BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan dan kemajuan teknologi informasi digital yang berbasis internet pada zaman sekarang ini semakin meningkat dengan cepat, perkembangan dan kemajuan teknologi informasi digital ini mencakup di seluruh negara-negara di dunia ini, terlebih lagi bagi negara-negara yang mempunyai keahlian di bidang ilmu teknologi informasi (IT), sudah tentu akan selalu merancang dan mengembangkan teknoligi informasi digital lebih maju lagi. Saat ini dapat dilihat bahwa perkembangan teknologi informasi digital dengan pesat meleset ke seluruh penjuru dunia melalui akses-akses internet atau dikatakan dengan dunia maya (*cyber world*). Bahkan tidak dapat dipungkiri lagi pada masa sekarang ini penggunaan internet atau dunia maya sudah merupakan menjadi kebutuhan setiap manusia melalui media sosial dalam melakukan komunikasi atau dikatakan dengan sistem komunikasi secara digitalisasi. Hal ini terlihat dari kehidupan sehari-hari penggunaan internet merupakan sudah menjadi kehidupan prioritas bagi manusia sebagai alat untuk saling berkomunikasi.

Dengan melihat perkembangan kemajuan teknologi informasi digital yang berbasis internet pada jaman sekarang ini, akan mempermudah manusia baik antar nasional ataupun internasional dalam menjalin hubungan

komunikasi. Perkembangan teknologi infomasi digital yang berbasis internet ini dapat digunakan secara positif atau negatif, tergantung kebutuhan penggunanya, sebagai contoh dalam penggunaan teknologi informasi digital secara positif antara lain ialah sebagai alat komunikasi, sebagai alat penyelidikan, sebagai alat pengamanan, sebagai pusat dan sumber ilmu pengetahuan dan sebagainya, sementara bila digunakan secara negatif teknologi informasi digital ini dapat mencuri data-data dari dari berbagai negara, dapat merusak jaringan keamanan dari suatu negara, dapat melakukan pengintaian dan penyerangan terhadap negara lain.

Perkembangan dan kemajuan teknologi ini merambah terhadap sistem pertahanan dan keamanan baik secara nasional maupun internasional, di setiap negara-negara yang sedang berkembang dan maju, terlebih lagi bagi negara-negara yang mengembangkan teknologi sebagai alat pertahanan dalam menghadapi suatu tantangan dari negara lain. Dengan adanya pengembangan teknologi informasi (TI) dalam bidang pertahanan (*cyber defense*) diharapkan mampu untuk menghadapi serangan (*cyber attack*) dari negara lain. pengembangan *cyber defense* ini sudah merambah ke tingkat Internasional dalam menjaga keamanan dunia internasional. Tidak menutup kemungkinan serangan-serangan antar negara melalui dunia maya sering terjadi, maka dari itu setiap negara mempunyai sistem pertahanan secara dunia maya atau yang disebut dengan *cyber defense* dalam mempertahankan serangan dunia maya dari negara lain.

Salah satu negara di Asia yang mulai tertarik mengembangkan teknologi informasi ini adalah China. China tertarik mengembangkan teknologi informasi mulai pada tahun 1990. Sue Duncan and Wang Mingjie mengatakan: "Ketertarikan China untuk membangun TI terlihat pada tahun 1990, melalui peningkatan anggaran yang besar pada saat pembangunan sains dan teknologi nasional".[1] Berdasarkan pernyataan di atas, jelas bahwa negara China mulai tertarik mengembangkan di bidang TI pada tahun 1990 dan hingga sekarang semakin maju dengan pesat. Seiring dengan kemajuan dalam pengembangan TI negara China selain mengembangkan *cyber attack* juga mengembangkan *cyber defense* dalam menangani *cyber attacks* dari luar. Dalam menangani *cyber attacks* dari negara-negara luar, sudah ribuan situs asing diblokir oleh pemerintah China dengan mengerahkan 30 ribu polisi *cyber*.

Dalam hal menangani permasalahan *cyber* ini, Pemerintah China Xi Jinping melalui diterjemahkan oleh Rogier Creemers, et al, melalui situs newamerica.org menekankan bahwa:

> *"Xi Jinping stressed that without cybersecurity, there is no national security, the economy and society will not operate in a stable manner, and the broad popular masses' interests will be difficult to guarantee. We must establish a correct cybersecurity view; strengthen cybersecurity protection of information infrastructure; strengthen the construction of comprehensive cybersecurity and information coordination mechanisms, methods, and platforms; strengthen the construction of cybersecurity incident response command capabilities; vigorously develop cybersecurity industries; move out in front; and prevent all possible trouble. We must implement critical information infrastructure protection responsibilities. As critical information infrastructure operators, sectors, and enterprises bear the primary responsibility for protection, competent authorities are to properly implement their supervisory and management responsibilities. We must, according to the*

[1] Sue, D., & Wang, M. (2006). *China 2006.* China: Foreign Languages Press. Hlm. 197

> *law, severely attack online hacking, telecommunications and network fraud, infringement of citizens' personal privacy, and other such unlawful and criminal conduct; sever the cybercrime value chain, continue to create a high-pressure situation, and safeguard the lawful rights and interests of the popular masses. We must deeply launch cybersecurity and knowledge technology propaganda and dissemination, and raise the broad popular masses' cybersecurity consciousness and protection capabilities".*[2]

Sampai Juni 2016, China telah memiliki 710 juta pengguna internet. Hal yang dihitung dalam statistik ini adalah mereka yang pernah setidaknya sekali mengakses dunia maya dalam enam bulan terakhir. Jumlah ini naik 3,1% dari hasil hitungan pada Desember 2015. Dengan demikian lebih dari separuh populasi China yang juga terbesar di dunia kini sudah bisa mengakses internet. Angka ini juga berarti pengguna internet di China dua kali lipat lebih banyak dibanding pengguna internet di Amerika Serikat[3]. China juga punya sistem monitoring yang disebut dengan *Great Firewall of China*. Ini merupakan proyek yang berada di bawa kendali *Ministry of Public Security*. Dimana China akan terus melakukan pengembangan dari *cyber defense* dalam memperkuat pertahanan dari serangan-serangan *cyber attack* negara lain. Greg Austin, dalam thediplomat.com menyebutkan bahwa:

> *"Overall, China's cybersecurity industrial complex is a work in progress. Two state-owned defense electronics companies, CEC and CETC—both Fortune 500—are the industry leaders, operating through their two main subsidiaries, ChinaSoft and China Cybersecurity. They are complemented by more than 400 privately-owned cybersecurity firms*

[2] Rogier, C., & dkk. (30 April 2018). *Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference*. Dipetik 10 Maret 2019, dari New Amerca: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/,

[3] Jemadu, L. (2016, Agustus 03). *Jumlah Pengguna Internet Cina Melejit, Lampaui 700 Juta Orang*. Diambil kembali dari Suara: https://www.suara.com/tekno/2016/08/03/132151/jumlah-pengguna-internet-cina-melejit-lampaui-700-juta-orang

> *in China, many of which are thriving off the back of rapidly rising demand for products and services. Among the leaders in this group is Qihoo 360".*[4]

Berdasarkan dari pernyataan diatas Negara China akan terus berupaya melakukan proses pengembangan *cyber defense* dengan memperkuat *cyber security* agar serangan *cyber* tidak mudah masuk dan menyerang melalui akses internet. Tetapi dasar pertahanan *cyber*, termasuk di Kementerian Keamanan Publik, tetap lemah. Ini adalah kesaksian banyak sumber China. Dari pengamatan analisis sektor swasta China dari tahun 2017 menempatkan peringkat keamanan *cyber security* pemerintahan di Lhasa (Tibet) dan Urumqi (Xinjiang) masih dalam kategori rendah bila ditinjau dari segi keamanan internal. Greg Austin juga menjelaskan bahwa:

> *"At the operational level, the cybersecurity of most Chinese government agencies and corporations remains weak to very weak. The biggest surprise in this regard is in the Ministry of Public Security, according to open source reporting inside China. Another surprise is a Chinese private sector analysis from 2017 which ranked government cybersecurity in Lhasa (Tibet) and Urumqi (Xinjiang) amongst the lowest in the country, in spite of the political sensitivity of these two locations from an internal security point of view".*[5]

Sementara itu Rogier Creemers, et al, dalam newamerica.com menyatakan bahwa:

> *"In the wake of the recent upgrade of China's cyberspace authorities from a central leading group to commission status, a National Cybersecurity and Informatization Work Conference took place in Beijing on April 20–21. Xi Jinping gave a speech outlining adjusted priorities for digital development, cybersecurity, and cyberspace governance after the 19th Party Congress".*

[4] Austin, G. (11 Juli 2018). *How Good are China's Cyber Defenses?* Dipetik 10 Maret 2019, dari The Diplomat: https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/
[5] *Ibid*

Sementara itu, China merupakan negara yang mempunyai perekonomian terbesar yang kedua di dunia dan memiliki senjata nuklir dengan menghabiskan banyak anggaran untuk pertahanan negaranya. China memiliki operasi informasi dalam peperangan informasi yang tercakup dalam konsep *"Network Warfare"* seperti yang pernah dilakukan dalam konsep *"cyber warfare"* dengan Amerika Serikat, diperkirakan *hacker army* China dari 50.000 hingga 100.000 orang. Terkait dengan kebijakan-kebijakan China dalam mengembangkan *cyber defense* yang semakin maju, tetapi masih bisa di retas oleh para *hacker-hacker* dari negara lain, sementara pertahanan mengenai *cyber defense* China yang begitu ketat.

Penggunaan internet China pada tahun 2010-2016 dapat lihat pada tabel berikut ini:

Tabel 1.1
Pengguna Internet China Tahun 2010-2016

Tahun	Pengguna Internet	Penetrasi (% dari Pop)	Populasi	Bukan Pengguna Internet
2010	459,952,277	34.3 %	1,340,968,737	881,016,460
2011	516,350,825	38.3 %	1,348,174,478	831,823,653
2012	573,330,272	42.3 %	1,355,386,952	782,056,680
2013	624,031,531	45.8 %	1,362,514,260	738,482,729
2014	675,131,785	49.3 %	1,369,435,670	694,303,885
2015	705,914,032	51.3 %	1,376,048,943	670,134,911
2016	721,434,547	52.2 %	1,382,323,332	660,888,785

Sumber: *Tim Berners-Lee*[6]

[6] Tim Berners-Lee. (1 Juli 2016). *China Internet Users*. Dipetik 17 April 2019, dari Internet Live Stats: http://www.internetlivestats.com/internet-users/china/

Dari tabel tersebut terlihat bahwa setiap tahun penggunaan internet di China ada peningkatan, dari total penduduk 1.382.323.332 jiwa, sebanyak 721.434.547 jiwa yang menggunakan internet. Artinya semakin banyak pengguna internet seiring dengan perkembangan populasi masyarakat China. Kemudian Menteri Keamanan Publik China juga mengatakan lebih dari 80 persen komputer dan websites di China mengalami *cyber attacks*, bahkan tahun 2011 *e-commerce, microblogging*, jaringan sosial dan *gaming websites* di China diretas.[7] Berdasarkan infomasi dari Tim Tekno Rakyatku, salah satu terkena serang *cyber* di Asia adalah China.

> "Beberapa Universitas, termasuk Universitas Nanchang, Universitas Shandong dan Universitas Ilmu Pengetahuan dan Teknologi Elektronik China, telah mengeluarkan peringatan di *Weibo* pada akhir pekan, mendesak mahasiswa untuk membuat cadangan file penting dan tidak membuka e-mail yang mencurigakan. Menurut majalah China Caijing, beberapa tesis dan proyek kelulusan siswa telah dilaporkan dienkripsi. Pihak berwenang juga telah mengeluarkan sebuah pemberitahuan pada hari Minggu, dengan mengatakan bahwa virus yang dijuluki *WannaCry* 2.0 telah menyebar. Menurut Global Times, provinsi Jiangsu dan Zhejiang merupakan daerah yang paling terkena dampak di Cina. Instansi yang terkena dampak mencakup universitas, stasiun kereta api, kantor pos, rumah sakit dan instansi pemerintah.[8]

Hal yang serupa yang informasi yang didapatkan oleh BBC yang menyatakan ada serangan peretas melanda 99 negara, salah satunya termasuk China. "Ada laporan yang menyebutkan serangan peretas itu telah melanda 99

---

[7] Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and U.S-China Relations.* Brookings: The John L. Thornton China Center and the 21s. Hlm. 4

[8] Tim Tekno Rakyatku. (15 Mei 2017). *Negara-negara Asia yang Terkena Serangan Cyber Ransomware*. Dipetik 17 April 2019, dari Tekno Rakyatku: http://tekno.rakyatku.com/read/48786/2017/05/15/negara-negara-asia-yang-terkena-serangan-cyber-ransomware

negara, di antaranya Inggris, AS, China, Rusia, Spanyol dan Italia.[9] Sebagaimana yang dikatakan oleh Zheng et al, mengemukakan bahwa pada awalnya tahun 1998-an Pemerintahan China mengeluarkan kebijakan *cyber censor* ketat. Namun secara perlahan kebijakan tersebut mengendur dari kebijakan sensor ketat *(strict censorship),* menjadi sensor sebagian *(half censorship),* dan otonomi terbatas *(limited self autonomy).*[10] Kemudian pada tahun 2000-2015, Pemerintah China mengeluarkan kebijakan berupa isolasi jaringan dan kontrol akses seperti yang dikemukakan oleh Zhen China telah melakukan kebijakan isolasi jaringan dan kontrol akses sejak tahun 2000 yang dikenal dengan nama the *Great firewall of China* atau kebijakan *Internet Censorship* untuk meningkatkan keamanan *cyber.*[11]

Selanjutnya untuk memperkuat menjaga kestabilan dan keamanan data-data informasi yang sangat penting atau rahasia, maka "kebijakan *cyber security* China akan mulai diberlakukan pada tanggal 1 Juni 2017. Dengan adanya hukum ini para penyedia layanan online dilarang mengumpulkan serta menjual informasi pribadi para penggunanya.[12] Dengan diberlakukannya kebijakan *cyber security* China, Badan *Cyber Security* China (CAC) telah menghapus 9.800 akun media sosial dari penyedia berita independen yang

[9] Tim BBC. (13 Mei 2017). *Serangan Siber Berskala Raksasa Menyerang Sejumlah Institusi di 99 Negara.* Dipetik 17 April 2019, dari BBC: https://www.bbc.com/indonesia/dunia-39906032
[10] Faida, R. E. (2015). Sensor Internet dan Securitization di Era Cyberwarfare: Studi Kasus Tiongkok . *Hubungan Internasional* , 31-46.
[11] Putri, N. T., Fasisaka, I., & Nugraha, A. S. (2015). Penanganan Cyber Attack Oleh Pemerintah Tiongkok Melalui Kebijakan Network Security Tahun 2000-2015. *Ilmu Sosial dan Ilmu Politik.* Hlm. 4.
[12] Dina. (30 Mei 2017). *China Bakal Berlakukan Kebijakan Cyber Security*. Dipetik 18 April 18, 2019, dari Jurnas: http://www.jurnas.com/artikel/16812/China-Bakal-Berlakukan-Kebijakan-Cyber-Security/

dianggap telah memposting konten sensasional, vulgar maupun berbahaya secara politik di dunia internet.[13] Dengan melihat perkembangan dan ketegangan antara negara-negara maju yang menguasai teknologi informasi yang merembes ke tingkat keamanan pertahanan kemiliteran seperti negara Amerika Serikat, Rusia, Italia dan negara lainnya serta termasuk didalamnya China. Dalam menghadapi gejolak perang *cyber* antar negara China membentuk *cyber defense* sebagai *cyber* pertahanan sekaligus *cyber* perlawanan balik dari penyerang.

Berdasarkan pembahasan diatas, maka timbul keingintahuan kebijakan *cyber defense* China dalam menangani permasalahan *cyber attacks* dari negara lain bisa masuk meretas website-website China, sehingga penelitian ini dilakukan dengan mengangkat judul "Kebijakan *Cyber Defense* China dalam Menghadapi Serangan *Cyber* Global". Diharapkan dari penelitian ini akan mendapatkan jawaban yang signifikan terhadap permasalahan *cyber defense* China dan dapat dijadikan sebagai referensi penelitian selanjutnya.

1.2 Pembatasan Masalah

Agar penelitian ini lebih terarah, maka dalam penelitian ini membatasi masalah tentang kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global dan dampak kebijakan China dalam melakukan *cyber defense* menghadapi serangan *cyber* global.

---

[13] Kartika, H. (13 November 2018). *Badan Cyber China Hapus 9.800 Akun Media Sosial Berbahaya di Dunia Maya*. Dipetik 17 April 2019, dari Internasional Kontan: https://internasional.kontan.co.id/news/badan-cyber-china-hapus-9800-akun-media-sosial-berbahaya-di-dunia-maya

1.3 Pertanyaan Penelitian

Salah satu persoalan mendasar dan menjadi bagian penting yang tak terpisahkan dalam penelitian adalah rumusan pertanyaan penelitian. Pertanyaan penelitian selalu diawali dengan munculnya masalah yang sering disebut sebagai fenomena atau gejala tertentu. Berdasarkan kajian referensi buku-buku dan metodologi penelitian penulis mengajukan pertanyaan penelitian:

1. Bagaimana kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global?
2. Bagaimana implikasi kebijakan *cyber defense* China terhadap serangan *cyber* global?

1.4 Tujuan Penelitian

Tujuan penelitian adalah pembahasaan mengenai rumusan dalam kalimat penelitian yang menunjukkan hasil didapatkan setelah proses penelitian terselesaikan.

Berdasarkan rumusan masalah di atas, maka tujuan penulisan karya ini adalah:

1. Untuk mengetahui kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global.
2. Untuk mengetahui implikasi kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global.

1.5 Manfaat Penelitian

Dengan adanya pelaksanaan penelitian ini, diharapkan dapat bermanfaat secara teoritis dan praktis.

1.5.1 Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan manfaat bagi para pembaca sebagai berikut :

a. Menambah referensi tentang kebijakan *cyber defense* China dalam menghadapi serangan *cyber*.
b. Sebagai sumber informasi bagi penelitian sejenis pada masa yang akan datang.
c. Sebagai kontribusi dalam bidang ilmu pengetahuan, khususnya mengenai kebijakan *cyber defense* China.

1.5.2 Manfaat Praktis

Selain bermanfaat secara teoritis, penelitian ini diharapkan dapat memberikan manfaat secara praktis yaitu :

a. Memberikan sumbangan ilmu pengetahuan dan hassil pemikiran bagi pihak universitas tentang kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global.

b. Memperluas wawasan bagi para pembaca tentang kebijakan *cyber defense* China dalam menghadapi serangan *cyber* global.
c. Memberikan rasa keingintahuan lebih lanjut tentang kebijakan *cyber defense* China dalam menghadapi serangan *cyber* pada tahun selanjutnya.

1.6 Sistematika Penulisan

Adapun susunan atau sistematika penulisan dalam skripsi ini, agar memudahkan pembaca untuk memahami skripsi ini, maka skripsi ini disusun dengan sistematika sebagai berikut:

BAB I: PENDAHULUAN

Bab pendahuluan merupakan tinjauan secara ringkas mengenai latar belakang masalah yang akan dibahas, perumusan permasalahan, kerangka konseptual, alur pemikiran, manfaat dan tujuan yang ingin dicapai oleh penulis serta sistematika penulisan dari skripsi ini. Menjelaskan secara garis besar pokok permasalahan yang akan diteliti sesuai dengan tujuan penelitian. Adapun isi dari Bab I meliputi: Latar belakang, Identifikasi masalah, Tujuan Penelitian, Batasan masalah, Manfaat penelitian dan Sistematika Penulisan.

BAB II: TINJAUAN PUSTAKA

Bab ini merupakan relevansi antara teori-teori dan kerangka konseptual digunakan oleh penulis untuk menganalisa permasalahan yang

akan dibahas berdasarkan bukti-bukti dari buku, artikel-artikel dan sumber-sumber lain yang berkaitan dengan permasalahan yang ingin diteliti oleh penulis. Landasan teori merupakan dasar pemikiran penulis untuk mengembangkan penelitian dari data-data yang telah ada.

BAB III: METODE PENELITIAN

Bab ini meliputi tempat dan waktu penelitian, desain penelitian yang berisikan: paradigma penelitian, metode penelitian, sifat penelitian, kemudian dilanjutkan dengan subyek dan obyek penelitian, teknik pengumpulan data, instrumen pengumpulan data dan teknik analisa data.

BAB IV: HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini penulis akan menguraikan kondisi perkembangan dari *cyber defense* China sebagai pertahanan dari serangan *cyber* global.

BAB V: PENUTUP

Bab ini merupakan bab terakhir dari proses penulisan skripsi ini yang memuat rangkuman tentang temuan penelitian yang disusun oleh penulis dari seluruh hal yang dikemukakan pada bab-bab sebelumnya dan di bab ini juga berisikan rekomendasi bagi penelitian di masa yang akan datang bagi para pembuat kebijakan dan juga akademisi.

\