BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan *Information and Communication Technolgi* (ICT) telah berkembang dengan sangat cepat. Kehadiran internet telah membawa pengaruh besar terhadap kehidupan masyarakat diseluruh dunia. Kemajuan internet telah menjadikan hubungan antar manusia menjadi lebih mudah tanpa terhalang oleh batas wilayah dan perbedaan waktu. ICT juga telah menyebabkan dunia ini seperti tidak ada batas wilayah (*borderless*) karena arus komunikasi telah berpindah kedalam *Cyberspace* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. *Cyberspace* atau ruang cyber didefiniskan lebih dari sekedar internet dan tidak hanya sekedar hubungan perangkat keras, perangkat lunak, dan sistem informasi, tetapi juga hubungan antar manusia dan interaksi sosial yang berada didalamnya. Sementara *International Standarization Organization* (ISO) memiliki definisi yang sedikit berbeda dimana organisasi ini mendefinisikan ruang cyber sebagai lingkungan yang kompleks, dihasilkan oleh manusia-manusia, perangkat lunak, layanan internet, perangkat teknologi serta jaringan yang saling terhubung (Klimburg, 2012:8).

Setelah perang dingin berakhir, persepektif keamanan dan hubungan internasional telah mengalami pergeseran yang signifikan. Pada masa perang dingin, keamanan lebih didominasi atau dikaitkan dengan konteks militer, sementara pasca perang dingin, muncul permasalahan-permasalahan baru terkait keamanan seperti konflik sosial, etnis, budaya, lingkungan, terorisme sampai dengan masalah ancaman cyber. Topik ruang cyber saat ini telah menjadi kajian berbagai bidang ilmu termasuk studi keamanan yang juga menjadi *sub-field* dalam ilmu hubungan internasional. Akan tetapi Ilmu hubungan internasional terutama bidang keamanan internasional dikatakan terlambat menjadikan topik cyber sebagai kajian ilmu hubungan internasional yang pada dasarnya ilmu hubungan

internasional mengkaji hubungan dan interaksi antar aktor atau negara-negara didunia (Cavelty, 2008:6).

Amerika Serikat merupakan negara yang paling memilki kontribusi dalam politik internasional, dinyatakan sebagai negara pemenang perang dunia dan perang dingin setelah melakukan persaingan ketat dengan Uni Soviet. Setelah berhasil bersaing dengan Uni Soviet, Amerika Serikat muncul sebagai negara *superpower*, memilki keunggulan kemampuan militer yang modern dan juga perekonomian yang stabil. Amerika serikat memiliki keunggulan dari segala sektor termasuk dalam sektor atau bidang teknologi yang menghasilakan ruang cyber. Kemampuan teknologi yang inovatif dan modern ini membuat Amerika Serikat sangat bergantung kepada ICT dan ruang cyber. Hampir seluruh fasilitas negara dan layanan publik di Amerika Serikat memanfaatkan ruang cyber seperti dalam bidang industri, perbankan, transportasi, sanitasi air, pelayanan kesehatan sampai dengan bidang pertahanan atau militer pun berbasis komputer dengan jaringan internet. Ketergantungan Amerika Serikat yang tinggi terhadap ICT dan ruang cyber pada akhirnya menimbulkan kerentanan dan menghadirkan ancaman baru pada sistem keamanan cyber atau yang disebut dengan ancaman cyber.

Ancaman cyber merupakan salah satu ancaman asimetris karena serangannya dapat dilakukan oleh beberapa orang atau banyak, tidak memerlukan biaya dan sumber daya yang besar. Selain itu memiliki dampak yang cepat, nyata, dan berkelanjutan (Cyber Threats to National Security,2010:2). Ancaman cyber terus berkembang dan akan berdampak kepada setiap individu, hal ini disebabkan karena ketergantungan global terhadap teknologi informasi dan komunikasi yang begitu tinggi baik untuk bertukar informasi, berbisnis, pembangungan infrastruktur, bidang militer dan yang lainnya. Ancaman cyber memang cukup sulit untuk di deteksi dan diatasi mengingat serangan-serangan cyber dapat dilakukan dari mana saja dan oleh siapa saja. Ancaman cyber sendiri memiliki banyak jenis salah satunya yaitu spionase cyber.

Amerika Serikat dan Cina yang merupakan dua negara dengan kekuatan ekonomi terbesar di dunia tengah memiliki masalah tentang kegiatan spionase cyber. Spionase cyber merupakan kegiatan mata-mata pada umumnnya namun

pada praktiknya aktivitas ini menggunakan atau memanfaatkan kecanggihan teknologi informasi dan komunikasi berbasis jaringan internet. Ruang cyber atau *cyberspace* yang merupakan manifestasi dari teknologi informasi dan komunikasi telah menyediakan lingkungan yang luar biasa luas untuk praktek spionase karena memberikan ruang gerak kepada kolektor asing dan memfasilitasi transfer informasi dengan jumlah besar yang membuat pemerintah kesulitan untuk menentukan pelaku spionase cyber. Pemerintah dan perusahaan swasta secara berkala menghadapi upaya pihak asing untuk mendapatkan informasi dan data dengan cara melakukan akses illegal melalui internet, misalnya menyamar sebagai pengguna resmi atau melalui pengenalan secara diam-diam menggunakan *malicious software* atau perangkat lunak berbahaya. Spionase cyber juga dapat dikatakan sebagai *Cyber Network Exploitation* (CNE) yang memungkinan melakukan kegiatan intelijen melalui penggunaan jaringan komputer untuk mengumpulkan data dari sistem informasi target atau musuh (Klimburg, 2012:16).

Ancaman spionase cyber menjadi salah satu dari banyaknya jenis ancaman cyber yang saat ini menjadi perhatian negara-negara di dunia sebagai akibat perkembangan teknologi informasi dan komunikasi yang sangat cepat dan luas di kalangan masyarakat global serta ketergantungan masyarakat global akan hal ini. Spionase pada dasarnya memiliki tujuan untuk mengisi kesenjangan dalam program penelitian, mengumpulkan dan memetakan perencanaan strategi dimasa depan, mempersingkat waktu penelitian dan pengembangan untuk teknologi militer, serta mengidentifikasi kerentanan dalam sistem dan mengembangkan penanggulangannya.

Pada tahun 2013, perusahaan keamanan komputer Amerika Serikat yaitu Mandiant mengeluarkan sebuah dokumen berupa laporan yang berjudul *APT 1: Exposing One of China's Cyber Espionage Units* yang mana dokumen ini berisikan tentang unit spionase cyber yang berasal dari Cina. Dalam laporan tersebut disebutkan adanya keterlibatan *People Liberation Army* (PLA) unit 61398 serta masyarakat sipil yang direkrut oleh militer untuk melaksanaan kampanye spionase cyber di berbagai negara di dunia termasuk Amerika Serikat yang disebut dengan nama *Advanced Persistent Threat* (APT). APT sendiri

berjumlah lebih dari dua puluh, akan tetapi dalam dokumen Mandiant hanya APT 1 saja yang difokuskan karena APT 1 merupakan aktor yang paling gigih melakukan kampanye spionase cyber sejak tahun 2006 (Mandiant, 2013:2). Permasalahan spionase cyber sendiri tidak hanya di alami oleh Amerika Serikat saja, banyak negara-negara barat menjadi target serangan cyber ini dan Amerika Serikat menjadi Negara yang mendapatkan serangan terbesar.

Sumber : Mandiant Report

Gambar 1 Peta aktivitas Global APT 1

Pada gambar terlihat aktivitas APT 1 di selruh dunia dengan jumlah 141 sasaran, dan Amerika Serikat menjadi negara dengan sasaran terbesar yaitu dengan jumla 115. Sasaran ini mengarah kepada sektor-sektor komersil dan juga pemerintahan. Dengan adanya kampanye spionase cyber Cina ini, ancaman cyber menjadi begitu nyata bagi Amerika Serikat. Isu keamanan cyber ini juga telah menjadi salah satu poros utama bagi hubungan Amerika Serikat dan Cina baik potensi konflik maupun kerjasama. Keamanan cyber menjadi perhatian utama banyak negara sebagai akibat dari ekspansi yang cepat dan terus berkembang terhadap kecanggihan teknologi internet, dan juga tumbuhnya ketergantungan dari pemerintah dan masyarakat akan sistem komunikasi dan informasi berbasis jaringan internet untuk segala bidang termasuk operasi militer dan kegiatan komersil (Masters, 2011:2-3).

Manuver Cina dalam memanfaatkan ruang cyber sangat menjadi perhatian Amerika Serikat terlebih dalam kegiatan spionase. Cina merupakan negara yang paling agresif melakukan spionase terhadap Amerika Serikat dengan skala yang besar dan terus meningkat (Report to Congress, 2009:179). *Hacker* China tercatat telah beberapa kali berhasil membobol data lembaga pemerintahan Amerika Serikat untuk informasi sensitif yang berkaitan dengan proyek-proyek pertahanan Amerika Serikat. Tidak hanya institusi pemerintah Amerika Serikat, kontraktor pertahanan Amerika Serikat pun juga menjadi sasaran spionase. Infiltrasi yang dilakukan Cina kedalam jaringan komputer untuk meretas dan mendapatkan informasi terkait indsutri pertahanan tersebut disebut oleh lembaga intelijen Amerika Serikat dengan operasi *Titan Rain* yang dilakukan sejak tahun 2003 sampai dengan 2006 (Robinson, 2013:62). Operasi ini merupakan operasi untuk melakukan eksfiltrasi data dan informasi sensitif dari lembaga-lembaga pemerintahan Amerika Serikat dan juga kontraktor pertahanan. Lockheed martin sebagai salah satu kontraktor pertahanan Amerika Serikat yang saat itu sedang mengembangkan pesawat jet terbaru untuk Amerika Serikat yaitu F-35 *Lightning II* menjadi salah satu sasaran dari operasi ini. Selain Lockheed Martin ada juga Redstone Arsenal sebagai kontraktor utama Amerika Serikat dalam sistem pertahanan senjata rudal (Signifcant Cyberattack Incidents, 2013:3). Pada tahun 2007, muncul kembali permasalahan yang sama namun pada tahun ini, nama operasinya berbeda yaitu *Byzantine Hades*. Operasi *Byzantine Hades* ini masih memiliki target yang sama dengan Operasi *Titan Rain* yaitu lembaga pemerintah dan juga kontraktor pertahanan dan berlanjut sampai tahun 2013. Dalam operasi ini, spionase cyber tidak hanya dilakukan oleh militer atau lembaga intelijen saja, ada juga sipil yang menjadi agen atau mata-mata untuk mengambil data-data dan informasi yang ditargetkan.

Operasi-operasi eksploitasi jaringan komputer tersebut menjadi salah satu masalah spionase cyber yang paling terlihat antara Amerika Serikat dan Cina yang mana terkait peretasan data teknologi tentang pesawat jet F-35 *Lightning* II dan pesawat jet F-22 milik Amerika Serikat tersebut muncul pada badan pesawat jet J-20 dan J-31 milik Cina (Tjoa, 2015:2). Kemunculan teknologi militer milik Amerika Serikat kedalam pesawat militer milik Cina merupakan satu hal yang

tidak pernah terduga sebelumnya, hal tersebut dikarenakan Amerika Serikat telah menerapkan kebijakan transfer teknologi senjata secara transparan kepada Cina dan hal ini tentu menjadi pukulan mendalam bagi Amerika Serikat dan kontraktor pertahanan sebagai produsen. Pada tahun 2006, dimana masalah spionase cyber Cina ini mulai muncul kepermukaan publik, Amerika Serikat melakukan sebuah tanggapan dari masalah spionase cyber yang mana tujuannya adalah untuk menghentikan distribusi perangkat keras dan program-program palsu dari Cina yang dinamakan denga operasi *Network Raider* dan *Cisco Raider*. Hal ini dilakukan dengan alasan bahwa spionase cyber Cina dapat dilakukan karena penyebaran perangkat keras dan perangkat lunak yang berasal dari Cina telah ditanami program mata-mata sehingga Cina bisa dengan sangat mudah melakukan kampanya spionase menggunakan perangkat cyber terhadap Amerika Serikat (Federal Bureau of Investigation, 2010:1-2).

Negara-negara barat terutama Amerika Serikat meyakini bahwa semakin banyak serangan cyber pada sektor komersil dan lembaga pemerintah tidak hanya berasal dari orang-orang Cina, tetapi juga kemungkinan besar dari pemerintah Cina terutama militer. Menurut John. L Thornton dari *China Center and the 21st Century Defense Initiative* mengatakan bahwa banyak isu-isu kebijakan yang masuk dalam ranah keamanan cyber berdampak terutama kepada hubungan luar negeri yang mana akan terus tumbuh dan berkembang di masa mendatang. Isu-isu seperti ini apabila tidak dapat diatasi dengan baik bisa menjadi sumber utama adanya gesekan hubungan antar negara terutama dalam hubungan Amerika Serikat dan Cina itu sendiri (Lieberthal dan Singer, 2012:4).

II.2 Rumusan Masalah

Sebagai suatu wilayah baru, ruang cyber saat ini telah menjadi arena baru dalam pelaksanaan politik internasional. Segala sesuatu yang ada didalam ruang cyber mampu membawa dampak nyata terhadap kehidupan manusia termasuk hubungan antar negara. Masalah spionase cyber Cina yang ada di Amerika sudah dimulai sejak lama dan pemerintah Amerika Serikat juga sudah melakukan tanggapan atas hal tersebut. Akan tetapi upaya yang ditempuh oleh pemerintah

Amerika Serikat tampak belum mampu untuk mengatasi permasalahan spionase cyber yang ada, maka dari itu penulis menarik kesimpulan untuk merumuskan sebuah pertanyaan penelitian **"Bagaimana Amerika Serikat mengatasi ancaman spionase cyber yang berasal dari Cina pada tahun 2009-2013?"**

I.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

a. Mengetahui kondisi keamanan cyber di Amerika Serikat.
b. Memahami masalah spionase cyber antara Amerika Serikat dengan Cina
c. Menganalisa upaya-upaya Amerika Serikat untuk mengatasi masalah ancaman spionase cyber.

I.4 Manfaat penelitian

Manfaat yang diperoleh oleh penulis dalam penelitian ini adalah:

a. Secara akademis manfaat yang didapatkan dalam penelitian ini adalah untuk memberikan informasi dan data didalam jurusan ilmu hubungan internasional terutama konsentrasi pengkajian strategis mengenai kemanan didalam bidang cyber.
b. Secara praktis dapat membantu memahami hubungan antara Amerika Serikat dan Cina didalam ruang cyber.

I.5 Tinjauan Pustaka

Untuk menjawab rumusan permasalahan penelitian ini, penulis melakukan tinjauan terhadap karya akademis atau penelitian yang memiliki kemiripan, dan atau yang berhubungan dengan penelitian ini. Adapun beberapa tulisan yang dijadikan tinjauan bagi penulis antara lain:

Dalam artikel jurnal yang berjudul ***China's Use of Cyber Warfare: Meets Strategic Detterence*** (Hjortdal, 2011:3) ini menjelaskan adanya tiga alasan dalam menggunakan perangkat cyber sebagai unsur yang menentukan dalam pembuatan strategi Cina untuk bermain didalam sistem internasional. Tiga alasan tersebut adalah pencegahan melalui infiltrasi infrastruktur penting, spionase militer untuk mendapatkan pengetahuan dalam bidang militer, dan spionase industri untuk mendapatkan keuntungan ekonomi. Cina memiliki kepentingan lebih besar dibandingkan dengan Amerika Serikat dalam penggunaan dunia maya secara ofensif untuk tujuan politik dengan cara memata-matai Amerika Serikat.(

Meskipun Cina terlihat seperti Negara yang paling aktif dalam meluncukan serangan cyber di dunia, Cina juga merupakan Negara yang menjadi korban terhadap serangan cyber yang dilakukan oleh banyak negara termasuk Amerika Serikat dan negara-negara barat lainnya (Hjortdal, 2011:6) Untuk menghadapi tantangan baru ini Amerika Serikat telah membentuk Cyber Command untuk melakukan koordinasi dan persiapan Negara menghadapi ancaman cyber yang datang. Melalui *cybercomm* Amerika Serikat melakukan dua jenis operasi cyber sekaligus yaitu ofensif dan defensive. Dalam dinamika *Cyber Network Operations* (CNO) menyatakan bahwa mempertahankan adalah hal yang paling sulit dibandingkan dengan menyerang. Negara banyak meraih keuntungan dengan menggunakan cyber sebagai alat dan media secara ofensif dan agresif dikarenakan secara fakta akan sangat sulit untuk membuktikan secara langsung aktor yang bermain di belakang serangan tersebut. Ada kemungkinan Cina akan terus melakukan *build-up* kemampuannya di dunia maya dalam jangka panjang guna melakukan ekspansi dibidang politik, pertahanan, dan ekonomi agar bisa menjadi Negara adikuasa.

Kedua, artikel jurnal yang berjudul ***China-United States War in Cyberspace, Reality or Hype?*** **(**Kozlowski, 2014:4) ini memperlihatkan apakah perang di dunia maya antara Amerika Serikat dan Cina mencerminkan situasi nyata di ranah maya atau tidak. Hubungan Amerika Serikat dan Cina didunia maya cukup sulit dan kompleks serta penuh ketegangan. Sebagian besar hacker Cina berfokus pada spionase cyber. Spionase telah menjadi bagian kompetisi

antara negara-negara sejak awal dan tidak dapat dikasifikasikan sebagai kegiatan perang. Hacker Cina melakukan hal yang sama dengan mencoba mencuri informasi dalam rangka untuk mendapatkan keuntungan atau mencapai tingkat yang sama seperti Amerika Serikat. Mereka tidak menghancurkan data yang dicuri, sehingga mereka tidak merusak file penting. Cina memiliki kepentingan dalam spionase cyber untuk mendapatkan rencana bisnis atau skema persenjataan.

Tidak ada peperangan terbuka didunia cyber antara Amerika Serikat dan Cina, akan tetapi banyak orang lebih mempersepsikan ketegangan yang ada sebagai perang dingin diranah cyber (Kozlowski, 2014:11) Hal tersebut dilihat dari kesamaan antara situasi saat ini di dunia maya dan persaingan sengit antara Amerika Serikat dan Uni Soviet pada masa perang dingin. Selama perang dingin kedua Negara mencoba untuk mencuri informasi tentang rencana pembuatan jenis-jenis senjata baru serta teknologi baru dan yang lainnya. Sementara saat ini hal itu terjadi antara Amerika Serikat dan Cina. Satu satunya perbedaan adalah bahwa selama perang dingin antara Amerika Serikat dan Uni Soveiet menggunakan metode klasik karena sebagian besar dokumen dan berkas-berkas perencanaan berbentuk cetakan atau versi kertas.Saat ini ketika sebagian besar data atau informasi dirubah menjadi bentuk digital, popularitas spionase cyber semakin berkembang. Cina memiliki kepentingan dalam spionase cyber untuk mendapatkan informasi terkait bisnis dan ekonomi serta informasi terkait bidang pertahanan untuk memodrenisasi sistem persenjataannya.

Ketiga yaitu artikel yang berjudul ***China vs US, cyber superpowers compared*** (INFOSEC, 2013:1-4) ini memaparkan bahwa pemerintah Amerika Serikat telah melaporkan beberapa berita tentang serangan cyber yang secara terus menerus berasal dari Cina. Sebagian besar dari penyerang bertujuan untuk melakukan spionase namun tidak dipungkiri juga bahwa mereka tidak melakukan operasi sabotase. Pemerintah Amerika Serikat mengkonfirmasi bahwa adanya tentanra Cina yang dilatih untuk melakukan operasi cyber. Kelompok hacker yang terdapat dalam pasukan elit Cina dikenal dengan sebutan *cyber blue team* yang terlibat dalam operasi ofensif dan defensive untuk melindungi Negara dari serangan cyber. Pemerintah Cina juga mengkonfirmasi keberadaan tim atau

tentara cybernya dibentuk untuk menjaga keamanan internet dari angkatan bersenjata karena sebenarnya keamanan cyber adalah masalah internasional dan dapat membawa pengaruh kepada baik sipil maupun militer.

Cina mulai menerapkan strategi perang informasi pada tahun 1995 serta melakukan sejumlah latihan cyber untuk mengeksploitasi kerentanan dalam komunikasi militer dan swasta. Pada tahun 2000, pemerintah Cina membentuk unit strategi perang informasi, pasukan jaringan yang bertanggung jawab memerangi musuh melalui jaringan komputer untuk memanipulasi sistem informasi. Akan tetapi jika berbiacara mengenai Cina dan cyber, terdapat unit utama yang dikenal sebagai PLA GSD departemen ketiga dan departemen keempat, mereka dianggap sebagai pemain yang sebenarnya dalam perkembangan infrastruktur cyber di Cina. GSD departemen ketiga Cina bertanggung jawab untuk memantau komunikasi asing dan melakukan pengawasan terhadap target utama diseluruh dunia. Departemen ini juga melakukan penjaminan keamanan jaringan komunikasi dan komputer PLA. Sementara departemen keempat berada dibawah kendali PLA yang bertanggung jawab dalam masalah intelijen elektronik, mengharuskan mereka untuk mengumpulkan dan memelihara database pada sinyal elektronik. Sementara itu PLA satuan 61398 atau yang dikenal dengan *Advanced Persistent Threat 1* (APT1) bertanggung jawab untuk melakukan kampanye spionase cyber secara terus menerus terhadap pemerintah asing dan diduga menjadi sumber utama serangan cyber Cina.

Tidak ada keraguan bahwa dalam jangka pendek kedua Negara ini akan terus saling serang meskipun kedua Negara akan terus meningkatkan keamanan cybernya. Konflik baru dan masa depan akan melibatkan aktor baru dalam scenario geopolitik seperti hacker indepent, hacker yang didukung oleh Negara, pernjahat cyber serta teroris cyber yang dapat mempengaruhi keseimbangan antara dua Negara besar ini. Konsep ancaman dunia maya semakin berkembang dari hari ke hari dan setiap pemerintah memerlukan strategi yang tepat untuk mereduksi ancaman yang ada serta menjamin keamanan informasinya.

Dari ketiga tinjauan pustaka yang digunakan oleh penulis memiliki perbedaan dengan penelitian yang akan dilakukan oleh penulis. Namun ketiga

tinjauan pustaka ini akan menjadi acuan atau bahan pendukung untuk menganalisa penelitian yang dilakukan oleh penulis. Dari jurnal yang ditulis oleh magnus hjortdal melihat permasalahan dan alasan mengapa Cina melakukan spionase cyber terhadap Amerika Serikat. Sementara, pada tinjauan pustaka kedua, penulis melihat bagaimana situasi hubungan atau interaksi antara Amerika Serikat dengan Cina diruang cyber. Sedangkan pada tinjauan pustaka yang ketiga, penulis melihat aktor-aktor yang terlibat dalam masalah spionase cyber Cina dan Amerika Serikat, Dengan ketiga tinjauan pustaka tersebut tidak ada yang membahas tentang seperti apa atau apa yang dilakukan oleh Amerika Serikat untuk mengtasi ancaman cyber atau spionase cyber. Sehingga pembahasan lebih dalam mengenai upaya Amerika Serikat dalam mengatasi masalah spionase cyber yang berasal dari Cina belum dilakukan oleh penelitian siapapun

I.6 Kerangka Pemikiran

I.6.1 Spionase Cyber

Spionase didefinisikan sebagai praktek mata-mata atau menggunakan mata-mata untuk mendapatkan informasi tentang rencana dan kegiatan terutama dari pemerintah asing ataupun pesaing bisnis sebuah perusahaan (United States Office of the National Counterintelligence Executive, 2011:iii-iv). *Cyberspace* telah menyediakan lingkungan yang luar biasa luas untuk praktek spionase karena memberikan ruang gerak kepada kolektor asing dengan relatif anonimitas, memfasilitasi transfer informasi dengan jumlah besar, dan membuat pemerintah kesulitan untuk menentukan pelaku spionase. Beberapa Negara mendefinisikan ini sebagai akses yang tidak sah terhadap data atau informasi dan dianggap sebagai ancaman. Pemerintah dan perusahaan swasta secara berkala menghadapi upaya pihak asing untuk mendapatkan informasi dan data dengan cara melakukan akses illegal melalui internet, misalnya menyamar sebagai pengguna resmi atau melalui pengenalan secara diam-diam menggunakan *malicious software* atau perangkat lunak berbahaya. Spionase cyber juga dapat dikatakan sebagai *Cyber Network Exploitation* (CNE) yang memungkinan melakukan kegiatan intelijen melalui

penggunaan jaringan komputer untuk mengumpulkan data dari system informasi target atau musuh (Klimburg, 2012:16).

Pengumpulan intelijen pada umumnya tidak dianggap illegal, sub-set dari tindakan yang jatuh pada spionase pada umumnya dianggap sebagai kejahatan dibawah kode hukum dari banyak negara. Kegiatan ini dilakukan oleh agen yang dipekerjakan oleh pihak militer dari suatu negara tertentu, lembaga pemerintah, perusahaan komersial, organisasi kriminal, atau oleh individu. Dalam spionase cyber, agen memanfaatkan dunia maya sebagai sumber daya untuk kegiatan intelijen mereka dengan cara menghadang arus informasi di jaringan komputer atau sistem komputer. Melakukan *cracking* dan inflitrasi teknik, perangkat lunak dan perangkat keras atau pendekatan lainnya yang sejenis. Data yang dikumpulkan dianalisis dan digunakan dalam menyusun laporan intelijen untuk entitas komisioner. Dalam kegiatan spionase cyber juga dibutuhkan pengumpulan dan analisi informasi *open source* yang tersedia untuk umum pada halaman web internet atau melalui jaringan sosial media (Sigholm, 2015:21).

Dalam beberapa pandangan, spionase cyber dianggap sebagai bagian penting persaingan ekonomi global dan pemantauan kemampuan cyber musuh dianggap penting untuk keamanan nasional (Sigholm, 2015:22). Banyak Negara menggunakan spionase untuk mengacu pertumbuhan ekonomi yang cepat berdasarkan pada teknologi yang canggih, menargetkan inisiatif ilmu pengetahuan dan teknologi dari negara negara lain. Ketika spionase cyber dimotivasi oleh tujuan Negara maka biasanya yang menjadi target utamanya adalah kekayaan intelektual komersil dari perusahaan swasta. Semua masalah yang berkaitan dengan perlindungan kekayaan intelektual akan berlaku untuk spionase cyber. Hal ini dilihat dari ukuran perusahaan global dan ketergantungan pemerintah terhadap sektor swasta untuk layanan infrastruktur dan layanan penting lainnya, serta pendpatan pajak yang cukup besar, maka menyerang sektor swasta dengan spionase cyber dapat menjadi bagian dari spionase cyber yang dimotori oleh Negara (Bayuk, 2012:145).

I.6.2 *National Cyber Security (NCS)*

Dalam buku *National Cyber Security Framework Manual* yang diterbitkan oleh NATO CCD COE, dikatakan bahwa tidak ada definisi yang jelas secara universal tentang apa yang dimaksud dengan keamanan cyber nasional. Akan tetapi NCS memiliki dua akar istilah yang jelas yaitu istilah keamanan cyber dan istilah keamanan nasional dimana kedua istilah ini memiliki definisi yang berbeda. NCS merupakan kombinasi dari dua akart istialah yang kemudian dijadikan sebagai sebuah konsep strategi.

Topik keamanan cyber itu sendiri merupakan bagian dari strategi keamanan nasional, dan terkadang berfungsi sebagai kontrol untuk pergeseran paradigma terhadap strategi keamanan nasional yang lebih komprehensif. Sebagai isu utama dalam keamanan nasional, keamanan cyber merupakan tantangan strategis yang sangat sulit sehingga memerlukan upaya yang terkoordinasi dan terfokus dari seluruh lapisan masyarakat, pemerintah federal, pemerintah negara bagian dan lokal, sektor swasta, dan individu. Upaya yang dibentuk oleh system ini merupakan bagian dari tiga dimensi NCS, yaitu: (Klimburg, 2012: 29-31)

a. ***Governmental***, untuk menghadapi tantangan atas keamanan cyber membutuhkan peran dari badan pemerintah dalam berbagai bentuk, termasuk militer, penegak hukum, peradilan, perdagangan, infrastruktur, telekomunikasi dan badan lainnya. Karena sifat keamanan cyber yang tidak terlihat, dibutuhkan upaya yang lebih seperti menciptakan koordinasi antar lembaga pemerintah tersebut untuk membangun tindakan yang koheren.
b. ***International***, tidak ada NCS yang mengabaikan dimensi internasional ini. Setiap aktor Negara maupun non-negara untuk memajukan kepentingannya membutuhkan kerjasama dengan berbagai mitra internasional. Hal ini berlaku di berbagai tingkat mulai dari perjanjian yang mengikat secara internasional (misalnya konvensi kejahatan cyber eropa), hingga kesepakatan politik yang mengikat. Oleh karena itu, penekanan harus berada di semua pihak yang menjalin hubungan dengan aktor dalam sistem tertentu tetapi tidak terbatas pada bidang

internet saja dan perlunya pembentukan aktor non-negara yang fleksibel untuk bekerjasama dengan aktor global lainnya.

c. ***National***, kerjasama dengan kontraktor keamanan dan perusahaan infrastruktur selalu dipandang sebagai peranan penting dalam keamanan nasional. Ekspansi yang terus-menerus dari jumlah para pelaku di dunia maya yang berhubungan dengan keamanan nasional dalam setiap negara tertentu telah membuat beberapa pemerintah memutuskan untuk membuat strategi komprehensif mereka secara keseluruhan, termasuk seluruh masyarakat atau seluruh negara.

I.6.3 Diplomasi

Dalam hubungan internasional, diplomasi menjadi bagian penting untuk melaksanakan politik internasional. Diplomasi sangat erat dengan hubungan antar negara yang mana menurut Martin Griffiths dan Terry O'Callaghan mendefinisikan diplomasi yaitu "*diplomasi merupakan proses keseluruhan yang dilakukan oleh suatu Negara dalam melaksanakan hubungan internasional*" (Griffiths dan Terry, 2002:79). Dalam hal-hal tertentu pengertian diplomasi sama dengan politik internasional akan tetapi secara spesifik dapat dibedakan dimana diplomasi berkaitan dengan cara-cara dan mekanisme, sedangkan politik luar negeri menyangkut maksud dan tujuan dari apa yang telah terumuskan dalam sebuah kebijakan luar negeri suatu negara. Kebijakan luar negeri sendiri menyangkut substansi dan isi-isi dari hubungan luar negeri, sedangkan diplomasi mengenai masalah metodologi untuk melaksanakan politik luar negeri.Menurut Martin Griffiths, diplomasi memiliki tiga fungsi utama yaitu *intelligence gathering*, *image management*, dan *policy implementation*. Ketiga fungsi ini saling berkaitan dan bertujuan untuk menciptakan citra yang menguntungkan bagi suatu negara.

Sedangkan menurut G.R Berridge di dalam bukunya yang berjudul *Diplomacy: Theory and Practice*, mengartikan diplomasi yaitu sebuah dasar kegiatan politik baik sumber daya dan kemampuan keterampilan, dan sebagai bahan utama dari kekuasaan. Tujuan utamanya adalnh untuk memungkinkan suatu negara dalam mengamankan kebijakan luar negeri Negara tanpa memaksa dengan

menggunakan kekuatan, propaganda atau bantuan hukum. Jadi diplomasi yang dilakukan lebih mengedepankan komunikasi dengan cara negosiasi untuk mempromosikan kebijakan luar negeri suatu negara baik melalui perjanjian formal atau non formal (Berridge, 2002:1). Dengan melihat dua pengertian diplomasi diatas dapat disimpulkan bahwa diplomasi sebagai alat suatu negara untuk berinteraksi dengan negara lain baik dalam menyelesaikan konflik maupun untuk megamankan kebijakan suatu Negara dengan cara negosiasi serta keseluruhan tindakan yang berhubungan dengan interaksi internasional tanpa menggunakan kekerasan, propaganda, dan badan hukum.

I.7 Alur Pemikiran

I.8 Asumsi

Dalam melakukan penilitian ini penulis menarik beberapa asumsi dasar sebagai berikut:

a. Tingkat ketergantungan Amerika Serikat terhadap ruang cyber yang tinggi memunculkan celah bagi para aktor-aktor asing ini untuk melakukan serangan asimetris yang cukup sulit untuk ditangani bahkan oleh negara sebesar dan sekuat Amerika Serikat.

b. Spionase cyber membawa dampak berupa kerugian secara eknomi bagi sektor swasta dan juga menjadi ancaman bagi keamanan nasional Amerika Serikat.
c. Masalah keamanan cyber perlu diatasi dan menjadi tanggung jawab selueruh masyarakat Amerika Serikat, dan juga perlu adanya kerjasama antar negara untuk membangun lingkungan cyber yang aman dan terpercaya bagi para penggunanya.

I.9 Metodologi Penelitian

I.9.1 Jenis Penelitian

Jenis penelitian yang digunakan bersifat deskriptif dengan metode kualitatif. Metode kualitatif ini dimulai dengan mengumpulkan data, menganilisi data dan menginterpretasikannya. Metode deskriptif kualitatif dalam pelaksanaanya dilakukan melalui teknik survey, studi kasus, studi komparatif, studi tentang waktu dan gerak, analisis tingkah laku, dan analisis dokumenter (Suryana, 2010:16). Penulis berupaya memberikan deskripsi mengenai upaya Amerika Serikat untuk mengatasi ancaman spionase cyber Cina dengan mendeskripsikan terlebih dahulu kondisi dan keamanan cyber di Amerika Serikat kemudian masalah spionase cyber di Amerika Serikat.

I.9.2 Teknik Pengumpulan data

Data yang digunakan dalam penulisan ini adalah data primer dan sekunder yang dapat mendukung pencarian jawaban atas pertanyaan penelitian serta secara keilmuan dapat dibuktikan. Data primer yang digunakan adalah pernyataan resmi dari pemerintah seperti buku putih, kutipan pernyataan dari lembaga pemerintahan. Data sekunder yang digunakan yaitu berupa buku-buku, artikel-artikel yang berasal dari berbagai jurnal ilmiah studi Hubungan Internasional, majalah dan surat kabar serta artikel-artikel yang terdapat dalam situs internet.

I.9.3 Teknik Analisis Data

Teknik analisis data yang penulis gunakan untuk menganalisis masalah atau fenomena yang terjadi dalam penelitian bersifat deskriptif analisis. Sehingga suatu permasalahan dijelaskan berdasarkan fakta-fakta yang ada dan kemudian menghubungkan fakta yang ditemukan berdasarkan kerangka pemikiran yang digunakan. Analisis data dilakukan sesuai dengan kerangka pemikiran yang digunakan agar data yang diperoleh dari pengamatan dapat dijelaskan secara jelas. Dalam penelitian ini, penulis menganalisa secara deskriptif upaya Amerika Serikat mengatasi masalah spionase cyber Cina menggunakan kerangka pemikiran yang telah dipilih yaitu konsep *National Cyber Security*, konsep spionase cyber, dan teori diplomasi dan untuk menjelaskan data yang diperoleh.

I.10 Sistematika Penulisan

Dalam upaya memberikan pemahaman mengenai isi dari penelitian ini secara menyuluruh, maka penelitian ini dibagi menjadi 4 Bab yang terdiri dari bab dan sub-bab yang saling berkaitan satu sama lain. Bab-bab tersebut antara lain:

BAB I: PENDAHULUAN

Bab pertama ini akan berisikan sub-bab latar belakang mengenai terjadinya permasalahan. Sub-bab latar belakang ini juga berisi permasalahan pokok, tujuan, serta manfaat penelitian.Sub-bab lainnya adalah kerangka pemikiran, tinjauan pustaka, serta alur pemikiran. Sub-bab terakhir dalam bab ini adalah metode penelitian yang berisikan jenis penelitian, teknik pengumpulan data, teknik analisa data dan sistematika penulisan.

BAB II: SPIONASE CYBER CINA TERHADAP AMERIKA SERIKAT

Bab kedua penulis secara umum akan menjelaskan mengenai kemanan cyber di Amerika Serikat. Kemudian akan dilanjutkan dengan penejelasan masalah spionase cyber Cina yang ada di Amerika Serikat, dan Penjelasan dampak dari spionase cyber di Amerika Serikat.

BAB III: UPAYA AMERIKA SERIKAT MENGATASI ANCAMAN SPIONASE CYBER CINA

Bab ketiga ini akan berisi tentang penjelasan upaya-upaya Amerika Serikat untuk mengatasi masalah keamanan cyber dan ancaman cyber dari secara internal dan secara eksternal.

BAB IV: KESIMPULAN

Bab keempat akan menjadi penutup dari hasil penelitian dari penulis. Bab ini merupakan jawaban dari pokok permasalahan penelitian. Dalam bab ini penulis mencoba untuk menyimpulkan sebuah jawaban yang berasal dari analisis data yang di peroleh penulis pada bab II dan bab III