

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penulis menggunakan beberapa penelitian terdahulu yang menyajikan topik yang relevan dengan penulisan ini, antara lain:

Penelitian pertama adalah jurnal berjudul *Dampak Pembangunan Cyberpower Tiongkok Terhadap Kepentingan Amerika Serikat* yang ditulis oleh Dewi Triwahyuni dari Universitas Komputer Indonesia Bandung dan Yayan Mochamad Yani dari Universitas Padjajaran Bandung¹⁵. Peneliti mengemukakan bagaimana tujuan pembangunan *cyberpower* China dan dampaknya bagi kepentingan Amerika Serikat. Pernyataan tegas Presiden Xi Jinping bahwa China harus menjadi negara *cyberpower* menjadi fokus peneliti dalam melihat tujuan pembangunan *cyberpower* China. Peneliti ini penting bagi penulis karena adanya temuan bahwa dalam catatan Amerika Serikat, China adalah negara yang paling sering melakukan serangan *cyber* ke Amerika Serikat.

Persamaan penelitian di atas dengan penelitian ini terletak pada pembahasan mengenai tema permasalahan yaitu *cyberpower* antara China dan Amerika Serikat. Sedangkan perbedaan penelitian tersebut dengan penelitian ini terletak pada sudut pandang subjek penelitian. Penelitian sebelumnya berada

¹⁵Dewi Triwahyuni, dan Yayan Mochamad Yani, "Dampak Pembangunan Cyberpower Tiongkok terhadap kepentingan Amerika Serikat", *Jurnal Ilmu Politik dan Komunikasi*, Vol. VIII, No. 1, Jun (Bandung: Universitas Komputer Indonesia, 2018), hal 1-14.

dalam sudut pandang Amerika Serikat sementara penelitian ini akan lebih terfokus pada sudut pandang China.

Penelitian kedua adalah penelitian berjudul “*Motivasi China Menguasai Cyber Teknologi*” yang ditulis oleh Nadya Vira Meisitha, Agung Purwanto, dan Linda Dwi Eriyanti.¹⁶ Penelitian ini membahas motivasi China dalam menguasai *Cyber Teknologi*. Peneliti menunjukan bahwa China dan Amerika Serikat berpotensi untuk perang di Laut China, terutama atas isu Taiwan, Semenanjung Korea, dan Kepulauan Diayou sebagai pemicunya. Penelitian ini penting bagi penulis karena memberikan analisis bahwa China harus menguasai *cyber teknologi* pada peralatan perangnya untuk menghadapi ancaman perang, Amerika Serikat turut menggunakan basis *cyber teknologi* pada peralatan perangnya.

Persamaan penelitian di atas dengan penelitian ini adalah terletak pada pembahasan mengenai China ingin menguasai *cyberpower* dunia hingga tidak dapat ditandingi oleh negara lain. Sedangkan perbedaan penelitian terletak pada isu yang melatarbelakangi penelitian. Penelitian sebelumnya dilatarbelakangi oleh potensi perang di Laut China, sedangkan penelitian ini dilatarbelakangi oleh rivalitas siber China dan Amerika Serikat atas trend penggunaan teknologi sebagai basis pertahanan dan keamanan dalam berbagai sektor.

Penelitian ketiga berjudul “*The Strategic Support Force and the Future of Chinese Information Operations*” yang ditulis oleh Elsa B. Kania and John K.

¹⁶Nadya Vira Meisitha, Agung Purwanto, dan Linda Dwi Eriyanti, “Motivasi China Menguasai Cyber Teknologi”, *Student Research Article*, (Jember : Universitas Jember, 2014), hal 1-5.

Costello.¹⁷ Penelitian ini membahas reformasi SSF menjadi upaya PLA China untuk menyelesaikan masalah sebelumnya dan, membangun kemampuan tempur melalui kekuatan *cyber* militer negara. SSF dinilai akan meningkatkan kemampuan PLA untuk berperang khususnya perang informasi di masa. Penelitian ini penting bagi penulis karena memberikan pemaparan terkait modernisasi militer dan, ilmu pengetahuan dan teknologi pertahanan yang dilakukan oleh China.

Persamaan penelitian di atas dengan penelitian ini adalah kesamaan fokus penelitian terhadap strategi *cyber* China untuk keamanan. Sedangkan perbedaan penelitian terletak pada subjek penelitian. Penelitian diatas hanya terfokus pada keamanan siber China saja, sedangkan penelitian ini mengkaitkan keamanan siber China dan rivalitas sibernya dengan Amerika Serikat (lanskap analisis lebih luas dengan objek pembanding).

2.2 Kerangka Teori

2.2.1 Teori Cyberpower

Joseph S.Nye, JR dalam bukunya yang berjudul *Cyberpower* mengatakan (2010:4) “*Cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power*”. Pemikirnya menunjukan bahwa *cyberpower* dapat digunakan untuk memberikan hasil yang diinginkan dalam *cyberspace*. *Cyberspace* merupakan domain operasional yang dapat mengeksploitasi informasi melalui sistem yang

¹⁷Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations”, *The Cyber Defense Review*, Vol. 1, No. 1 – Vol 6, No 2, (New York: JSTOR, 2018), hal 105-122.

saling berhubungan dan infrastruktur yang terkait.¹⁸ Teori ini nantinya akan menjadi instrumen analisis yang akan selalu ada dalam pembahasan khususnya di bab 4 yang mengangkat judul pembahasan *Cyberpower* China dan Amerika Serikat.

Perilaku *cyberpower* bertumpu pada seperangkat sumber daya yang memiliki keterhubungan antara penciptaan, kontrol, dan komunikasi informasi berbasis komputer (infrastruktur, jaringan, perangkat lunak, dan keterampilan manusia). Selain itu, hambatan masuk dalam domain *cyber* sangat rendah sehingga memungkinkan keterlibatan aktor lain. Apabila tercipta ketergantungan pada sistem *cyber* hingga suatu negara memanfaatkan untuk kepentingan militer dan ekonomi, maka, hal ini dapat menciptakan kerentanan baru yang dapat dieksploitasi.¹⁹ Teori ini akan relevan dengan analisis penulis dikarenakan penulis meletakkan fokus yang bahwa *cyberpower* mempengaruhi keamanan, kestabilan dan kemajuan negara.

Kenyataan adanya rivalitas *cyber* antara China dan Amerika Serikat dengan memanfaatkan *cyberspace* sebagai salah satu basis keamanan menciptakan fakta baru dewasa ini. Fakta bahwa upaya strategi keamanan bukan lagi hanya dalam bentuk fisik namun juga *soft power* berupa penguasaan *cyberpower*. Pemikiran inilah yang dijadikan dasar bagi penulis untuk mengkorelasikan teori *cyberpower* bahwa perang jenis baru yang akan mungkin terjadi antara China dan Amerika Serikat akan dipengaruhi oleh pengembangan *cyberpower*.

¹⁸Joseph S.Nye, Jr, “*Cyberpower*”, *Belfer Center for Science and International Affairs*, (Cambridge: Harvard Kennedy School, 2010), hal 3.

¹⁹Ibid, hal 4.

Sebagaimana yang diketahui bahwa China semakin berambisi mengembangkan *cyberpower*. Pengembangan ini tidak terlepas dari upaya pengamanan wilayah dan kestabilan politik serta mengembangkan iklim bisnis ekonomi China dalam konteks global. Implikasi pengembangan *cyber* dilakukan dalam berbagai sektor vital dan saling memiliki korelasi satu dengan lainnya. Modernisasi Militer menjadi salah satu target dalam strategi *Five Years Plans of China*. Selain itu pengembangan *cyber* dalam industrialisasi semakin menunjukkan semakin jelas orientasi pengembangan yang dikejar oleh China.

Amerika Serikat tidak berbeda jauh dengan China. Kedudukannya sebagai negara hegemoni mulai terusik. Berbagai sikap yang ditujukan Amerika Serikat sangat jelas terlihat bahwa negara tersebut berusaha “menjegal” kebangkitan China dan memposisikan China sebagai pesaing. Kesadaran bahwa konteks persaingan dalam keamanan kontemporer telah berubah mendorong Amerika Serikat harus mampu bersaing dengan China. Amerika Serikat berusaha mengembangkan teknologi dan mengeluarkan berbagai kebijakan untuk menjaga posisinya. Amerika Serikat melihat bahwa pengembangan *cyber* yang dilakukan oleh China termasuk pengembangan teknologi *Artificial Intelligence* akan mengancam keamanan dan informasi. Banyaknya kasus *cyber espionage* yang dilaporkan telah dilakukan oleh China cukup menjadi alasan Amerika Serikat menaruh fokus pada China.

Teori *cyberpower* menurut penulis cocok untuk menganalisa rivalitas *cyber* China dan Amerika Serikat. Melalui teori ini penulis akan melakukan analisis pembuktian bahwa kedua negara mengintegrasikan kemampuan *cyber* dalam dalam berbagai sektor. Peneliti akan mengkaji bahwa hasil integrasi teknologi tersebut

memiliki *impact* terhadap rivalitas antara China dan Amerika Serikat. Penelitian ini turut akan mengkaji apakah pengembangan kekuatan *cyber* China dapat membawa kembali negara tersebut dalam romantisme kejayaan yang pernah dimilikinya.

2.2.2 Konsep *Competitive Strategy*

Strategi merupakan sebuah kata yang berasal dari bahasa Yunani, “*strategia*” yang diartikan sebagai “the art of the general” atau seni seorang panglima yang biasanya digunakan dalam peperangan.²⁰ Secara umum, strategi digambarkan sebagai cara untuk memperoleh kemenangan atau mencapai tujuan. Sementara itu, Kompetisi memiliki pengertian atas adanya persaingan untuk mencapai posisi yang lebih besar. Dalam setiap persaingan ini setiap aktor diharuskan memiliki mempunyai strategi bersaing.

Dalam perubahan pola persaingan yang sangat semakin cepat. Strategi harus menyesuaikan dengan kondisi yang ada untuk memperoleh peluang-peluang serta menghindari ancaman dari para pesaing. Strategi bersaing ini diperlukan untuk mengembangkan rencana pengembangan mengenai bagaimana persaingan mungkin terjadi, apa yang ingin dicapai, tujuan dan kebijakan apa yang harus dilakukan. *Competitive Strategy* atau Strategi Bersaing sendiri merupakan sebuah konsep yang telah dibicarakan oleh banyak pemikir Hubungan Internasional. Menurut Michael Porter, strategi bersaing adalah pencarian akan suatu posisi dalam sebuah persaingan di dalam suatu arena tempat persaingan terjadi.²¹

²⁰M. Suyanto, *Marketing Strategy*, (Yogyakarta: CV ANDI OFFSET, 2007), hal 106.

²¹ Michael E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance*, (New York: The Free Press, 1985), hal 1.

Strategi bersaing diperlukan untuk menghubungkan aktor kompetisi dengan kondisi lingkungan persaingan yang ada. Kompetisi menjadi inti dari keberhasilan dan kegagalan. Strategi bersaing bertujuan untuk membangun posisi yang menguntungkan dan berkelanjutan²² Terdapat dua hal utama yang mendasari pilihan strategi bersaing yaitu daya tarik industri untuk keuntungan jangka panjang dan faktor-faktor yang menentukan itu.²³ Konsep ini menjadi relevan dengan bagi penulis untuk menganalisa bagaimana China dan Amerika Serikat akan menggunakan *competitive strategy* nya terkait dengan persaingan kekuatan *cyber*. Nantinya konsep ini akan sangat berpengaruh terhadap pemaparan dalam bab 5 karena akan memberikan gambaran terkait *competitive strategy* yang digunakan khususnya China.

Kemampuan berkompetisi sendiri diperoleh melalui karakteristik dan sumber daya untuk memiliki kinerja yang lebih tinggi dibandingkan perusahaan lain pada industri atau pasar yang sama.²⁴ Dalam rivalitas yang terjadi antara Amerika Serikat dan China, kedua negara sebagai pelaku kompetisi saling bersaing untuk menemukan posisi yang lebih unggul dibandingkan pesaingnya. China dalam beberapa dekade terakhir telah menunjukkan perkembangan yang signifikan dalam bidang *cyber* dan diakui dalam kancah internasional. Sementara Amerika Serikat sebagai pemegang hegemoni merasa terganggu dengan peningkatan kemampuan China. Hal ini secara praktis menjadikan keduanya berusaha mencapai posisi yang lebih unggul mempertahankan posisinya dalam persaingan.

²²Ibid.

²³Ibid.

²⁴Binus University, "Competitive Advantage", Last Updated 26 Feb 2019, Diakses 28 Mar 2022. <https://bbs.binus.ac.id/gbm/2019/02/26/competitive-advantage/>

Inti dari persaingan adalah penentuan posisi.²⁵ Menurut Daphne, penting bagi suatu pelaku persaingan untuk melaksanakan suatu hal pada level yang lebih tinggi daripada pesaingnya di industri tersebut.²⁶ Hal ini menjadi bagian untuk mencapai keberhasilan dalam strategi bersaing. Merujuk pada 10 sektor utama dalam program *Made in China* menunjukkan bahwa China menerapkan strategi bersaingnya dengan meningkatkan kemampuan disektor teknologi. China sendiri telah bertransformasi menjadi pesaing kekuatan Amerika Serikat dengan memfokuskan pada pengembangan *cyber*. Pemaparan ini akan tampak dalam analisis di bab 5 khususnya di sektor ekonomi.

Sebagai negara dengan jumlah penduduk terbesar di dunia, China tentu perlu memastikan bahwa mereka memiliki sumber daya yang cukup untuk memenuhi kehidupan dan keamanan rakyatnya. Dari 2010 hingga saat ini, populasi China telah tumbuh menjadi 1,44 miliar (peningkatan 76 juta orang dalam sepuluh tahun) dengan pertumbuhan pengguna internet mencapai 539 juta. Selain itu, dalam iklim bisnis pengguna online di China telah meningkat pesat dan hal ini nyata berbeda dengan iklim bisnis yang ada di Amerika Serikat dimana penggunaan umum kartu kredit atau debit fisik masih menjadi hal yang umum.

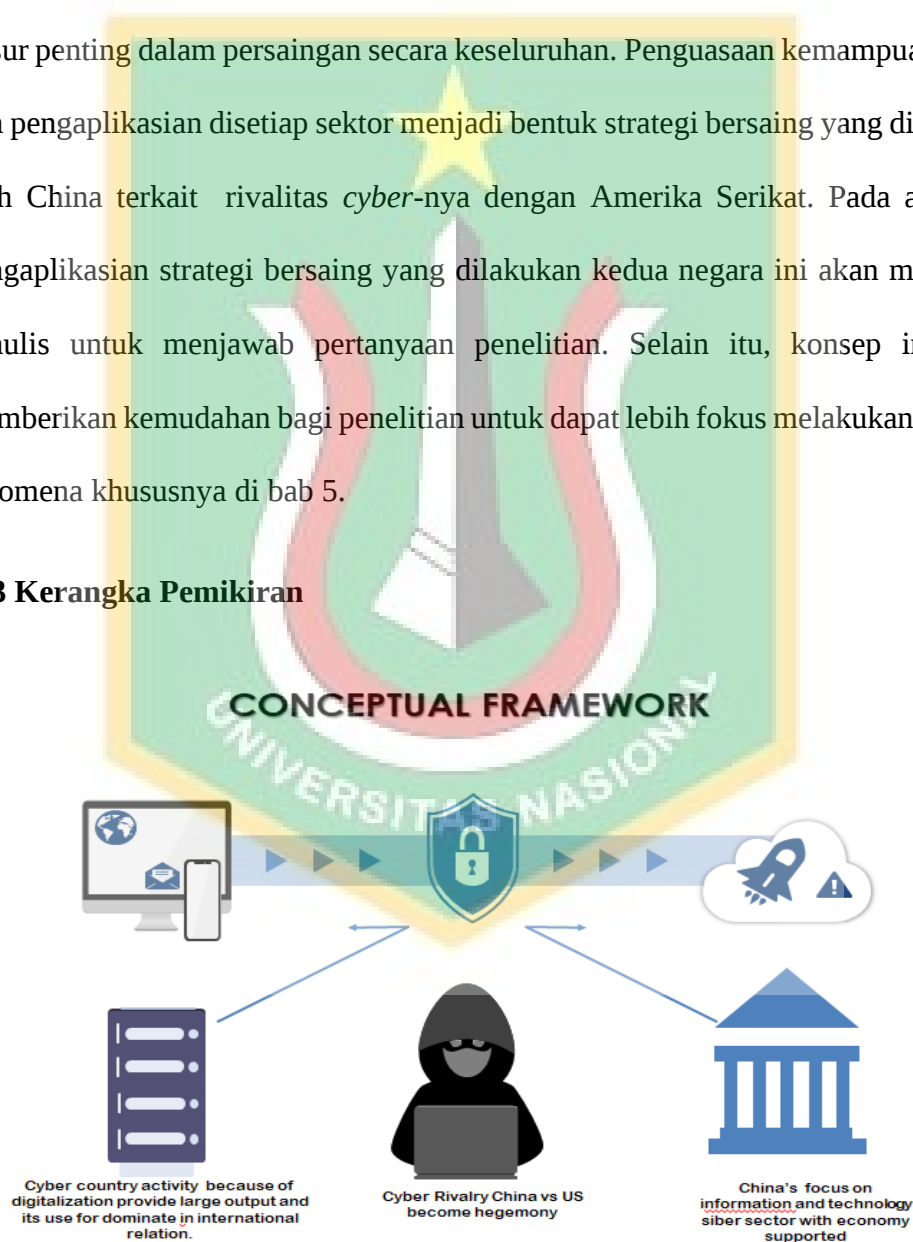
Melalui pengintegrasian kemampuan *cyber* dalam setiap sektor vital perkembangan negara, China harus memastikan keamanan dan kelangsungan hidup rakyatnya sebagaimana tujuan pembangunan mereka dalam *Five Years Plans*

²⁵Michael E. Porter, *The Competitive Advantage of Nations*, (New York: The Free Press, 1990), hal 75.

²⁶Leo Daphne, *MIAW-Management In Absurd Way* (Jakarta: PT Elex Media Komputindo, 2014), hal 67.

of China. Perkembangan teknologi dapat meningkatkan atau menurunkan skala ekonomi, memungkinkan hubungan timbal balik yang sebelumnya tidak ada, menciptakan peluang untuk keuntungan dalam bidang waktu, dan mempengaruhi hampir semua bidang penggerak²⁷. Pengembangan yang dilakukan China merupakan upaya untuk mewujudkan impian mereka. Strategi teknologi menjadi unsur penting dalam persaingan secara keseluruhan. Penguasaan kemampuan *cyber* dan pengaplikasian di setiap sektor menjadi bentuk strategi bersaing yang dilakukan oleh China terkait rivalitas *cyber*-nya dengan Amerika Serikat. Pada akhirnya pengaplikasian strategi bersaing yang dilakukan kedua negara ini akan mengarah penulis untuk menjawab pertanyaan penelitian. Selain itu, konsep ini akan memberikan kemudahan bagi penelitian untuk dapat lebih fokus melakukan analisis fenomena khususnya di bab 5.

2.3 Kerangka Pemikiran



²⁷Loc.Cit., Michael E. Porter.

Cyberpower menjadi isu yang banyak dibicarakan dalam dinamika hubungan internasional. Globalisasi menjadikan penggunaan teknologi menjadi hal yang tidak dapat terpisahkan dalam kehidupan internasional. *Borderless* yang tercipta atas berkembangnya teknologi digital menjadi sebuah ancaman bagi sebuah negara. Hal ini mendorong setiap negara untuk memiliki kesadaran bahwa digitalisasi harus dimanfaatkan. Setiap negara harus mampu melakukan pengembangan terhadap teknologinya.

Besarnya informasi yang dihasilkan dari *cyber activity* memicu kebocoran data dan secara tidak langsung meningkatkan persaingan antar negara hingga upaya saling mendominasi. Bentuk ancaman saat ini dapat dilakukan dengan berbagai sisi dengan memanfaatkan teknologi dan keikutsertaan aktor non negara. Sebagaimana pendapat Michael Sheehan bahwa *battlefields* berubah menjadi *battlespace* dengan melibatkan penggunaan kekuatan udara, data, dan satelit ruang angkasa. *Cyberspace* menjadi ruang virtual yang sangat terbuka, dan ketergantungan penggunaan menjadikan negara bergantung terhadap kemajuan teknologi dalam beragam aktivitasnya. Setiap negara harus mampu mengembangkan *cyberpower* nya.

Cyberpower telah menjadi dimensi baru dalam konteks keamanan kontemporer. China dan Amerika Serikat yang telah sejak lama berada dalam intensitas persaingan yang kuat menyadari dinamika ini. Bangkitnya kekuatan China menjadi sebuah ancaman bagi Amerika Serikat. Presiden Xin Jin Ping, China berambisi kuat untuk menjadi negara pusat *cyberpower* dunia. China melalui kebijakan *Five Years Plans of China* dan program *Made in China* telah

menempatkan fokusnya pada perkembangan *cyber* untuk mendorong perkembangan negara. Dinamika yang saat ini menjadikan negara meletakkan fokus terkait perkembangan *cyber* dalam berbagai sektor karena akan memberikan dampak yang beragam.

Semakin berkembang dan kuatnya kemampuan *cyber* negara akan mempengaruhi kestabilan negara. Bagaimana *cyber* menjadi intentitas penting dalam persaingan antara Amerika Serikat dan China menjadi fokus penulis dalam penelitian ini. Penelitian ini akan menganalisis secara mendalam bagaimana rivalitas kekuatan *cyber* antara Amerika Serikat dan China dalam kurun waktu 2016-2020. Penulis turut meletakkan fokus mendalam terkait pengembangan *cyber* yang dilakukan China dalam berbagai sektor kehidupan sehingga dianggap menjadi ancaman bagi posisi Amerika Serikat dikancah internasional.

Dalam penelitian ini, penulis menggunakan beberapa kerangka teoritis yang dianggap relevan. Pertama teori *Cyberpower* yang digunakan untuk memahami pemanfaatan *cyberpower* sebagai kekuatan utama yang dikembangkan oleh China dan Amerika Serikat. Kedua adalah konsep *Competitive Strategy* yang digunakan untuk mengkaji bagaimana China melakukan pengembangan *cyber* diberbagai sektor dengan bantuan ekonomi sehingga dianggap menjadi ancaman bagi posisi hegemoni Amerika Serikat.

Menurut Bogdan dan Taylor metodologi penelitian kualitatif merupakan prosedur penelitian yang memiliki hasil sebuah data deskriptif yang dituangkan dalam kata-kata yang tertulis dari suatu yang diamati³¹ Melalui pendekatan kualitatif, temuan dan data yang dikumpulkan akan dipadukan. Pengumpulan data yang dilakukan dalam penelitian ini tidak dimaksudkan untuk menguji hipotesis, melainkan untuk mendeskripsikan data yang ditemukan menyesuaikan dengan fokus penelitian yang diteliti. Penelitian mengenai rivalitas *Cyber China* dan Amerika Serikat tahun 2016-2020 menurut penulis relevan dengan menggunakan metode penelitian kualitatif dikarenakan memenuhi karakteristik penelitian kualitatif yaitu mengungkapkan data secara lebih mendalam yang dilakukan melalui data empirik.

3.2 Jenis Penelitian

Jenis penelitian ini adalah penelitian deskriptif. Menurut Sukmadinata, penelitian deskriptif merupakan bentuk penelitian yang ditujukan untuk mendeskripsikan fenomena-fenomena yang ada, baik fenomena alamiah ataupun buatan manusia.³² Fenomena tersebut dapat berbentuk aktivitas, karakteristik, perubahan, hubungan, kesamaan, dan perbedaan. Penelitian deskriptif berusaha untuk mendeskripsikan dan menginterpretasikan sesuatu dengan memperhatikan tentang fakta-fakta, karakteristik fenomena, dan subjek yang diteliti secara tepat.

³¹Lexy J Moleong, *Metodologi Penelitian Kualitatif*, (Bandung: Remaja Rosdakarya, 2000), hal 5.

³²Yanuar Ikbar, *Metodologi & Teori Hubungan Internasional*, (Bandung: PT Refika Aditama, 2014), hal 17-18.

Pendekatan deskriptif kualitatif menjadi desain pilihan yang tepat untuk dapat mendeskripsi langsung fenomena rivalitas *cyber* China dan Amerika Serikat. Hal ini dikarenakan penelitian deskriptif sangat berguna ketika peneliti ingin mengetahui mengenai fenomena yang terjadi, siapa yang terlibat, apa yang terlibat, dan bagaimana fenomena tersebut berlangsung. Selain itu, rivalitas *cyber* antara China dan Amerika Serikat berkaitan erat dengan fakta-fakta empirik yang membangun kondisi tersebut sehingga kecermatan peneliti sebagai instrumen penelitian menjadi kunci untuk mengambil kesimpulan yang tepat.

Peneliti akan berfokus untuk menemukan sifat dari fenomena tersebut, bagaimana rivalitas terbentuk dan bagaimana pengembangan *cyber* yang dilakukan oleh China terkait rivalitasnya dengan Amerika Serikat. Penyajian data deskriptif kualitatif akan dilakukan melalui ringkasan deskriptif langsung dari informasi data yang disusun dan diamati secara logis sehingga menghasilkan kesimpulan. Kesimpulan sendiri merupakan hasil produksi ringkasan deskriptif dari fenomena yang dipilih yang diatur sedemikian rupa sehingga temuan akan disajikan, dengan cara yang paling relevan.³³ Kesimpulan ini nantinya akan menjawab permasalahan dalam penelitian ini.

3.3 Teknik Pengumpulan Data

Dalam penelitian ini, penulis akan menggunakan studi kepustakaan dengan sumber data sekunder (sumber tidak langsung). Sebagaimana yang telah disebutkan sebelumnya bahwa peneliti akan mendeskripsikan fenomena yang terjadi sehingga

³³Vickie A. Lambert, and Clinton E. Lambert, "Qualitative Descriptive Research: An Acceptable Design", *The Pacific Rim International Journal of Nursing Research*, Vol. 16, No. 4, October - December (Nonthaburi: Thailand Nursing and Midwifery Council, 2012), hal 255-256.

penulis akan menggunakan data-data yang bersumber dari buku, literatur, catatan, dan laporan resmi yang berhubungan dengan topik penelitian. Data merupakan bahan keterangan tentang suatu objek yang ditemukan dalam penelitian dengan menekankan pada aspek materi.

Menurut Moh Nazir, studi kepustakaan merupakan sebuah teknik pengumpulan data melalui studi penelaahan terhadap buku, literatur, catatan, dan laporan yang berhubungan dengan masalah yang akan dipecahkan.³⁴ Studi kepustakaan merupakan teknik pengumpulan data yang akan dipergunakan oleh peneliti dalam penelitian ini. Berdasarkan penelaahan terhadap buku-buku dan literatur yang ada hubungannya dengan objek penelitian.

3.4 Teknik Pengolahan dan Analisis Data

Setelah mengumpulkan data penulis akan melakukan pemeriksaan terhadap keabsahan data. Hal ini dilakukan untuk mengelola dan mengklasifikasi data yang diperoleh sehingga nantinya data yang dipergunakan relevan dan valid untuk penelitian ini. Pengecekan keabsahan data akan menggunakan Triangulasi yaitu, teknik pemeriksaan keabsahan suatu data dengan memanfaatkan sesuatu yang lain.³⁵ Penulis akan melakukan pengecekan keabsahan penelitian dengan memanfaatkan sumber, metode, penyidik serta teori lainnya sebagai pembanding. Hal ini dilakukan untuk menghindari bias dan subjektivitas peneliti atas temuan yang dihasilkan.

³⁴Moh. Nazir, *Metode Penelitian* (Bogor: Ghalia, 2005), hal 47.

³⁵Op.Cit., Lexy J. Moelong, hal 4.

Analisis data sendiri merupakan proses vital dalam penelitian. Analisis data merupakan rangkaian kegiatan penelaahan, pengelompokan, sistematimisasi, penafsiran, verifikasi data sebuah fenomena memiliki nilai social, akademis dan ilmiah.³⁶ Analisis data memiliki tujuan untuk menyempitkan dan membatasi penemuan sehingga data dapat tersusun dengan baik. Penulis akan melakukan pengamatan data untuk menarik sebuah kesimpulan yang dapat menjawab permasalahan penelitian.

3.5 Aspek, Dimensi, dan Parameter

ASPEK	DIMENSI	PARAMETER
Kemampuan <i>Cyber Power</i>	<i>Cyber Power</i> China dan Amerika Serikat	• Kepentingan Nasional dalam Rivalitas • Pengembangan <i>Cyber Power</i>
Persaingan <i>Cyber Power</i>	Dominasi dalam Persaingan	• Sektor Ekonomi • Sektor Kontrol Politik dan Perlindungan Jaringan • Sektor Teknologi dan Informasi • Sektor Militer • <i>Cyber Hegemony</i>

Penelitian ini akan berfokus pada 2 aspek yaitu, Kemampuan *Cyber Power* dan Persaingan *Cyber Power*. Dalam aspek kemampuan cyber power, penulis

³⁶Mamik, *Metodologi Kualitatif*, (Sidoarjo: Zifatama Publisher, 2015), hal 133.

menganalisa tentang Cyber Power China dan Amerika Serikat sebagai dimensi penelitian. Sementara untuk parameter, penulis berfokus pada kepentingan nasional dalam rivalitas dan pengembangan cyber power. Kedua parameter ini akan membantu penulis untuk mengetahui secara mendalam mengenai kemampuan cyber power kedua negara. Dalam proses analisa, penulis akan mengaplikasikan teori Cyber Power sebagai kerangka berfikir. Pembahasan pada aspek ini akan dikupas secara mendalam pada pembahasan dalam bab 4.

Sementara untuk aspek kedua yaitu Persaingan Cyber Power, penulis menggunakan dimensi dominansi dalam persaingan. Penulis akan berfokus pada 5 parameter yaitu Cyber Power Sektor Ekonomi, Sektor Kontrol Politik dan Perlindungan Jaringan, Sektor Teknologi dan Informasi, Sektor Militer, dan Cyber Hegemony. Pemaparan terkait aspek kedua akan secara mendalam pada bab 5. Penulis akan mengaplikasikan concept strategi bersaing dalam menganalisa bagaimana strategi dan persaingan cyber yang tercipta antara China dan Amerika Serikat. Seluruh aspek, dimensi, dan parameter ini akan membantu penulis dalam menentukan fokus penelitian dan menjawab penelitian.

BAB IV

CYBERPOWER CHINA DAN AMERIKA SERIKAT

4.1 *Cyberpower* China

China dikenal sebagai negara dengan jumlah penduduk terbesar serta pertumbuhan ekonomi yang tinggi di dunia. Saat ini negara tersebut tengah berusaha meningkatkan kemampuannya dalam memproduksi senjata dan pertahanannya sendiri. Setelah berakhirnya Perang Dingin, wilayah Asia Timur menjadi pusat perhatian internasional.³⁷ Posisi kawasan yang strategis menjadikan kawasan ini menjadi medan persaingan khususnya antara China dan Amerika Serikat untuk mengusahkan kepentingan nasional masing-masing. Meskidemikian lingkungan politik internasional kawasan Asia Timur jauh lebih berkembang dibanding pada masa Perang Dingin. Perkembangan ini dikarenakan berkembangnya hubungan multilateral antara negara-negara kepentingan.³⁸ Walaudemikian, unsur-unsur konflik dan ancaman keamanan masih tetap ada dan terjadi khususnya di wilayah Semenanjung Korea.

Sejak 1991, China telah mengupayakan peningkatan pendanaan dan pengembangan teknologi cyber. Pengembangan dilakukan diberbagai sektor baik sektor pemerintahan, militer dan sipil. Pengembangan ini merupakan upaya holistik China untuk membangun kekuatan politik dan ekonominya. Pengembangan dan peningkatan teknologi cyber sengaja diupayakan untuk meningkatkan kemampuan

³⁷Op.Cit., Lalu Azhar Rafsanjani, Lalu Putrawandi Karjaya, dan Khairur Rizki, "Rivalitas Amerika Serikat (AS) dan China dalam menjaga Security Order di Asia Timur", hal 28.

³⁸Ibid, hal 28.

cyber sebagai sarana asimetris dalam melawan *hegemony* Amerika Serikat. Hal ini tidak terlepas atas kesadaran China bahwa, dunia maya dapat menjadi sebuah domain perang. Selain itu dalam konteks kekuatan militer, *cyberpower* dianggap setingkat dengan kekuatan darat, laut dan udara, yang dapat mengantarkan negara pada kemenangan atau kekalahan.³⁹

Secara perlahan namun pasti, China telah berkembang menjadi salah satu kekuatan dunia maya terkemuka di dunia, dan terus mengembangkan kapasitasnya. China turut melakukan akuisisi teknologi asing terutama dalam sektor pertumbuhan industri, dan hal ini membantu China untuk melompati perkembangan. Transfer teknologi asing memungkinkan China untuk melewati penelitian dan pengembangan yang mahal selama bertahun-tahun dengan berfokus pada keuntungan yang dimiliki perusahaan dan militer asing.

Salah satu bentuk upaya transfer teknologi yang dilakukan China adalah melalui *joint ventures*, yang secara rutin ditekankan oleh China untuk masuknya asing ke pasarnya. Contoh *joint venture* yang dilakukan China adalah dalam proyek pesawat A320 oleh Airbus. *Joint ventures* ini berhasil memberikan China wawasan tentang aeronautika canggih.⁴⁰ Dalam contoh lainnya yaitu, *joint ventures* China dengan Lucent Technologies (Amerika Serikat), dan Alcatel (Prancis) memungkinkan China untuk menciptakan industri serat optik domestik, memungkinkan PLA untuk membuat jaringan Command, Control,

³⁹Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security", *USAWC Strategy Research Project*, March, (Pennsylvania : U.S Army War College, 2011), hal 2.

⁴⁰*Ibid*, hal 24.

Communications, Computers and Intelligence (C4I) canggih, sensor dalam susunan sonar, jaringan area lokal di kapal perang, dan amunisi berpemandu presisi.⁴¹

Cyberpower bagi China tidak hanya menjadi wadah untuk sebuah keterhubungan tetapi turut menjadi kekuatan yang harus dikendalikan dan dikembangkan. Sebagaimana yang diketahui bahwa *cyberspace* merupakan wilayah terbuka maka, diperlukan kontrol menyeluruh dan keterlibatan banyak pihak untuk memastikan pengembangan *cyber* di dalam aktivitas negara menjadi bernilai positif. Dalam hal ini China sangat menyadari bahwa pengembangan dan kontrol atas *cyberpower* menjadi dua hal yang tidak dapat dipisahkan. Pengembangan *cyberpower* dalam berbagai sektor terutama ekonomi akan semakin mendorong peningkatan iklim bisnis China dalam konteks global. Sementara kontrol atas *cyberpower* akan menjaga kestabilan wilayah dan politik China dari berbagai ancaman yang mungkin saja muncul baik dari dalam ataupun luar.

Ralp Langner, salah satu pendiri The Langner Group (sebuah konsultan pertahanan siber internasional) mengatakan bahwa *cyberpower* merupakan sebuah kemampuan terorganisir masyarakat untuk memanfaatkan teknologi digital dalam hal pengawasan, eksploitasi, subversi, dan pemaksaan dalam konflik internasional.

⁴² Sementara Mayor E.Lincoln Bonner dalam tesisnya yang berjudul *Cyberpower: Attack and Defense Lessons from Land, Sea, and Air Power* mengatakan

⁴¹Ibid, hal 24.

⁴²CIRSD.Com, “*Cyberpower - An Emerging Factor in National and International Security.*” Diakses pada 21 May 2022. <https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-interntional-security>

cyberpower menggabungkan kualitas yang melekat pada kekuatan darat, laut, dan udara sehingga menjadi sebuah kekuatan yang bersama.⁴³ Dimana strategi pertahanan data di dunia maya diperlukan untuk menyortir, menghubungkan, dan mengasimilasi besarnya aliran informasi yang ada. Secara tidak langsung hal ini menunjukkan bahwa *cyberpower* merupakan sebuah kekuatan yang kompleks namun sangat potensial.

Secara keseluruhan, strategi China dalam meningkatkan kemampuan *cyberpower*nya melalui beberapa lapisan. China menyadari bahwa untuk menciptakan *cyberpower* yang kuat maka harus ada keterpaduan di setiap lapisan. Keterpaduan ini dikarenakan adanya sebuah keterikatan atas setiap aktivitas yang dilakukan oleh warga negara baik *state* dan *non state* dengan perkembangan teknologi. Setiap aktivitas memiliki aliran informasi dan jaringannya masing-masing. Maka penting bagi China untuk memastikan perkembangan teknologi dapat terus berjalan namun pertahanan atas aliran informasi didalamnya harus turut tetap terjaga. Merujuk pada ketersediaan informasi berada dalam ruang siber atau *cyberspace* maka sudah sewajarnya jika China mengembangkan *cyberpower*nya untuk menjaga aliran informasi yang dimilikinya.

⁴³Mayor E. Lincoln Bonner, "*Cyberpower: Attack & Defense Lessons from Land, Sea, and Air Power*", (Tesis, School of Advanced Air and Space Studies Air University, Alabama, 2011), hal 6. Accessed May, 22, <https://www.hsdl.org/?view&did=812459>

4.2 Perkembangan Internet Masyarakat China

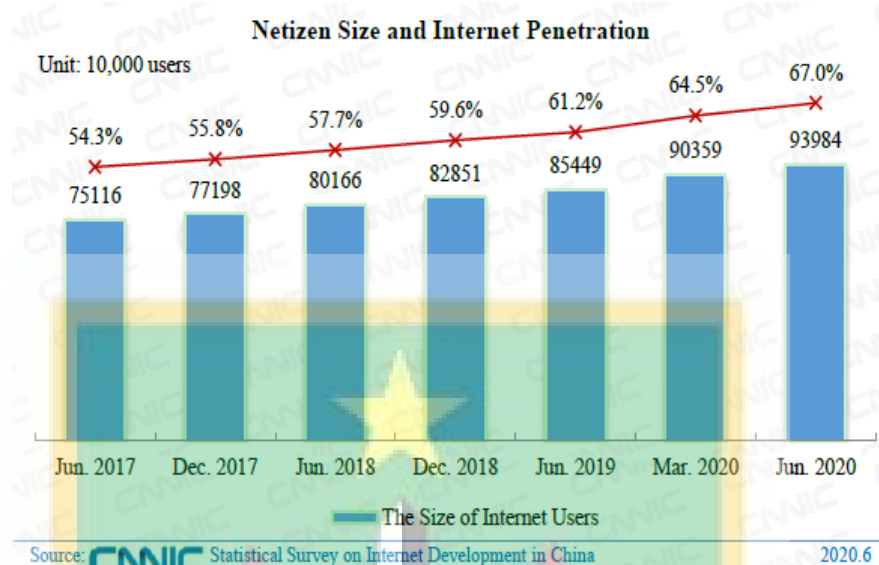
Perkembangan internet dan teknologi di China dapat dikatakan sedikit lebih terlambat dibandingkan dengan Amerika Serikat. Namun, hari ini internet memberikan kontribusi besar untuk semua pertumbuhan dan perkembangannya. Internet di China telah meningkat secara signifikan dalam 10 tahun terakhir, dari hanya 10% dari populasi yang memiliki akses ke Internet kini angka tersebut telah melebihi 50% – lebih dari 700 juta netizen.

Berdasarkan data CNNIC atau *China Internet Network Information Center* total pengguna internet di China pada bulan Juni 2020 meningkat 67% dibandingkan tahun 2017 dengan total pengguna internet mencapai 939,84 miliar.⁴⁴ Sementara itu, lalu lintas saluran internet pada kuartal pertama 2020 mencapai 745 miliar GB, terdapat kenaikan sebesar 78,9 miliar GB dibandingkan kuartal ke 2 tahun 2019 yang hanya mencapai 666 miliar GB.⁴⁵ Secara total sejak Juni 2017 hingga Juni 2020 lalu lintas internet China telah mengalami kenaikan sebesar 656,1 miliar GB. Angka ini tentu bukan angka yang sedikit, namun realitas pertumbuhan internet di China menunjukkan semakin besar dan pentingnya internet bagi masyarakat. Secara detail tingkat pertumbuhan internet dapat dilihat dalam gambar 1 dan 2 dibawah ini.

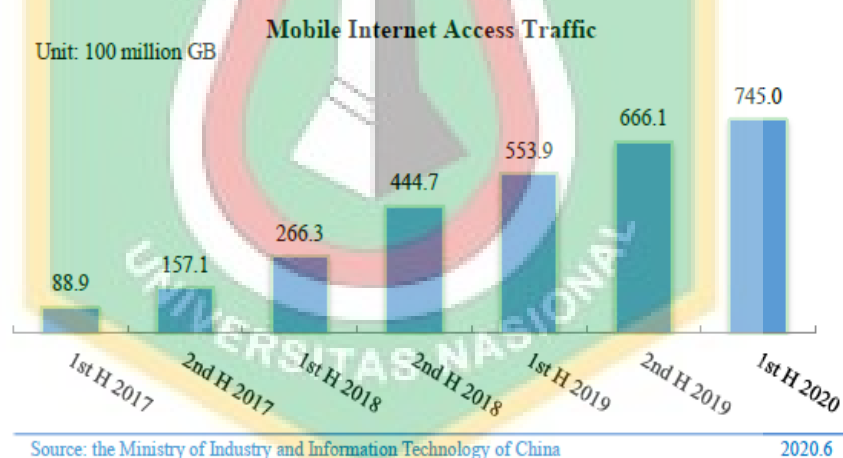
⁴⁴Loc.Cit., CNNIC, Statistical Report on Internet Development in China, 2020, hal 13.

⁴⁵Ibid, CNNIC, Statistical Report on Internet Development in China, 2020, hal 6.

Gambar 4.2.1 Pengguna Internet dan Penetrasi Internet



Gambar 4.2.2 Lalu Lintas Saluran Internet



Sumber : China Internet Network Information Center

Ketika membicarakan pertumbuhan internet maka kita tidak dapat memisahkan diri atas kemajuan teknologi. Kemajuan internet akan beriringan dengan perkembangan teknologi. Namun realitas yang berkembang saat ini, kemajuan

teknologi dalam tingkat global sangat berorientasi pada teknologi buatan barat. Dalam hal ini China cenderung skeptis atas perkembangan teknologi yang telah ada sebelumnya.

China melihat ketergantungan pada teknologi buatan barat merupakan sebuah kelemahan karena dapat dimanfaatkan oleh pihak lawan. Oleh karena itu, China berusaha untuk menciptakan kemandirian teknologinya sendiri. Sejak Kongres Nasional BPK ke 18 dibawah kepemimpinan XI Jinping, China berusaha membangun infrastruktur baru seperti jaringan 5G dan internet industri.⁴⁶ Selain itu *access broadband* perkotaan dan pedesaan terus ditingkatkan dan aplikasi internet terus dikembangkan.

Perkembangan yang dilakukan oleh China ini merupakan implementasi untuk mewujudkan komitmen China yang menginginkan sirkulasi internet domestik sebagai andalan. Meningkatnya sirkulasi internet hanya dapat terjadi apabila infrastruktur jaringan yang menjadi lebih canggih, pengguna internet yang besar, dan kaya akan aplikasi yang komprehensif.⁴⁷ China yakin bahwa jika kestabilan internet dan pertumbuhan infrastruktur yang baik dapat tercipta maka, China akan mampu menyelesaikan pembangunan masyarakat dan memastikan keberhasilan Rencana Lima Tahun ke-13.

⁴⁶CNNIC, Statistical Report on Internet Development in China, (Beijing: CNNIC, 2020), hal 14

⁴⁷Ibid.

4.3 Mimpi Besar China menjadi *Cyberpower Hegemony*

Perkembangan teknologi dan internet di China tidak terlepas dari tekad negara tersebut untuk menjadi pemimpin dalam teknologi informasi dan komunikasi secara lebih luas. Hal ini diadopsi melalui 15 tahun strategi pembangunan (2006–2020) dengan memprioritaskan 'informatisasi' layanan publik dan ekonomi, serta memastikan keamanan nasional melalui sarana dunia maya.⁴⁸ Dibawah pemerintahan presiden ke 5 China, Xi Jinping, tepatnya sejak akhir 2012, China berkeinginan kuat untuk dapat membangkitkan kejayaan China. Zhōngguó mèng (Impian China) menjadi slogan yang digunakan Presiden Xi.

Secara garis besar, perwujudan Impian China menurut Xi Jinping terdapat dalam kata kunci: kebangkitan besar bangsa Tionghoa. Xi Jinping turut menyatakan bahwa mewujudkan kebangkitan besar bangsa Tionghoa merupakan impian terbesar bangsa Tionghoa pada abad ini. Jika dilihat dari kacamata politik, slogan yang disampaikan oleh Presiden Xi Jinping merupakan upayanya untuk menarik perhatian rakyat dan membangkitkan semangat masyarakat China. Selain itu, slogan tersebut menunjukkan kearah mana kebijakan-kebijakan politik yang akan dibuat oleh pemerintah.

China turut ingin menjadi *counter-hegemony* dikawasan Asia Timur. Keinginan ini didasari pada pengalaman pahit dimana China mengalami kekalahan dari AS pada Krisis Taiwan 1995-1996 dimana saat itu Amerika Serikat melakukan

⁴⁸Tobias Feakin, *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities*, Special Report, June, Issue 50, (Canberra: ASPI, 2013), hal 2.

gunboat diplomacy dengan mengirim US 7th Fleet-nya ke Taiwan.⁴⁹ Pada pemerintahan Deng Xiao Ping, China mulai mengalami perkembangan pesat di bidang ekonomi sebagai akibat dari implementasi kebijakan *open door*. Kebijakan tersebut membuat China menjadi lebih terbuka terhadap investasi asing yang kemudian mempengaruhi modernisasi industri di China sehingga China dapat tumbuh menjadi negara industri yang mandiri.⁵⁰ Perkembangan ini yang kemudian terus dikembangkan oleh pemerintahan Presiden Xi Jinping.

Sementara itu untuk mengatasi rentannya keamanan kawasan Asia Timur dimana aliansi dibentuk Amerika Serikat semakin kuat turut meningkatkan keinginan China untuk menjaga kawasan-kawasan sengketa sebagai wilayahnya, seperti Taiwan, Laut China Timur, dan Laut China Selatan. China memulai modernisasi militernya dengan serius setelah krisis Selat Taiwan tahun 1995-1996, karena insiden tersebut secara tidak langsung memperlihatkan kelemahan China untuk mencegah intervensi asing dalam perselisihan kedaulatan China.⁵¹ Sehingga modernisasi militer dapat menjadi cara untuk menegaskan kembali posisinya terhadap Taiwan agar pihak asing sulit mengintervensi masalah internalnya. Selain itu, peningkatan kekuatan pertahanan menjadi penting bagi China untuk mempersiapkan diri menghadapi potensi-potensi ancaman baik dari internal maupun eksternal.

Pemikiran modernisasi inilah yang pada akhirnya dikembangkan oleh Presiden Xi Jinping dengan memanfaatkan konsep dan jaringan *cyber* bagi

⁴⁹Op.Cit., Lalu Azhar Rafsanjani, Lalu Putrawandi Karjaya, Khairur Rizki, “Rivalitas Amerika Serikat (AS) dan China dalam menjaga *Security Order* di Asia Timur”, hal 33.

⁵⁰Ibid. hal 34.

⁵¹Ibid.

perthanan negara. Pada bab selanjutnya akan dibahas bagaimana perkembangan militer China menggunakan *cyberpower* untuk menciptakan *cyber defense* negara. Kesadaran bahwa dinamika politik dan munculnya berbagai permasalahan di dalam negeri China, terutama permasalahan kesenjangan sosial dan kemiskinan yang tak kunjung usai menjadi pendorong mengapa China memaksimalkan pertumbuhan dan pertahanan negara melalui perkembangan *cyber*. Besarnya harapan kebangkitan dan kesejahteraan melalui slogan yang ingin dihidupkan Xi Jinping telah menjadi harapan bagi seluruh rakyat China.

Presiden Xi Jinping memberikan penekanan bahwa Impian China adalah mimpi seluruh rakyat Tionghoa, hal ini menjadikannya lebih mudah untuk mengasosiasikan mimpi masing-masing rakyat dengan mimpi negara. Sejarah mencatat bahwa China pernah menjadi sebuah bangsa yang besar sejak masa dinasti hingga abad ke-18. Baru pada saat imperialisme Barat mulai masuk melalui Perang Candu pada tahun 1840 dan memaksa China untuk membuka pintu perdagangannya, kekuasaan China perlahan mulai mundur.

Setelah Perang Candu, China mulai memasuki abad yang disebut dengan “abad penghinaan”. Wilayah yang semula berada di bawah kedaulatan China menjadi terpecah-pecah dan terjajah. Di tengah desakan dan ancaman imperialisme Barat itulah rakyat China kemudian mulai bangkit dan melakukan perlawanan. Pembentukan Partai Komunis China dan berdirinya Republik Rakyat China di bawah pimpinan Mao Zedong dianggap sebagai titik terbukanya jalan China untuk

kembali mendapatkan apa yang menjadi haknya. Wilayah-wilayah yang semula diduduki oleh pemerintah kolonial berhasil dimiliki kembali.⁵²

Semangat kebangkitan bangsa selalu mewarnai pemerintahan China dari masa ke masa. Hampir semua presiden China akan menggunakan landasan kebangkitan nasional China pada masa pemerintahannya, hanya saja konteks yang digunakan berbeda-beda. Hanya pada masa Mao Zedong saja yang tidak menggunakan konsep kebangkitan bangsa Tionghoa didalam pemerintahannya.

Gagasan mengenai kebangkitan nasional bangsa Tionghoa sendiri pertama kali digagas oleh Sun Yatsen sebelum terbentuknya Republik Rakyat China, Sementara di era modern saat ini konsep kebangkitan nasional bangsa Tionghoa baru digunakan kembali pada awal tahun 1980an. Seruan mengenai kebangkitan nasional tersebut menempatkan PKT sebagai pemegang tugas utama dalam mengembalikan posisi kejayaan China.⁵³

Masa lalu yang gelap dan menyakitkan menjadi pelajaran penting bagi China untuk terus berkembang menjadi negara yang dihormati. Saat runtuhnya Uni Soviet dan munculnya Amerika Serikat sebagai negara adidaya nyatanya semakin memberikan pengaruh bagi para pemikir strategis China untuk mewujudkan mimpi besar tersebut.⁵⁴ Elit kebijakan China, seperti mantan wakil presiden CCP Sekolah Partai Pusat Zheng Bijian melihat konfigurasi kekuatan global kontemporer ditandai dengan “satu negara adidaya” (Amerika Serikat) dan “banyak kekuatan besar”

⁵²Op.Cit., Hayati Nufus, “Impian Tiongkok: Nasionalisme Tiongkok Melintas Batas dalam Pembangunan Tiongkok”, hal 46.

⁵³Ibid, hal 47.

⁵⁴Shalendra D.Sharma, *China and India in The Age of Globalization*, (New York: Cambridge University, 2009), hal 213.

(Perancis, Inggris, Jepang, China, dan Rusia). Namun disisi lain, China memiliki tugas utama untuk melindungi kepentingan nasionalnya tetapi dibayangi oleh hegemoni Amerika Serikat yang dinilai berusaha menahan kebangkitan China.⁵⁵

Impian kebangkitan China yang digagas oleh Xi Jinping secara jelas mengandung nilai sejarah yang tinggi. Semangat kebangkitan sudah dimiliki oleh bangsa Tionghoa bahkan sejak mereka dihadapkan pada Perang Candu ataupun perang melawan Jepang. Harapan akan China yang lebih baik, kebahagiaan hidup generasi-generasi selanjutnya telah membentuk kekuatan dan semangat dalam diri masing-masing rakyat China untuk mengusahakan kebangkitan tersebut. Oleh karena itu, gagasan tentang Impian China ini merupakan mimpi yang penuh dengan harapan.

Impian tersebut nyata terus tumbuh dan berkembang seiring dengan dinamika dan perkembangan zaman. Perkembangan teknologi dan kemampuan yang tengah dilakukan oleh Presiden Xi Jinping nyatanya tidak melepaskan impian besar China sebagai kekuatan pendorong. Kesadaran akan perang jenis baru dimasa mendatang menjadikan China terus melakukan pengembangan dalam sektor teknologi dan informasi. Dalam laporan akhir tahun 2020, *World Intellectual Property Organization* (WIPO), diketahui bahwa China mengajukan sekitar 68.720 paten dan kekayaan intelektual. Hasil ini lebih banyak dari paten yang diajukan oleh Amerika Serikat pada tahun yang sama.⁵⁶ China berusaha menciptakan kebangkitan

⁵⁵Ibid.

⁵⁶Muhammad Rizki Akbar, "Standard China 2035" dan Mimpi Tiongkok untuk Standardisasi Teknologi Dunia." Last update 15 Feb 2022. Diakses 28 May 2022.
<https://politik.brin.go.id/kolom/politik-internasional/standard-china-2035-dan-mimpi-tiongkok-untuk-standardisasi-teknologi-dunia>

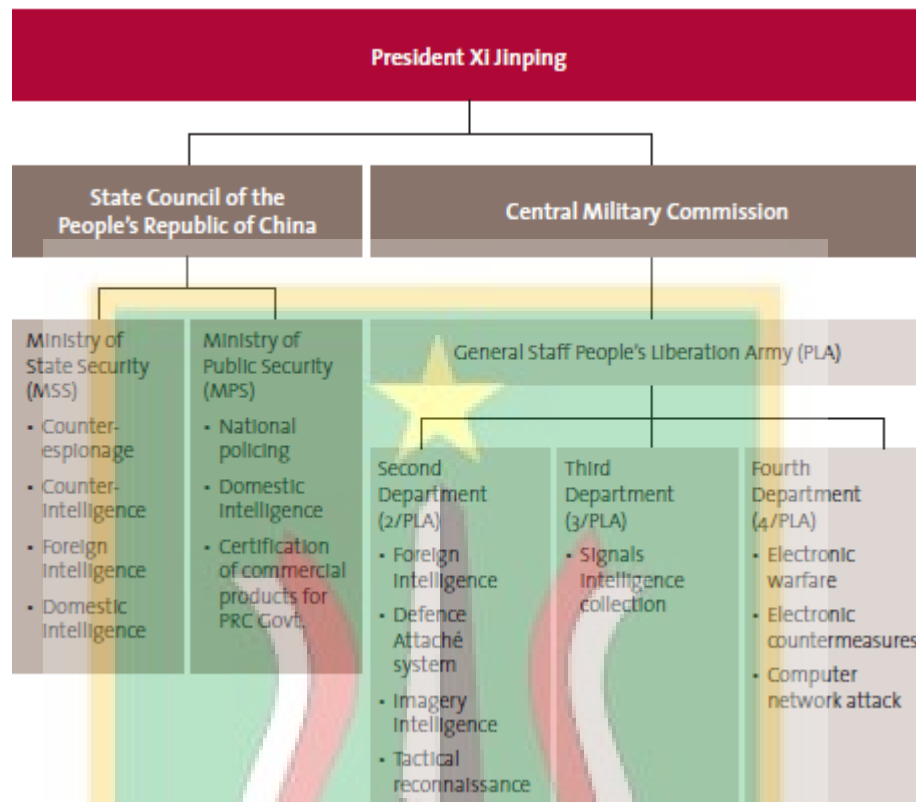
impian tersebut melalui berbagai penyesuaian dinamika yang terjadi saat ini dan salah satunya adalah kekuatan *cyber*.

4.3.1 *Cyberpower sebagai Cyber Defense*

Cyberpower merupakan kemampuan bangsa-bangsa membangun kontrol serta memberikan pengaruh melalui ruang siber dan menjadi sebuah kekuatan nasional lain bagi negara. Kemampuan *Cyberpower* bertumpu kepada kemampuan negara dalam mengembangkan sumber daya yang dimilikinya dalam dunia *cyber* sebagai pertahanan dan kekuatan nasional. Tujuan dari pengembangan ini untuk mendorong negara mencapai tujuan dan sasaran nasionalnya.

Globalisasi berhasil mendorong perkembangan teknologi dan menjadikan negara membutuhkan jaringan komputer, infrastruktur telekomunikasi, program dan perangkat lunak, dan orang-orang dengan keterampilan yang diperlukan. Seperti halnya kekuatan darat, laut, udara, negara dapat menghasilkan efek di dalam dunia maya melalui kekuatan ruang angkasa. Serangan dunia maya cenderung memiliki kemampuan penyebaran secara cepat sehingga ketika negara menggunakan *cyberpower* nya kepada musuh bukan hanya dapat merusak basis data musuh, tetapi dapat menjatuhkan jaringan pertahanan baik udara, laut, darat, dan mengganggu sinyal satelit. Hal ini menjadikan banyak negara mengembangkan *cyberpower* sebagai basis pertahanan termasuk China. China sendiri diketahui memiliki unit PLA khusus yang bertugas terkait kekuatan pertahanan *cyber* negara.

Gambar 4.3.1 China Military Organization



Sumber : ASPI Scpecial Report

Sebuah negara pasti akan membentuk tentara untuk mempertahankan wilayah dan kestabilan negara baik termasuk didalamnya kekuatan luar angkasa untuk bertahan melawan serangan sejenis, dan melakukan pengamatan dalam hal ini China memiliki 2 Badan Utama yaitu *State Council* dan *Central Millitary Commision*. *State Council* terdiri atas 2 Badan Sipil yaitu, Pertama, *Ministry of State Security (MSS)* atau Kementerian Keamanan Publik yang bertanggung jawab atas serangan spionase, serangan intelijen, intelijen asing, dan intelijen domestik. Kemampuan siber MSS relatif tidak diketahui, tetapi diperkirakan telah mengembangkan upaya untuk meningkatkan pengumpulan data politik dan

ekonomi tentang pemerintah asing, organisasi non-pemerintah, dan mereka yang menentang pemerintahan. Kedua, *Ministry of Public Security (MPS)* atau Kementerian Keamanan Publik yang bertanggung jawab atas kepolisian nasional dan, pada tingkat yang lebih rendah, intelijen domestik. MPS juga secara aktif mendukung penelitian keamanan informasi, sertifikasi produk komersial untuk digunakan oleh Pemerintah China, kontrol perusahaan keamanan informasi komersial dan pendanaan akademik.⁵⁷

Sementara itu, Intelijen militer adalah tugas PLA. Departemen Kedua dari Departemen Staf Umum PLA (2PLA) bertanggung jawab atas pengumpulan intelijen asing, sistem Atase Pertahanan, intelijen citra dan pengintaian taktis. Departemen Ketiga (3PLA) adalah agen pengumpulan dan analisis sinyal utama (SIGINT). 3PLA mengawasi salah satu infrastruktur SIGINT dan pengumpulan siber terbesar dan tercanggih di dunia, dan tentu saja operasi asli terbesar di kawasan Asia-Pasifik dan mengelola sekitar 12 biro operasional dan tiga lembaga penelitian dan memulihkan volume data yang sangat besar. Departemen Keempat (4PLA) bertanggung jawab atas peperangan elektronik, penanggulangan, dan serangan jaringan komputer. Perbedaan utama antara 4PLA dan 3PLA adalah misi ofensif 4PLA.⁵⁸

⁵⁷Op.Cit., Tobias Feakin, *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities*, hal 3.

⁵⁸Ibid.

Kerangka strategis pertahanan China mencakup empat ketentuan utama yang diarahkan untuk mengembangkan sistem militer dan pertahanannya. **Pertama**, China melakukan modernisasi pertahanan negara dan angkatan bersenjata melalui informasi. Hal ini termasuk melakukan pengembangan atas jaringan militer dan kemampuan dunia maya. **Kedua**, koordinasi pembelanjaan pertahanan nasional dan pembangunan ekonomi dengan penekanan pada penyediaan sumber daya yang cukup untuk militer dan industri serta teknologi penggunaan ganda. **Ketiga**, reformasi pertahanan negara dan angkatan bersenjata, termasuk ilmu pengetahuan dan teknologi, pengadaan, penelitian dan pengembangan, dan manufaktur, sekali lagi menekankan pertahanan terpadu dan industri tujuan ganda sipil. Reformasi juga mencakup sistem mobilisasi pertahanan negara yang lebih baik. **Keempat**, lompatan jauh pengembangan ilmu dan teknologi militer; yaitu, melewati jalur perkembangan bertahap yang diambil Amerika Serikat untuk membangun kekuatan jaringan dan dimaksudkan untuk menyamai kemampuan Amerika Serikat.⁵⁹

Pemikiran modernisasi dan reformasi industri pertahanan yang dilakukan China sendiri dimulai pada tahun 1991, tepatnya ketika Amerika Serikat memenangkan Perang Teluk. China terkesan dengan bagaimana keunggulan teknologi tinggi dalam militer menjadi nilai keuntungan tersedia bagi sebuah negara.⁶⁰ Bagi China, Amerika Serikat menunjukkan jenis peperangan baru. Perang dimana komputer dan teknologi canggih menciptakan kecerdasan waktu nyata dan

⁵⁹Op.Cit., Colonel Jayson M. Spade, *China's Cyberpower and America's National Security*, hal 17.

⁶⁰Ibid.

menjadi senjata rahasia dalam peperangan. Militer China menyebut Perang Teluk sebagai 'transformasi besar', dan selama sisa tahun 1990-an terjadi banyak kontemplasi, refleksi dan diskusi di kalangan strategis tentang bagaimana China dapat beradaptasi dengan ruang pertempuran baru ini.⁶¹

China akhirnya memutuskan bahwa penting bagi sebuah negara untuk memiliki kekuatan teknologi tinggi dibandingkan lawannya. Dalam buku yang berjudul *Unrestricted Warfare* (1999) yang ditulis oleh dua kolonel senior PLA China, Qiao Liang dan Wang Xiangsui, mungkin bagi aktor negara dan non-negara untuk melawan superior teknologi secara asimetris. *Unrestricted Warfare* menjadi sebuah buku yang meletakkan dasar-dasar pemikiran China terkait dunia maya. Bagaimana negara dapat mengambil keuntungan dari kelemahan yang diciptakan oleh kemampuan konvensional superior musuh, dan dunia maya menjadi sarana terbaik untuk memperoleh hal ini.⁶²

Pemikiran tersebut telah menunjukkan bahwa China menyadari perang masa depan menggunakan serangan asimetris terhadap semua elemen kekuatan nasional, yaitu ekonomi, politik, informasi, dan militer. Semua elemen ini dapat digunakan sebagai sarana untuk menghalangi, mengintimidasi, atau mengalahkan musuh yang secara militer lebih unggul. Alih-alih mencoba menandingi kekuatan militer

⁶¹Loc.Cit., Tobias Feakin, *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities* hal 2.

⁶²Ibid.

Amerika Serikat, China dapat menargetkan kelemahan Amerika Serikat, khususnya ketergantungannya pada teknologi informasi dan satelit.⁶³

China secara bertahap menciptakan kekuatan pertahanan yang modern dan terinformasi. Kekuatan dimana mereka mampu melakukan operasi bersama dengan berpusat pada sebuah jaringan dan bertempur melalui dunia maya. Reformasi militer yang dilakukan China dilakukan melalui revisi doktrin, pendidikan dan pelatihan untuk mendukung kekuatan berjaringan dan berteknologi tinggi bagi kesatuan PLA. Tujuannya reformasi ini tak lain adalah untuk mengubah konsep tentara massal menjadi militer yang lebih kecil, namun lebih mampu memenangkan perang melalui kekuatan berteknologi tinggi yang menekankan pada jaringan komunikasi sebagai pertahanan negara.

Modernisasi alutsista militer mencakup teknologi-teknologi canggih seperti kemampuan C4ISR (command, control, communications, computer, intelligence, surveillance, dan reconnaissance). Modernisasi militer ini dianggap penting untuk meningkatkan kemampuan personel militer PLA, karena bagi China kualitas personel adalah lebih penting daripada kuantitas. Dalam dua dekade lebih, China telah berhasil mengubah imej PLA menjadi pasukan dengan kekuatan militer yang profesional dan kompeten serta mampu menjadi salah satu yang terkuat di dunia

⁶³Op.Cit., Colonel Jayson M. Spade, "China's Cyberpower and America's National Security", hal 18.

yang mana sebelumnya PLA dikenal sebagai *junkyard army* atau militer dengan alutsista yang tidak mumpuni.⁶⁴

Bagi China, kedaulatan dunia maya adalah bagian dari bidang keamanan informasi yang sangat penting karena menyangkut kebutuhannya untuk mengontrol kestabilan tentang negara, dan masyarakat. China berfokus pada kontrol dan manajemen atas Internet dan isinya. Dengan cara ini, kedaulatan siber mendorong keamanan siber sebagai sarana untuk menjaga keamanan siber di China. Didukung dengan kondisi perekonomian yang kuat, China mendukung proses *military build-up* dan *arms build-up* dalam militernya, serta modernisasi dan peningkatan kapabilitas militer penting untuk menjamin keamanan internal dan eksternal bagi kelangsungan aktifitas ekonominya.⁶⁵

Tentara PLA diarahkan untuk memiliki berkekuatan yang lebih modern untuk mendukung kepentingan nasionalnya baik secara domestik maupun internasional, dan juga untuk menghalau dan melawan ancaman-ancaman militer lainnya yang datang dari luar. Melalui kekuatan militer China tidak hanya dapat mengontrol kekuasaan atas wilayahnya sendiri tapi sekaligus untuk meningkatkan kekuatan pertahanan untuk menghadapi adanya potensi ancaman dari luar.

⁶⁴Op.Cit., Lalu Azhar Rafsanjani, “Rivalitas Amerika Serikat (AS) dan China dalam menjaga Security Order di Asia Timur”, hal 35.

⁶⁵Ibid.

4.3.2 Kebijakan Presiden Xi Jinping

Pada 2015, Perdana Menteri Li Keqiang meluncurkan “Made in China” atau MIC 2025 sebuah inisiatif yang bertujuan untuk memodernisasi kemampuan industri China. Strategi 10 tahun yang komprehensif ini sangat berfokus pada manufaktur cerdas di 10 sektor strategis dan bertujuan mengamankan posisi China sebagai pembangkit tenaga listrik global dalam industri teknologi tinggi seperti robotika, penerbangan, dan kendaraan energi baru seperti listrik dan biogas.⁶⁶ Rencana tersebut melibatkan penggantian ketergantungan China pada impor teknologi asing dengan inovasinya sendiri dan menciptakan perusahaan China yang dapat bersaing baik di dalam negeri maupun global.

MIC 2025 dipandang sebagai inisiatif untuk mengamankan posisi China sebagai pembangkit tenaga listrik global dalam industri teknologi tinggi. Tujuannya adalah untuk mengurangi ketergantungan China pada impor teknologi asing dan berinvestasi besar-besaran dalam inovasinya sendiri untuk menciptakan perusahaan China yang dapat bersaing baik di dalam negeri maupun global dengan memastikan bahwa inovasi, kualitas produk, efisiensi, dan integrasi mendorong manufaktur di 10 industri utama. Industri-industri tersebut antara lain teknologi informasi canggih; peralatan mesin otomatis dan robotika; peralatan kedirgantaraan dan aeronautika; peralatan teknik kelautan dan pelayaran berteknologi tinggi; peralatan transportasi kereta api modern; kendaraan hemat energi dan energi baru; peralatan listrik; bahan baru; obat dan alat kesehatan; dan peralatan pertanian. MIC 2025 bagi

⁶⁶Institute for Security & Development Policy, “Made in China 2025”, June (Stockholm: ISDP, 2018), hal 2.

China merupakan kesempatan untuk berintegrasi penuh ke dalam rantai manufaktur global dan bekerja sama secara lebih efektif dengan ekonomi industri.

Sejak beberapa tahun terakhir China secara besar-besaran mempercepat perkembangan teknologi serta industri domestik yang menghasilkan produk-produk seperti 5G, Artificial Intelligence (AI), panel surya dan mobil listrik. Upaya yang dilakukan China menunjukkan isyarat bahwa China telah mengambil langkah serius dalam pengembangan teknologi. Inisiatif Made in China 2025 menjadi langkah Presiden Xi Jinping untuk mengubah citra China sebagai pabrik dunia yang memproduksi barang-barang murah menjadi *technological powerhouse* yang mampu berperan sebagai pemimpin dalam kemajuan teknologi dunia.⁶⁷ Citra baru ini akan mendorong pertumbuhan ekonomi China.

Sementara itu, dalam cetak biru 13th Five Year Plan (FYP) tahun 2016-2020, Presiden Xi Jinping berfokus pada peningkatan pembangunan ekonomi selama periode pertumbuhan ekonomi yang melambat. Target dan prioritas pemerintah dalam FYP ke 13 ini adalah membentuk model bisnis untuk perusahaan asing di China. Target dan inisiatif pertumbuhan ekonomi yang luas dalam rencana tersebut berdampak pada lingkungan bisnis secara keseluruhan, sementara rencana lokal dan industri dapat mendorong arah dukungan pemerintah dan pertumbuhan di masa depan. FYP 13 ini menerapkan strategi pengembangan berbasis inovasi. Made in China 2025 dan Internet Plus menjadi bentuk implementasi kebijakan nasional pemerintah China untuk mewujudkan impian

⁶⁷Loc.Cit., Muhammad Rizki Akbar, <https://politik.brin.go.id/kolom/politik-internasional/standard-china-2035-dan-mimpi-tiongkok-untuk-standardisasi-teknologi-dunia/>.

China. Pemerintah China turut menyerukan promosi pendekatan manajemen daftar negatif baru untuk mengatur investasi asing di pasar China sebagai upaya Manajemen Penanaman Modal Asing dinegaranya.⁶⁸

Dalam cetak biru FYP ke 13 tersebut tampak China berusaha mengejar pengembangan dengan didorong oleh inovasi, memastikan bahwa bisnis rintisan dan inovasi. Dengan memastikan pengetahuan dan teknologi akan menjadi lebih tertanam dalam ekonomi, sehingga inovasi akan dialokasikan untuk efek yang lebih besar, terobosan besar akan dibuat dalam teknologi inti di sektor-sektor utama, dan kapasitas inovasi China akan melihat peningkatan menyeluruh. Pemenuhan tujuan ini akan membantu China menjadi negara yang kaya akan inovasi.⁶⁹ China mengintegrasikan inovasi dalam sains dan teknologi mengambil peran utama dalam perkembangannya.⁷⁰ Perkembangan China dibawah Pemerintahan Presiden Xi Jinping tampak dalam laporan 13th Five Year Plan sebagai berikut :



⁶⁸USCBC, “Official 13th Five-Year Plan Outline Released.” Diakses 4 May 2022. <https://www.uschina.org/policy/official-13th-five-year-plan-outline-released>

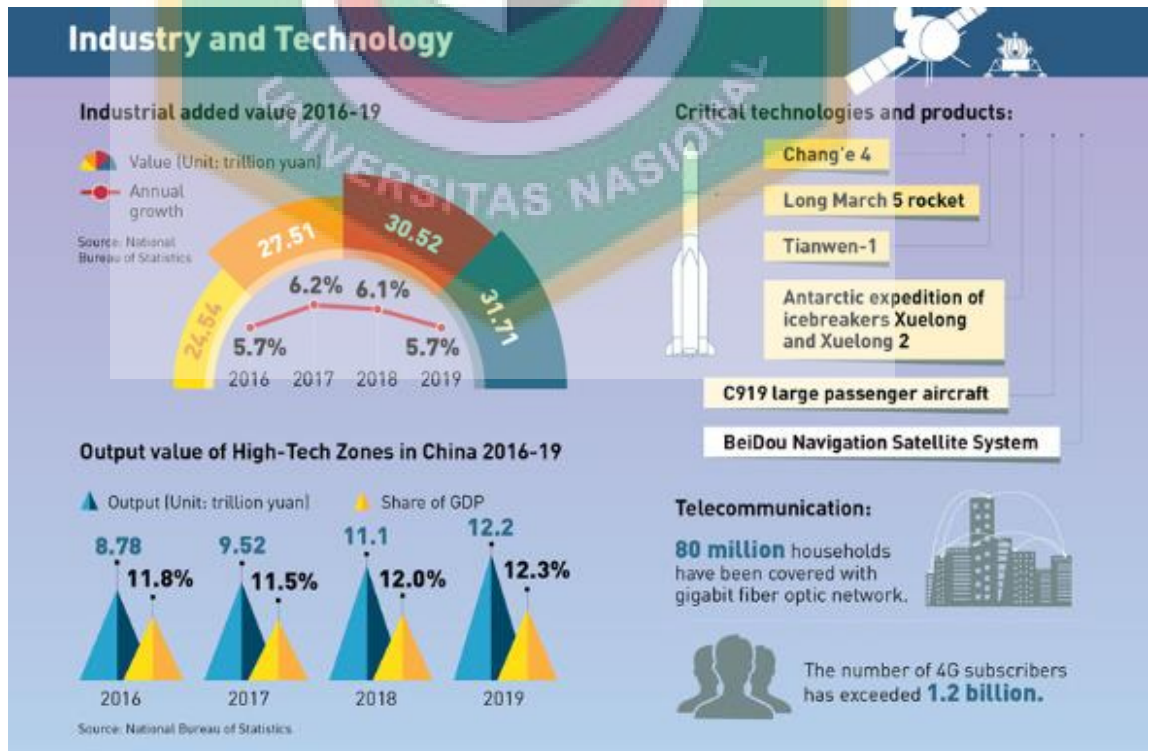
⁶⁹13th Five Year Report, Chapter 3, Major Objectives

⁷⁰13th Five Year Report, Chapter 6 - Ensure Innovation in Science and Technology Takes a Leading Role

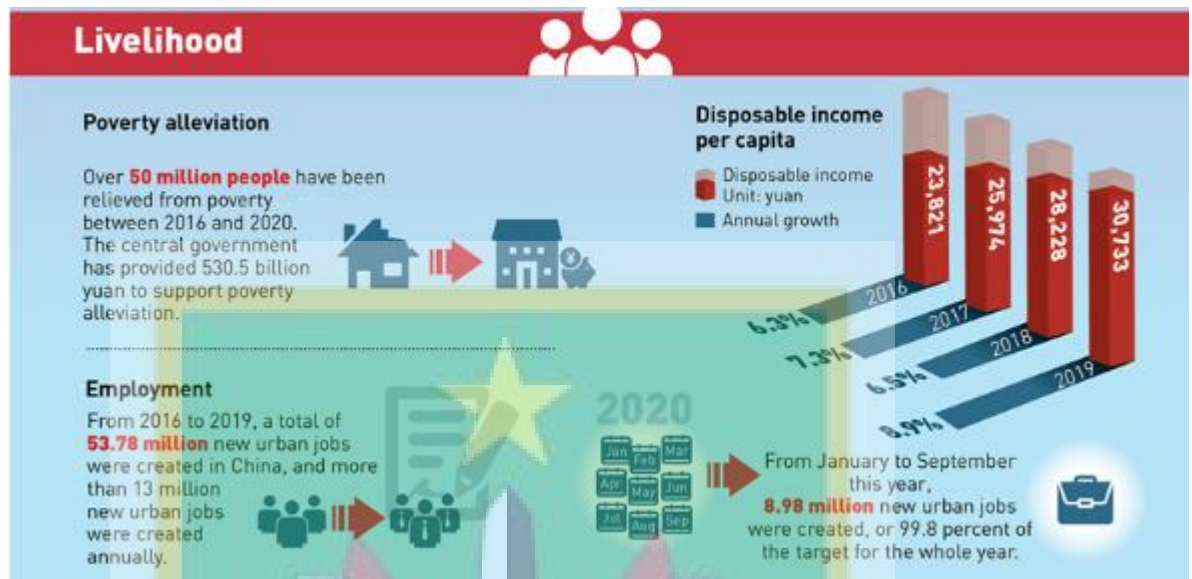
Gambar 4.3.2.1 Laporan Pertumbuhan Ekonomi dari Rencana Lima Tahun ke-13 China tahun 2016-2020



Gambar 4.3.2.2 Laporan Pertumbuhan Industri dan Teknologi dari Rencana Lima Tahun ke-13 China Tahun 2016-2020



Gambar 4.3.4.3 Pertumbuhan di China tahun 2016-2020



Sumber: Globaltimes.com

Dalam Laporan 13th Five Year Plan 2016 – 2020, diketahui bahwa China telah membuat langkah besar dalam meningkatkan ekonomi, penghidupan masyarakat, dan bidang lainnya. China telah berkontribusi lebih dari 30 persen terhadap pertumbuhan ekonomi global, dengan PDB mencapai hampir 100 triliun yuan (\$14,9 triliun). Lebih dari 50 juta orang telah dibebaskan dari kemiskinan, dan 53,78 juta pekerjaan baru di perkotaan telah diciptakan. Pembawa standar baru dalam teknologi muncul, termasuk kereta api berkecepatan tinggi, Sistem Satelit Navigasi BeiDou dan pesawat penumpang domestik C919. Perkembangan teknologi yang pesat ini dapat dikaitkan dengan investasi dalam penelitian dan pengembangan, yang berjumlah 2,17 triliun yuan pada 2019, menyumbang 2,19 persen dari PDB dan naik 56,3 persen dari 2015.⁷¹

⁷¹Globaltimes.com, “Summary of the 13th Five-Year Plan 2016-20.” Last updated 26 Oct 2020. Diakses pada 4 May 2022.

World Bank merilis laporan yang disiapkan atas permintaan pemerintah China tentang perspektif pengetahuan dan inovasi untuk strategi pembangunan China. Sementara para peneliti menganalisis bahwa China melakukan investasi besar-besaran dalam infrastruktur informasi dan telekomunikasi, infrastruktur utama ekonomi pengetahuan dan masyarakat informasi sebagai salah satu fondasi pengetahuan pembangunan ekonomi.⁷² Implikasi inovasi ilmiah dan teknologi dalam seluruh bidang pengembangan tampak dalam kebijakan Made In China 2025 yang dicanakan oleh Presiden Xi Jinping. China melakukan inovasi teknologi disetiap bidang dengan memperkuat penelitian dasar, mendukung inovasi utama, inovasi berdasarkan integrasi teknologi yang ada, dan inovasi berdasarkan impor dan asimilasi, dan meningkatkan kapasitas inovasi China sendiri, untuk menyediakan dan kekuatan pendorong yang tak habis-habisnya untuk pembangunan ekonomi dan sosial.⁷³ Dalam Laporan FYP ke 13 Chapter 6 sebagai upaya mempercepat perluasan ekonomi informasi, China memastikan memasukan perkembangan teknologi informasi, melaksanakan strategi pengembangan siber nasional, mempercepat pengembangan teknologi digital.⁷⁴ China turut memodernkan pembangunan infrastrukturs (Part 7), Urbanisasi (Part 8), Agricultural (Part 4), dan pemaksimalan modernisasi industri (Part 5). Pada

[https://www.globaltimes.cn/content/1204685.shtml#:~:text=During%20the%2013th%20Five%2DYear,trillion%20yuan%20\(%2414.9%20trillion\).](https://www.globaltimes.cn/content/1204685.shtml#:~:text=During%20the%2013th%20Five%2DYear,trillion%20yuan%20(%2414.9%20trillion).)

⁷²Francoise Mengin, *Cyber China – Reshaping National Identities in The Age of Information*, (New York: Palgrave Macmillan, 2004), hal 51.

⁷³Central Committee of The Communist Party of China, *13th Five Year Report*, Part 1, Chapter 6: Ensure Innovation in Science and Technology Takes a Leading Role.

⁷⁴Op.Cit., Central Committee of The Communist Party of China, *13th Five Year Report*, Part 6, The Cyber Economy

akhirnya kebijakan yang tampak dalam Laporan ke 13 FYP china menunjukan upaya China berusaha memodernisasi setiap sektor pembangunannya dengan berbasiskan pada teknologi.

4.3.3 Keterlibatan *State* dan *Non State Actor*

Sebagaimana yang sebelumnya dipaparkan bahwa *cyberpower* merupakan kekuatan yang kompleks. Oleh karena itu diperlukan keterlibatan setiap pihak untuk memastikan berjalanannya pengembangan *cyberpower* berada dalam kontrol yang jelas. Atas dasar ini pemerintah China menaruh perhatian yang besar terhadap keterlibatan *non-state actor* termasuk didalamnya individu atau kelompok terutama hacker, ataupun para pelaku industri. Mayor Jenderal (telah pensiunan) sekaligus mantan direktur Staf Umum Departemen Komunikasi PLA dan bertanggung jawab atas perang informasi, Dai Qingmin, percaya bahwa dalam persaingan kekuatan *cyber* dibutuhkan kekuatan semua orang China yang memiliki keterampilan komputer sebagai kekuatan tempur tambahan yang potensial. Dalam *China's National Defense* 2008, China memandang penting terhadap perusahaan-perusahaan dan industri teknologi tinggi China untuk menunjang *cyberpower* China.

China berusaha memobilisasi kemampuan jaringan dan informasi warga dalam berbagai sektor sebagai strategi pengembangan *cyberpower* negara khususnya operator jaringan komputer yang sudah terampil. PLA China tidak hanya merekrut pekerja teknologi informasi dan akademisi, tetapi turut membentuk unit

milisi di dalam perusahaan telekomunikasi dan IT sipil.⁷⁵ Kebijakan pertahanan China menyerukan masyarakat untuk menciptakan pembangunan ekonomi dan pertahanan nasional yang saling terkoordinasi, dan hal ini haruslah terkoordinasi dalam pembangunan sosial dan ekonomi di masyarakat.

Pada tahun 1950-an hingga awal 1980-an, industri pertahanan China adalah perusahaan yang dimiliki sepenuhnya oleh pemerintah. Namun, pemerintah China akhirnya mulai melakukan konversi industri pertahanan dengan menjual beberapa industri militer dan mengizinkan perusahaan swasta China untuk menawar kontrak. Pada awal 2000an, pemerintah mulai melakukan investasi dalam penelitian dan pengembangan (R&D) yang dilakukan perusahaan swasta.⁷⁶ Konversi industri pertahanan ini pada akhirnya mendorong pengembangan teknologi *dual-use*, menciptakan sistem kolaborasi yang terintegrasi antara pertahanan, industri, universitas, dan lembaga penelitian. Hal ini menjadi implementasi koordinasi pemerintah china terkait pembangunan sosial dan ekonomi di masyarakat untuk menunjang pertahanan nasional.

Swasembada industri yang berhubungan dengan pertahanan merupakan upaya pemerintah untuk meningkatkan kemampuan militer China secara keseluruhan, dan memajukan pembangunan ekonomi dan kemakmuran. Pada akhirnya tercipta sebuah keterkaitan antara PLA, industri China, dan peretas. Keterkaitan antara industri-milisi memberikan akses PLA ke perusahaan mana pun

⁷⁵Op.Cit, Colonel Jayson M. Spade, . “China’s *Cyberpower* and America’s National Security.” hal 20-21.

⁷⁶Ibid, hal 23.

yang melakukan bisnis dengan telekomunikasi militer atau perusahaan IT, melalui jaringan perusahaan atau melalui produk yang dikembangkan oleh perusahaan. Meski demikian, sampai sejauh mana negara mempercayai atau mengendalikan komunitas peretas tidak diketahui. Sulit untuk mengetahui secara pasti motif aktivitas para aktor secara individu terutama mereka yang memang sangat paham akan dunia *cyber*. Hal inilah yang menjadi sulitnya menganalisis dengan pasti aktivitas *non-state* aktor mana sajakah yang didasari oleh kepentingan pemerintah terutama militer.

4.1 **Cyberpower Amerika Serikat**

Sebagaimana yang diketahui bahwa Amerika Serikat merupakan negara pemegang *hegemony* dunia sejak Perang Dingin berakhir. Sejak 1957 dimana Rusia meluncurkan satelit bernama SPUTNIK berhasil memicu Amerika Serikat untuk menyaingi perlombaan teknologi luar angkasa dengan Rusia. Keberhasilan Amerika Serikat dengan meluncurkan satelit pertamanya yang bernama TELSTAR pada 10 Juni 1962, dan disusul satelit ERLY BIRD tahun 1965 menunjukkan kemampuan rivalitas teknologi Amerika Serikat.⁷⁷ Potensi satelit yang dapat menerima dan memancarkan sinyal sinya siaran ketempat yang lebih luas menjadikan teknologi satelit banyak dipergunakan bahkan hingga saat ini.

Kemenangan Amerika Serikat dalam perang Dingin menjadikan perkembangan teknologi Amerika Serikat menjadi lebih unggul lterlebih dahulu dibandingkan negara lain. Amerika Serikat telah lebih dulu berhasil membangun

⁷⁷Mohammad Zamroni, "Perkembangan Teknologi Komunikasi dan Dampaknya Terhadap Kehidupan", *Jurnal Dakwah*, Vol 10, No 2. (Yogyakarta: UIN Sunan Kalijaga, 2009), hal 206.

keunggulan teknologinya. Saat ini militer Amerika Serikat sangat bergantung pada dunia maya, mengandalkan jaringan global yang terdiri dari 15.000 jaringan area lokal dan 7 juta komputer yang dihubungkan oleh lebih dari 100.000 sirkuit telekomunikasi, yang tersebar di pangkalan-pangkalan di seluruh dunia.⁷⁸ Sementara itu, perkembangan jaringan yang terjadi di Amerika Serikat turut menjadi jaringan utama dari Internet sipil global. Banyak perusahaan telekomunikasi milik swasta adalah penyedia layanan Internet, dan tidak sedikit yang mengoperasikan infrastruktur melalui dunia maya.

Jaringan global yang dimiliki Amerika Serikat menyimpan dan mengirimkan informasi yang tidak terklasifikasi, baik yang bersifat publik ataupun rahasia. Meluasnya penggunaan teknologi dan komputer jaringan menjadikan Amerika Serikat berkembang menjadi pusat gravitasi strategis. Namun, kondisi memungkinkan musuh memperoleh pengetahuan tentang informasi yang dimiliki Amerika Serikat sehingga memungkinkan pihak lain untuk dapat mengganggu infrastruktur sipil dan ekonomi. Sekali-lagi kemampuan *cyberpower* negara disisi dapat menjadi nilai positif namun disisi lainnya selalu dibayangkan-bayang oleh mungkinya kebocoran data. Semakin mudah informasi di akses maka, semakin rentan pula tingkat pertahanan informasi tersebut.

Militer AS diketahui sangat bergantung pada satelit untuk banyak fungsi penting seperti navigasi darat, udara, dan laut, pengawasan dan pengintaian,

⁷⁸Op.Cit.,Colonel Jayson M. Spade, . “China’s Cyberpower and America’s National Security., hal 30-31.

penargetan senjata pemogokan presisi, peringatan dini, dan komunikasi.⁷⁹ Jaringan jaringan yang terbentuk bahkan menjadi platform tujuan umum yang luas di mana pasar keuangan, bisnis, dan perdagangan, serta diplomasi, mata-mata, keamanan nasional, dan perang bergantung. Catatan sejarah menunjukkan bahwa kemajuan teknologi akan membawa pengaruh yang besar di bidang ekonomi, politik dan militer.⁸⁰ Namun disisi lain dapat menjadi bom atom apabila negara tidak mampu menjaga pertahanan jaringan informasi yang ada didalamnya. Terlebih bagi jaringan informasi Amerika Serikat yang telah sejak lama menjadi pusat dari sumber informasi dunia.

4.4.1 Masa Kejayaan *Cyberpower* Amerika Serikat

Secara sejarah penduduk Amerika Serikat telah lebih dahulu menikmati kemajuan teknologi. Hal inilah yang menjadi penyebab mengapa kehidupan masyarakat Amerika Serikat lebih aktif dan bergantung pada penggunaan internet dan teknologi informasi (IT) dalam berbagai sektor kehidupan. Sejak 1990, telekomunikasi dan komputer di Amerika Serikat telah menduduki posisi paling strategis. Terutama pada tahun 2013 yang dianggap sebagai masa revolusi teknologi ketiga yaitu penggabungan komputer dan komunikasi.⁸¹ Amerika Serikat dalam 40 tahun terakhir telah berhasil menghadirkan penggunaan dunia maya hingga berkembang secara pesat dan menembus hampir setiap dimensi interaksi manusia. Eksplorasi ruang angkasa, kesehatan, sistem pertahanan, bisnis, dan

⁷⁹Ibid, hal 22.

⁸⁰Op.Cit., Mohammad Zamroni, *Perkembangan Teknologi Komunikasi dan Dampaknya Terhadap Kehidupan*”, hal 207.

⁸¹Ibid, hal 208.

telekomunikasi menjadi fokus utama Amerika Serikat selama beberapa waktu terakhir. Amerika Serikat bahkan memiliki beberapa raksasa internet yang dikenal sangat mendominasi atas berbagai beberapa lapisan baik menengah dan atas internet contohnya sistem operasi (iOS, Windows, Android), mesin pencari (Google), jejaring sosial (Facebook), ritel online (Amazon), over the-top TV (Netflix), browser (Google Chrome, Apple Safari, Microsoft Explorer), dan nama domain (ICANN).⁸²

Google sebagai salah satu perusahaan teknologi terbesar di dunia, melihat sekitar 3,5 miliar pencarian per hari.⁸³ Google sendiri tak memiliki pedoman atau batasan konten dalam mesin pencariannya. Hal ini dikarenakan tujuan pencarian adalah untuk mengidentifikasi informasi yang relevan berdasarkan pencarian pengguna, dan bukan untuk memutuskan apakah materi tersebut “benar atau salah”. Terlepas dari fungsi pencariannya, Google juga memberikan kesempatan iklan berjalan dalam platformnya dengan kebijakan bahwa semua iklan harus “jelas dan jujur, dan memberikan informasi yang dibutuhkan pengguna untuk membuat keputusan yang tepat”.⁸⁴ Namun, dalam praktiknya beberapa penayangan iklan Google turut menimbulkan kekhawatiran karena adanya upaya pelanggaran privasi pengguna dan menghasilkan hal yang diskriminatif.

⁸²Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure”, *Journal of Information Policy*, Vol. 7 (Pennsylvania: Penn State University, 2017), hal 229.

⁸³Spandana Singh and Margerite Blase, *How Internet Platforms Are Addressing Election and Voter Suppression-Related Misinformation and Disinformation*, Protecting The Vote report (Washington DC: New America, 2020), hal 22.

⁸⁴Ibid.

Google turut menyediakan Google News yaitu sebuah agregator yang membantu menghubungkan pengguna ke berbagai outlet berita dan media. Platform ini menggunakan algoritme untuk menentukan bagaimana peringkat berita, yang bergantung pada faktor-faktor seperti relevansi konten, keunggulan, lokasi.⁸⁵ Besarnya informasi yang tersedia di Google turut dimanfaatkan oleh pemerintah Amerika Serikat. Contohnya pada Agustus 2020, Google merilis posting blog dengan langkah-langkah tambahan yang mereka ambil untuk memerangi informasi yang salah seputar pemilu Amerika Serikat tahun 2020. Mereka bekerja sama dengan badan terkait dan membentuk tim yang ditugaskan untuk bekerja sama untuk mencegah serangan yang didukung pemerintah dan kampanye phishing pada pengguna Google. Hasilnya, terlacak terdapat lebih dari aktivitas dari 270 kelompok yang tujuannya mencakup “pengumpulan intelijen, mencuri kekayaan intelektual, menargetkan pembangkang dan aktivis, serangan dunia maya yang merusak, atau menyebarkan disinformasi terkoordinasi.”⁸⁶

Keberhasilan Google nyatanya turut mengubah cara hidup orang banyak di seluruh dunia. Raksasa teknologi tersebut mungkin tidak mengatur perangkat keras, atau infrastruktur material, namun mereka berhasil menguasai dimana jaringan informasi dalam kehidupan sehari-hari, termasuk bisnis, pemerintah, masyarakat. Hal ini tentu memungkinkan untuk menjadi keuntungan bagi kemampuan *cyber* Amerika Serikat. Karena keberadaan jaringan informasi ini sangat dapat dipergunakan untuk menunjang jaringan informasi lawan terutama terkait

⁸⁵Ibid, hal 25.

⁸⁶Ibid, hal 26.

rivalitas *cyber* yang berlangsung. Dominasi teknologi ini menggambar bagaimana internet berada dan mendapat dukungan oleh tata kelola internet global yang bersifat multi-stakeholder.

Keterlibatan negara asal (home country) dalam jalannya aktivitas perusahaan multinasionalnya saat ini tidak terbatas pada lingkup wilayah teritori negaranya saja, namun telah meluas hingga keluar wilayah negaranya. Jaringan internet yang terbentuk didukung oleh banyak kepentingan komersial, pakar teknis, organisasi non-pemerintah serta Amerika Serikat, dan demokrasi kapitalis Barat.⁸⁷ Dominasi raksasa teknologi tersebut turut membentuk citra internet dan komunikasi Amerika Serikat. Agenda "kebebasan internet" Departemen Luar Negeri Amerika Serikat cocok dengan ideologi Amerika Serikat yang selama ini digaungkan. Amerika Serikat berusaha mempertahankan dominasi raksasa teknologinya melalui promosi dan disandangkan kedalam kebijakan luar negeri Amerika Serikat.⁸⁸

Tatanan komunikasi dunia yang bersifat multilateral menjadi sangat berkembang. Menurut Edward Snowden, adanya program pengawasan internet yang dipimpin Badan Keamanan Nasional Amerika Serikat memperkuat dominasi AS atas internet. Bahkan dalam kesepakatan dagang antara Organisasi Perdagangan Dunia dan negara-ke-negara diapit oleh model Tata Kelola Internet multi-stakeholder.⁸⁹ Secara sederhana kondisi menunjukan bahwa keberadaan media komunikasi dapat dipergunakan sebagai “alat atau senjata politik” dalam

⁸⁷Op.Cit., Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure”, hal 230.

⁸⁸Ibid, hal 228.

⁸⁹Ibid.

persaingan *cyberpower*. Munculnya sistem komunikasi dan media global memainkan peran kunci dalam rivalitas ini.

4.4.2 Peningkatan *Cyberpower* Amerika Serikat

Seiring meningkatnya penggunaan dunia maya maka, penyalahgunaan ruang maya turut meningkat. Insiden serangan siber diseluruh dunia meningkat, baik di sektor pemerintah maupun swasta. Beberapa serangan turut menimbulkan kerugian secara finansial. Serangan *cyber* tersebut secara signifikan dapat mempengaruhi berbagai sektor penting terutama ekonomi dan infrastruktur sipil. Beberapa serangan mungkin murni dilakukan oleh kelompok swasta namun terdapat kecenderungan yang meningkat atas penggunaan *cyber* attack dalam konflik negara. Persaingan *cyberpower* antara Amerika Serikat dan China tidak terlepas dari dugaan Amerika Serikat bahwa China telah berulang kali menargetkan Amerika Serikat.

Menurut Laporan Mandant, perusahaan teknologi swasta di Amerika Serikat, memaparkan bahwa salah satu unit spionase siber Tentara Pembebasan Rakyat China (PLA) yang telah meretas sistem komputer New York Times selama 2012 dan 2013. Hingga Amerika Serikat mengumumkan bahwa peningkatan prioritas terkait masalah siber. Puncaknya ketika isu serangan siber diangkat dalam percakapan pertama antara Presiden Obama dan Presiden baru China Xi Jinping.⁹⁰

⁹⁰Loc.Cit., Tobias Feakin, *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities*, hal 2.

Hal ini menjadikan masalah dunia maya telah berubah dari masalah teknis tingkat rendah menjadi masalah strategis yang penting.

Jenderal James Cartwright, mantan Komandan Komando Strategis Amerika Serikat kemudian menyatakan bahwa, China telah melakukan semacam pengintaian dan pemetaan jaringan komputer pemerintah dan swasta di Amerika Serikat. China turut diduga memiliki jaringan yang diperlukan untuk melakukan serangan semacam itu dan memiliki kemampuan untuk melumpuhkan infrastruktur penting serta komando dan kontrol militer.⁹¹ Selain itu, upaya China mengembangkan *cyberpower* adalah untuk kelangsungan hidup rezim, kedaulatan nasional dan integritas teritorial, dan menjadi pesaing *hegemony* Amerika Serikat.⁹² China dinilai tengah berusaha keras menghalangi keterlibatan Amerika Serikat dalam kepentingan vital China dengan menunjukkan bahwa negara tersebut memiliki kemampuan ofensif dibawah kontrol internal pemerintah.

Kesadaran pemerintah Amerika Serikat bahwa secara keseluruhan jaringan informasi mereka rentan terhadap eksploitasi dan serangan dunia maya China memaksa mereka untuk mengambil sikap dan melakukan pengembangan untuk menyaingi persaingan kekuatan *cyber* dengan China. Amerika Serikat memandang bahwa PLA atau Tentara Pembebasan China sedang melakukan persiapan perang *cyber*. PLA tengah melakukan pengintaian di *Cyberspace*, berusaha menciptakan kemampuan untuk merugikan ekonomi dan merusak infrastruktur penting, bersiap

⁹¹Op.Cit, Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure", hal 33.

⁹²Ibid, hal 27.

untuk mengganggu sistem komunikasi dan informasi yang diperlukan untuk mendukung konflik senjata konvensional, dan bersiap melakukan operasi psikologis untuk mempengaruhi pendirian orang Amerika.⁹³

Kondisi yang tercipta pada akhirnya memaksa Amerika Serikat untuk mengubah struktur keamanan nasionalnya untuk mengatasi perkembangan kekuatan *cyber* China di dunia maya. Menurut studi pemerintah Amerika Serikat dan lembaga *think tank* menunjukkan bahwa China memiliki tiga tujuan utama keamanan nasional yaitu, **Pertama**, mempertahankan kelangsungan hidup rezim (kekuasaan Partai Komunis Tiongkok (PKT)), **Kedua**, mempertahankan kedaulatan nasional dan integritas teritorial, dan **Ketiga**, menetapkan China sebagai kekuatan regional dan dunia. Hal utama lainnya adalah China tengah mempertahankan pembangunan ekonomi dan sosial yang stabil, modernisasi militer, dan mencegah kemerdekaan Taiwan.⁹⁴

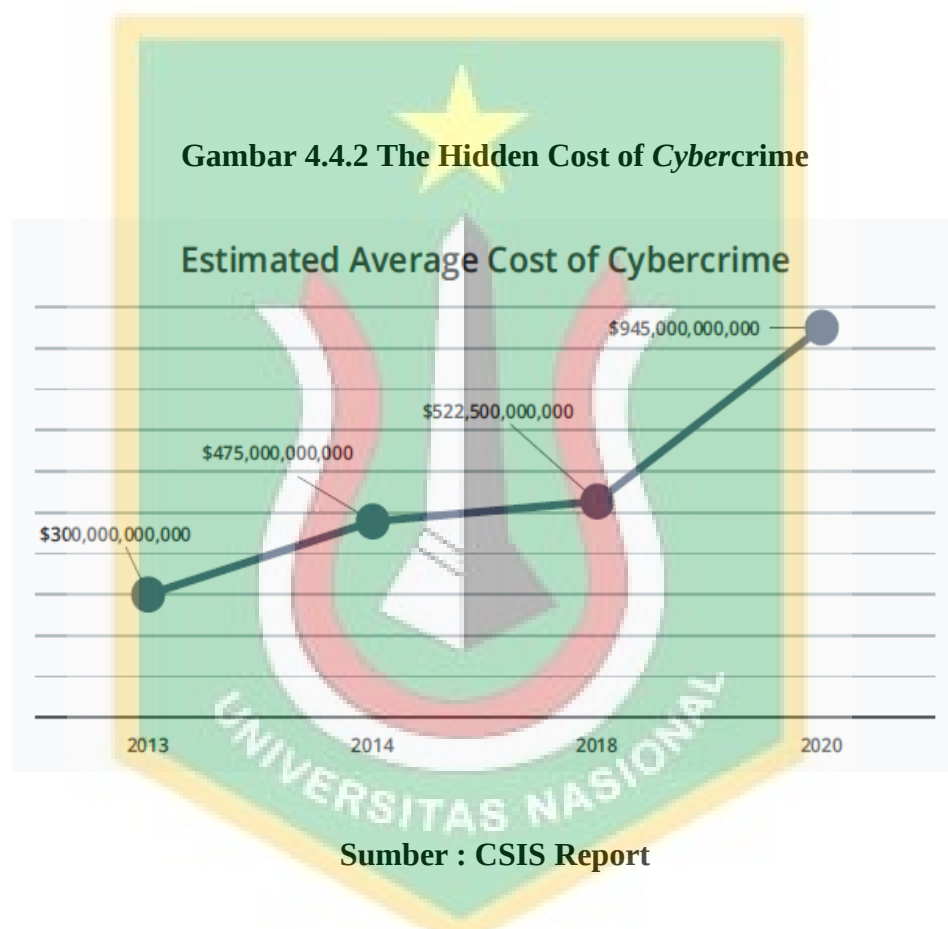
Meningkatnya aktivitas siber berbahaya di Amerika Serikat secara nyata menargetkan banyak orang, merusak keamanan nasional, dan memengaruhi hampir setiap sektor ekonominya.⁹⁵ Pihak lawan memanfaatkan alat kejahatan dunia maya dan mempekerjakan penjahat dunia maya untuk mencuri rahasia keamanan nasional dan kekayaan intelektual Amerika Serikat. Menurut penilaian Dewan Penasihat Ekonomi Gedung Putih dalam laporan *Executive Office of The President United States (EOP)* tahun 2018, aktivitas siber yang berbahaya telah merugikan ekonomi

⁹³Loc.Cit., Colonel Jayson M. Spade “China’s *Cyberpower* and America’s National Security.”, hal 2.

⁹⁴Ibid, hal 12.

⁹⁵Allison Peters, “Unpacking US *Cyber* Sanctions”. Last updated 29 Jan 2021. Diakses pada 19 Jun 2022. <https://www.thirdway.org/memo/unpacking-us-cyber-sanctions>

Amerika Serikat sekitar \$ 57 miliar hingga \$ 109 miliar pada tahun 2016.⁹⁶ Selain itu, peningkatan aktivitas siber berbahaya turut meningkatkan dampak global.



Pada bulan Desember 2020, Pusat Studi Strategis dan Internasional (CSIS) melaporkan bahwa biaya kejahatan dunia maya global mencapai lebih dari \$ 900 milyar dan peningkatan hampir mencapai 50% dibandingkan 2018.⁹⁷ Berdasarkan

⁹⁶The Council of Economic Advisers, “The Cost of Malicious *Cyber* Activity to the US Economy”, February, (Washington DC: Executive Office of The President of United States, 2018), hal 1.

⁹⁷Zhanna Malekos Smith, and Eugenia Lostri, *The Hidden Cost of Cybercrime* (Washington DC: CSIS, 2020), hal 3.

data dalam laporan tahun 2018 tersebut, diketahui bahwa kejahatan dunia maya merugikan ekonomi global lebih dari \$ 600 miliar dengan peningkatan lebih dari 50% dalam dua tahun terakhir.

4.4.3 Kepentingan Amerika Serikat dalam persaingan *Cyberpower*

Perkembangan China sejatinya masih menjadi perdebatan bagi posisi Amerika Serikat dalam tingkat global. Amerika Serikat masih dianggap menonjol dan menjadi negara paling kuat didunia dimana kekuatan dan pengaruhnya tidak terbatas termasuk sektor *cyberpower* yang dimilikinya. Namun, bagi Amerika Serikat apabila ada pertanyaan siapakah “pesaing sejawat” yang setaraf maka jawabannya adalah China.⁹⁸ Kritik yang Amerika Serikat kepada China adalah China tengah mengumpulkan kekuatan yang dibutuhkan, dan hal ni akan berdampak pada perubahan ketertiban internasional dengan ditandai sebagai “pengganggu atau kekuatan revisionis” yang berusaha mengubah sistem internasional untuk kepentingannya.⁹⁹

Bernstein dan Murro, menyatakan bahwa lebih dari satu dekade China sedang berusaha mengganti dominasi kekuatan Amerika Serikat di Asia.¹⁰⁰ John Mearsheimer dalam bukunya yang berjudul *The Tragey of Great Power Politic* mengatakan bahwa semakin kuatnya kekuatan yang dimilikinya akan mendorong China berperilaku seperti perimbangan kekuatan kekuatan di masa lalu hingga mengancam perdamaian dan stabilitas internasional.¹⁰¹ Selain itu, semakin

⁹⁸Op.Cit., Shalendra D.Sharma, *China and India in The Age of Globalization*,, hal 211.

⁹⁹Ibid., hal 220.

¹⁰⁰Ibid.

¹⁰¹Ibid.

meningkatnya kemampuan China turut akan menjadikannya semakin condong kehadiran China sebagai pesaing hegemoni secara nyata.¹⁰² Hal inilah yang pada akhirnya menjadikan persaingan dominasi global antara Amerika Serikat dan China berlangsung cukup lama.

Amerika Serikat sebagai unipolar sejak Perang Dingin sendiri telah berhasil memimpin dalam hal mengembangkan strategi domestik untuk mengatasi keamanan siber. Ketergantungan Amerika Serikat terhadap jaringan digital yang dimilikinya tidak hanya akan memengaruhi aspek ekonomi tetapi juga militer. Selain itu, sebagai negara adidaya ekonomi dan militer dunia, Amerika Serikat terus-menerus menghadapi serangan terhadap jaringan sibernya di semua sektor.

Departemen Pertahanan Amerika Serikat secara khusus melihat China sebagai pesaing dekat, terutama setelah adanya Revolusi PLA dalam Urusan Militer (RMA) sebagai program modernisasi dengan potensi untuk menantang kehadiran militer Amerika Serikat dan proyeksi kekuatan di wilayah. Selain itu, Amerika Serikat sendiri turut melihat bahwa adanya integrasi para peretas dan komunitas hacker di China dalam strategi perang *cyber* China. Dalam sektor industri dan ekonomi, Amerika Serikat melihat bahwa China memainkan peran untuk memperoleh informasi dan memperkuat *cyberpower* negara tersebut melalui pengembangan teknologi dan invasi industri perusahaan sipil. Bagi Amerika Serikat informasi yang terdapat dalam dunia maya menjadi prioritas bagi kebijakan politik domestik Amerika Serikat mengingat eksistensinya yang sangat vital.

¹⁰²Ibid.

Bagi Amerika Serikat, China berusaha mencari informasi dengan menggunakan industri IT-nya. Informasi-informasi yang diterima kemudian digunakan oleh China untuk menciptakan kerentanan sistem bagi Amerika Serikat. Amerika Serikat sendiri melakukan pelarangan secara khusus terhadap beberapa perusahaan IT China contohnya Huawei. Amerika Serikat memandang Huawei sebagai pemasok informasi utama bagi PLA China. Hal ini sendiri dilakukan oleh Amerika Serikat tak lama setelah media melaporkan bahwa peretas China telah membobol jaringan komputer pemerintah India.¹⁰³

Berdasarkan data dari Specops jumlah serangan *cyber* yang terjadi di wilayah Amerika Serikat berada dalam urutan tertinggi¹⁰⁴ Pada tahun 2012 berdasarkan laporan Government Technology China menjadi negara nomor 1 dengan aktivitas *cyber attack* didunai dengan 40 persen¹⁰⁵. Hal ini tentu saja menjadi ancaman bagi wilayah vital Amerika Serikat. Disisi lain Amerika Serikat turut menyakini jika persaingan *cyberpower* secara luas menggunakan spionase siber dalam skala besar akan memberikan keuntungan politik, militer, atau komersial. Pemerintah Amerika Serikat sendiri tidak menyangkal bahwa secara rutin mereka terlibat dalam kegiatan mata-mata untuk memajukan keuntungan ekonomi

¹⁰³Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 27.

¹⁰⁴Specopssoft.com, "The countries experiencing the most 'significant' *cyber-attacks*". Last updated 13 July 2020. Diakses 15 July 2022. <https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/>

¹⁰⁵Noelle Knell, "Top 10 Countries Where *Cyber Attacks* Originate." Last updated 23 Apr 2013. Diakses 15 July 2022. <https://www.govtech.com/security/hacking-top-ten.html>

Amerika, yang merupakan bagian dari definisi luas pemerintah tentang perlindungan keamanan nasional Amerika Serikat.¹⁰⁶

Perlindungan nasional harus dilakukan secara merata karena setiap perusahaan ataupun lembaga berbagi kerentanan *cyber* yang sama. Kemajuan teknologi yang dialami oleh Amerika Serikat menjadikan negara tersebut membangun jaringan sistem keamanan informasi dalam bidang militer, agraria, sistem pengaturan lalu lintas, air dan sanitasi, energi dan transportasi sangat tergantung pada peranan komputer dan dunia maya¹⁰⁷. Ketergantungan ini menjadi sebuah ancaman bagi Amerika Serikat. Apabila sistem keamanan informasi tersebut diretas, secara otomatis kehidupan negara Amerika Serikat dapat mengalami kelumpuh dan mengakibatkan dampak yang serius disemua sektor termasuk ekonomi.

Kerusakan akibat serangan siber dan pencurian siber dapat meluas dari target awal ke perusahaan yang terkait secara ekonomi, sehingga memperbesar kerusakan ekonomi.¹⁰⁸ Hal ini menjadikan serangan siber terhadap sektor infrastruktur penting dapat sangat merusak ekonomi Amerika Serikat secara global. Garis antara aktor negara-bangsa dan penjahat dunia maya non-negara,

¹⁰⁶Sinan Ulgen, *Governing Cyberspace*, (Washington DC: Carnegie Europe, 2016), hal 55.

¹⁰⁷Op.Cit., Dewi Triwahyuni, dan Tine Agustin Wulandari, Dampak Pembangunan *Cyberpower* Tiongkok terhadap kepentingan Amerika Serikat”, hal 113.

¹⁰⁸Loc.Cit., The Council of Economic Advisers, “The Cost of Malicious *Cyber* Activity to the US Economy”, hal 1.

bagaimanapun, telah kabur karena negara cenderung bersekongkol dan secara langsung menggunakan penjahat dunia maya non-negara sebagai alat negara.¹⁰⁹



¹⁰⁹Loc.Cit., Allison Peters, “Unpacking US Cyber Sanctions”. Last updated 29 Jan 2021. Diakses pada 19 Jun 2022. <https://www.thirdway.org/memo/unpacking-us-cyber-sanctions>.

BAB V

PERSAINGAN KEKUATAN CYBER CHINA DAN AMERIKA SERIKAT

5.1 Kesiapan China dan Amerika Serikat dalam Persaingan Cyber

Persaingan *cyberpower* yang terjadi antara China dan Amerika Serikat menunjukkan adanya bentuk persaingan mode baru yang tidak bersifat konvensional. Persaingan *cyberpower* menunjukkan sebuah pembatasan perang terbaru mode baru, namun dengan luas cakupan yang lebih besar dengan meliputi darat, laut, udara, dan ruang angkasa. Medan persaingan dalam perang jenis baru ini juga menjadi jauh lebih sulit dibandingkan dengan konflik konvensional. Hal ini dikarenakan sulit untuk menentukan identitas pihak yang berperang secara jelas. Tanpa adanya identifikasi yang jelas ini membuat pemerintah tidak dapat mengembangkan strategi untuk merespons lawan secara yang tepat.¹¹⁰ Kesulitan terbesar untuk menghadapi persaingan ini terletak pada tanggung jawab negara untuk mencegah wilayahnya dipergunakan melalui serangan siber oleh entitas yang tidak berafiliasi dengan pemerintah karena banyaknya aktor yang terlibat.

Sebagai negara hegemoni, Amerika Serikat yang telah sejak lama memiliki pengaruh yang cukup kuat dalam kancah internasional tentu tidak ingin kalah dalam persaingan ini. Peningkatan aktivitas *cyber* yang dilakukan pihak lawan memaksa Amerika Serikat menggunakan pengaruh yang dimilikinya termasuk dalam sektor ekonomi. Globalisasi pasar ekonomi dan keinginan menciptakan alat baru untuk memerangi ancaman terhadap keamanan telah berkontribusi terhadap terciptanya

¹¹⁰Op.Cit., Sinan Ulgen, *Governing Cyberspace*, hal 62.

inovasi substansial terkait penggunaan langkah-langkah ekonomi koersif seperti sanksi. Program sanksi terus berkembang dalam berbagai ukuran dan cakupan. Mereka dapat bersifat komprehensif (yaitu, pembatasan perdagangan dan aktivitas komersial dengan seluruh negara) atau ditargetkan (yaitu, pembatasan aktivitas individu dan/atau badan tertentu).¹¹¹

Amerika Serikat sendiri memiliki tujuh bidang penting yang menjadi fokus utamanya. Ketujuh bidang ini sebenarnya saling terkait dan membutuhkan kerjasama dari pemerintah, mitra internasional, dan sektor swasta yang ada. Tujuh area prioritas dunia maya internasional Amerika Serikat, yaitu :¹¹²

1) Ekonomi

Amerika Serikat mengutamakan adanya inovasi dan keterbukaan pasar

2) Melindungi Jaringan

Tingkatkan keamanan, keandalan, dan ketahanan global jaringan menjadi hal penting yang perlu dijamin oleh negara

3) Penegakan Hukum

Memperluas kerjasama penegakan hukum dan peraturan hukum sebagai upaya menciptakn pertahanan jaringan informasi

¹¹¹Loc.Cit., Allison Peters, “Unpacking US Cyber Sanctions”. Last updated 29 Jan 2021. Diakses pada 19 Jun 2022. <https://www.thirdway.org/memo/unpacking-us-cyber-sanctions>.

¹¹²Op.Cit., Dewi Triwahyuni, Yayan Mochamad Yani, and Arry Bainus, Dampak Pembangunan Cyberpower Tiongkok terhadap kepentingan Amerika Serikat”, hal 303.

4) Militer

Mempersiapkan tantangan keamanan kontemporer abad ke-21, karena cakupan keamanan jauh lebih kompleks dibandingkan sebelumnya

5) Tata Kelola Internet

Mempromosikan keefektifan dan struktur tata kelola internet yang inklusif dalam segala aktivitas masyarakatnya

6) Pembangunan Internasional

Memperluas pembangunan kapasitas gedung, keamanan dan kemakmuran dicapai melalui perdagangan internasional

7) Kebebasan Internet

Amerika Serikat mendukung privasi sebagai kebebasan mendasar dalam aktivitas internetnya

Dalam menjalankan strateginya, Amerika Serikat memandang penting beberapa prinsip dasar atas strategi mereka. **Pertama**, kegiatan pengamanan dunia maya merupakan upaya nasional. **Kedua**, prinsip melindungi privasi dan kebebasan sipil. Pemerintah Amerika Serikat menganggap bahwa penyalahgunaan dunia maya adalah pelanggaran terhadap privasi dan kebebasan warga negara. Hal ini nyatanya menjadi norma yang kontradiktif dalam pandangan pemerintah China. Pemerintah China cenderung menggunakan internet sebagai alat propaganda dengan melakukan kontrol yang kuat sehingga warganya tidak memiliki hak penuh atas

kebebasan dunia maya. **Ketiga**, prinsip kekuatan regulasi dan pasar. Peraturan pemerintah tidak akan menjadi sistem utama dalam pengamanan dunia maya. Peraturan yang lebih luas harus dilakukan untuk mengupayakan perusahaan dapat mengatur sistem informasi sehingga hal ini tidak akan menciptakan pendekatan keamanan siber yang gagal.

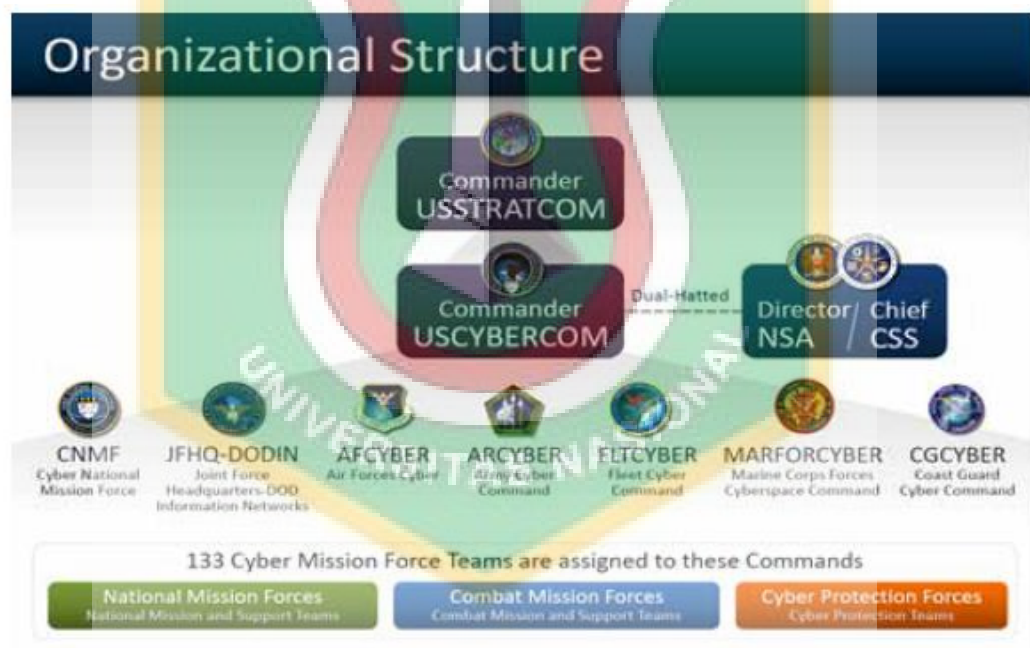
Sementara itu, terkait persaingan *cyberpower* dengan China, Amerika Serikat menggunakan pengaruh ekonomi untuk menjegal perkembangan *cyberpower* China. Salah satunya adalah pembatasan produk Huawei dalam pasar Amerika Serikat. Strategi Siber Nasional Amerika Serikat sedikit banyak menyatakan bahwa sanksi ekonomi termasuk kedalam strategis pemerintah Amerika Serikat dalam berurusan dengan aktor *cyber* jahat.¹¹³ Pemerintah Amerika Serikat melakukan advokasi dengan negara-negara lain untuk menetapkan rezim sanksi dunia maya dan berkoordinasi secara multilateral untuk menjatuhkan sanksi. Upaya Amerika Serikat ini menjadi hal penting untuk menahan konflik dunia maya karena dapat menciptakan konsekuensi serangan yang tidak terduga. Selain itu, Amerika Serikat secara serius mengeluarkan sejumlah rumusan Kebijakan Luar Negeri terkait *cyberspace* atau dunia maya menyusul sejumlah perilaku China di ruang maya yang mempengaruhi kepentingan nasional Amerika Serikat.

Pada sektor militer Amerika Serikat mengacu pada aplikasi kekuatan *cyber* sebagai Operasi Jaringan Komputer (CNO) dan membaginya menjadi tiga kategori:

¹¹³Loc.Cit., Allison Peters, "Unpacking US Cyber Sanctions". Last updated 29 Jan 2021. Diakses pada 19 Jun 2022. <https://www.thirdway.org/memo/unpacking-us-cyber-sanctions>.

Pertahanan Jaringan Komputer (CND), Serangan Jaringan Komputer (CNA), dan Eksploitasi Jaringan Komputer (CNE). Kategori-kategori secara analog sejalan dengan pemikiran dalam Tentara Pembebasan Rakyat China. Kemampuan ofensif kekuatan *cyber* Amerika Serikat adalah CNA dan CNE¹¹⁴. Selain itu, untuk mengamankan posisi Amerika Serikat di kawasan Asia Timur, Amerika Serikat turut membangun aliansi kekuatan terutama dengan Jepang dan Korea Selatan. Amerika Serikat menjadikan *US Cyber Command* atau Komando Siber menjadi senjata perang di dunia maya.

Gambar 5.1 U.S Cyber Command



Sumber : USNR

¹¹⁴Loc.Cit., Colonel Jayson M. Spade, "China's Cyberpower and America's National Security.", hal 2.

Komando Siber mencakup enam markas tingkat operasional elemen yaitu Komando Siber Angkatan Darat (*Army Cyber Command*), Komando Siber Armada (*Fleet Cyber Command*), Udara Force *Cyber* (*Air Force Cyber*), Komando *Cyberspace* Pasukan Korps Marinir (*Ar Marine Corps Forces Cyberspace Command*), Markas Besar Pasukan Gabungan – Departemen Pertahanan Jaringan Informasi (*Joint Forces Headquarters - Department of Defense Information Network Command*), dan Pasukan Misi Nasional Siber (*Cyber National Mission Force*).¹¹⁵

Selain itu, Amerika Serikat dan Jepang juga menyepakati beberapa perjanjian bilateral untuk menjaga eksistensinya di kawasan Asia Timur, salah satunya membentuk San Fransissco Treaty dan Japan-US Security Treaty. Kedua perjanjian tersebut berisikan kewajiban Jepang untuk dapat mengembalikan wilayah okupasi dan kewenangan Amerika Serikat. Hal ini menjadikan Amerika Serikat memiliki pangkalan militer di sana. Perjanjian ini sendiri didirikan dalam rangka menjaga stabilitas keamanan kawasan dan global. Amerika Serikat memiliki hak untuk mempertahankan kekuatan darat, laut dan udaranya di Jepang. Kekuatan ini dapat dipergunakan: (1) untuk mempertahankan perdamaian dan keamanan di wilayah tanpa perlu menunggu konsultasi terlebih dahulu; (2) tetapi apabila konsultasi memang diperlukan, Amerika Serikat dapat melakukan tindakan untuk mempertahankan Jepang dari serangan pihak luar.

¹¹⁵Catherine S. Deppa, "U.S. Cyber Command: An Overview", *American Intelligence Journal*, Vol. 34, No. 1 (Culllen: National Military Intelligence Association, 2017), hal 13.

Perjanjian tersebut turut merinci bahwa apabila ada operasi yang dijalankan menggunakan basis Jepang oleh pihak lain harus melakukan konsultasi terlebih dahulu dengan pemerintah Jepang¹¹⁶. Selain itu, Amerika Serikat membentuk kerjasama dengan Korea dengan menyepakati *Mutual Defense Treaty* yang berisi tentang kesepakatan untuk menjaga perdamaian internasional, kewajiban untuk berdiskusi dalam mengambil tindakan dari ancaman ketika salah satu atau keduanya merasa terancam, dan diizinkan untuk angkatan militer Amerika Serikat (darat, laut, maupun udara) untuk beroperasi di wilayah administrasi Korea Selatan.¹¹⁷

Amerika Serikat turut membentuk kebijakan *Taiwan Relations Act*, dan menjadi salah satu pemasok senjata utama bagi Taiwan dalam rangka menjaga perdamaian dan pembangunan pertahanan bagi Taiwan. Menurut *Bill Clinton*, peranan Amerika Serikat di kawasan Asia Timur sebagai bentuk implementasi kebijakan *engagement and enlargement* yang berisi: (1) Memperkuat persatuan kawasan melalui pembangunan aliansi; (2) Mempertahankan kehadiran kekuatan militer Amerika Serikat di Asia Timur; dan (3) Membangun institusi regional.¹¹⁸ Melalui aliansi yang terbentuk Amerika Serikat berusaha mengamankan posisinya dan secara tak langsung memberikan pengaruhnya terhadap kebijakan negara lain untuk menyesuaikan atau mengikuti kepentingan Amerika Serikat. Wilayah Asia Timur merupakan wilayah domain China. Hal inilah yang menjadi alasan mengapa Amerika Serikat menaruh perhatian besar terhadap wilayah tersebut. Secara

¹¹⁶Loc.Cit., Lalu Azhar Rafsanjani, Lalu Putrawandi Karjaya, Khairur Rizki, "Rivalitas Amerika Serikat (AS) dan China dalam menjaga Security Order di Asia Timur, hal 33.

¹¹⁷Ibid.

¹¹⁸Ibid.

sederhana Amerika Serikat berusaha mengepung China sebagai upayanya mengamankan posisi dan strategi mereka.

Pada tahun 2015 Amerika Serikat menerbitkan sebuah dokumen yang berjudul “The Department of Defense (DoD) Cyber Strategy”. Dokumen ini menjadi pernyataan keseriusan Amerika Serikat terkait strategi pertahanannya.¹¹⁹ Pengeluaran dokumen ini menunjukkan bagaimana Amerika Serikat meletakkan perhatian yang khusus atas perkembangan *cyberpower* China. Amerika Serikat memandang perlu untuk mempersiapkan secara matang kebijakan luar negerinya untuk menghadapi kekuatan siber China. Kemampuan *cyberpower* China secara nyata telah mendorong Amerika Serikat untuk melakukan hal tersebut.

Dilain pihak pemerintah China tepatnya pada Maret 2017 merilis sebuah dokumen tentang strategi kerjasama internasional di dunia maya. Sebagai tujuan dasar dari pertukaran internasional dan kerjasama di dunia maya, China menetapkan enam tujuan strategis dalam dokumen ISCC, yaitu:¹²⁰

- 1) Melindungi kedaulatan dan keamanan
- 2) Mengembangkan sistem aturan internasional
- 3) Mempromosikan tata kelola internet yang baik
- 4) Melindungi hak dan kepentingan yang sah warga negara

¹¹⁹Op.Cit, Dewi Triwahyuni, Yanyan Mochamad Yani, Arry Bainus, Dampak Pembangunan Cyberpower Tiongkok terhadap kepentingan Amerika Serikat”, hal 301.

¹²⁰Ibid., 303.

5) Mempromosikan kerjasama ekonomi digital

6) Membangun platform pertukaran budaya dunia maya

Terkait rivalitas *cyber*nya dengan Amerika Serikat, strategi keamanan *Cyber* China terdiri atas 3 komponen penggerak utama yaitu, komponen ekonomi, politik, dan militer.¹²¹ Selain itu China berfokus kepada perilaku politik luar negeri yang mengupayakan secara aktif dan percaya diri untuk mempromosikan ide-ide yang dimilikinya. China berusaha meyakinkan masyarakat internasional untuk dapat beradaptasi dengan nilai-nilai dan pemikiran China dalam keamanan jaringan. Dengan lebih banyak keterlibatan dalam komunitas internasional, China mencoba memberi sinyal bahwa negara adalah aktor yang bertanggung jawab dan dapat diajak bekerjasama terkait masalah teknologi.

China menyatakan keinginannya untuk berperilaku baik di dunia maya, meskipun beberapa negara menganggap hal tersebut hanyalah sikap dipermukaan dan sebagai jargon untuk mencegah kebisingan dari aktor internasional lainnya.¹²² Pemerintah China membentuk "Central Internet Security and Information Leading Group (CISILG)" dimana Presiden Xi Jinping secara langsung terjun sebagai pihak pengambil keputusan dan penanggung jawab atas penentuan strategi *cyber* China. China memahami bahwa dunia maya sebagai sesuatu yang sangat terintegrasi dengan masyarakat. Hal ini menjadikan dunia maya menjadi tidak terpisahkan dari aliran umum pemerintahan.

¹²¹Ibid.

¹²²Ibid.

China di bawah pemerintahan Presiden Xi Jinping pada tahun 2016 mengeluarkan rencana Lima Tahun ke-13 (The 13th Five-Year Plan). Kebijakan ini mengumumkan satu set baru tentang prinsip-prinsip pembangunan untuk mengejar pertumbuhan ekonomi berbasis inovasi, seimbang, hijau, dan terbuka yang memungkinkan manfaatnya dapat dirasakan secara luas. FYP ke-13 juga memperluas komitmen yang dinyatakan pemerintah China terhadap inovasi, yang sebelumnya pernah ditekankan dalam FYP ke-12 serta peningkatan kualitas hidup warga. Upaya peningkatan pada dasarnya telah yang dimulai ketika FYP ke-11 dengan memprioritaskan lingkungan, kesehatan, pendidikan, dan kesejahteraan sosial.

Lima tema utama dalam cetak biru FYP 13 China terkait pembangunan masa depan China mencakup detail sebagai berikut :¹²³

1. Inovasi

Inovasi adalah landasan strategi utama dalam pembangunan dalam FYP ke-13 dan menjadi komponen penting untuk menggerakkan manufaktur China ke atas rantai manufaktur bernilai tambah dan meningkatkan daya saing global dengan mengedepankan keunggulan teknologi di masa depan. Di bawah FYP ke-13, pada tahun 2020 pemerintah berupaya meningkatkan peringkat inovasi globalnya dari 18 menjadi 15.

¹²³Katherine Koleski, "The 13th Five-Year Plan", Staff Research Report, February (Washington DC: United States-China Economic and Security Review Commission, 2017), hal 3.

2. Pembangunan Terkoordinasi

Sebagai upaya mengatasi kesenjangan yang semakin melebar dalam pembangunan ekonomi regional, konstruksi berlebihan, duplikasi struktur industri, dan kurangnya layanan publik. Pemerintah China berusaha meningkatkan koordinasi kebijakan, sumber daya, dan perencanaan kota antar pemerintah melalui urbanisasi, hukou (reformasi sistem pendaftaran rumah tangga), dan pembentukan megaregion Beijing-Tianjin-Hebei dan Sabuk Ekonomi Yangtze.

3. Pertumbuhan Hijau

FYP ke-13 memperkuat keinginan pemerintah China untuk mengatasi degradasi lingkungan yang parah di China dan membangun sektor energi bersih, manufaktur hijau, dan jasa lingkungan. Target terkait lingkungan mencapai 10 dari 25 target yang ditetapkan dalam FYP ke-13, dan ke-10 tersebut adalah target mengikat yang harus dipenuhi pada tahun 2020. Target tersebut berusaha menetapkan batas penggunaan energi untuk kualitas udara kota, intensitas karbon dioksida, dan pengurangan kontaminasi tanah dan air yang lebih baik.

4. Keterbukaan

Untuk mendukung keterbukaan yang lebih besar, FYP ke-13 menjabarkan tujuan memperluas ekspor dan memilih impor, meningkatkan investasi keluar dan masuk, mempromosikan penggunaan internasional renminbi (RMB), dan meningkatkan peran China dalam tata kelola ekonomi global.

Pemerintah China sedang berusaha untuk memperluas perdagangan antar regional dan internasional melalui penciptaan megaregion Beijing-Tianjin-Hebei, Sabuk Ekonomi Yangtze, dan inisiatif Satu Sabuk, Satu Jalan. Demi kelancaran tujuan industri dan ekonomi China yang lebih luas, FYP ke-13 juga berjanji untuk melonggarkan pembatasan investasi asing di sektor-sektor tertentu seperti perawatan lansia, perbankan, dan keuangan, dan mendorong impor teknologi dan peralatan canggih serta produk konsumen berkualitas tinggi.

5. Pertumbuhan inklusif

Pemerintah China mengejar pertumbuhan inklusif untuk semua warga negara China dengan menetapkan target untuk mengentaskan kemiskinan, meningkatkan standar hidup, meningkatkan aksesibilitas dan keterjangkauan layanan kesehatan dan layanan sosial lainnya, dan mempromosikan pendidikan.

Keberhasilan pemerintah dalam mengatasi tantangan struktural China dan memastikan kemakmuran jangka panjang dan pertumbuhan ekonomi melalui FYP ke-13 sangat bergantung pada kemampuan pemerintah untuk membuat *tradeoff* yang memerlukan peran pasar yang lebih besar, mengatasi kepentingan yang mengakar, dan menarik pendanaan baru dari sektor swasta. Jika diterapkan, transisi China menuju konsumsi domestik yang lebih besar dan pertumbuhan ekonomi yang lebih didorong oleh pasar dapat membuka peluang bagi bisnis selama pemerintah China mengizinkan mereka mengakses pasar. Namun, kebijakan ini turut memiliki

resiko kegagalan apabila pemerintah China gagal menerapkan reformasi yang diperlukan dapat menyebabkan stagnasi ekonomi China, dengan dampak negatif bagi pertumbuhan ekonomi global. Selain itu, ketergantungan China yang berkelanjutan pada pertumbuhan ekonomi yang dipimpin oleh negara daripada pertumbuhan berbasis pasar yang lebih merupakan tantangan yang cukup besar bagi perusahaan-perusahaan Amerika Serikat yang menghadapi persaingan dari perusahaan-perusahaan China di China dan luar negeri.¹²⁴

5.2 Keunggulan *Cyberpower* China dan Amerika Serikat

Sebagai negara dengan warisan pengalaman yang panjang, Amerika Serikat secara mandiri lebih memiliki manajemen jaringan yang canggih, sejalan dengan praktik global meski Amerika Serikat memiliki perangkat keras dan lunak yang heterogen.¹²⁵ Pengalaman perjalanan pemeliharaan pusat data yang ter-instrumentasi dengan baik dan dapat menjangkau serta berjalan diberbagai kondisi menjadi keunggulan bagi kekuatan *cyber* Amerika Serikat. Kondisi ini tentu berbeda dengan China yang lebih terlambat dalam mengamankan posisi jaringannya dalam kancah global. Bayang-bayang dominasi jaringan Amerika Serikat akan terus menghampiri dan membatasi keleluasaan jangkauan China.

Meski demikian, dibandingkan dengan Amerika Serikat, China dalam beberapa waktu terakhir telah bekerja secara lebih terfokus untuk menciptakan strategi siber nasional yang terintegrasi, dan terkoordinasi melalui tindakan dan infrastruktur

¹²⁴Ibid.

¹²⁵Eric Heginbotham, et all. "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities." (California: RAND, 2015), hal 279.

pemerintah, militer, industri, dan pendidikan. China bahkan mendirikan Pangkalan Keamanan Informasi PLA yang tersentralisasi, dan dinyatakan berperan sebagai pertahanan siber, di dalam Markas Besar Staf Umum. Divisi ini bahkan dekat dengan para pembuat keputusan negara Jaringan nasional China dan sangat mirip dengan intranet nasional yang kemudian membagi lagi jaringan untuk pemerintah, komersial/swasta, dan penggunaan akademis.¹²⁶ China memiliki infrastruktur fisik, baik secara langsung atau dalam kemitraan dengan perusahaan swasta, dan mengontrol gerbang nasional ke Internet global. China juga memiliki sistem penyaringan konten yang berkembang dengan baik yang disebut 'Tembok Siber Hebat' atau “Great Wall China”. Secara sederhana China memiliki kemampuan untuk memantau dan mengontrol informasi yang masuk dan keluar negaranya bahkan mematikan aliran data yang dianggap sebagai sebuah ancaman.

Kemampuan China dalam memantau dan mengontrol jaringan informasi negara tentu menjadi nilai tambah bagi China dibandingkan dengan Amerika Serikat. Jika diperhatikan lebih mendalam, saat ini kepemilikan dan kendali banyak elemen inti infrastruktur internet global misalnya, kabel bawah laut serat optik, jaringan pengiriman konten (CDN), nomor sistem otonom (ASN), dan titik pertukaran internet (IXPs), sangat tersebar ke seluruh dunia, terutama Eropa dan BRICS (yaitu, Brasil, Rusia, India, China, dan Afrika Selatan). Hal ini mencerminkan fakta bahwa sebenarnya semakin banyak multipolar yang muncul dalam koneksi internasional dan secara tidak langsung menunjukan bahwa kedudukan Amerika Serikat

¹²⁶Loc.Cit., Colonel Jayson M. Spade, “China’s *Cyberpower* and America’s National Security.”, hal 38.

mengalami kemerosotan sementara.¹²⁷ Kondisi menjadi peluang bagi China dalam persaingan *cyber* dengan Amerika Serikat. Bagaimana dan apakah China mampu meningkatkan kemampuannya dapat menuntun negara tersebut kepada kondisi yang lebih tinggi.

5.3 Persaingan *Cyberpower* China dan Amerika Serikat

Cyberspace atau dunia maya merupakan sebuah domain fisik dan virtual. Bagian fisiknya adalah jutaan teknologi informasi dan komunikasi jaringan yang diaktifkan melalui berbagai perangkat baik komputer, server, router, prosesor, satelit, saklar, dan kabel. Sementara bagian virtual dibentuk oleh koneksi elektronik dan data yang dikirim atau disimpan dalam potongan-potongan infrastruktur fisiknya. Secara global data-data tersebut kemudian akan ditransmisi, disimpan dan dijaga oleh pemerintah, baik data publik dan swasta. Namun, perkembangan teknologi yang semakin cepat dan pesat saat ini nyatanya berhasil melampaui batas-batas organisasi dan geopolitik. Hal inilah yang pada akhirnya menjadikan sebuah data menjadi rentan untuk diakses oleh pihak lain.

Dalam catatan sejarah, persaingan antara China dan Amerika Serikat merupakan sisa permusuhan Perang Dingin. Persepsi diri China sangat dipengaruhi oleh sejarah dan peradaban kunonya, mendahului Amerika Serikat dalam waktu ribuan tahun. Sebagai negara-bangsa tertua di dunia, mereka sangat sensitif terhadap kritik atau campur tangan dari luar. Sementara posisi Amerika Serikat sebagai pemenang tunggal dalam Perang Dingin dan menjadikan negara tersebut

¹²⁷ Loc.Cit., Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure", hal 229.

memiliki *hegemony* yang kuat selama bertahun-tahun menjadikan China merasa tidak aman akan posisinya. Adanya persaingan akan jati diri dan pengakuan akan status negara menjadikan persaingan keduanya semakin meningkat dan terus berlanjut. Sejalan dengan perkembangan zaman permusuhan Amerika Serikat dan China di dunia maya telah menjadi isu yang menonjol dalam hubungan bilateral kedua negara.

Bagi China prioritas utama dalam strategi *cyber* adalah kepentingan untuk mewujudkan stabilitas sosial dan nasional keamanan. Kedua hal tersebut merupakan dua point utama kepentingan China terkait kebijakan yang dibelakukannya. Sementara pada saat yang sama, China berusaha memegang kontrol atas akses kepada jaringan informasi yang dimilikinya.¹²⁸ Hal ini merupakan bagian dari sebuah proses yang telah lama dilakukan oleh China sejak negara tersebut didirikan. Oleh karena itu, China membutuhkan lingkungan internasional yang dapat memberikan jaringan informasi bagi perkembangan *cyber* mereka. China akhirnya mengambil langkah-langkah terkait dengan strategi internasional dengan memasukan perkembangan *cyber* dalam sektor ekonomi. Hal ini diupayakan China untuk memperoleh keuntungan dari sisi ekonomi dibandingkan sisi militer. Hal ini dikarenakan strategi militer akan yang berpotensi untuk membuat negara lain waspada dan merasa terancam. Sementara ekonomi, secara perlahan dapat menunjang pertumbuhan dan perkembangan China dalam

¹²⁸Op.Cit., Dewi Triwahyuni, Yayan Mochamad Yani, and Arry Bainus, Dampak Pembangunan Cyberpower Tiongkok terhadap kepentingan Amerika Serikat”, hal 303.

sektor lain, karena tidak menuntup kenyataan bahwa untuk melakukan modernisasi militer haruslah ditunjang oleh pendaan yang kuat.

Sementara bagi Amerika Serikat, dunia maya atau *cyberspace* adalah dunia yang sangat penting di semua sektor masyarakat Amerika. Baik di pemerintahan, perdagangan, akademisi, dan sektor kehidupan swasta, dunia maya di Amerika Serikat telah mendukung ratusan triliun transaksi. Layanan jaringan listrik, sistem air, layanan kesehatan, penegakan hukum, dan panggilan darurat hanyalah salah satunya beberapa peran penting dunia maya bagi warga. Sementara itu, komunikasi, penelitian dan pengembangan, kolaborasi lembaga pendidikan dan sektor swasta, militer komando dan kontrol, pekerjaan intelijen, dan pemerintahan pekerjaan administrasi adalah peran penting dari dunia maya untuk pemerintah Amerika Serikat. Sama seperti China, dunia maya sangat penting dalam jaringan global United Militer negara, baik dari percakapan sehari-hari hingga masalah operasi militer.

The White House sendiri mengkategorikan keamanan siber dalam lima tingkat ancaman, yaitu ancaman terhadap usaha kecil atau pengguna rumahan, ancaman terhadap perusahaan besar, ancaman terhadap yang penting sektor dan infrastruktur (seperti pemerintah atau universitas), ancaman terhadap isu-isu nasional dan kerentanan memiliki implikasi di tingkat nasional, serta ancaman yang potensi untuk menyentuh tingkat global. Semua ancaman di lima level dimungkinkan karena jaringan yang saling berhubungan. Amerika Serikat melihat bahwa berbagai serangan *Cyber* yang dilakukan oleh China merupakan upaya negara tersebut untuk

mengganggu akses ke server Amerika Serikat atau merusak file data yang diperlukan.¹²⁹

Menurut Li Zhang, *Director of Institute of Information and Social Development Studies at the China Institutes of Contemporary International Relations (CICIR) Beijing*, terdapat sejumlah faktor penting terkait kemampuan *cyberpower*, yaitu :¹³⁰

1. Kemampuan Internet dan Teknologi Informasi (IT)

Suatu negara harus mampu melakukan inovasi kemampuan untuk mempromosikan dan menerapkan kemampuan ini ke industri, dan kemampuannya untuk menggunakan teknologi ini untuk mengubah industri.

2. Kemampuan IT Industri

Suatu negara haruslah memiliki kemampuan memimpin industri IT. Saat ini industri IT sangat memonopoli aplikasi dan layanan terkait. Hal ini dikarenakan arah pembangunan ke depan adalah monopoli arus informasi global. Sejalan dengan perkembangan maka industri pun akan turun berkembang, dan teknologi diperlukan untuk menciptakan kemudahan dan efisiensi dalam industri.

3. Kemampuan Pasar Internet

¹²⁹Op.Cit., Eric Heginbotham, "Scorecard 9: U.S. and Chinese *Cyberwarfare* Capabilities.", hal 260.

¹³⁰Li Zhang, "A Chinese Perspective On War", *International Review of the Red Cross*, Vol. 94, No 886, (Cambridge: International Review of the Red Cross, 2012), hal 3.

Hal ini bergantung pada ukuran dan skala infrastruktur internet domestik suatu negara, tingkat keterpaduan infrastruktur IT, jumlah pengguna internet, jumlah komputer yang dimiliki, dan sebagainya. Semakin baik keterpaduan infrastruktur maka semakin baik buat jaringan internet yang terbentuk.

4. Pengaruh Budaya Internet

Hal ini bergantung pada apakah bahasa nasional adalah bahasa yang umum digunakan di Internet atau apa bahasa situs web pilihan di negara tersebut, apa kontennya, jumlahnya, dan kualitas website negara, bagaimana tingkat pengaruh website negara baik domestik maupun internasional, dan sebagainya.

5. Kemampuan Diplomasi/Kebijakan Luar Negeri Internet

Faktor ini mempertimbangkan sejauh mana melalui metode seperti memerangi kejahatan internet, membangun jaringan generasi berikutnya, dan menetapkan nama domain, suatu negara dapat menggunakan pengaruhnya untuk memainkan peran utama dalam administrasi internasional internet.

6. Kekuatan Militer Dunia Maya

kekuatan *cyberpower* militer negara harus mampu mempertahankan infrastruktur IT nasional dan militer utama dari serangan. Selain itu, *cyber* militer negara harus memiliki kemampuan pencegahan dan ofensif jaringan

termasuk kemampuan untuk mencuri rahasia dan mencegah orang lain mencuri rahasianya.

7. Kepentingan nasional dalam Mengambil Bagian dalam Strategi Dunia Maya

Tidak cukup bahwa suatu negara hanya memiliki sebagian atau seluruh kemampuan yang disebutkan di atas. Selain itu, kekuatan siber suatu negara sangat bergantung pada ada atau tidaknya keinginan untuk memiliki dan menggunakan kekuatan tersebut.

Pada akhirnya adanya perbedaan penafsiran dan kepentingan masing-masing negara menjadikan persaingan *cyberpower* menjadi tidak terelakan. Semakin berkembang dan agresifitas *cyberpower* China secara nyata menkhawatirkan Amerika Serikat. Sementara dominasi *cyber* dan teknologi Amerika Serikat secara tidak langsung menciptakan kekhawatiran bagi China. Dinamika persaingan *cyber* pun menjadi pasang surut. Namun satu hal yang jelas bahwa ketika sebuah negara berusaha mempelajari kemampuan negara lain dalam perang dunia maya maka, negara tersebut juga harus mempertimbangkan bagaimana *cyberpower* negara tersebut.

Persaingan *cyberpower* yang terjadi merupakan realitas yang tidak dapat ditapikan dalam dinamika hubungan internasional. Perang informasi menjadi strategis perang yang berasal dari esensi Sun Tzu dan Clausewitz karena merupakan jenis perang yang mampu memaksa musuh untuk melakukan kehendak lawan dengan menginduksi kelumpuhan strategis untuk mencapai tujuan yang diinginkan

dan perebutan ini dilakukan dengan hampir tidak ada penerapan kekuatan fisik.

¹³¹Persaingan yang terjadi diantara kedua negara tersebut berada dalam satu kompetensi di level yang sama. Dimana baik Amerika Serikat dan China berusaha mengungguli pesaingnya untuk meraih kemenangan yang lebih tinggi. Oleh karenanya perlu pemahaman dan pengembangan secara seksama dan menyeluruh diseluruh sektor kehidupan sehingga salah satu negara tersebut dapat bertahan dan muncul sebagai pemenang kompetensi.

5.3.1 *Cyberpower* Sektor Ekonomi

Sebagaimana yang telah dipaparkan sebelumnya bahwa sebagai negara hegemon Amerika Serikat tentu harus merespon kemajuan teknologi informasi global untuk mengamankan posisi mereka. Amerika Serikat membuat perusahaan multinasionalnya untuk dapat masuk ke pasar China. Amerika Serikat sendiri diketahui memiliki keunggulan dalam teknologi perangkat lunak. Sementara China mencoba mengangkat pasar internal dengan mempromosikan penggandaan standar teknis dalam produk China untuk menyenangkan perusahaan domestiknya sendiri. Pemerintah China berusaha membuat perusahaan dalam negeri mereka dapat bersaing dengan hegemoni perusahaan milik Amerika Serikat.¹³²

Melalui berbagai upaya yang dilakukan China, pemerintah China setidaknya berhasil membuat perusahaan China mampu bersaing dalam masalah hardware, meskidemikian dalam sektor software Amerika Serikat masih lebih

¹³¹Christian Czosseck , and Kenneth Geeres, *The Virtual Battlefield: Perspectives on Cyber Warfare*, (Amsterdam: IOS Press BV, 2009), hal 15.

¹³²Op.Cit., Dewi Triwahyuni, Yanyan Mochamad Yani, Arry Bainus, Dampak Pembangunan *Cyberpower* Tiongkok terhadap kepentingan Amerika Serikat”, hal 304.

unggul. Perangkat keras seperti router dari Huawei, ponsel Xiaomi, dan ponsel ZTE dapat menarik minat masyarakat cukup tinggi. Tetapi untuk dapat menang di pasar perangkat lunak, China harus memiliki kemampuan untuk menemukan dan memperbarui perangkat di komputer, sementara dalam hal penelitian dan pengembangan, perusahaan Amerika Serikat memiliki anggaran yang lebih besar dan masih memegang dominasi global yang kuat. Selain itu, dominasi yang telah lebih dulu ada bagi perangkat lunak Amerika Serikat menjadikan sulit bagi China untuk menlampau pasar tersebut.

Pemerintah China menyadari bahwa industri berat dan manufaktur kelas bawah tidak dapat menciptakan mesin pertumbuhan yang berkelanjutan maupun pekerjaan yang sesuai dengan angkatan kerja China yang semakin terdidik dan terampil. Oleh karenanya, sebagai penegasan The 13th Five-Year Plan, pemerintah China menegaskan kembali dukungannya untuk inisiatif Made in China 2025 (中国制造 2025 atau zhongguo zhizao) dan “Internet Plus” (互联网+; hulianwang). Inisiatif ini diupayakan untuk mempercepat transisi China ke manufaktur cerdas yang bernilai tambah lebih tinggi dengan berfokus pada inovasi dan meningkatkan industri yang sedang berkembang, seperti peralatan kelas atas, sirkuit terpadu, biomedis, komputasi awan, Internet seluler, dan e-commerce.¹³³

Untuk mendukung sektor-sektor ini, pemerintah China cukup memiliki juara lokal dan nasional, menegosiasikan transfer teknologi sebagai harga akses pasar, mengatur investasi asing dan impor teknologi melalui katalog pemerintah,

¹³³Op.Cit., Katherine Koleski, “The 13th Five-Year Plan”, hal 9.

mempromosikan standar teknologi China di dalam negeri dan internasional, dan mendukung ekspor China yang lebih besar melalui “Going Out Strategy”. Dalam kebijakan Made in China 2025, pemerintah China memfokuskan 12 target utama dengan tenggat waktu 2020 dan 2025 yang berfokus pada peningkatan inovasi, produktivitas, kualitas, digitalisasi, dan efisiensi China.

Tabel 5.3.1.1 Made in China 2025 (2020 and 2025 Target)

Target	2015 (Actual)	2020	2025
R&D spending as a share of operating revenue	0.95%	1.26%	1.68%
Number of patents per 100 million RMB of total revenue	0.44	0.7	1.1
Quality competitiveness index*	83.5	84.5	85.5
Growth of industrial value-added	5.9%	7.9%	9.9%
Average annual productivity growth	6.6%	7.5%	6.5%
Penetration of broadband internet	50%	70%	82%
Use of digital design tools in R&D	58	72	84
Use of numerical control machines in key production processes	33	50	64
Change in industrial energy intensity from 2015 levels	—	-18%	-34%
Change in carbon dioxide emissions intensity from 2015 levels	—	-22%	-40%
Change in water usage intensity from 2015 levels	—	-23%	-41%
Reuse of solid industrial waste as a share of total waste	65%	73%	79%

Catatan*: Indeks ini meninjau pelaksanaan manajemen mutu dan pengawasan dan peningkatan mutu yang direncanakan berdasarkan data dari 250.000 perusahaan.

Sumber: Gov.cn

Berdasarkan data tahun 2015 tampak bagaimana pemerintah China berusaha menetapkan targetnya untuk kemajuan China pada 2020 dan 2025. China sendiri

diketahui selalu melakukan review dan analisis terkait pertumbuhan nasionalnya setiap lima tahun sekali. Jika merujuk pada FYD ke -13 maka tampak pemerintah China menargetkan sebesar 72% penggunaan digital desain bagi research and developmentnya. Hal ini sejalan dengan keinginan China untuk memajukan industrinya menjadi lebih berteknologi.

Sementara itu, dalam kebijakan Made in China 2025 pemerintah China telah menetapkan sepuluh sektor utama perkembangan sebagai berikut :¹³⁴

Gambar 5.3.1.2 10 Sektor arget perkembangan China

Made in China 2025 (2015)	Strategic Emerging Industries (2010)	Strategic Industries (2006)	Heavyweight Industries (2006)
(1) New energy vehicles	(1) Clean energy technologies	(1) Armaments	(1) Machinery
(2) Next-generation IT	(2) Next-generation IT	(2) Power generation and distribution	(2) Automobiles
(3) Biotechnology	(3) Biotechnology	(3) Oil and petrochemicals	(3) IT
(4) New materials	(4) High-end equipment manufacturing	(4) Telecommunications	(4) Construction
(5) Aerospace	(5) Alternative energy	(5) Coal	(5) Iron, steel, and nonferrous metals
(6) Ocean engineering and high-tech ships	(6) New materials	(6) Civil aviation	
(7) Railway	(7) New energy vehicles	(7) Shipping	
(8) Robotics			
(9) Power equipment			
(10) Agricultural machinery			

Source: Gov.cn

Gambar diatas menunjukan bagaimana perbandingan sektor-sektor yang menjadi fokus China untuk mengembangkan *cyberpower*nya. Pada dasarnya banyak dari sektor baru dalam kebijkana Made in China yang merupakan pengembangan dari industri strategis yang telah lama dipegang China. Misalnya, sektor pengembangan IT generasi berikutnya yang sebernarnya telah ada sebagai industri baru yang strategis pada tahun 2010 dan industri kelas berat pada tahun

¹³⁴Ibid., hal 9.

2006. Hanya saja pengembangan dalam Kebijakan Made in China lebih terfokus pada kemampuan *cyber*. Melalui pengembangan yang terfokus ini, industri manufaktur China berhasil tumbuh lebih kuat, dan “Made in China” dapat dilihat dimana-mana.¹³⁵

Sebagaimana yang diketahui kemunculan China sebagai kekuatan ekonomi dunia merupakan kenyataan yang tidak dapat dipungkiri oleh negara manapun termasuk Amerika Serikat. Sejak 1978, China telah bertransformasi menjadi sebuah negara dengan 2 sistem yaitu secara politik tetap berideologikan komunis namun secara ekonomi menjadi kapitalis atau sistem sosialisme pasar. Pemerintah China menjadi lebih terbuka terhadap barat dan internasional dan hal ini menjadi salah satu penyebab meningkatnya ekspor China. Keikutsertaan dan keaktifan China ekonomi global terbukti dari beberapa perusahaan China yang mulai prestasi sebagai perusahaan kelas satu dunia. Salah satu contohnya Huawei. Dalam laporan tertulis majalah *The Economist* menyajikan fakta perusahaan Huawei asal China berhasil menggeser posisi *Errisson Swedia* sebagai perusahaan pembuat perkakas telekomunikasi terbesar di dunia dan menjadikan Huawei sebagai pemain global.

Keberhasilan Huawei kemudian disusul oleh perusahaan China lainnya seperti *Lenovo* yang berhasil menantang *Hewlett Packard* sebagai produsen PC terbesar. Huawei nyatanya berhasil menjadi standar perusahaan China untuk menguasai barat. Keberhasilan Huawei sendiri diklaim karena keberaniannya dalam memasarkan produk berkualitas dengan harga murah. Huawei secara bertahan

¹³⁵Qunhui Huang, *Understanding China's Manufacturing, Industry*, (Beijing: Chinese Academy of Social Sciences, 2022), hal 1.

berhasil membentuk jaringan internasional. Secara perlahan Huawei berhasil membangun 20 pusat penelitian dan pengembangan di mancan negara seperti China, AS, Jerman, Swedia, India, Rusia dan Turki.¹³⁶

Keberhasilan Huawei untuk mengembangkan fitur-fitur canggih dalam produk handphonenya berhasil menarik minat pasar dalam hal komunikasi terutama dunia maya. Huawei berhasil memberikan kemudahan pengguna layanan internet. Huawei pun berhasil masuk dan beredar luas dalam pasar Amerika Serikat ini. Bahkan berkat keberhasilan Huawei di pasar Amerika Serikat, Huawei berhasil melakukan banyak kerjasama dengan perusahaan domestik Amerika Serikat dan melakukan merger serta akuisisi di Amerika Serikat. Hasilnya, banyak dari perusahaan swasta di Amerika yang menggunakan produk telekomunikasi Huawei termasuk produksi Handphone Huawei yang berhasil menyaingi kecanggihan smartphone Apple buatan Amerika Serikat.

Meskipun demikian dibalik keberhasilan Huawei di pasar Amerika Serikat nyatanya memberikan pandangan lain bagi negeri paman Sam tersebut. Amerika Serikat nampaknya belum dapat percaya sepenuhnya terhadap teknologi yang dimiliki Huawei. Selain adanya perbedaan ideologi, hubungan kedua negara turut diwarnai dengan rasa saling curiga dan tuduhan akan kejahatan dan pelanggaran kepada negara lawan. Hal ini nyatanya berimbas bagi perusahaan Huawei. Pemerintah Amerika Serikat melihat Huawei sebagai perusahaan pemerintah China

¹³⁶Renne R.A Kawilarang, "Huawei, ZTE, dan Tuduhan Spionase Paman Sam." Last update 10 Oct 2012. Diakses pada 3 July 2022. <https://www.viva.co.id/ragam/fokus/358320-huawei-zte-dan-tuduhan-spionase-paman-sam>

yang memiliki misi memata-matai Amerika Serikat melalui jaringan internet. Pemerintah Amerika Serikat melihat pemerintah China menjalankan kebijakan nasional pengintaian dunia melalui *cyber*. Huawei dianggap sebagai salah satu wadah China untuk mengumpulkan informasi sistem telekomunikasi Amerika Serikat kepada pemerintah China. Meskipun Huawei membantah tuduhan tersebut namun nyatanya Amerika telah menetapkan sikap untuk memblokir Huawei dari pasar Amerika Serikat.

Sikap yang dilakukan Amerika Serikat bagi China dinilai sebagai persaingan tidak sehat karena pemerintah tersebut melarang Huawei untuk berkembang di negara tersebut dengan alasan keamanan nasional. Tunduhan Amerika Serikat dianggap tidak mendasar dan mengabaikan realitas teknis dan dagang. Meski demikian dalam investigasi Kongres yang dilakukan Amerika Serikat mengatakan bahwa mereka memperoleh dokumen yang diberikan oleh mantan pegawai perusahaan. Dalam dokumen tersebut dikatakan bahwa Huawei memberikan "layanan jaringan khusus" kepada sebuah divisi di militer China yang sering disebut sebagai "unit khusus perang siber".¹³⁷ Hal inilah yang menjadikan Amerika Serikat bersikap skeptis terhadap Huawei.

Pada 13 Agustus pemerintah Amerika dibawah pemerintahan Presiden Donald Trump secara resmi melarang pemerintahnya menggunakan produk telekomunikasi Huawei dan beberapa perusahaan China lainnya. Hal ini secara resmi menjadika Huawei dalam daftar hitam perdagangan Amerika Serikat.

¹³⁷Viva.Co.Id, "AS Tuduh Huawei dan Alat Mat-mata China", Last update 8 Oct. Diakses 5 July 2022.<https://www.viva.co.id/berita/dunia/357663-as-tuduh-huawei-dan-zte-alat-mata-mata-china>

Larangan tersebut turun menjadi bagian dari Undang-Undang Otorisasi Pertahanan.¹³⁸ UU ini bukan hanya mencakup peralatan dan layanan telekomunikasi saja, apa pun yang dianggap "substansial", "penting" atau "kritis" akan dilarang termasuk layanan jaringan dan ponsel cerdas dari negeri tirai bambu tersebut. Akibat larangan ini Huawei diblokir sehingga tidak dapat menyertakan perangkat lunak dan layanan Google dengan ponsel Android-nya melalui Google.

Amerika Serikat yang sudah lebih dulu mapan dalam kemampuan ekonomi hingga menjadikannya disegani tentu berusaha mempertahankan pengaruhnya pada sistem ekonomi internasional untuk terus menghasilkan pundi-pundi bagi Amerika Serikat. Status tersebut menjadikan Amerika Serikat akan melakukan apapun dan tidak memberikan kesempatan bagi negara lain untuk melawa Amerika Serikat termasuk China. Peristiwa pemblokiran Huawei menjadi contoh bagaimana persaingan pengembangan teknologi di sektor ekonomi dapat memaksa suatu negara untuk mengambil sikap. Ketika Huawei tengah berkembang pesat di pasar telekomunikasi Amerika Serikat, negara tersebut justru dianggap sebagai ancaman bagi keamanan nasional. Amerika Serikat memainkan pengaruh dan dominasi atas perangkat lunaknya hingga akhirnya Huawei tidak bisa beroperasi.

Sebernarnya baik Amerika Serikat dan China telah sejak lama berkerjasama namun nyata beberapa hal sensitif seringkali mewarnai hubungan kerjasama keduanya. Perkembangan ekonomi China secara tidak langsung telah menciptakan

¹³⁸Ivan P. "AS Bersiap Larang Penggunaan Teknologi Huawei dan ZTE". Last updated 15 Aug 2018. Diakses 15 Jul 2022.<https://beritagar.id/artikel/sains-teknologi/as-bersiap-larang-penggunaan-teknologi-huawei-dan-zte>

kekhawatiran Amerika Serikat atas manipulasi mata uang China. Hal ini tampak dari besarnya devisa US Dollar yang dimiliki China dan bagaimana China mulai menyebarkan luaskan mata uang Yuan yang dimilikinya sebagai transaksi internasional. Selain itu Amerika Serikat melihat semakin aktifnya China dalam pasar global memberikan dampaknya terhadap ekonomi mereka yaitu kekhawatiran bahwa China akan memblokir partisipasi Amerika Serikat dalam kelompok ekonomi Asia-Pasifi, dan kegelisahan umum tentang pertumbuhan kehadiran China di Afrika dan Amerika Latin.¹³⁹

Keberlangsungan industri dan perusahaan sektor swasta tidak terlepas dari keamanan siber. Dalam perjalanan transaksi, industri ekonomi turut merancang sistem mereka untuk mencegah terjadinya kejahatan siber, baik oleh pelaku individu, kelompok kepentingan ataupun negara tertentu. Perusahaan menerapkan standar terkait praktik bisnis terbaik untuk menciptakan tingkat keamanan yang dibutuhkan dalam menjamin keamanan bisnis mereka. Dari perspektif sektor swasta, keamanan adalah tanggung jawab mereka, pertahanan adalah tanggung jawab pemerintah.¹⁴⁰

¹³⁹Op.Cit., Colonel Jayson M. Spade, "China's Cyberpower and America's National Security.", hal 16.

¹⁴⁰Niels Nagelhus Schia and Lars Gjesvik, "China's cyber sovereignty Norwegian Institute of International Affairs", *Policy Brief*, Mar, (Oslo: NUPI, 2017) hal 2.

5.3.2 *Cyberpower Sektor Politic Control and Network Protection*

Penggunaan dunia maya akan melibatkan banyak aktor didalamnya, bukan hanya individu sebagai aktor langsung namun juga aktor penting lainnya. Akses informasi dunia maya turut disandingkan dengan istilah kebebasan. Dalam persaingan *cyber*, sulitnya penyelesaian masalah antara China dan Amerika Serikat juga berawal dari istilah kebebasan yang memiliki perbedaan pemahaman dan praktik dari masing-masing negara. Jika umumnya kebebasan dilihat sebagai kebebasan individualistis, yang menekankan pada kebebasan pengguna selama tidak membahayakan pengguna lain. Kebebasan di sini juga dapat diartikan dalam konteks masyarakat, dimana setiap masyarakat haruslah menyesuaikan diri dengan kerangka aturan dan norma tertentu. Kebebasan juga dapat dilihat dalam konteks negara atau perusahaan, yaitu bagaimana negara mengontrol jaringan internet informasi yang keluar dan masuk negaranya. Umumnya negara akan memblokir konten pornografi atau pemikiran radikal, misalnya, atau perusahaan menggunakan internet untuk kepentingan ekonominya.¹⁴¹

China dikenal sebagai negara yang memiliki proteksionisme yang kuat terhadap penggunaan internet. Pemerintah memiliki wewenang yang besar dalam mengontrol aliran data yang masuk dan keluar. Sebagaimana yang diketahui bahwa Pemerintah China turut melibatkan *non-state actor* dalam upaya pengembangan *cyber*nya. Namun, pemerintah China tetap melakukan pengendalian jaringan komputer negara. Hal ini dikarenakan masih adanya kekhawatiran bahwa

¹⁴¹Op.Cit., Dewi Triwahyuni, Yayan Mochamad Yani, and Arry Bainus, Dampak Pembangunan Cyberpower Tiongkok terhadap kepentingan Amerika Serikat”, hal 305.

hacktivisme dapat berbalik melawan Partai. Penguatan berulang-ulang di China atas undang-undang anti-peretasan domestiknya menunjukkan bahwa negara tersebut memiliki kekhawatiran atas kemampuan pada populasi independen peretas.¹⁴²

Kebijakan *The Great Wall* yang dijalankan oleh China menunjukkan upaya China untuk menunjukan indikator lain tingkat kompetensi didalam dunia maya. Pengguna internet di China menggunakan berbagai metode, termasuk jaringan pribadi virtual (VPN), situs cermin dari halaman yang diblokir yang dimiliki oleh layanan komputasi asing, dan layanan proxy sederhana.¹⁴³ Pembatasan akses jaringan menjadi kebijakan yang dilakukan China meminimalisir kebocoran data akibat kemudahan akses jaringan. Sekali lagi, pemerintah China memiliki kontrol jaringan yang kuat untuk akses informasi warga negaranya.

Tujuan utama dari kontrol ini adalah penyensoran yaitu membatasi paparan warga China terhadap "ide borjuis-liberal" dan "anti-sosialis"¹⁴⁴ China berusaha mengkombinasikan pemantauan jaringan untuk membentuk garis pertahanan yang dapat dikendalikan pemerintah. Ketika pemerintah Amerika Serikat menolak untuk mengatur keamanan jaringan internal yang tidak terlepas dari kebebasan dan liberalism yang dijunjungnya. Hal ini berbeda dengan pemerintah China yang mengamankan dan memberlakukan langkah-langkah pengamanan Internet yang ketat dengan memasukkan peraturan tentang perangkat keras dan perangkat

¹⁴²Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security." hal 22.

¹⁴³Op.Cit., Eric Heginbotham, Scorecard 9: U.S. and Chinese *Cyberwarfare* Capabilities." , hal 259.

¹⁴⁴Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 39.

lunak¹⁴⁵ Bahkan pada akhir Desember 2016, CAC (Cyberspace Administration of China) mempresentasikan strategi baru untuk keamanan siber. Ini termasuk peringatan bahwa penggunaan internet untuk 'pengkhianatan, pemisahan diri, pemberontakan, subversi atau mencuri atau membocorkan rahasia negara akan dihukum', juga memperingatkan terhadap siapa pun yang bekerja dengan kekuatan luar yang mencoba untuk menumbangkan otonomi China.¹⁴⁶

Apa yang disebut 'kebebasan internet' Barat sebenarnya adalah jenis hegemoni dunia maya yang diberlakukan oleh Amerika Serikat. Di era informasi, merebut dan mempertahankan keunggulan di dunia maya lebih penting daripada merebut komando laut dan udara pada Perang Dunia II.¹⁴⁷ Amerika Serikat melalui pengaruhnya berusaha untuk menyebarluaskan paham kebebasannya agar diakui dan disetujui oleh banyak negara lain. Kondisi ini tentu sangat berkebalikan dengan yang ada di China dimana segala aktivitas dan jaringan internet disana sangat dibatasi dan diawasi oleh pemerintah.

Bagi China internet disatu sisi dianggap sebagai ancaman besar bagi stabilitas negara, tetapi juga diperlukan untuk tujuan pembangunan negara tersebut. Mencapai keseimbangan yang tepat antara keterbukaan dan represi adalah masalah yang rumit. Salah satu cara utama China mencoba untuk menyeimbangkan kedua kekhawatiran ini adalah dengan mempromosikan perusahaan domestik dan

¹⁴⁵Ibid.

¹⁴⁶Ibid. Niels Nagelhus Schia and Lars Gjesvik, "China's cyber sovereignty Norwegian Institute of International Affairs", hal 2.

¹⁴⁷Loc.Cit., Tobias Feakin, *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities*, hal 2.

memberi mereka saham dalam rezim.¹⁴⁸ Avery Goldstein dalam bukunya yang berjudul *Rising to the Challenge : China's Grand Strategi and International Security*, memberikan gambarannya tentang bagaimana China kontemporer di seluruh dunia. Avery berpendapat bahwa, kunci untuk memahami implikasi peningkatan ekonomi dan kapabilitas militer, serta motivasi diplomatik dan kebijakan luar negeri China dan bagaimana dunia (khususnya Amerika Serikat) untuk merespon “grand strategi” China ini.¹⁴⁹

Adanya perbedaan pandangan terkait kebebasan internet menunjukan bahwa negara memainkan doktrin dalam kebijakan politiknya. Doktrin sendiri merupakan komponen penting dari kekuatan *cyber* suatu negara. Ini tidak hanya menunjukkan kepentingan relatif dari operasi dunia maya, tetapi juga dapat memberikan petunjuk tentang keefektifannya.¹⁵⁰ Sejak dua puluh tahun yang lalu, China telah memperkenalkan konsep *local wars under informationized conditions* atau perang lokal di bawah kondisi informasi. Pemerintah telah menyerukan kekuatan tempur yang mampu memenangkan teknologi tinggi perang modern, dan menyediakan sarana asimetris dimana pihak yang awanya lemah dapat mengalahkan yang kuat.¹⁵¹ Doktrin ini pada akhirnya mendorong para pemimpin China untuk memodernisasi spektrum luas kemampuan perang konvensional. Hal ini nyatanya berlanjut hingga kepemimpinan Xi Jinping.

¹⁴⁸Loc.Cit., Niels Nagelhus Schia and Lars Gjesvik, “China’s cyber sovereignty Norwegian Institute of International Affairs”, hal 2.

¹⁴⁹Op.Cit., Shalendra D.Sharma, *China and India in The Age of Globalization*, hal 213-214.

¹⁵⁰Ibid., hal 272.

¹⁵¹Ibid.

Perbedaan dan keluasan konteks membuat kebebasan berinternet menjadi tujuan yang sangat sulit diwujudkan. Paradigma perang siber yang berbeda antara China dan Amerika Serikat menunjukkan bahwa dunia siber dan karakter bebas yang berbeda menciptakan konflik kepentingan. Meskipun seringkali Amerika Serikat menekan dan berharap China dapat menciptakan nilai demokrasi dan melindungi kebebasan internet di negaranya. Namun, dalam kenyataannya kemajuan teknologi di China tetap berjalan dengan proteksionisme yang kuat oleh pemerintah. Hingga memunculkan anggapan bahwa perkembangan *cyber* China menjadi sebuah kebijakan yang merugikan Amerika Serikat. China mampu meretas situs militer, situs ruang publik dan situs perusahaan multinasional dan mencuri data penelitian dari sana. Data tersebut kemudian digunakan untuk mengembangkan perusahaan domestik di China.

Sementara Amerika Serikat sendiri lebih terbuka akan kebebasan internet warganya. Hal ini terlihat dari mudahnya akses jaringan informasi melalui beragam perangkat dan produk telekomunikasi dan teknologi. Hal ini tentu sangat berbeda dengan kondisi yang berada di China. Bahkan untuk mencari informasi mengenai negara tirai bambu tersebut sangat terbatas oleh penggunaan bahasa yang berbeda. Selain memang akses informasi kedalam dan luar telah dibatasi. Hal ini nyatanya menjadi nilai positif dan negatif tersendiri bagi kedua negara. Keterbukaan disatu sisi memang memberika kemudahan akses dan pelayanan bagi masyarakat, namun disisi lain dapat menjadi ancaman kebocoran informasi. Memahami kekuasaan di

era informasi berarti memahami hubungan antara teknologi dan kekuasaan.¹⁵² Jika membandingkan dalam sektor network proteksions maka China dapat dikatakan lebih unggul dibanding Amerika Serikat.

5.3.3 *Cyberpower* Sektor Teknologi dan Informasi

Ketika berbicara mengenai *cyberpower* maka bidang teknologi dan informasi menjadi hal utama yang perlu diperhatikan. Amerika Serikat hingga saat ini diketahui mendominasi dalam hal perangkat lunak. Meskipun disatu sisi China telah membuat kemajuan besar dalam perangkat keras yang dimilikinya seperti Huawei atau pengembangan 5G dan Artificial intelligent (AI) atau penasionalisasi websitenya masing-masing. Namun, perusahaan Amerika Serikat seperti Microsoft, Intel, Google, Facebook, dan Apple masih mendominasi perangkat lunak secara global serta menciptakan standarisasi atas perangkat lunak secara de facto.¹⁵³

Sebagaimana yang telah disebutkan bahwa besarnya dominasi teknologi dan informasi Amerika Serikat nyatanya memicu penolakan dan ketidakpercayaan China. China menyakini bahwa Amerika Serikat memiliki kemampuan untuk merusak atau mengganggu fungsi perangkat apa pun dengan perangkat lunak buatan Amerika Serikat.¹⁵⁴ Termasuk didalamnya memperoleh informasi pribadi dan negara secara menyeluruh melalui jaringan teknologi dan informasi mereka. Selain itu, perusahaan teknologi dominan Amerika Serikat ini sedikit banyak turut

¹⁵²Madeline Carr, *US Power and The Internet In The International Relations*, (New York: Palgrave Macmillan, 2016), hal 182.

¹⁵³Op.Cit., Eric Heginbotham, "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities.", hal 270.

¹⁵⁴Ibid.

mempengaruhi dan bertanggung jawab kepada pemerintah atas pertimbangan negara terkait strategi pertahanan *cyber*.

Oleh karena penolakan dan ketidakpercayaan kepada Amerika Serikat pada akhirnya maka mendorong negara tersebut untuk mengembangkan sistem operasinya sendiri yaitu Kylin. Bahkan system operasi ini turut dipergunakan oleh PLA. Kylin mungkin lebih aman daripada sistem operasi Microsoft yang digunakan di Amerika Serikat. Selain itu senjata *cyber* yang dirancang untuk Linux, UNIX, dan sistem berbasis Windows mungkin tidak bekerja melawan Kylin.¹⁵⁵ Karena system operasi ini tidak terhubung dengan jaringan informasi eksternal, sehingga lebih meminimalisir celah kebocoran data. China berusaha mempersempit kesenjangan dalam teknologi secara keseluruhan.¹⁵⁶

Pada perkembangan konvensional teknologi satelit dipadukan dengan senjata pintar yang dipandu secara presisi yang dapat membantu perencana militer untuk menentukan dengan tepat perkiraan kerusakan dari serangan terhadap penduduk sipil. Kondisi ini tidak berlaku dalam perang dunia maya yang dikenal tidak memiliki batasan wilayah. Tidak seperti senjata konvensional atau nuklir, senjata siber memiliki kemampuan unik untuk replikasi dan diseminasi. Akibatnya, para perencana militer tidak dapat mengetahui sebelumnya skala dan cakupan kehancuran yang ditimbulkan oleh senjata siber. Itu juga merupakan argumen untuk penciptaan aturan baru untuk dunia maya yang mirip dengan perjanjian perlucutan

¹⁵⁵Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 39.

¹⁵⁶Loc.Cit., Eric Heginbotham, "Scorecard 9: U.S. and Chinese *Cyberwarfare* Capabilities.", hal 270.

senjata yang ada untuk senjata konvensional dan nuklir.¹⁵⁷ Peluncuran senjata siber yang menargetkan kemampuan online musuh nyatanya dapat dengan mudah merusak infrastruktur sipil secara tidak terdeteksi.

Selain itu, kaitannya dengan pengembangan *cyberpower*, pemerintah China turut mengembangkan kebijakan “Internet Plus”.¹⁵⁸ Besarnya sumber daya manusia yang tentu menjadi keunggulan tersendiri. Pemerintah China mengoptimalkan manufaktur, keuangan, perawatan kesehatan, dan pemerintahan, rencana Internet Plus ditujukan untuk membangun perusahaan sektor Internet seluler domestik, komputasi awan, data besar, dan Internet of Things di negara itu dan menciptakan pesaing global dengan membantu ekspansi perusahaan domestik di luar negeri.¹⁵⁹ Administrasi Cyberspace China dan Kementerian Keuangan meluncurkan Dana Investasi Internet China senilai \$14,9 miliar (RMB 100 miliar) pada bulan Januari untuk menyediakan investasi ekuitas di perusahaan sektor Internet dan Internet China. The Agriculture Bank of China, China Development Bank, dan Bank Industri dan Komersial China bahkan menyediakan jalur kredit sebesar \$22,4 miliar (RMB 150 miliar) untuk perusahaan yang telah diinvestasikan oleh dana tersebut.¹⁶⁰

China memang sangat mendorong pendanaan bagi pengembangan teknologi perusahaan swasta negaranya, namun hal ini bukan berarti tanpa hambatan. Selain Huawei sebenarnya sudah perusahaan teknologi China yang diberikan sanksi oleh Amerika Serikat yaitu, ZTE. Perusahaan teknologi China ini

¹⁵⁷Loc.Cit., Op.Cit., Sinan Ulgen, *Governing Cyberspace*, hal 62.

¹⁵⁸Loc.Cit., Katherine Koleski, “The 13th Five-Year Plan”, hal 12.

¹⁵⁹Ibid.

¹⁶⁰Ibid.

nyatanya menjadi perusahaan China yang pertama kali dikenakan sanksi tepatnya pada 2017. Menurut Bloomberg, Amerika Serikat menjatuhkan sanksi terhadap ZTE berupa larang pembelian komponen elektronik buatan AS, terutama chip telekomunikasi yang dibuat oleh Qualcomm. Meskipun larangan itu akhirnya dicabut setelah ZTE sepakat membayar denda.¹⁶¹ Belajar dari peristiwa Huawei yang dilarang menggunakan layanan google melalui perangkat Androidnya atau dari peristiwa ZTE yang menggunakan chip telekomunikasi cukup memperlihatkan bahwa perusahaan China masih bergantung pada teknologi buatan Amerika Serikat.

Diketahui hingga saat ini, Amerika Serikat masih menjadi negara pembuat chip terbaik di dunia. China memang sudah berkembang jauh hingga dapat memproduksi banyak elektronik, tetapi tanpa chip dari negara Amerika Serikat ini, produk buatan perusahaan China akan tetap kekurangan kualitas dan standard global. Padahal pada akhir 2018, penjualan Huawei diketahui mampu melampaui penjualan Apple dan menjadi perusahaan pembuat smartphone terbesar kedua di dunia setelah Samsung.¹⁶² Peningkatan China inilah salah satunya menjadi pemikiran Amerika Serikat atas larangan Amerika Serikat kepada perusahaan teknologi China. Larang Amerika Serikat dilakukan lebih kepada upaya Amerika

¹⁶¹Iskandar, "Headline: AS Larang Huawei, Buntut Perang Dagang atau Persaingan Bisnis?." Last updated 22 May 2019. Diakses 20 July 2022. <https://www.liputan6.com/tekno/read/3971492/headline-as-larang-huawei-buntut-perang-dagang-atau-persaingan-bisnis>

¹⁶²Ibid.

Serikat untuk mempersulit China sebagai pesaing utama perusahaan teknologi Amerika Serikat.

Menurut laporan MIT Technology Review, perusahaan teknologi China diketahui tengah berlomba mengembangkan teknologi 5G. Huawei bahkan ingin menjadi andalan Pemerintah China untuk mendominasi jaringan nirkabel supercepat dunia sebagai pembuktian diri sebagai salah satu perusahaan teknologi top di dunia. China yang memiliki ambisi untuk menjadi negara *Superpower* dunia dinilai tentu akan melindungi dan membantu perusahaan ini. Bahkan perusahaan ini digadang-gadang dapat menjadi penguasa 5G dalam 5 tahun ke depan. Namun, dengan dimasukkannya Huawei dalam daftar hitam perdagangan di Amerika Serikat tentu sedikit banyak dapat menurunkan persentasi keberhasilan.

Larangan yang diberlakukan secara otomatis memberikan kesempatan bagi kompetitor lainnya untuk dapat mengembangkan jaringan 5G. Hingga nantinya jaringan ini tidak dikuasai hanya oleh perusahaan China, Huawei. Bagi Amerika Serikat akan sangat berbahaya apabila perusahaan China tersebut berhasil menguasai jaringan 5G. Kekhawatiran ini berkaitan dengan segala kompleksitas dan risiko keamanan yang dibawa oleh perusahaan teknologi China.

Keputusan dan pemikiran Amerika Serikat sebagai negara dominan nyatanya turut mempengaruhi negara lain. Pada 15 Juli 2020, Pemerintah Inggris turut menyatakan melarang pengembangan jaringan 5G oleh Huawei dengan alasan

keamanan Nasional.¹⁶³ China memandang sikap Inggris ini sebagai bentuk dukungan atas sikap yang lebih dulu diambil oleh sekutunya yaitu Amerika Serikat. Sementara itu, Menteri Digital dan Kebudayaan Inggris, Oliver Dowden, mengakui bahwa keputusan yang diambil oleh pemerintahan Inggris memang dipengaruhi oleh sanksi Amerika Serikat. Bahkan, Inggris memberikan izin kepada operator jaringan lain yaitu BT dan Vodafone untuk dapat mengganti semua peralatan 5G dari Huawei hingga 2027. Peristiwa ini menunjukan bahwa pada dasarnya dalam persaingan di level yang sama setiap negara berusaha menciptakan kemajuannya masing-masing

China memang memiliki keunggulan disektor teknologi terlihat dari bagaimana negara tersebut berhasil mengembangkan jaringan 5G. Namun, Amerika Serikat turut memiliki kemampuan untuk mencegah keunggulan China. Selain itu, masih bergantungnya China atas teknologi perangkat lunak dan keras Amerika Serikat turut menunjukan bahwa Amerika Serikat pada kondisi tertentu masih memiliki keunggulannya tersendiri. Kondisi ini membuktikan bahwa dalam persaingan kekuatan tampak nyata dan terlihat. Negara mana yang memiliki comparative lebih tinggi dapat lebih unggul dibanding negara lain.

¹⁶³CNN Indonesia.com, “Inggris Resmi Larang Huawei Kembangkan 5G” Last update 15 July 2020. Diakses 28 July 2022. <https://www.cnnindonesia.com/teknologi/20200715020658-185-524746/inggris-resmi-larang-huawei-kembangkan-5g>

5.3.4 *Cyberpower* dalam Sektor Militer

Keamanan *cyber* haruslah menjadi masalah penting bagi keamanan nasional dan pertahanan negara termasuk perlindungan terhadap kedaulatan teritorial. Karena pemerintah, infrastruktur penting, dan layanan darurat bergantung pada Internet maka, dunia maya tidak dapat dibiarkan begitu saja ketika interaksi kerjasama dan kemitraan antara sektor publik dan swasta berlangsung. Pertahanan membutuhkan cara berpikir baru tentang keamanan infrastruktur siber dan pendekatan yang serupa dimana pemerintah mengawasi keamanan tetapi dalam cakupan yang lebih luas. Sushil Jajodia mengatakan terdapat 7 point cakupan terkait kesadaran situasional *cyber*. **Pertama**, kesadaran akan situasi yang terjadi saat ini; **Kedua**, mewaspadaai dampak serangan *cyber*; **Ketiga**, mewaspadaai bagaimana situasi tersebut berkembang; **Keempat**, mewaspadaai perilaku actor; **Kelima**, menyadari mengapa dan bagaimana situasi saat ini disebabkan; Keenam, kesadaran akan kualitas informasi; dan **Ketujuh**, menilai bagaimana masa depan yang mungkin terjadi dari situasi saat ini.¹⁶⁴

Keamanan *cyber* membutuhkan kemauan dan kepemimpinan yang kuat dari eksekutif nasional.¹⁶⁵ Sejak era reformasi, militer China telah melakukan ekspansi baik kuantitatif dan peningkatan kualitatif dalam segi personil dan kapabilitas. Mantan Menteri Luar Negeri Amerika Serikat Condole Rice mengamati bahwa karena tidak ada negara yang mengancam China, menjadikan peningkatan militer negara tersebut menjadi terlalu besar demi mencapai kepentingan regional,

¹⁶⁴Sushil Jajodia, dkk, *Cyber Situational Awareness*, (London: Springer, 2010), hal 3-4.

¹⁶⁵Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 41.

Meskipun demikian, hal ini dinilai kurang konsisten dengan tujuan yang pernah disampaikan oleh Beijing tentang “peaceful rise”.¹⁶⁶ Meskipun angka yang tepat mengenai pengeluaran militer China sulit didapatkan, namun ada konsensus yang menyatakan bahwa pengeluaran militer China mengalami peningkatan yang tajam dalam dua dekade terakhir.¹⁶⁷ Anggaran belanja China dibagi menjadi tiga kategori yaitu personel, operasi, dan peralatan. Namun, pemerintah China dianggap menghilangkan beberapa kategori yang relevan seperti pembelian senjata, penelitian militer, pengeluaran pembangunan, dan pendapatan Tentara Pembebasan Rakyat (PLA), belum lagi prosedur akuntansi dan audit yang kurang jelas. Hal ini secara jelas sangat relatif mudah bagi PLA untuk menyembunyikan asetnya dan menimbulkan kecurigaan bahwa pengeluaran militer China sesungguhnya dapat dua atau tiga kali lebih tinggi dari angka resmi.¹⁶⁸ Modernisasi militer yang ambisius dengan cepat berhasil mengubah negara tersebut menjadi kekuatan yang tangguh dan menjadi pesaing strategi sejati bagi Amerika Serikat.¹⁶⁹

Terlepas dari angka yang tepat mengenai anggaran pertahanan, PLA China secara jelas tengah berada dalam ambisi untuk meningkatkan kemampuan militernya (baik kualitatif ataupun kuantitatif) menjadi kemampuan militer yang offensive. Dengan kata lain, China secara aktif mengupayakan perubahan militernya dari tentara berprinsipkan Mao Zedong yang berorientasi massa, infanteri-berat “People War” menjadi kekuatan modern dan tangkas yang mampu

¹⁶⁶Op.Cit., Shalendra D.Sharma, *China and India in The Age of Globalization*, hal 221.

¹⁶⁷Ibid.

¹⁶⁸Ibid.

¹⁶⁹Loc.Cit., Shalendra D.Sharma, *China and India in The Age of Globalization*, hal 211.

memproyeksikan kekuatan di dunia. Untuk mewujudkan hal tersebut, Beijing melakukan banyak investasi pada Angkatan Laut Perairan Biru, Akuisisi Pesawat Tempur Canggih, Kapal Selam, Pengisian Bahan Bakar Penerbangan, Miniatur Hulu Ledak Nuklir Ganda, dan Taktis Senjata Nuklir. Secara tidak langsung China tengah melakukan “Revolusi Militer” yang ambisius dan komprehensif. Kondisi jelas menghawatirkan tetangga China terutama Amerika Serikat. Peningkatan militer yang dilakukan China turut menjadi sebuah kekhawatiran akan prinsip proliferasi senjata mengingat China menjadi salah satu negara yang menjual senjata termasuk didalamnya rudal balistik kepada pihak ketiga yang tidak bereputasi.¹⁷⁰

China menggambarkan bahwa perang informasi (yang mencakup perang elektronik dan operasi dunia maya) sebagai bentuk perang yang paling penting. Dalam dokumen PLA, *Science of Military Strategy 2013*, menetapkan bahwa “Pihak yang memegang superioritas perang jaringan dapat mengadopsi perang kerja jaringan untuk menyebabkan disfungsi dalam sistem komando musuh, kehilangan kendali atas pasukan operasional dan kegiatan, dan ketidakmampuan senjata dan peralatan. Hingga mengambil inisiatif dalam konfrontasi militer, dan menciptakan kondisi untuk memperoleh kemenangan akhir dalam perang.”¹⁷¹ Hal ini terbukti dimana dalam beberapa waktu terakhir operasi siber China menarik perhatian besar terkait kecurigaan pencurian data industri secara besar-besaran, dan upaya tanpa henti China untuk mengakses rahasia militer negara lawan.

¹⁷⁰Ibid, hal 222.

¹⁷¹Op.Cit., Eric Heginbotham, “Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities.”, hal 272.

Berdasarkan spekulasi dari sumber-sumber publik selama bertahun-tahun diketahui bahwa peretas militer China terlibat dalam spionase dunia maya perusahaan.¹⁷² Salah satunya dalam laporan perusahaan keamanan siber Mandiant tahun 2013. Mandiant menemukan fakta bahwa militer China (PLA) melakukan upaya spionase dunia maya dengan target komersial milik Amerika Serikat.¹⁷³ Dalam laporannya diketahui bahwa Unit 61398, dari Biro Kedua, milik Departemen ke-3 dari Departemen Staf Umum PLA, telah mencuri ratusan terabyte data dari setidaknya 141 organisasi di berbagai industri mulai tahun 2006.¹⁷⁴

Presiden Xi Jinping pada tahun 2015 dan 2016 mengumumkan reformasi untuk pengaturan ulang layanan operasi bersama di samping pengawasan PKC yang ketat demi menjamin militer tunduk pada partai. PLA mereorganisasi perintah dan struktur birokrasinya, membentuk lembaga baru untuk menangani domain konseptual seperti *cyber*. Dalam buku putih China Military Strategy 2015 pemerintah menjuluki dunia maya sebagai salah satu komando baru tertinggi dalam strategi kompetisi dan menyatakan bahwa Partai Komunis China akan membentuk kekuatan dunia maya yang kuat. Sejalan dengan reformasi untuk Layanan China pada 2015 dan 2016, pemerintah China berhasil melahirkan Strategic Support Force (SSF).¹⁷⁵

¹⁷²Ibid., hal 271.

¹⁷³Ibid.

¹⁷⁴Ibid.

¹⁷⁵Caitlin Campbell, "China's Military: The People's Liberation Army (PLA)," *Congressional Research Service*, June, R46808, (Washington DC: CRS, 2021), hal 24.

SSF merupakan divisi yang bertugas untuk mengkonsolidasikan kantor atau fungsi dunia maya yang berbeda di dalam PLA dan mereka ditempatkan satu atap dibawahnya. SSF bertugas untuk melakukan operasi *cyber* ofensif dan defensif atas pencurian kekayaan intelektual (IP). Unit *cyber* SSF ditugaskan untuk mempersiapkan medan perang masa depan dengan menggunakan serangan ofensif di dunia maya. Mereka akan berusaha menurunkan komando dan kontrol musuh, komunikasi, mengumpulkan inteligen, dan membuat keputusan.

Salah satu tujuan utama SSF adalah mengganggu informasi dan memanfaatkannya untuk mengalahkan musuh di awal konflik. Sejak didirikan, SSF terus mendukung layanan dan mengintegrasikan efek siber dalam latihan, permainan perang, dan perencanaan. Pernyataan Presiden Xi pada 2019 menandakan pergeseran pandangan China dari perang informasi ke perang yang lebih cerdas dimana negara tersebut akan menampilkan penggabungan dunia maya dengan domain kognitif yang didorong oleh kemampuan Artificial Intelligence.¹⁷⁶ Upaya yang dilakukan oleh pemerintah China merupakan aksi nyata bahwa kekuatan perang kontemporer berbeda dengan kekuatan konvensional dimana operasi jaringan komputer hanya membutuhkan sejumlah kecil personel dan investasi dana yang relatif rendah untuk mencapai tujuan operasi.¹⁷⁷ Hal inilah yang tengah diwujudkan oleh China.

¹⁷⁶The Mad Scientist Laboratory blog “‘Intelligentization’ and a Chinese Vision of Future War.”, Last updated 19 Dec 2019. Diakses 29 July 2022. <https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/>

¹⁷⁷Loc.Cit., Eric Heginbotham, “Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities.”, hal 272-273.

Pada dasarnya paradigma berfikir terkait kekuatan perang kontemporer antara China dan Amerika Serikat tidak jauh berbeda. Namun, terdapat tumpang tindih terkait pembagian operasi jaringan militer antara Amerika Serikat dan China. Jika Amerika Serikat hanya membagi operasi jaringan komputer menjadi tiga bagian komponen yaitu, eksploitasi jaringan komputer, serangan jaringan komputer, dan pertahanan jaringan komputer.¹⁷⁸ Sementara menurut China, tiga bagian komponen operasi jaringan militer itu terdiri atas pengintaian jaringan, serangan jaringan dan operasi pertahanan, dan pencegahan jaringan.¹⁷⁹

Sikap kedua negara yang sama-sama memasukan kemampuan *cyber* menjadi bagian penting dalam jaringan operasi militernya menunjukkan bahwa persaingan *cyberpower* dapat terjadi dikarenakan adanya serangan terhadap sistem militer. Serangan *cyber* suatu negara secara nyata dapat merendahkan sarana pertempuran musuh.¹⁸⁰ Sebagaimana yang telah dijabarkan bahwa penggunaan *cyber* oleh pihak lawan akan sangat berisiko terhadap kebocoran data. Kebocoran data yang diperoleh ini tidak menutup kemungkinan bahwa akan disalah gunakan terutama sebagai strategi militer lawan. Oleh karena itu, pengaman melalui *cyber* harus menjadi perhatian khusus untuk memastikan kedaulatan dan keamanan negara.

¹⁷⁸Ibid., hal 259.

¹⁷⁹Ibid, hal 273.

¹⁸⁰Ibid, hal 259.

5.4 *Cyber Hegemony*

Ketika membicarakan kekuatan dunia maya secara komprehensif kata tersebut mengacu pada kemampuan suatu negara untuk mengambil tindakan dan memberikan pengaruh di dunia maya.¹⁸¹ Apa yang dulunya merupakan domain dimana perusahaan Amerika Serikat dapat beroperasi secara bebas sementara perusahaan China masih dalam tahap mengejar ketertinggalan telah terganti oleh ketidaksepakatan yang semakin vokal tentang bagaimana hal itu dikelola.¹⁸² Kini dunia maya menjadi ruang terbuka yang memberikan kesempatan dan akses yang sama besar bagi setiap negara untuk ikut terlibat dan menunjukan diri. China yang dalam beberapa tahun terakhir telah berfokus atas pengembangan *cyber*-nya mulai menunjukan posisinya. Keikutsertaan China turut dipengaruhi oleh anggapan bahwa Amerika Serikat selama ini telah melakukan militerisasi dunia maya dan memicu perlombaan senjata dunia maya internasional.¹⁸³ Hal ini menjadikan dunia maya sebagai medan pertempuran penting baru bagi keduanya untuk memperebutkan pengaruh global.¹⁸⁴

Bagaimana perkembangan *cyber* yang dimiliki China menjadikan Amerika Serikat mau tidak mau harus mengakui bahwa status adidaya yang dimiliki selama ini mulai ditantang oleh kemampuan China. Amerika Serikat harus mengakui bahwa seperti halnya Uni Soviet dan Amerika Serikat tidak pernah berperang

¹⁸¹Op.Cit., Li Zhang, "A Chinese Perspective On War", hal 3.

¹⁸²Op.Cit., Niels Nagelhus Schia and Lars Gjesvik, "China's *cyber* sovereignty Norwegian Institute of Internasional Affairs", hal 1.

¹⁸³Op.Cit., Sinan Ulgen, *Governing Cyberspace*, hal 64.

¹⁸⁴Matthew Bey, "Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition", *The Cyber Defense Review*, Vol. 3, No. 3, December (New York: Army Cyber Institute, 2018), hal 31.

nuklir, kemampuan dunia maya China tidak berarti bahwa perang dunia maya tidak dapat dihindari.¹⁸⁵ Ditambah dengan peningkatan pertahanan siber nasional yang dilakukan China, menjadikan Amerika Serikat harus terlibat langsung dengan China. Hal ini secara jelas menunjukkan adanya rivalitas persaingan dimana posisi China dinilai dapat menyaingi bahkan mengancam keberadaan Amerika Serikat. Terlebih dengan pernyataan Presiden Xi untuk mewujudkan impian China sebagai pusat *Cyberpower* global.

Persaingan kedua negara untuk saling memimpin menciptakan kompetensi diantara keduanya. Persaingan ini terjadi karena saat ini China jauh lebih siap dan mapan dalam menghadapi Amerika Serikat. Pada tahun 1985 Profesor Harvard Business School, Michael Porter, menjelaskan bahwa sebuah perusahaan harus menciptakan tujuan, strategi, dan operasi yang jelas dan berkelanjutan.¹⁸⁶ China dalam persaingan ini tampaknya telah lebih siap mengembangkan kemampuan cyber secara lebih ofensif dan siap pakai dengan struktur pertahanan di seluruh lapisan negara. Komponen kunci ini nyatanya menjadi bagian penting dalam strategi siber China. Sebaliknya, Amerika Serikat tampaknya berada pada posisi yang lebih dirugikan. Hal ini dikarenakan kerentanan infrastruktur yang dimilikinya lebih didokumentasikan secara publik dibandingkan China. Mudah-mudahan akses informasi ini tentu sangat memungkinkan bagi China untuk melakukan pemetaan dan eksploitasi melalui jaringan komputer PLA. Jika China memiliki

¹⁸⁵Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 50.

¹⁸⁶Chey Yuanita, "Competitive Advantage Adalah: Pengertian, Cara Kerja, Jenis, dan 3 Contohnya dalam Bisnis.", Last updated 17 Mar 2022. Diakses 05 Aug 2022. <https://www.ekrut.com/media/competitive-advantage-adalah>

potensi menjadi kekuatan dunia maya maka, negara tersebut memiliki kemampuan untuk menghalangi atau mengalahkan Amerika Serikat melalui dunia maya.¹⁸⁷

Kemudahan akses informasi diperoleh China menjadi salah satu keuntungan bagi China. Kondisi ini secara praktis telah memberikan manfaat yang lebih menguntungkan bagi China. Selain itu, berdasarkan pemaparan yang sebelumnya telah disampaikan bahwa China mengembangkan kemampuan *cyber* yang dimiliki dengan menuangkan kedalam 10 sektor tujuan pembangunan bangsa. China turut mengutamakan inovasi produk dan pengembangan teknologi dalam setiap sektornya. Tampak dari bagaimana negara tersebut berhasil mengembangkan jaringan 5G dan AI dan berakhir mendorong Amerika Serikat untuk menggunakan kemampuan ekonomi dan politiknya untuk menekan dominasi China semakin menunjukkan keberhasilan China dalam pemenuhan kebutuhan layanan teknologi dengan cara yang baru. Produk Huawei menjadi sangat inovatif dan menarik minat pasar yang besar. Menurut Nouzy, kemampuan dalam inovasi perusahaan akan mampu menciptakan produk dan layanan terbaru, sehingga produk perusahaan diminati pasar.¹⁸⁸

Keberhasilan China pada dasarnya merupakan gerbang pembuka dari impian mereka untuk menjadi *Cyberpower* dunia. Yang artinya mereka mampu menurunkan dominasi Amerika Serikat yang awalnya sangat tersentris. Kondisi ini bagi Amerika Serikat jelas menjadi ancaman besar. Amerika Serikat

¹⁸⁷Loc.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security", hal 39.

¹⁸⁸Loc.Cit., Diakses 06 Aug 2022. <https://bbs.binus.ac.id/gbm/2019/02/26/competitive-advantage/>.

membutuhkan perubahan dramatis dalam strategi siber nasionalnya untuk memasukkan prioritas federal pertahanan siber, peningkatan yang diatur atau diatur dalam keamanan jaringan infrastruktur penting dan pemerintah, diskusi bilateral dengan China, dan upaya internasional untuk mengatur dunia maya.¹⁸⁹ Amerika Serikat harus mampu melakukan pengorganisasi dengan lebih baik jika negara tersebut masih ingin mengamankan posisi hegemoni yang selama ini dimilikinya. Meskipun kecenderungan strategi pertahanan terfokus pada serangan *cyber* dan meningkatkan kemampuan internal, namun Amerika Serikat turut membutuhkan strategi internasional terkait dengan dunia maya. Hal ini dikarenakan jaringan informasi memiliki pengaruh yang sangat luas maka akan jauh lebih baik apabila negara tersebut mampu menciptakan kondisi kestabilan bersama untuk mencegah perkembangan kekuatan *cyber* China.

Selama dua puluh tahun PLA China memang menerbitkan artikel tentang apa yang dapat mereka lakukan dengan kekuatan dunia maya. Namun, China memiliki asumsi bahwa artikel yang selama ini sering disampaikan oleh Amerika Serikat terkait perkembangan *cyber* China hanyalah sebuah tanggapan. Hal ini dikarenakan hingga saat ini, pemerintah Amerika Serikat telah mengeluh tetapi tidak menanggapi secara hukum, militer, atau ekonomi terhadap intrusi dunia maya China. Hal ini membuat China berasumsi bahwa Amerika Serikat tidak mau atau tidak mampu merespons. Bahaya dalam ambiguitas ini adalah bahwa China atau

¹⁸⁹Op.Cit., Colonel Jayson M. Spade, "China's Cyberpower and America's National Security.", hal 40.

Amerika mungkin mengalami serangan siber yang serius dan menyalahkan pihak lain, yang memicu pembalasan dan eskalasi berikutnya.¹⁹⁰

Ketika China dan Amerika Serikat tengah saling membangun modernisasi militer lengkap untuk menunjang kemampuan *cyberpower*. Diwaktu yang bersamaan China dianggap telah lebih dulu mempersiapkan konflik bersenjata dengan Amerika Serikat dengan mencari keuntungan militer diwilayah perang asimetris.¹⁹¹ Potensi kemerdekaan Taiwan adalah alasan yang paling mungkin untuk munculnya konflik militer China-Amerika. Namun, adanya kekuatan siber China yang kuat dapat menjadi sumber pengadaan kekuatan besar bagi PLA China. Selain itu, SDA yang melimpah dapat semakin mendorong kemungkinan perang yang paling umum. Dengan dua ekonomi terbesar dunia yang dipertaruhkan, China dan Amerika Serikat mungkin memperebutkan akses ke minyak atau mineral tanah yang terbatas. Kemungkinan perang hampir selalu ada. Seperti persenjataan nuklir Soviet, kepemilikan senjata siber China tidak meningkatkan kemungkinan perang, melainkan kekuatan sibernya merupakan faktor yang harus dipertimbangkan dan dikurangi.¹⁹²

Kemampuan yang ditunjukkan China terkait eksploitasi jaringan komputer telah menggarisbawahi kerentanan Amerika Serikat terhadap serangan dunia maya dari negara tirai bambu tersebut atau bahkan kemungkinan serangan lain lain dengan kemampuan serupa. Hal ini menjadi competitive China terkait persaingan

¹⁹⁰Ibid, hal 47.

¹⁹¹Ibid, hal 51.

¹⁹²Ibid.

cyberpower yang tengah terjadi. Ditambah dengan postur keamanan dunia maya Amerika Serikat saat ini tidak dapat mempertahankan dengan jaringan nasional dan infrastruktur pentingnya secara terpadu. Serangan kepada badan pertahanan Amerika Serikat sangat mungkin menimbulkan perpecahan karena kurangnya koordinasi negara dan komunitas internasional yang tentu akan saling berselisih mengenai norma dan aturan dunia maya. Amerika Serikat telah kehilangan satu point dibanding China.

China berhasil menunjukkan perbedaan dirinya dengan Amerika Serikat dalam persaingan ini. China melalui beragam kebijakan dan pengembang yang dilakukan baik melalui pemerintah atau *non state actor* nya berhasil meraih kesuksesan berdasarkan faktor-faktor kritis. Keserasian antara kompetensi yang membedakan dari sebuah pesaing lain dan faktor-faktor kritis untuk meraih sukses dalam kompetisi akan mendorong pelaku tersebut mempunyai prestasi yang jauh lebih baik daripada para pesaingnya.¹⁹³

Memastikan keamanan siber nasional memang tidak akan mudah atau murah. Namun nyatanya hingga saat dengan berkomitmen pada pencegahan nuklir, Amerika Serikat mampu bertahan dari posisinya hegemoninya dan dengan kapasitas untuk menghalangi atau mengalahkan musuh-musuhnya.¹⁹⁴ Saat ini kondisi tersebut harus dipadukan dengan model multilateral yang lebih berpusat pada negara dengan mempromosikan pemikiran kritis terkait kepentingan nasional

¹⁹³Loc.Cit., Diakses 06 Aug 2022. <https://bbs.binus.ac.id/gbm/2019/02/26/competitive-advantage/>.

¹⁹⁴Op.Cit., Colonel Jayson M. Spade, "China's *Cyberpower* and America's National Security.", hal 40.

bangsa. Beberapa kekuatan negara seperti India, China, Rusia, dan Brasil, masing-masing dengan caranya sendiri untuk melawan apa yang mereka lihat sebagai dominasi tata kelola internet Amerika Serikat dan negara-negara kapitalis Barat. Karena lokus infrastruktur material internet condong ke negara-negara ini, masuk akal bahwa mereka akan mendapatkan lebih banyak pengaruh atas kebijakan dan praktik yang membentuknya.¹⁹⁵

Pada saat yang sama, China dan Amerika Serikat merupakan mitra dagang utama yang saling memperluas ekspansi ekonomi, dan menciptakan ketergantungan ekonomi. Namun, mengingat perbedaan kedua negara dalam nilai-nilai, sistem politik, dan kepentingan nasional, tetap memunculkan kekhawatiran yang jelas akan bagaimana lintasan masa depan yang dipilih China.¹⁹⁶ Dapatkah China melaksanakan “peaceful rising” nya dijalankannya untuk mendapatkan status sebagai negara dengan kekuatan besar? ¹⁹⁷

Amerika Serikat harus menciptakan keseimbangan seiring dengan modernisasi militer yang dilakukan oleh China. Amerika Serikat perlu secara khusus mengenali bagaimana modernisasi secara umum yang diberlakukan oleh pertahanan PLA China. Hal ini dikarenakan China telah memodernisasi sistem persenjataannya dan peningkatan kemampuan personilnya seiring dengan ekspansi ekonomi. Semakin

¹⁹⁵Loc.Cit., Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure”, hal 230.

¹⁹⁶Loc.Cit., Shalendra D.Sharma, *China and India in The Age of Globalization*, hal 211.

¹⁹⁷Ibid.

meningkat perekonomian China maka semakin besar pula perkembangan kekuatan *cyber* yang dapat dilakukan China. Trend ini pasti akan terus berlanjut.¹⁹⁸

Secara pasti Amerika Serikat perlu mewaspadaai bahwa modernisasi senjata berpotensi menimbulkan destabilisasi. Perlu pertimbangan kekuatan untuk memperoleh kemampuan secara khusus dapat menekan ancaman yang muncul. Meskidemikian memahami struktur dan strategi dunia maya China bukanlah tugas yang mudah mengingat betapa tertutupnya negara tersebut akan akses informasi dari luar. China dianggap tengah menganalisis tentang mengalahkan Amerika Serikat dengan menyerang pusat gravitasnya terutama atas ketergantungannya pada jaringan.

Rivalitas *cyber* yang dibarengi oleh serangan terhadap sistem pemerintah dan non-pemerintah, sebagian besar dilakukan untuk menurunkan keinginan musuh untuk berperang. Dalam persaingan *cyberpower* jaringan yang dimiliki suatu negara harusnya terintegrasi. Hal ini bertujuan untuk mempertahankan keunggulan informasi baik terkait informasi medan perang tradisional (fisik) dan jaringan (virtual) dengan mengendalikan aliran informasi yang tersedia untuk musuh. Meskidemikian masih terdapat pandangan terkait signifikansi *cyberpower* antara Amerika Serikat dan China. China melihat bahwa kemampuan mengungkapkan jaringan dan penguatan menyeluruh akan sangat penting untuk pengamanan jaringan. Sementara Amerika Serikat masih memandang bahwa *cyberpower*

¹⁹⁸Ibid, hal 223.

bukanlah kekuatan perang utama dan negara tetap perlu menguatamakan penguasaan kekuatan fisik.

Amerika Serikat dan China saat ini secara jelas tengah berada dalam kondisi dimana keduanya saling berkompetensi untuk saling mengungguli satu sama lainnya. Meskidemian penguasaan Amerika Serikat terhadap komputer selama beberapa puluh telah menjadi keunggulan tersendiri. Keunggulan ini nyataanya dipergunakan oleh negara tersebut untuk menjadi kekuata dan persaingan. Amerika Serikat telah sejak lama diketahui bahwa ekonomi negara tersebut bergantung pada suatu revolusi teknologi.¹⁹⁹ Amerika Serikat memiliki kemampuan kepemilikan perangkat lunak dan sistem operasi dunia yang lebih diakui dibandingkan China. Windows, Google, ataupun Chip telekomunikasi yang menjadi standard dalam telekomunikasi nyataanya masih diperlukan oleh China. Persaingan *cyberpower* menjadikan sebuah kemampuan negara yang tidak dapat dinilai dengan mudah jika hanya berdasarkan indikator kuantitatif seperti halnya keamanan konvensional. Melainkan telah menciptakan bentuk peperangan yang relatif baru dan berkembang pesat namun tidak mudah untuk diukur tapi dapat dirasakan.

Amerika Serikat yang telah memiliki hegemoni internasional membawa fondasi yang jauh lebih baik untuk pertempuran daripada yang dilakukan China. Selain itu, pengaruh dari dominasi Amerika Serikat nyataanya tidak semudah itu dapat tergantikan. Meskipun China lebih mengungguli Amerika Serikat dalam beberapa tahun terakhir. Namun dalam kancah global posisi Amerika Serikat masih

¹⁹⁹Nathan Edmonson, *Technology Cycles and US Economy Policy In The Early 21st Century*, (New Jersey: Transaction Publisher, 2012), hal 161.

disegani oleh banyak negara. Banyak pemikiran dan sikap Amerika Serikat baik secara langsung atau tidak dapat mempengaruhi keputusan negara lain. Seperti dalam halnya keputusan pemerintah Inggris yang turut melarang pengembangan jaringan 5G China karena terpengaruhi oleh sikap Amerika Serikat. Hal ini secara tidak langsung menunjukkan Amerika Serikat juga memiliki strategi bersaingnya sendiri.

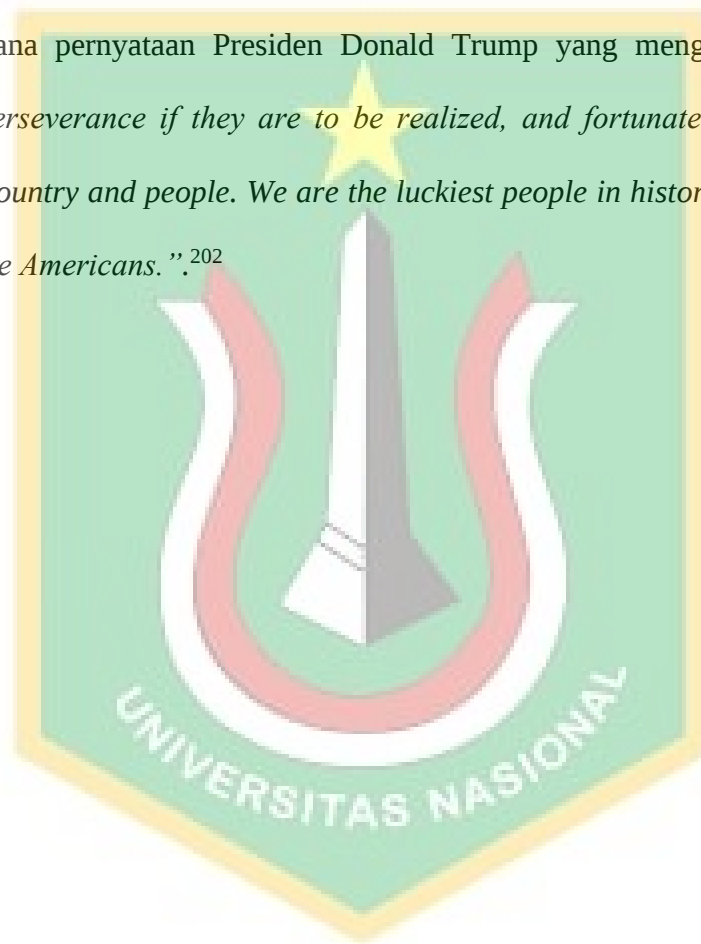
Mungkin benar bahwa dalam sebuah persaingan sebuah negara terkadang harus dapat bersikap ofensif, atau defensif. China sendiri berada pada posisi yang semakin agresif dan mengancam Amerika Serikat. China memaksimalkan strategi bersaing dengan menghasilkan barang dan jasa yang lebih baik dengan harga lebih kompetitif dibanding Amerika Serikat. Namun hal ini bukan berarti Amerika Serikat adalah lawan yang mudah. Dalam dunia persaingan global yang semakin meningkat, peranan dan hubungan yang telah terbentuk sebelumnya menjadi semakin penting. Keunggulan bersaingpun harus dapat diciptakan dan dipertahankan melalui proses cenderung terpusat dan terlokalisasi.²⁰⁰

Menurut *International Institute for Strategic Studies (IISS)*, dan Pusat Belfer Center Harvard Kennedy School, kedua lembaga index tersebut menempatkan Amerika Serikat pada posisi teratas dalam daftar kemampuan siber negara. Sementara China, keduanya sepakat untuk menempatnya di posisi kedua. Penilaian keduanya menyimpulkan bahwa meskipun China telah mengalami

²⁰⁰Sampoernauniversity.ac.id, "Competitive Advantage: Keunggulan Bersaing Suatu Bangsa." Last Update 27 Jan 2022. Diakses 08 Aug 2022. <https://www.sampoernauniversity.ac.id/id/competitive-advantage/>

perkembangan yang signifikan namun kedua masih menemukan banyak kekurangan China sehingga mencegah negara tersebut untuk dapat melampaui status Amerika Serikat. Menurut mereka untuk memposisikan China diposisi teratas masih diperlukan waktu yang lama untuk membiat China duduk dalam posisi yang setara dengan Amerika Serikat dalam hal kekuatan *cyber*.²⁰¹

Sebagaimana pernyataan Presiden Donald Trump yang mengatakan “*Dreams require perseverance if they are to be realized, and fortunately we’re a hard-working country and people. We are the luckiest people in history, just by the fact that we are Americans.*”²⁰²



²⁰¹B. K. Williams, “Evaluating China's Road to Cyber Super Power.” LLNL-TR-829221, November (California: Lawrence Livermore National Lab, 2021), hal 2.

²⁰²Thomas W. Pauken, *US vs China, From Trade War to Rciprocal Deal*, (Singapore: World Scientific, 2020), hal 61.

BAB VI

PENUTUP

6.1 Kesimpulan

Persaingan *cyberpower* antara China dan Amerika Serikat semakin meningkat, tetapi Amerika Serikat lebih unggul dibanding China karena Amerika Serikat telah terlebih dulu memiliki dominasi kekuasaan global dibandingkan China. Dominasi kekuasaan yang dimiliki Amerika Serikat sejak pada Perang Dingin hingga memunculkan Amerika Serikat sebagai pemegang hegemoni dunia nyatanya masih sulit tergantikan. Meskipun China dalam beberapa waktu terakhir telah mengalami perkembangan *cyber* yang pesat khususnya di bidang teknologi. Namun, pengaruh Amerika Serikat dalam tatanan Global tidak bisa begitu saja tergantikan. China masih membutuhkan waktu untuk dapat memperoleh pengakuan secara global untuk dapat menggantikan posisi dan pengaruh Amerika Serikat.

Rivalitas yang terjadi antara Amerika Serikat dan China menunjukkan bahwa dinamika hubungan internasional saat ini semakin kompleks dan kemampuan *cyberpower* menjadi penting untuk menjamin dan menciptakan keamanan serta kestabilan negara. Hal ini sesuai dengan pandangan Joseph S.Nye, JR dalam bukunya yang berjudul *Cyberpower*, bahwa negara harus mampu memanfaatkan *Cyberpower* untuk menciptakan keuntungan dan mengejar pengembangan. Selain itu, Amerika Serikat dan China menggunakan *competitive strategy*-nya masing-masing untuk saling mendominasi satu sama lain. Hal ini terlihat dari bagaimana China mengejar orientasi pengembangan teknologi diberbagai sektor khususnya

ekonomi seperti pengembangan 5G dan kebijakan *Made in China*. Sementara itu, sikap dan tindakan Amerika Serikat masih mempengaruhi bagaimana keputusan negara lain. Larangan perdagangan Huawei yang dikeluarkan oleh Amerika Serikat berpengaruh terhadap keputusan pemerintah Inggris sehingga negara tersebut ikut melarang pengembangan jaringan 5G China menjadi bukti bahwa pengaruh Amerika Serikat masih cukup kuat.

Cyberspace atau dunia maya telah menjadi media baru dalam perang kontemporer yaitu perang tak terbatas jarak dan waktu. *Cyberspace* memberikan kesempatan bagi setiap negara untuk ikut terlibat. Jika konsep perang konvensional serangan terfokus pada serangan fisik maka, seiring dengan perkembangan teknologi sebuah negara harus siap dan mampu mengamankan diri atas dari berbagai sisi. Dalam catatan Mandiant, China menjadi pelaku serangan siber tertinggi dunia dengan Amerika Serikat sebagai korbannya. Perkembangan teknologi telah menjadi suatu entitas yang tidak terpisahkan dari kehidupan manusia, dan negara harus mampu mengimbangi perkembangan teknologi menjadi bagian dari strategi pertahanan dan keamanan negara.

Pemerintah China dibawah pemerintahan Presiden Xi mengeluarkan kebijakan Made in 2025 sebagai implementasi Rencana Lima Tahun ke 13 China dengan mengedepankan inovasi teknologi pada kesepuluh sektor utama pengembangan. Hal ini menunjukkan bahwa negara tersebut secara serius mengubah arah pandangan negaranya menjadi jauh kedepan. China menjadikan teknologi sebagai bagian dari strategi pertahanan dan kekuatan negara. Kesadaran bahwa perang dimasa depan bukan hanya tentang pertandingan senjata namun juga kekuatan

non fisik mendorong negara tersebut untuk mengembangkan *cyberpower* negara melalui berbagai lapisan.

Terkait strategi persaingannya, China berhasil dalam mengembangkan jaringan 5G, kontrol pemerintah yang kuat atas aliran informasi yang masuk dan keluar, dukungan pemerintah dalam sektor ekonomi, dan reformasi PLA China serta modernisasi militer. Selain itu kemudahan publisitas informasi Amerika Serikat turut menjadi keuntungan bagi China dalam memperoleh informasi. Namun, disatusisi China masih terbayang-bayang oleh standard global yang telah ada sebelumnya. Dimana banyak perusahaan teknologi Amerika Serikat seperti Google atau pun Qualcomm sebagai teknologi yang masih diperlukan China untuk dapat memasuki pasar global.

Amerika Serikat memang lebih mudah dan rentan untuk kemungkinan kebocoran informasi karena lebih terbukanya aliran informasi dinegara tersebut. Namun, perusahaan-perusahaan raksasa asal negara tersebut telah menjadi bagian dalam strategi bersaing Amerika Serikat. Kematangan dan pengaruh perusahaan swasta ini menjadi *factor* utama mengapa China sulit menggeser dominasi Amerika Serikat meskipun negara tersebut sudah lebih fokus dalam mengembangkan kemampuan *cybernya*.

Kemampuan Amerika Serikat dalam memainkan pengaruh ekonomi dan politiknya menjadi upaya negara tersebut menekan perkembangan China. Pada akhirnya Amerika perlu mewaspadai modernisasi dan pengembangan *cyberpower* yang dilakukan oleh China. Tidak menutup kemungkinan dalam beberapa tahun

kedepan China dapat melampaui Amerika Serikat apabila negara tersebut tetap konsisten dengan peningkatan yang tengah dilakukannya. Dinamika Hubungan Internasional yang sarat akan perubahan menjadikan segala kemungkinan menjadi dapat terjadi dan setiap negara termasuk Amerika Serikat harus memiliki kesadaran akan perubahan dinamika keamanan global.

6.2 Saran

Amerika Serikat perlu lebih memahami dan menganalisis secara lebih mendetail bagaimana keberhasilan China dalam mengembangkan *cyberpower*nya. Selain itu, Amerika Serikat perlu menciptakan perimbangan kekuatan untuk memperoleh kemampuan secara khusus sehingga negara tersebut dapat lebih menekan ancaman yang muncul. Amerika Serikat perlu mengambil Tindakan secara lebih terkoordinasi untuk dapat meningkatkan kemampuan *cyberpower*nya di segala lapisan masyarakat.

Amerika Serikat juga harus menciptakan keamanan domestiknya untuk meminimalisir kebocoran informasi. Selain itu, pada sektor militer Amerika Serikat harus mampu memastikan modernisasi teknologi selalu terbaharukan dengan memaksukan komponen siber sebagai senjata pertahanan. Amerika Serikat juga harus lebih mampu mengkoordinasi dan memberikan ruang bagi *actor non state* untuk dapat menjadi bagian dari strategi pengembangan *cyber*. Karena apabila China dapat terus melakukan inovasi dalam pengembangan teknologi maka tidak menutup kemungkinan apa yang dimiliki oleh Amerika Serikat saat ini dapat diambil alih oleh China.

DAFTAR PUSTAKA

BUKU

- Anggito, Albi, dan Johan Setiawan. *Metodologi Penelitian Kualitatif*. Sukabumi: CV Jejak, 2018.
- Carr, Madeline. *US Power and The Internet In The International Relations*. New York: Palgrave Macmillan, 2016.
- Czosseck, Christian, and Kenneth Geeres. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press BV, 2009.
- Daphne, Leo. *MIAW-Management In Absurd Way*. Jakarta: PT Elex Media Komputindo, 2014.
- Edmonson, Nathan. *Technology Cycles and US Economy Policy In The Early 21^s Century*. New Jersey: Transaction Publisher, 2012.
- Harrison, Lisa. *Political Research: An Introduction*, terj Tri Wibowo. London: Routledge, 2007.
- Huang, Qunhui. *Understanding China's Manufacturing Industry*. Beijing: Chinese Academy of Social Sciences, 2022.
- Ikbar, Yanuar. *Metodologi & Teori Hubungan Internasional*. Bandung: PT Refika Aditama, 2014.
- Jajodia, Sushil, dkk. *Cyber Situational Awareness*. London: Springer, 2010.
- Mamik. *Metodologi Kualitatif*. Sidoarjo: Zifatama Publisher, 2015.
- Mengin, Françoise. *Cyber China – Reshaping National Identities in The Age of Information*. New York: Palgrave Macmillan, 2004.
- Moleong, Lexy J. *Metodologi Penelitian Kualitatif*. Bandung: Remaja Rosdakarya, 2000.
- Nazir, Moh. *Metode Penelitian*. Bogor: Ghalia, 2005.
- Pauken, Thomas W. *US vs China, From Trade War to Reciprocal Deal*. Singapore: World Scientific, 2020.
- Perwita, Anak Agung Banyu. *Dinamika Keamanan dalam Hubungan Internasional dan Implikasinya bagi Indonesia*. Bandung: Universitas Khatolik Parahyangan, 2018.
- Porter, Michael E. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: The Free Press, 1985.
- Porter, Michael E. *The Competitive Advantage of Nations*. New York: The Free Press, 1990.
- Sharma, Shalendra D. *China and India in The Age of Globalization*. New York: Cambridge University, 2009.
- Subadi, Tjipto. *Metode Penelitian Kualitatif*. Surakarta: Muhammdiyah University Press, 2006.
- Suyanto, M. *Marketing Strategy*. Yogyakarta: CV ANDI OFFSET, 2007.

JURNAL

- Arianto, Adi Rio. "Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21." *Jurnal PIR*, Vol. 1, No. 2 (Februari, 2017): 116-117.
- Bey, Matthew. "Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition." *The Cyber Defense Review*, Vol. 3, No. 3 (December, 2018): 31.
- Campbell, Caitlin. "China's Military: The People's Liberation Army (PLA)," *Congressional Research Service*, R46808, (June, 2021): 24.
- Deppa, Catherine S. "U.S. Cyber Command: An Overview", *American Intelligence Journal*, Vol. 34, No. 1 (2017): hal 13.
- Faida, Rahma Eliya. "Sensor Internet dan Securitization di Era Cyberwarfare: Studi Kasus Tiongkok." *Jurnal Hubungan Internasional*, Vol. VIII, No. 1 (Januari-Juni, 2015): 32.
- Heginbotham, Eric, et all. "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities." (2015): 2-279.
- Institute for Security & Development Policy, "Made in China 2025", (June, 2018): 2-31.
- Jr, Joseph S.Nye. "Cyberpower." *Belfer Center for Science and International Affairs* (May, 2010): 1-24.
- Kania, Elsa B, and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *The Cyber Defense Review*, Vol. 1, No. 1 – Vol 6, No 2 (2018): 105-122.
- Koleski, Katherine. "The 13th Five-Year Plan", *Staff Research Report*, (February, 2017): 3-12.
- Lambert, Vickie A., and Clinton E. Lambert. "Qualitative Descriptive Research: An Acceptable Design." *The Pacific Rim International Journal of Nursing Research*, Vol. 16, No. 4 (October – December, 2012): 255-256.
- Meisitha, Nadya Vira, Agung Purwanto, dan Linda Dwi Eriyanti. "Motivasi China Menguasai Cyber Teknologi." *Student Research Article* (2014): 1-5.
- Nufus, Hayati. "Impian Tiongkok: Nasionalisme Tiongkok Melintas Batas dalam Pembangunan Tiongkok" *Jurnal Penelitian Politik*, Vol 11, No. 2 (Desember, 2014): 43-54.
- Nursita, Rizki Dian. "Cyberspace: Perdebatan, Problematika, Serta Pendekatan Baru dalam Tata Kelola Global." *Dauliyah Journal*, Vol. 4, No. 1 (2019): 81.
- Rafsanjani, Lalu Azhar, Lalu Puttrawandi Karjaya, dan Khairur Rizki, "Rivalitas Amerika Serikat (AS) dan China dalam menjaga Security Order di Asia Timur" *Indonesian Journal of Gobar Discourse*, Vol. 2, No. 1, (Januari – Juni, 2020): 28-35.
- Schia, Niels Nagelhus, and Lars Gjesvik. "China's cyber sovereignty Norwegian Institue of Internasional Affairs", *Policy Brief* (March, 2017): 1-2.
- Spade, Colonel Jayson M. "China's Cyberpower and America's National Security." *USAWC Strategy Research Project* (March, 2011): 2-50.

- The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the US Economy", (February, 2018): 1.
- Triwahyuni, Dewi, dan Yanyan Mochamad Yani. "Dampak Pembangunan Cyberpower Tiongkok Terhadap Kepentingan Amerika Serikat." *Jurnal Ilmu Politik dan Komunikasi*, Vol. VIII, No. 1 (Juni, 2018): 1-14.
- Ulgen, Sinan. *Governing Cyberspace*. Washington DC: Carnegie Europe, (2016): 55-64.
- Williams, B. K. "Evaluating China's Road to Cyber Super Power." LLNL-TR-829221 (November, 2021):2.
- Winseck, Dwayne. "The Geopolitical Economy of the Global Internet Infrastructure", *Journal of Information Policy*, Vol. 7 (2017): 229.
- Zamroni, Mohammad. "Perkembangan Teknologi Komunikasi dan Dampaknya Terhadap Kehidupan", *Jurnal Dakwah*, Vol 10, No 2. (2009): 206-208.
- Zhang, Li. "A Chinese Perspective On War", *International Review of the Red Cross*, Vol. 94, No 886, (2012): 3.

TESIS

- Bonner, Mayor E. Lincoln., *Cyberpower: Attack & Defense Lessons from Land, Sea, and Air Power*. (Tesis, School of Advanced Air and Space Studies Air University, Alabama, 2011) Accessed May, 22, <https://www.hsdl.org/?view&did=812459>

DOKUMEN LEMBAGA

- Central Committee of The Communist Party of China. (2016). *13th Five Year Report*, Part 1, Chapter 6: Ensure Innovation in Science and Technology Takes a Leading Role.
- CNNIC. (September, 2020). *Statistical Report on Internet Development in China*. CNNC Report.
- Feakin, Tobias. (June, 2018). *Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities*. Special Report, ASPI.
- Singh, Spandana and Margerite Blasé. (2020). *How Internet Platforms Are Addressing Election and Voter Suppression-Related Misinformation and Disinformation*. Protecting The Vote report, New America.
- Smith, Zhanna Malekos and Eugenia Lostr. (December, 2019). *The Hidden Cost of Cybercrime*. CSIS Report
- United States Census Bureau. (August, 2018). *Computer and Internet Use in the United State: 2016*. U.S Department of Commerce.

WEBSITE

- Akbar, Muhammad Rizki. "Standard China 2035" dan Mimpi Tiongkok untuk Standardisasi Teknologi Dunia." Last update 15 Feb 2022, Diakses 28 May 2022. <https://politik.brin.go.id/kolom/politik-internasional/standard-china-2035-dan-mimpi-tiongkok-untuk-standardisasi-teknologi-dunia>

- BBC.Com, "Microsoft accuses China over email cyber-attacks." Last updated 3 Mar 2021, Diakses 15 November 2021. <https://www.bbc.com/news/business-56261516>
- Binus University, "Competitive Advantage", Last Updated 26 Feb 2019, Diakses 28 Mar 2022. <https://bbs.binus.ac.id/gbm/2019/02/26/competitive-advantage/>
- CIRSD.Com, "Cyberpower - An Emerging Factor in National and International Security" Diakses 21 May 2022. <https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-interntional-security>
- CNN Indonesia.com, "Inggris Resmi Larang Huawei Kembangkan 5G" Last update 15 July 2020. Diakses 28 July 2022. <https://www.cnnindonesia.com/teknologi/20200715020658-185-524746/inggris-resmi-larang-huawei-kembangkan-5g>
- Globaltimes.com, "Summary of the 13th Five-Year Plan 2016-20." Last updated 26 Oct 2020, Diakses pada 4 May 2022. [https://www.globaltimes.cn/content/1204685.shtml#:~:text=During%20the%2013th%20Five%2DYear,trillion%20yuan%20\(%2414.9%20trillion\).](https://www.globaltimes.cn/content/1204685.shtml#:~:text=During%20the%2013th%20Five%2DYear,trillion%20yuan%20(%2414.9%20trillion).)
- Iskandar. "Headline: AS Larang Huawei, Buntut Perang Dagang atau Persaingan Bisnis?." Last updated 22 May 2019. Diakses 20 July 2022. <https://www.liputan6.com/tekno/read/3971492/headline-as-larang-huawei-buntut-perang-dagang-atau-persaingan-bisnis>
- Ivan P. "AS Bersiap Larang Penggunaan Teknologi Huawei dan ZTE". Last updated 15 Aug 2018. Diakses 15 Jul 2022. <https://beritagar.id/artikel/sains-tekno/as-bersiap-larang-penggunaan-teknologi-huawei-dan-zte>
- Knell, Noelle. "Top 10 Countries Where Cyber Attacks Originate." Last updated 23 Apr 2013. Diakses 15 July 2022. <https://www.govtech.com/security/hacking-top-ten.html>
- Peters, Allison. "Unpacking US Cyber Sanctions". Last updated 29 Jan 2021. Diakses pada 19 Jun 2022. <https://www.thirdway.org/memo/unpacking-us-cyber-sanctions>
- Renne R.A Kawilarang, "Huawei, ZTE, dan Tuduhan Spionase Paman Sam." Last update 10 Oct 2012. Diakses pada 3 July 2022. <https://www.viva.co.id/ragam/fokus/358320-huawei-zte-dan-tuduhan-spionase-paman-sam>
- Specopssoft.com, "The countries experiencing the most 'significant' cyber-attacks". Last updated 13 July 2020, Diakses 15 July 2022. <https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/>
- The U.S Census Bureau. "Computer and Internet Use in the United States: 2018." Last updated 8 Oct 2021. Diakses 27 Mar 2022. <https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html>

- USCBC, "Official 13th Five-Year Plan Outline Released." Diakses 4 May 2022.
<https://www.uschina.org/policy/official-13th-five-year-plan-outline-released>
- Viva.Co.Id, "AS Tuduh Huawei dan Alat Mat-mata China", Last update 8 Oct.
Diakses 5 July 2022.<https://www.viva.co.id/berita/dunia/357663-as-tuduh-huawei-dan-zte-alat-mata-mata-china>
- Yuanita, Chey. "Competitive Advantage Adalah: Pengertian, Cara Kerja, Jenis, dan 3 Contohnya dalam Bisnis.", Last updated 17 Mar 2022. Diakses 05 Aug 022. <https://www.ekrut.com/media/competitive-advantage-adalahb>

