganalisa dampak pembangunan *cyberpower* Tiongkok berpengaruh terhadap sektor ekonomi dan stabilitas keamanan kawasan Asia Timur

1.4.1 Kegunaan Penelitian

1.4.1.1 Kegunaan Teoritis

Kegunaan teoritis pada penelitian adalah untuk memperluas kajian mengenai cyber teknologi Tiongkok ataupun menambah rujukan mengenai dampak pembangunan cyberpower Tiongkok di kawasan Asia Timur.

1.4..1.2 Kegunaan Praktis

Melalui penelitian ini, kegunaan bagi peneliti untuk memperoleh gelar Sarjana S1 (Strata Satu) pada Program Studi Hubungan Internasional Universitas Komputer Indonesia, Juga dalam penelitian ini yakni ditujukan bagi peneliti sendiri sebagai khazanah keilmuan dan berguna bagi berbagai pengkaji, khususnya hubungan internasional mengenai berbagai data mengenai topik penelitian cyber teknologi.