BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi yang terbentuk oleh berbagai jaringan yang semakin mengglobal memunculkan ancaman dari terjadinya *cyberwarfare* dan secara perlahan menjadi perhatian utama para pemimpin politik dan militer di seluruh dunia terkait dengan keamanan nasional. *Cyberwarfare* umumnya merujuk kepada tindakan suatu negara atau organisasi internasional yang memanfaatkan *cyber space* untuk menyerang dan merusak jaringan komputer atau informasi negara lain dengan menggunakan berbagai *cyber attack*. Ketika suatu negara menjadi target dari *cyber attack* yang dilakukan aktor tertentu, negara tersebut tidak hanya menghadapi risiko hilangnya privasi dan data yang dimiliki oleh warganya, namun juga kehilangan kekuatan industri dan keuangan, serta keuntungan geopolitik (Burk & Kallberg, 2016). Sistem, jaringan serta situs web merupakan target utama dari *cyberwarfare* untuk melumpuhkan lawan baik dengan melakukan kerusakan ataupun gangguan. Upaya *cyber attack* yang memanfaatkan domain perang non-tradisional khususnya *cyber space* dapat menghantam titik-titik penting dari suatu masyarakat yang bergantung terhadap teknologi dan jaringan modern (Eun & Abmann, 2014). Kapabilitas *cyber* suatu negara tidak dibatasi oleh batas-batas geografis sehingga *cyber attack* memiliki kemampuan tersendiri untuk menembus bentuk-bentuk pertahanan nasional tradisional dan berpotensi mendatangkan bencana bagi institusi ataupun masyarakat yang ada di suatu negara. Walaupun *cyberwarfare* sendiri tidak mungkin secara langsung menimbulkan korban jiwa yang besar,

cyberwarfare dapat berfungsi secara efektif sebagai alat pemaksaan politik serta unjuk kekuatan. Hal tersebut menyebabkan *cyberwarfare* tidak hanya mengancam negara-negara kecil yang memiliki tingkat keamanan *cyber* yang lemah, namun juga berpotensi menjadi ancaman bagi keamanan nasional di negara-negara kuat seperti Amerika Serikat dan Tiongkok (Liff, 2012). Selain itu, belum terbentuknya badan atau aturan yang kuat untuk mengatur dan menegakkan interaksi antar negara dan aktor non-negara dalam *cyber space* menyebabkan tidak adanya batasan bagi aktor-aktor tertentu untuk memiliterisasi *cyber space* ataupun melakukan *cyber attack* demi mencapai kepentingan mereka.

Tiongkok adalah salah satu negara yang telah mengembangkan kemampuan *cyber* dalam skala besar, di mana *cyber space* merupakan salah satu area yang mendapatkan ekspansi terbesar dalam pembangunan kekuatan pertahanan dan militernya. Berbeda dengan Amerika Serikat yang memiliki kekuatan militer yang sangat kuat dan luas sehingga mampu mencapai *full-spectrum dominance* dan mendominasi seluruh dimensi dari ruang pertempuran, Tiongkok lebih memilih menggunakan kapabilitas khusus seperti *cyberwarfare* untuk mengimbangi ketertinggalan teknologi militer dengan Amerika Serikat (Heginbotham, 2015). Dalam era informasi, Tiongkok percaya bahwa memiliki dan menjaga dominasi dalam *cyber space* merupakan hal yang lebih penting dibandingkan dengan penguasaan laut dan udara ketika Perang Dunia II. Bagi Tiongkok, karakteristik dari *cyber space* dan operasi jaringan komputer yang tidak membutuhkan biaya yang tinggi namun memiliki pemanfaatan yang luas dan risiko yang rendah dibandingkan dengan kekuatan konvensional membuka peluang asimetris di mana aktor yang lemah dapat mengalahkan aktor yang jauh lebih kuat. Walapun demikian,

kapabilitas *cyberwarfare* yang dimiliki Tiongkok hingga saat ini masih memiliki batasan dan kelemahan yang dapat dengan mudah dieksploitasi oleh lawannya, khususnya Amerika Serikat. Salah satunya adalah lemahnya kemampuan Tiongkok untuk melindungi, memantau, menganalisis, mendeteksi, dan merespons aktivitas ilegal atau asing dalam sistem informasi dan jaringan computer Tiongkok. Selama beberapa dekade, budaya militer di Tiongkok lebih menekankan terhadap pentingnya faktor manusia dalam peperangan dengan menggunakan kekuatan atau senjata secara massal dan cenderung mengabaikan pengembangan peralatan atau teknologi (Wortzel, 2014). Ketertinggalan tersebut selanjutnya diperburuk oleh ancaman dari *cyber superiority* yang dimiliki oleh Amerika Serikat.

Dapat dikatakan bahwa Amerika Serikat memiliki keunggulan kekuatan yang sangat tinggi dalam *cyber space*, di mana batas geografis tidak mempengaruhi proyeksi kekuatannya. Dikarenakan perannya dalam penciptaan dan pengembangan Internet, Amerika Serikat mampu mempertahankan pengaruh yang sangat besar atas operasi dan tata kelolanya. Saat ini, sepuluh dari 13 *root server* yang bertanggung jawab atas fungsionalitas dari internet secara global berada di wilayah Amerika Serikat, dan Tiongkok, seperti banyak negara lain, masih bergantung pada teknologi dari perusahaan teknologi dan informasi Amerika Serikat (Haizler, 2017). Selain itu, Amerika Serikat juga dianggap mempunyai kapabilitas *cyber* ofensif terkuat di dunia meskipun tetap menghadapi kerentanan yang signifikan dalam aspek *cyber* defensifnya. Kapabilitas *cyber* ofensif Tiongkok tertinggal jauh di belakang Amerika Serikat sehingga terdapat kemungkinan bahwa mereka tidak mampu melakukan *cyber attack* dengan tingkat

kerusakan yang lebih besar ataupun setara dalam skala dan cakupan dibandingkan dengan *cyber attack* Amerika Serikat terhadap Tiongkok. Penyebaran virus Stuxnet menjadi contoh penting bagi Tiongkok di mana virus tersebut merupakan demonstrasi *cyberwarfare* pertama yang dapat menimbulkan kerusakan fisik dari jarak jauh di negara lain. Selain itu, Selain itu, publikasi Snowden terkait operasi *cyber* Amerika Serikat juga menjadi kekhawatiran dan dorongan tersendiri bagi Tiongkok untuk mengembangkan kapabilitas *cyberwarfar*-nya, di mana Amerika Serikat terungkap secara aktif telah menargetkan universitas, pejabat publik dan bisnis di Tiongkok.

Perkembangan *cyberwarfare* di Tiongkok telah dimulai pada tahun 1990-an yang pada saat itu disebut sebagai *information warfare* (xìnxī zhànzhēng). Ketergantungan militer Amerika Serikat dalam menggunakan informasi dan jaringan pada saat Perang Teluk pertama dan intervensi Balkan menjadi titik awal Tiongkok untuk mengembangkan kemampuan *cyber*, di mana ahli-ahli strategis Tiongkok pada saat itu menyimpulkan bahwa pihak yang dapat mendominasi aspek konflik dalam *cyber space* akan memperoleh keuntungan strategis (Kozlowski, 2015). Peng Guangqian dan Yao Yunzhu (2005) berpendapat bahwa dengan hadirnya teknologi-teknologi tinggi, hasil dari perang tidak hanya ditentukan oleh jumlah sumber daya, tenaga kerja dan teknologi yang dikhususkan untuk berperang, namun juga membutuhkan adanya kontrol informasi yang kuat di medan perang melalui perolehan, transmisi, dan manajemen informasi. Tujuan utama dari *information warfare* sendiri adalah untuk mendapatkan keunggulan informasi, mengganggu kapabilitas informasi musuh serta mempetahankan sistem dan kemampuan informasi Tiongkok sendiri. Konsep dasar dari *information warfare* mencoba untuk

mengeksploitasi penggunaan teknologi informasi tingkat tinggi ke dalam kemampuan komando dan kontrol sebagai cara untuk memastikan kelancaran arus informasi. Keberhasilan berbagai kegiatan militer sangat tergantung terhadap bagaimana teknologi informasi menghubungkan antara unit-unit militer dengan sistem militer. Praktik dari strategi *information warfare* lebih mengarah kepada peningkatan kesiapan *cyber* Tiongkok secara konstan, di mana Tiongkok secara rutin melakukan pengintaian informasi serta penetrasi jaringan kepada negara lain yang dipandang sebagai ancaman ataupun memiliki kepentingan tertentu bagi Tiongkok.

Pada awal abad ke-21, Tiongkok mulai mengalami pertumbuhan yang cepat dan masif dalam skala kapabilitas *cyberwarfare*-nya dan cenderung menggunakan kapabilitas *cyber* secara ofensif terhadap pemerintahan dan militer negara lain. Contoh utama dari serangan tersebut adalah operasi Titan Rain yang menargetkan jaringan pemerintah dan kontraktor Amerika Serikat serta operasi Ghost Net yang menyerang target-target diplomatik di PBB. Namun, saat ini Tiongkok lebih berfokus untuk meluaskan serangannya terhadap target-target sipil, termasuk infrastruktur nasional yang vital serta perusahaan-perusahaan yang memiliki pengaruh ekonomi atau komersil yang luas (Siboni, 2012). Hal ini didorong oleh dugaan Tiongkok mengenai keinginan Amerika Serikat untuk mempertahankan dan memperkuat *cyber superiority* secara agresif serta kesadaran terkait aktivitas berbagai negara-negara barat lainnya yang secara aktif memanfaatkan kontraktor pertahanan seperti Lockheed Martin, Boeing, Northrop Grumman, dan Raytheon untuk pengembangan dan penyebaran kapabilitas *cyber*. Hal ini menyebabkan adanya fokus terhadap pengembangan teknologi dan ilmu pengetahuan

dalam aktivitas *cyberwarfare* Tiongkok, di mana pengintaian informasi dan *cyber attack* Tiongkok cenderung menargetkan terhadap informasi atau data terkait penelitian dan pengembangan terbaru yang selanjutnya dapat digunakan untuk memperkuat kapabilitas Tiongkok. Pada dasarnya, pengembangan kapabilitas *cyber* Tiongkok merupakan respon terhadap perubahan pendekatan dan praktik *cyberwarfare* oleh negara lain yang cenderung telah mengembangkan kekuatan militer *cyber* masing-masing dan memunculkan insekuritas bagi Tiongkok terhadap keamanan masionalnya (Jinghua, 2019).

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah disampaikan, peneliti kemudian mengajukan pertanyaan penelitian berupa: Bagaimana Tiongkok mengembangkan dan menggunakan kapabilitas *cyberwarfare* dalam menghadapi *cyber superiority* yang dimiliki oleh Amerika Serikat?

1.3 Tujuan Penelitian

Penelitan ini bertujuan untuk menjelaskan penggunaan dan pengembangan kapabilitas *cyberwarfare* Tiongkok dalam menghadapi *cyber superiority* yang dimiliki oleh Amerika Serikat.

1.4 Tinjauan Pustaka

Dalam tinjauan literatur ini, peneliti menghadapi kesulitan dalam menemukan literatur-literatur yang relevan dengan topik pembahasan penelitian. Hal tersebut dikarenakan keterbatasan sumber yang membahas mengenai kapabilitas *cyber* yang dimiliki oleh suatu negara secara mendalam, di mana negara cenderung menutupi ataupun

tidak mengakui operasi dan kekuatan *cyber* yang dimilikinya. Walaupun demikian, dari sumber literatur yang diperoleh peneliti berupaya untuk mengelaborasinnya sehingga dapat mengarah kepada kerangka pemikiran dengan menunjukan bagaimana suatu negara mengembangkan dan menggunakan kapabilitas *cyberwarfare* secara ofensif baik sebagai jalan untuk mencapai kepentingan nasional, mempertahankan keamanan ataupun sebagai *deterrence* dalam menghadapi aktor-aktor yang lebih kuat.

Literatur pertama yang peneliti tinjau adalah *Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Sŏn'gun Era* oleh Daniel A. Pinkston tahun 2016. Dalam literatur ini, Pinkston mengkaji bagaimana Korea Utara mengembangkan dan memanfaatkan kapabilitas *cyberwarfare* untuk mendukung kepentingan nasional Korea Utara khususnya dalam bidang militer serta sebagai upaya untuk mengejar ketertinggalannya dengan Korea Selatan. Fondasi dari kapabilitas *cyberwarfare* Korea Utara mulai muncul pada tahun 1980-an, di mana Korea Utara mendirikan pabrik perakitan komputer pertamanya pada tahun 1983 dan dua tahun kemudian membuka perguruan tinggi komputasi elektronik. Pada tahun 1986, Korea Utara membentuk Pusat Informasi Pyongyang (PIC) yang bertugas menciptakan sistem dan perangkat lunak otomatis untuk proses industri domestik mereka. Kim Jong-il, pemimpin Korea Utara pada saat itu, mendorong Tentara Rakyat Korea (KPA) untuk selalu meningkatkan kapabilitas *cyberwarfare* dan percaya bahwa perang di masa mendatang akan bertransformasi menjadi perang informasi. Pada tahun 1990-an, KPA mencoba untuk mempelajari konsep *information warfare* yang dikembangkan oleh PLA Tiongkok. Hal tersebut disebabkan adanya kesamaan pandangan antara Korea Utara dan

Tiongkok yang melihat bahwa *cyberwarfare* dapat digunakan untuk membuka peluang asimetris dan mengkompensasi kelemahan kapabilitas konvensional. KPA sendiri tidak pernah secara resmi mempublikasikan doktrin mereka, sehingga untuk memahami doktrin terkait *cyber space* Korea Utara hanya dapat disimpulkan melalui media, jurnal akademik, kesaksian pembelot serta analisis aktivitas *cyber* Korea Utara di masa lalu. Menurut Alexandre Mansourov (dalam Pinkston, 2016), KPA memiliki pandangan yang berbeda mengenai konsep *cyberwar* (싸이버戰) dan *cyberwarfare* (싸이버 戰爭), di mana *cyberwar* dilihat sebagai salah satu metode dalam melaksanakan perang, sedangkan *cyberwarfare* merupakan cara untuk mempengaruhi tindakan musuh dan memaksanya untuk melakukan sesuatu sesuai dengan kepentingan Korea Utara.

Awal dari penggunaan operasi jaringan komputer ataupun *cyber attack* oleh Korea Utara untuk menyerang aktor lain khususnya Korea Utara hingga saat ini masih belum diketahui secara pasti. Namun berdasarkan Kim Huˇnggwang, direktur eksekutif North Korea Intellectuals Solidarity, Korea Utama pertama kali mencoba untuk menggunakan *cyber attack* pada tahun 2004. Pinkston melihat bahwa aktivitas *cyber attack* Korea Utara sesuai dengan paradoks kestabilan–ketidakstabilan dalam *cyber space*, di mana Korea Utara tidak akan terhalang untuk melakukan tindakan pada spektrum konflik kelas rendah seperti *cyber attack*. Namun, karakteristik dari *cyber space* yang tidak dibatasi oleh batas-batas geografis tradisional memberikan Korea Utara kemampuan untuk menimbulkan ketidakstabilan kepada aktor lain khususnya Korea Selatan melalui *cyber space*.

Berdasarkan berbagai *cyber attack* yang berasal dari Korea Utara, penggunaan eksploitasi jaringan komputer sangat umum digunakan oleh Korea Utara, di mana mereka

mencoba untuk mengumpulkan berbagai data dari sistem informasi ataupun jaringan musuh. Dalam kasus Korea Selatan, Pyongyang memiliki keunggulan tersendiri dikarenakan tingginya tingkat konektivitas dan keterbukaan jaringan di Korea Selatan, yang selanjutnya membuka potensi yang luas untuk melakukan pengumpulan data melalui *cyber space*. Walaupun demikian, berbeda dengan *cyber attack* yang umumnya memiliki sifat *plausible deniability* di mana suatu negara dapat menyalahkan aktor lain seperti peretas patriotik ataupun hacktivis terkait aktivitas *cyber*-nya, Korea Utara sangat membatasi penggunaan internet secara umum, sehingga *cyber attack* yang berasal dari wilayah Korea Utara hampir dapat dipastikan dilakukan ataupun didukung oleh negara.

Literatur kedua yang peneliti ambil adalah *Iran and Cyberspace Warfare* oleh Gabi Siboni dan Sami Kronenfeld tahun 2012. Literatur tersebut membahas aspek-aspek yang mendorong perkembangan terkait kemampuan dan strategi *cyber* yang dimiliki oleh Iran. Sebagai negara yang pernah menjadi korban langsung dari *cyber attack* paling merusak hingga saat ini yaitu Stuxnet, Iran secara bertahap telah mencoba untuk memperkuat tingkat pertahanan *cyber* serta membangun kapabilitas *cyberwarfare* ofensif. Siboni dan Kronenfeld selanjutnya memberikan dua asumsi yang mendasari pendekatan Iran terhadap operasi *cyber*. Pertama, dibutuhkan adanya pembangunan kemampuan pertahanan dalam *cyber space* untuk menghadapi serangan dari negara ataupun aktor lainnya yang dipandang menentang Iran. Kedua, perlunya pembangunan kapabilitas *cyberwarfare* ofensif yang memungkinkan Iran untuk melawan keunggulan dan hegemoni Amerika Serikat dalam *cyber space*. Dalam bidang pertahanan, Iran mencoba untuk menciptakan sistem proteksi teknologi yang efektif, komprehensif, dan

terdepan untuk mempertahankan infrastruktur penting dan data sensitif dari *cyber attack* seperti Stuxnet. Selain itu, Iran juga berupaya untuk mengekang dan menggagalkan aktivitas *cyber* dari partai-partai oposisi domestik dan penentang rezim, di mana *cyber space* berperan sebagai platform komunikasi yang penting untuk menyebarluaskan informasi dan mengatur kegiatan anti-pemerintah.

Sementara dalam bidang ofensif, strategi *cyber* Iran berfokus kepada strategi asimetris dengan menggunakan kapabilitas *cyberwarfare* ofensif sebagai alat yang efektif untuk menimbulkan kerusakan yang signifikan kepada musuh yang memiliki keunggulan secara militer atau geostrategis. Dalam beberapa dekade terakhir, Iran telah melakukan perluasan strategi terhadap konstelasi *cyber* nasionalnya melalui pembentukan badan dan organisasi *cyber* dalam setiap kementerian pemerintah yang relevan. Tujuannya adalah untuk menciptakan keselarasan organisasi yang hierarkis dan luas berdasarkan rencana aksi yang jelas, alokasi sumber daya yang dipikirkan secara matang, serta distribusi tanggung jawab dan kapabilitas untuk mengamankan dan menyebarkan informasi, pengetahuan dan data.

Perkembangan dari strategi dan kekuatan *cyber* Iran selanjutnya menunjukan persiapan sistematis dan pembentukan organisasi dengan tujuan utama untuk menjadi aktor utama dalam *cyberwarfare*. Berdasarkan pengamatan Siboni dan Kronenfeld, Iran mengalami kemajuan secara konsisten dalam kemampuan operasi *cyber* yang didukung oleh infrastruktur sains Iran yang sangat maju dan banyaknya tenaga terampil yang tersedia. Upaya *cyber attack* yang dilakukan oleh Iran terhadap perusahaan minyak Arab Saudi Aramco pada Agustus 2012 membuktikan cepatnya perkembangan kapabilitas

cyberwarfare ofensif Iran serta seberapa jauh mereka berani untuk menggunakan kapabilitas tersebut. Iran tidak hanya menggunakan kapabilitas yang dimiliknya sebatas untuk operasi spionase atau pengumpulan intelijen, namun juga melakukan penghancuran data dan komputer target secara lengkap dan total apabila sesuai dengan kepentingan Iran. Dalam operasi *cyberwarfare* ofensif Iran, Pengawal Revolusi Iran merupakan salah satu aktor dengan tingkat kapabilitas *cyber* tertinggi di dunia, di mana pada tahun 2008 Iran telah merekrut sekitar 2.400 profesional dan memiliki anggaran hingga US$ 76 juta.

Siboni dan Kronenfeld melihat bahwa Pengawal Revolusi juga mempunyai hubungan secara aktif dengan kelompok-kelompok peretas Iran dalam menghadapi musuh Iran, baik domestik maupun internasional. Dengan menggunakan kelompok-kelompok tersebut, pemerintah Iran dan Pengawal Revolusi dapat menjaga jarak dan membantah tuduhan terkait keterlibatan mereka dalam operasi *cyberwarfare* hingga *cybercrime*. Kelompok-kelompok peretas Iran secara konsisten terlibat dalam berbagai *cyber attack* terhadap jaringan-jaringan tertentu, penyebaran materi yang mendukung pemerintah Iran, pencurian informasi, penipuan kartu kredit hingga menganggu atau mengubah rute lalu lintas internet. Pendekatan ini tidak hanya digunakan oleh Iran, namun juga negara-negara dengan aktivitas *cyber* yang tinggi seperti Tiongkok dan Rusia. Dapat dilihat bahwa faktor *plausible deniability* menjadi pertimbangan utama Iran dalam mengembangkan kapabilitas *cyberwarfare* ofensif yang selanjutnya dapat digunakan untuk menyerang infrastruktur kritis di negara-negara yang menjadi musuh Iran seperti Amerika Serikat dan Israel, namun tetap memishakan diri dari keterlibatan terkait aktivitas tersebut.

Literatur ketiga yang kemudian ditinjau peneliti adalah *Cyber Security: China and Russia's Erosion of 21st Century United States' Hegemony* oleh Cyril K. Yancey tahun 2019. Kemunculan Tiongkok dan Rusia yang menatang hegemoni Amerika Serikat, penggunaan *cyberwarfare* kemudian digunakan untuk memiringkan keseimbangan kekuatan saat ini demi kepentingan kedua negara tersebut. Kemampuan ekonomi Amerika Serikat yang kuat, militer aktif yang besar, serta *soft power* internasional yang luas menyebabkan posisinya sebagai hegemon dunia saat ini. Namun, Yancey melihat bahwa berbagai kampanye dan aktivitas *cyber* yang dilakukan oleh Tiongkok dan Rusia mampu menimbulkan risiko strategis jangka panjang bagi Amerika Serikat dan memperlemah hegemoninya. Hambatan-hambatan tradisional yang umumnya mencegah negara-negara yang lebih lemah terlibat dalam konflik dengan negara kuat, seperti kurangnya angkatan bersenjata atau sumber daya militer, menjadi tidak relevan dengan kepemilikan dan penggunaan kapabilitas *cyberwarfare* ofensif. Negara-negara ini tidak membutuhkan modal yang dibutuhkan saat melancarkan serangan dan memperoleh keuntungan tersendiri dalam suatu konflik. Menurut Yancey, luasnya penggunaan *cyber space* menyebabkan kekuatan *cyber* dan kemajuan teknologi suatu negara dapat menjadi ukuran yang lebih akurat dari kemampuan militer abad ke-21 dikarenakan potensi dari berbagai *cyber attack*.

Hingga saat ini, Tiongkok telah mencoba untuk menantang Amerika Serikat melalui pengembangan dan pengunaan *cyberwarfare* yang bertujuan untuk melemahkan *hard power* yang telah dimiliki oleh Amerika Serikat sebelumnya. Ketika *cyberwarfare* secara penuh mengambil alih kepraktisannya di abad ini, sejumlah besar pengeluaran

yang digunakan Amerika Serikat untuk pengembangan nuklir dan bentuk-bentuk *hard power* tradisional lainnya dapat melemah. Selain upaya pertikaian hegemonik oleh Tiongkok, perkembangan dan kesediaan Rusia untuk menggunakan senjata dunia maya menambah ancaman tambahan bagi keamanan nasional Amerika Serikat secara keseluruhan, serta infrastruktur dunia maya dunia. Yancey menyimpulkan bahwa ancaman utama bagi hegemoni Amerika Serikat datang dalam bentuk *cyber*, dengan Rusia dan Tiongkok memperoleh keunggulan melalui kurangnya aturan dan hukuman, seperti yang ditunjukkan oleh berbagai insiden *cyber attack* yang mereka jalankan selama ini. Dimasukkannya kapabiltias *cyberwarfare* dalam kesiapsiagaan militer memiliki potensi untuk menggeser ukuran kekuatan saat ini, yang selanjutnya mengubah persaingan hegemonik yang berpihak kepada Tiongkok dan Rusia. Negara-negara yang mungkin tidak memiliki ukuran kekuatan tradisional, seperti pasukan tetap yang besar atau pengeluaran militer yang tinggi, dapat memperoleh kekuasaan melalui pengembangan *cyberwarfare* dan mengejar ketertinggalannya.

Berdasarkan tiga literatur yang telah peneliti paparkan di atas, peneliti menyimpulkan bahwa untuk menjawab rumusan masalah dibutuhkan adanya pemahaman mengenai pandangan serta definisi dari hal-hal yang berhubungan dengan *cyber space* bagi suatu negara untuk mengetahui bagaimana negara tersebut mengembangkan dan menggunakan kapabilitas *cyber* mereka. Walaupun terdapat perbedaan kepercayaan dan doktrin terkait bagaimana kapabilitas *cyberwarfare* digunakan oleh suatu negara, terdapat persamaan kepercayaan bahwa *cyberwarfare* memberikan kesempatan bagi negara-negara yang mengalami ketertinggalan secara kekuatan untuk memperoleh keunggulan

asimetris serta memiliki *deterence* terhadap aktor yang lebih kuat. Selain itu, karakteristik *plausible deniability* yang dimiliki oleh *cyberwarfare* kemudian menjadi alasan penting mengapa berbagai negara lebih merasa aman untuk mengembangkan dan menggunakan kapabilitas *cyber* mereka, di mana suatu negara dapat melakukan serangan terhadap aktor lain tanpa harus menghadapi konsekuensi secara langsung.

1.5 Kerangka Pemikiran

Berdasarkan tinjauan literatur yang telah peniliti lakukan, negara cenderung menggunakan kapabilitas *cyberwarfare* ofensif sebagai cara untuk mengejar ketertinggalan kekuatan melalui keunggulan asimetris serta sebagai upaya *deterence* dalam menghadapi aktor yang lebih kuat. Penulis menggunakan beberapa pendekatan teoritis untuk menganalisis upaya *cyberwarfare* ofensif yang digunakan oleh negara. Pembahasan mengenai *cyberwarfare* cenderung befokus kepada keamanan dan persaingan, distribusi kekuasaan, keuntungan ofensif dibandingkan defensif, dan manfaat strategi *deterence*.

Untuk melihat bagaimana suatu negara mengembangkan dan menggunakan kapabilitas *cyberwarfare*, peneliti menggunakan teori *offense-defense balance*. Berdasarkan teori ini, faktor teknis dan geografis secara langsung mempengaruhi apakah penggunaan serangan atau pertahanan memiliki keuntungan dalam potensi perang, dan kedua hal tersebut akan mempengaruhi bagaimana dua kombatan potensial mempersiapkan diri untuk konflik dan bereaksi terhadap krisis (Shaheen, 2014). Umumnya, teori *offense-defense balance* digunakan untuk membuat beberapa prediksi tentang bagaimana negara berperilaku ketika mereka percaya terdapat ketidakseimbangan

antara posisi ofensif dan defensif. Pilihan untuk mempertahankan superioritas ofensif dianggap lebih menguntungkan dalam hal menghasilkan hasil konflik dengan cepat serta membuat konflik lebih murah dan tidak terlalu merusak. Dalam *cyberwarfare*, pengembangan kapabilitas *cyberwarfare* ofensif bisa menjadi opsi yang menarik mengingat karakternya yang berbeda dan tidak dapat ditiru secara luas, serta pada saat ini sangat sulit dihadapi dengan mekanisme pertahanan apa pun. Keuntungan-keuntungan yang diasosiasikan dengan superioritas ofensif seperti serangan pertama dan perebutan inisiatif membuat negara-negara terlibat dalam perlombaan senjata untuk memperoleh superioritas terhadap musuh-musuhnya. Namun, superioritas dalam pertahanan juga mampu meningkatkan *deterrence* dan tidak membutuhkan suatu aktor untuk menyamai kekuatan dengan aktor lainnya. Keseimbangan antara ofensif dan defensif dalam *cyber space* secara signifikan mirip dengan yang ada dalam peperangan konvensional dikarenakan sisi defenfsif dari keseimbangan yang jauh lebih lemah, yang pada gilirannya memberikan keunggulan atas sisi ofensif (Shaheen, 2014).

Pendekatan kedua yang peneliti gunakan adalah teori neorealisme ofensif John J. Mearsheimer yang melihat bahwa kebutuhan terhadap keamanan serta bertahan hidup menyebabkan negara untuk memaksimalkan kekuatan atau kapabilitas agresif, di mana negara-negara cenderung tidak bekerja sama dan lebih memilih untuk mengurangi kekuatan lawan serta meningkatkan kekuatan sendiri. Pada dasarnya, neorealisme ofensif mengacu kepada turunan dari teori neorealisme Kenneth Waltz yang menyatakan bahwa struktur anarkis dari sistem internasional telah memaksa negara-negara untuk mengejar kekuatan untuk memastikan kelangsungan hidup mereka. Dalam sistem yang anarki,

tidak ada otoritas yang berada di atas negara serta sulit untuk dipastikan apakah suatu negara tidak akan menyerang negara lainnya, sehingga negara harus menjadi cukup kuat untuk melindungi dirinya sendiri apabila menghadapi serangan. Namun, berbeda dengan Waltz yang percaya bahwa negara seharusnya tidak mencoba untuk memaksimalkan kekuatan mereka dikarenakan akan mendorong reaksi oleh negara-negara untuk melakukan *balancing* ketika suatu negara dianggap memperoleh terlalu banyak kekuatan, Mearsheimer (2007) memandang upaya untuk mengumpulkan kekuatan sebanyak mungkin merupakan strategi yang tepat bagi negara-negara dan menjadi hegemoni adalah jalan yang terbaik untuk mengamankan kelangsungan hidup negara. Mearsheimer selanjutnya menuliskan lima asumsi utama tentang sistem internasional yang mendorong negara untuk merumuskan kebijakan agresif.

Asumsi pertama adalah kekuatan-kekuatan besar merupakan aktor utama dalam politik dunia yang bekerja dalam sistem anarkis. Namun, anarki yang dimaksud adalah hanya sebatas tidak adanya otoritas terpusat atau kekuatan utama yang berdiri di atas negara. Asumsi kedua, setiap negara memiliki kemampuan militer ofensif dan mampu untuk menimbulkan kerusakan atau kerugian terhadap negara-negara tetangganya, meskipun kemampuan tersebut bervariasi di antara negara-negara dan dapat berubah seiring waktu. Asumsi ketiga adalah bahwa negara tidak pernah bisa memastikan tentang intensi dari negara lain. Asumsi keempat, tujuan utama negara adalah bertahan hidup, di mana setiap negara akan berusaha untuk mempertahankan integritas teritorial dan otonomi tatanan politik domestik mereka. Asumsi kelima adalah bahwa negara

merupakan aktor rasional, yang artinya negara mampu menghasilkan strategi yang baik untuk memaksimalkan prospek suatu negara dalam bertahan hidup.

Ketika kelima asumsi tersebut digabungkan bersama, selanjutnya menghasilkan tiga pola perilaku negara yakni: ketakutan, *self-help*, dan pemaksimalan kekuatan. Adanya ketidakpercayaan di antara negara-negara kemudian menyebabkan negara untuk beroperasi dalam sistem *self-help* di mana menjadi negara paling kuat dalam sistem dipandang sebagai cara terbaik untuk memastikan kelangsungan hidup suatu negara. Selanjutnya, negara-negara akan mencoba untuk memaksimalkan kekuatan mereka dan mempengaruhi keseimbangan kekuatan melalui penggunaan berbagai alat dan jalan, meskipun penggunaan tersebut dapat menyebabkan negara lain curiga atau bermusuhan. Ketidakpastian dari intensi negara-negara menyebabkan kapabilitas menjadi hal terpenting bagi negara, di mana negara akan berbohong, menipu dan menggunakan kekerasan apabila hal tersebut dapat membantu untuk mendapatkan keunggulan. Seluruh kekuatan-kekuatan besar memiliki kecenderungan revisionis hingga mereka mencapai hegemoni dan menghasilkan persaingan keamanan yang konstan (Mearsheimer, 2007). *Cyber space* dan anarki memiliki keterkaitan yang erat, di mana hingga saat ini belum ada konsesus bersama terkait regulasi *cyberwarfare* yang ditandai oleh kurangnya kesepakatan dan kerja sama antara negara, hukum internasional, dan institusi tentang tata kelola *cyber* secara global. Walaupun terdapat beberapa organisasi yang relevan seperti International Telecommunications Union (ITU) dan Internet Corporation for Assigned Names and Numbers (ICANN), fungsi dan kompetensinya organisasi tersebut tidak mencakup hingga manajemen konflik (Craig & Valeriano, 2018). Tidak adanya aturan

internasional yang secara tegas mengatur penggunaan *cyberwarfare* didorong oleh kecenderungan negara-negara, baik kekuatan besar ataupun kecil, untuk tidak mengakui kepemilikan ataupun penggunaan kapabilitas *cyber*. Ketika melihat perkembangan *cyberwarfare* saat ini, dapat ditemukan bahwa negara-negara telah mencoba untuk mencapai *cyber superiority* serta upaya-upaya militerisasi dalam *cyber space* dalam menghadapi elemen ketidakpastian dari *cyberwarfare*. Dapat dikatakan bahwa *cyberwarfare* merupakan domain lain dari dunia politik yang telah dimiliterisasi untuk memastikan keamanan serta membatasi keamanan aktor lain. Selain itu, *cyberwarfare* juga memberikan kesempatan bagi suatu negara untuk menghancurkan keamanan dan otonomi nasional negara lain dan menciptakan kerentanan yang sangat berbahaya yang dapat mengancam kelangsungan hidupnya dan rakyatnya.

Setiap konflik memiliki karakteristik asimetris di mana kerentanan dan perbedaan dalam kekuatan akan selalu ada. Namun, konsep dari strategi asimetris telah lama ada dan secara universal telah didefinisikan dalam pemikiran militer. Secara umum, strategi asimetris sangat berhubungan dengan sumber daya militer yang tidak setara dan penggunaan metode yang tidak konvensional untuk mengeksploitasi kerentanan musuh (Kukkola & Nikkarila, 2017). Keunggulan dari strategi asimetris adalah setiap aktor strategis baik lemah ataupun kuat dapat menerapkannya secara optimal. Keterampilan dan kecakapan yang memadai adalah satu-satunya atribut yang dibutuhkan oleh strategi asimetris. Aktor non-negara yang lemah mungkin memiliki insentif lebih besar untuk mengadopsi strategi asimetris itu untuk mengatasi kurangnya pilihan yang tersedia, namun tidak ada alasan bahwa aktor negara yang kuat tidak dapat melakukan hal yang

sama (Breen & Geltzer, 2011). Konsep tradisional dari strategi asimetris sendiri selalu terikat sebagai senjata atau upaya yang digunakan oleh aktor yang lebih kecil dan lemah. Namun, dalam konteks *cyber space*, strategi asimetris menjadi lebih luas dan digunakan oleh aktor-aktor yang semakin kuat dengan dampak yang mengesankan. Menurut Kukkola & Nikkarila (2017), terdapat dua alasan mengapa hal tersebut terjadi.

Pertama, *cyber space* bersifat artifisial dan dapat dapat dibentuk sesuai dengan kebutuhan dan kepentingan keamanan negara. Kedua, terdapat beberapa negara yang bersedia untuk menerapkan konsep jaringan tertutup yang dikontrol secara nasional dengan membatasi jaringan, mengendalikan infrastruktur, dan membatasi aliran informasi. Dari satu sisi, dorongan untuk membangun kedaulatan *cyber* dapat dilihat sebagai tindakan untuk membatasi dan mengendalikan asimetri yang didorong oleh penyebaran kekuasaan dan kerentanan yang terlihat. Tetapi dari sudut pandang yang lain, proses tersebut cenderung bersembunyi di balik pembangunan jenis asimetri yang berbeda.

Selanjutnya, *cyberwarfare* juga membuka kesempatan bagi negara-negara untuk melakukan *cyber deterrence*. McKenzie (2017) mendefinisikan *deterrence* sebagai pencegahan tindakan baik melalui adanya ancaman yang nyata ataupun keyakinan bahwa biaya dari tindakan akan lebih besar daripada manfaat yang dirasakan. *Deterrence* dapat dibagi menjadi dua opsi, yakni *deterrence* aktif dan *deterrence* pasif. Libicki (2009, dalam McKenzie, 2017) menjelaskan *deterrence* pasif sebagai pencegahan melalui penolakan seperti kemampuan untuk menggagalkan serangan dan *deterrence* aktif sebagai pencegahan melalui hukuman seperti ancaman pembalasan. Dari sudut pandang

cyber, *deterrence* pasif mencakup berbagai tindakan yang diambil untuk mengamankan jaringan dari serangan atau untuk membangun jaringan tangguh yang mampu meminimalkan efek serangan. Tindakan-tindakan tersebut merupakan bagian penting sistem dan doktrin keamanan yang baik namun tidak memiliki peran yang aktif dalam mencegah terjadinya *cyber attack*. Sebagai alternatif, *deterrence* aktif dalam *cyber space* membawa ancaman serangan balasan ataupun respon yang tidak diinginkan terhadap *cyber attack* ataupun insiden yang terjadi di dalam *cyber space*.

Tujuan utama dari *cyber deterrence* sendiri adalah untuk untuk mengurangi risiko *cyber attack* ke tingkat yang dapat diterima dengan biaya yang dapat diterima, di mana negara yang berada dalam posisi defensif mampu meminimalkan potensi tindakan ofensif dengan mengancam untuk melakukan pembalasan yang kuat (Iasiello, 2013). Namun, *cyber deterrence* bukanlah solusi satu-satunya untuk menghadapi pelaku ancaman *cyber* yang ingin mengeksploitasi jaringan sektor publik dan swasta dikarenakan terlalu banyak variabel yang belum dieksplorasi dan rencana yang belum dikembangkan untuk menjadikan tindakan tersebut berjalan efektif.

1.6 Hipotesis

Berdasarkan kepada kerangka pemikiran yang telah dipaparkan sebelumnya, peneliti merumuskan hipotesis bahwa dalam menghadapi *cyber superiority* yang dimiliki oleh Amerika Serikat, Tiongkok mencoba untuk mengembangkan dan menggunakan kapabilitas *cyberwarfare* ofensif dengan menargetkan tidak hanya kepada institusi atau infrastruktur yang dimiliki oleh negara, namun juga berfokus kepada target-target sipil.

1.7 Metodologi Penelitian

1.7.1 Definisi Konseptual & Operasionalisasi Konsep

1.7.1.1 Cyberwarfare

Untuk mendefinisikan *cyberwarfare*, terdapat tiga hal yang perlu diperhatikan. Pertama, penggunaan istilah *cyberwarfare* harus berhubungan langsung dengan operasi jaringan komputer. Kedua, peperangan psikologis yang terjadi di *cyber space* tidak dianggap sebagai *cyberwarfare*. Ketiga, dalam *cyberwarfare* terdapat tujuan politik atau militer secara langsung dibalik suatu serangan, baik dengan maksud koersif ataupun sebagai kekuatan strategis. Berdasarkan ketiga hal tersebut, Liff (2012) menulis bahwa *cyberwarfare* merupakan keadaan konflik antara dua atau lebih aktor politik yang dicirikan oleh penggunaan serangan jaringan komputer untuk menyerang warga sipil ataupun infrastruktur militer dengan maksud koersif untuk mendapatkan konsensi politik dan melemahkan pertahanan musuh. *Cyber space* saat ini telah menjadi ruang publik yang diperebutkan dan dimiliterisasi, dimana lemahnya pengawasan serta tidak adanya norma global memungkinkan negara yang agresif dan bermusuhan untuk melakukan berbagai *cyber attacks* kepada negara lain dan institusi yang ada (Burk & Kallberg, 2016). Pada dasarnya, *cyber space* merujuk kepada seluruh jaringan komputer di dunia dan semua yang mereka hubungkan dan kendalikan melalui kabel, serat optik, atau nirkabel. Tidak hanya internet, namun berbagai jaringan komputer lain, termasuk jaringan yang tidak seharusnya dapat diakses melalui internet. Bagian lain dari *cyber space* adalah jaringan transaksional yang melakukan hal-hal seperti pengiriman data terkait aliran uang, perdagangan pasar saham, dan transaksi kartu kredit.

Sementara *cyber attack* umumnya dipahami sebagai serangan yang dimulai dari komputer terhadap situs internet, jaringan, atau komputer individu yang membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem ataupun informasi yang disimpannya. Untuk menghadapi terjadinya *cyberwarfare*, negara-negara mencoba membentuk unit militer *cyber* sebagai bentuk pertahanan dan melihat internet terbuka sebagai ancaman keamanan nasional yang harus diatur dan diawasi. Namun, upaya tersebut dilihat kurang efektif dikarenakan kebanyakan negara masih menangani pertahanan *cyber* melalui pandangan militer tradisional yang tidak mempertimbangkan faktor-faktor yang hanya terdapat dalam *cyber space* seperti anonimitas, tidak adanya objek yang bersifat permanen, dan tidak adanya pengukuran efektivitas (Burk & Kallberg, 2016).

1.7.1.2 Cyber Superiority

Cyber superiority didefinisikan sebagai tingkat dominasi dalam *cyber space* oleh satu aktor yang memungkinkan pelaksanaan operasi yang aman dan kuat dari aktor tersebut, serta dapat terhubung dengan kekuatan darat, udara, laut, dan ruang angkasa pada waktu dan lingkungan operasi tertentu tanpa campur tangan ataupun gangguan oleh musuh. Dominasi dalam *cyber space* hanya dapat dicapai jika suatu aktor memiliki kemampuan untuk mengumpulkan informasi, menyerang dan mencegat aktivitas *cyber* aktor lain sehingga mampu mencegah keterlibatan luar, dan kemungkinan juga memanfaatkan kapabilitas *cyber* untuk menghancurkan atau merusak sistem *cyber* dari aktor lain. Aktor-aktor dalam *cyber space* berusaha menghubungkan cara dan sarana *cyber*-nya, sementara pada saat yang sama musuh akan berusaha menghalangi mereka

mencapai tujuan yang telah ditentukan. Aktor yang berada di posisi bertahan dapat mengganggu sarana atau cara penyerang, dan penyerang selanjutnya dapat mencoba untuk merusak pertahanan yang ada.

Alasan mengapa negara-negara saat ini mencoba untuk memiliki *cyber superiority* adalah dikarenakan pentingnya kapabilitas *cyberwarfare* untuk mengidentifikasi dan mengganggu operasi informasi musuh. Melalui kapabilitas *cyberwarfare* yang tinggi, suatu negara dapat melebihi kemampuan militer musuh di semua domain, memperluas opsi bagi pembuat keputusan dan komandan operasional kami, dan menghasilkan efek terintegrasi. Selain itu, pengetahuan dan informasi ancaman yang diperoleh dari pengoperasian dalam *cyber space* dapat membuat elemen kunci kekuatan ekonomi lebih kuat dan dapat dipertahankan.

1.7.1.3 Strategi Cyber Tiongkok

Cyber space memberikan kemampuan bagi suatu negara untuk melawan kepentingan politik, ekonomi, dan keamanan aktor lain tanpa harus keluar dari perbatasannya. Melalui *cyber attack*, negara memiliki peluang yang tidak dapat disangkal untuk merusak atau mengganggu infrastruktur penting secara serius, melumpuhkan aktivitas bisinis, melemahkan jaringan keamanan, dan menyerang alat dan perangkat yang digunakan masyarakat suatu negara untuk berkomunikasi dan menjalankan bisnis. Hal ini selanjutnya mendorong beberapa negara untuk mengembangkan strategi *cyberwarfare* ofensif untuk mendukung kepentingannya. Terdapat tiga alasan utama mengapa suatu negara mempertahankan dan memanfaatkan kemampuan *cyber* secara ofensif (Hjortdal, 2011). Pertama, untuk melemahkan negara lain dengan menginfiltrasi

infrastruktur penting mereka secara tidak langsung. Kedua, untuk mendapatkan informasi dan pengetahuan melalui aktivitas spionase di *cyber space* yang dilihat mampu untuk meningkatkan pengembangan militer. Ketiga, untuk mendapatkan keuntungan ekonomi melalui kemajuan teknologi yang dicapai oleh pihak lain, contohnya adalah dengan spionase industri.

Kemampuan *cyber* sendiri bukanlah subjek yang dibahas oleh negara secara terbuka, dikarenakan dapat menimbulkan kerugian bagi suatu negara untuk mempublikasikan bahwa negara tersebut memata-matai negara lain atau menyebabkan jaringan negara lain mengalami kerusakan (Hjortdal, 2011). Hal tersebut menyebabkan *cyberwarfare* memiliki aspek *plausible deniability*, dimana aktor A (penyerang) mempunyai kemampuan untuk melakukan *cyber attack* kepada aktor B (target) dengan cara yang sedemikian rupa sehingga sulit untuk membuktikan bahwa aktor A yang bertanggung jawab terhadap serangan tersebut. Adanya *plausible deniability* kemudian membentuk pandangan dari beberapa aktor bahwa *cyber attack* dapat dilakukan tanpa adanya ancaman hukuman, sehingga menurunkan biaya potensial yang dikeluarkan oleh penyerang dan membuat penggunaan serangan jaringan komputer lebih dipilih dibandingkan dengan serangaan konvensional (Liff, 2012).

1.7.2 Jenis Penelitian

Jenis penelitian yang digunakan adalah eksplanatif dikarenakan penelitian ini bertujuan untuk menjelaskan sebuah fenomena. Fenomena yang ada dalam penelitian ini adalah upaya dan strategi Tiongkok menghadapi *cyber superiority* Amerika Serikat dalam melalui pengembangan kapabilitas *cyberwarfare* ofensif.

1.7.3 Jangkauan Penelitian

Jangkauan penelitian ini dibatasi pada awal tahun 2003 hingga akhir tahun 2015. Awal jangkauan penelitian dipilih oleh peneliti berdasarkan rangkaian *cyber attack* secara masif yang dilakukan oleh Tiongkok yang disebut sebagai Titan Rain pada tahun 2003. Sementara itu peneliti membatasi data-data hingga akhir tahun 2015 dikarenakan terbatasnya data mengenai kapabilitas *cyber* Tiongkok.

1.7.4 Teknik Pengumpulan Data

Pengumpulan data dalam penelitian ini melalui studi kepustakaan yang mencakup di dalamnya buku teks, jurnal ilmiah, berita online, dokumen-dokumen, dan situs resmi yang berkaitan dengan kebijakan normalisasi dan peran pemimpin dalam pengambilan kebijakan luar negeri.

1.7.5 Teknik Analisis Data

Analisis data yang diperoleh penulis diolah menggunakan teknik kualitatif. Teknik kualitatif ini digunakan untuk menganalisis data-data yang berupa informasi baik berupa angka maupun kata yang bersifat kualitatif untuk menjawab rumusan masalah.

1.7.6 Sistematika Penulisan

Penelitian ini ditulis ke dalam lima bab. Bab II menjelaskan doktrin dan penerapan Tiongkok mengenai *cyber space* dan *cyberwarfare*. Bab III berisi penjelasan dinamika hubungan Tiongkok dan Amerika Serikat dalam *cyber space*. Bab IV adalah analisis penggunaan kapabilitas *cyberwarfare* ofensif oleh Tiongkok. Bab V merupakan kesimpulan.